Random walks on Arakelov class groups

Boer, K. de

6. Ideal sampling

6.1. Summary

Many algorithms in cryptography and algorithmic number theory rely on finding elements α in an ideal $\mathfrak{a}$ such that their quotient $\alpha\mathfrak{a}^{-1}$ is easy to factor (e.g., prime, near-prime or B-smooth). Such algorithms are typically analyzed only heuristically, by treating $\alpha\mathfrak{a}^{-1}$ as a uniform ideal, and applying density results for the sets of prime ideals or smooth ideals. The result of this chapter allows to adjust this strategy and make the reasoning rigorous.

The beginning of this chapter is devoted to showing that, for an ideal $\mathfrak{a}$ that is uniformly distributed in the Arakelov class group, one can rigorously analyze the probability of $\alpha\mathfrak{a}^{-1}$ being in a certain ideal set (e.g., the prime ideals or smooth ideals). This probability can be shown to be very much related to the *density* of the ideal set involved, a notion from analytic number theory.

In the later part of this chapter we invoke the random walk theorem from Chapter 4, which allows to randomize any fixed ideal $\mathfrak{a}$ into a randomly distributed ideal $\tilde{\mathfrak{a}}$ in the Arakelov class group. This *randomized* ideal can then be used to sample an $\alpha \in \tilde{\mathfrak{a}}$ from, with a rigorous probability. Sampling α from $\tilde{\mathfrak{a}}$ instead of $\mathfrak{a}$ does not affect the usefulness of α, since the randomization – apart from a small distortion – happens only by multiplying $\mathfrak{a}$ with small prime ideals. I.e., the quotient $\alpha\mathfrak{a}^{-1}$ only differs from $\alpha\tilde{\mathfrak{a}}^{-1}$ by small prime factors, meaning that if the one is easy to factor, the other is as well.

6.2. Introduction

In this chapter, we apply the random walk theorem of Chapter 4 to tackle the following problem that arises in multiple number-theoretic contexts [BF14; BP17; Buc88]. Let K be a number field, of degree n and discriminant Δ_K. Given an ideal $\mathfrak{a} \subset K$, sample an element $\alpha \in \mathfrak{a}$ such that the ideal $\alpha\mathfrak{a}^{-1}$ is easy to factor. In some cases (e.g., [BF14; Buc88; LL+93]), the fraction $\alpha\mathfrak{a}^{-1}$ is required to only have small prime factors, whereas in other cases (e.g., [BP17]), the fraction $\alpha\mathfrak{a}^{-1}$ is required to be a near-prime (i.e., at most one of its prime factors is allowed to be large).

In the literature and computer algebra systems (e.g., [CS08, §6.5] [BCP97; PAR19]), this task is performed by computing a reasonably short basis of the ideal $\mathfrak{a}$ (by means of LLL, for example) and repeatedly randomly sampling reasonably short elements $\alpha \in \mathfrak{a}$ using this basis, until $\alpha\mathfrak{a}^{-1}$ is of the desired form. Assuming heuristically that the ideals $\alpha\mathfrak{a}^{-1}$ are more or less randomly distributed among ideals of bounded norm, one can use specific density results for subsets of ideals to obtain a heuristic estimate for the success probability of this method.

Even though the above approach appears to work in many practical cases, it is generally hard to prove anything in the direction of a rigorous lower bound for the success probability. A first obstacle is that the ideal $\alpha\mathfrak{a}^{-1}$ is not 'random enough' as, for example, it always lies in the ideal class $[\mathfrak{a}]^{-1}$. Even for principal ideal domains, a second obstacle is that the number of generators of (α) may vary unpredictably among sub-ideals (α) of $\mathfrak{a}$, resulting in some sub-ideals of $\mathfrak{a}$ to be sampled more often than others, making the distribution of $\alpha\mathfrak{a}^{-1}$ skewed.

6.2.1. Our Technique

To resolve these issues, we slightly modify both the ideal $\mathfrak{a}$ and the way $\alpha \in \mathfrak{a}$ is sampled. More precisely, the ideal $\mathfrak{a}$ is replaced by $\tilde{\mathfrak{a}} = \mathfrak{a} \cdot \prod_i \mathfrak{p}_i$, where each $\mathfrak{p}_i$ is a small, random prime ideal. The element α is then sampled

uniformly in the ideal $\tilde{\mathfrak{a}}$ intersected with a 'distorted box' in the canonical embedding space $K_{\mathbb{R}}$. More specifically, in the case of a totally real number field, the box is chosen as $\mathcal{N}(\tilde{\mathfrak{a}})^{1/n} \cdot B_{r,x} = \mathcal{N}(\tilde{\mathfrak{a}})^{1/n} \cdot \prod_j [-re^{x_j}, re^{x_j}] \subseteq K_{\mathbb{R}}$ with large enough $r > 0$, where $x_j \in \mathbb{R}$ satisfy $\sum_j x_j = 0$ and are distributed according to a Gaussian distribution.

This procedure mimics a random walk in the Arakelov class group, where multiplying by small primes accounts for the randomization at the finite places, whereas the distortion of the sampling boxes accounts for the randomization at the infinite places.

The idea behind this procedure is that, while it is hard to predict exactly how many generators of the ideal (α) are in $\mathfrak{a} \cap \mathcal{N}(\mathfrak{a})^{1/n} \cdot B_{r,0}$, the average number of such generators in $\tilde{\mathfrak{a}} \cap \mathcal{N}(\tilde{\mathfrak{a}})^{1/n} \cdot B_{r,x}$ is accurately predictable whenever $\tilde{\mathfrak{a}}$ and x are adequately randomized. Indeed, this quantity is given by the number of points of a shifted Log-unit lattice, intersected with a simplex; this number of points is hard to estimate for a given shift of the Log-unit lattice, but it is predictable on average, according to the following fact.

Lemma 6.1. *Let $S \subset \mathbb{R}^n$ be a measurable set and $\Lambda \subset \mathbb{R}^n$ a full rank lattice. Then, for a uniformly chosen $c \in \mathbb{R}^n/\Lambda$ it holds that $\mathbb{E}[|(\Lambda + c) \cap S|] = \mathrm{Vol}(S)/\mathrm{Vol}(\Lambda)$.*

Algorithmically, sampling uniformly in a box $\mathcal{N}(\mathfrak{a})^{1/n} \cdot B_{r,x}$ and element of an ideal $\mathfrak{a}$ can be done in polynomial time with an LLL reduced basis, whenever $\log r = \mathsf{poly}(n, \log|\Delta_K|)$. One can also strengthen this reduction as in [BF14; Buc88] for other time-quality trade-offs. Denoting $\mathcal{S}_B$ the set of B-smooth ideals, and $\delta_{\mathcal{S}}[t]$ the density of ideals of norm $\leq t$ which belong to a given set of ideals $\mathcal{S}$, our (slightly simplified) main result is the following.

Main theorem. *Let $\mathcal{S}$ be any set of integral ideals. Assuming the Riemann hypothesis for Hecke L-functions, there exists some $B = \mathsf{poly}(\log|\Delta_K|)$, such that Algorithm 7 outputs in time $\mathsf{poly}(\log|\Delta_K|, \mathrm{size}(\mathcal{N}(\mathfrak{a})))$ an element $\alpha \in \mathfrak{a}$ such that $(\alpha)/\mathfrak{a} \in \mathcal{S} \cdot \mathcal{S}_B$ with probability at least $\frac{1}{3}\delta_{\mathcal{S}}[r^n] - 2^{-n}$.*

Since $\mathcal{N}((\alpha)/\mathfrak{a}) \approx r^n$, we have therefore formalized the heuristic that element sampling probability matches ideal density, up to a loss of $1/3$ on the probability, and up to an extra smooth ideal in $\mathcal{S}_B$. Moreover, the original purpose, namely finding a $\alpha \in \mathfrak{a}$ such that $\alpha\mathfrak{a}^{-1}$ can be easily factored, is not spoiled.

Including the modulus $\mathfrak{m}$

The non-simplified main result of this chapter (see Theorem 6.9) involves a *modulus* $\mathfrak{m} \subseteq \mathcal{O}_K$, an ideal that is to be 'avoided' in the computations.

Specifically, the main theorem states the probability that $(\alpha)/\mathfrak{a}$ is in a given ideal set, *given* the fact that $\alpha \equiv \tau$ modulo $\mathfrak{m}$ for some fixed given $\tau \in K^{\mathfrak{m}}$. This particular generalization is included because of its usefulness for the computation of the power residue symbol (see Chapter 7). One recovers the main theorem, as described in this introduction, by putting $\mathfrak{m} = \mathcal{O}_K$.

6.2.2. Applications

As a direct application, one can prove that sampling $\alpha \in \mathfrak{a}$ such that $\alpha\mathfrak{a}^{-1}$ is a near-prime can be done efficiently in cyclotomic fields. This proves that the 'principalization step' in the power residue symbol algorithm of the author of this PhD thesis [BP17, §5.2] runs in polynomial time in the special case of cyclotomic number fields, and more generally in any family of number fields with small Dedekind zeta residue ρ_K.

The most general version of the result of this chapter (Theorem 6.9), involving a modulus $\mathfrak{m}$ has even farther consequences. It does not only allow to remove one specific heuristic ([BP17, §5.2]), but can actually be applied in order to prove that the *entire* (slightly modified) algorithm for the power residue symbol is efficient (see Chapter 7).

We also hope that our technique could be helpful in proving other heuristic algorithms such as the index calculus algorithms of [Buc88; BF14] (computing class groups and unit groups), though other obstacles are expected. Not

only does it require universal bounds on the density of B-smooth ideal in large-degree number field, one also needs to ensure sufficient independence of the obtained multiplicative relations. For the second obstacle, further randomization techniques could turn out useful.

6.2.3. Related Works

We note that the issues we mention above have been circumvented in special cases. Building on a result of Seysen [Sey87], Hafner and McCurley [HM89] gave a provable algorithm for computing class-group and unit group of imaginary quadratic fields. This algorithm involves a random walk in the class group, which is used to prove that one can find a B-smooth *principal* ideal relatively efficiently. The idea of performing a random walk in the class group was reused in the algorithms of Buchmann [Buc88] and Biasse and Fieker [BF14], in a heuristic way. Finally, we note also that Schoof [Sch08] rephrased Buchmann's algorithm in the terms of Arakelov theory, and we heavily borrowed from his formalism.

6.3. Preliminaries

An important concept that plays a large role throughout the entire proof of the main theorem is that of a *generator of an Arakelov ray divisor*. This can be seen as a generalization of a generator of a principal ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, which is an $\alpha \in \mathcal{O}_K$ satisfying $(\alpha) = \mathfrak{a}$. Such a generator α of the ideal $\mathfrak{a}$ is called τ-equivalent (with respect to a modulus $\mathfrak{m}$) if $\alpha \equiv \tau \bmod \mathfrak{m}$ (note that this definition only makes sense if $\mathfrak{m}$ and $\mathfrak{a}$ are coprime).

The generalization to Arakelov ray divisors is very similar. As we can see Arakelov ray divisors as ideal lattices $x\mathfrak{a}$, a generator of such divisor is just an element in $K_{\mathbb{R}}$ of the shape $x\alpha$, where α is a generator of $\mathfrak{a}$. Of course, if $\mathfrak{a}$ is not a principal ideal, there are no such generators. The τ-equivalent generators are just those $x\alpha \in K_{\mathbb{R}}$ for which $\alpha \equiv \tau \bmod \mathfrak{m}$. The precise definition is as follows.

Definition 6.2 (Generators of an Arakelov ray divisor)**.** *Let $\tau \in K^{\mathfrak{m}}$ and let $\mathbf{a} \in \mathrm{Div}_{K^{\mathfrak{m}}}$ be an Arakelov ray divisor with an infinite part $\mathbf{a}_\infty$ and a finite part $\mathbf{a}_{\mathrm{f}}$ (see Equation (2.13)). We define the set of τ-equivalent generators $\mathrm{Exp}(\mathbf{a})^{\times}_{\tau} \subseteq K_{\mathbb{R}}$ of $\mathbf{a}$ by the following rule*

$$\mathrm{Exp}(\mathbf{a})^{\times}_{\tau} := \begin{cases} \mathrm{Exp}(\mathbf{a}_\infty) \cdot (\kappa \cdot \mathcal{O}_K^{\times} \cap \tau K^{\mathfrak{m},1}) \subseteq \mathrm{Exp}(\mathbf{a}) & \text{if } \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) = (\kappa) \\ & \text{for some } \kappa \in K^{\mathfrak{m}} \\ \emptyset & \text{otherwise} \end{cases}$$

Equivalently, we can write

$$\mathrm{Exp}(\mathbf{a})^{\times}_{\tau} = \{\alpha \in \mathrm{Exp}(\mathbf{a}) \mid (\mathrm{Exp}(-\mathbf{a}_\infty) \cdot \alpha) = \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) \text{ and } \mathrm{Exp}(-\mathbf{a}_\infty) \cdot \alpha \in \tau K^{\mathfrak{m},1}\}.$$

The following specialization of the random walk theorem of Chapter 4 is tailored to the purposes of this chapter. These purposes require both N and B to be polynomially small, and s to be rather small as well, to ease sampling in the log-normally distorted box. There is no specific reason we chose *this* particular instantiation below, except for concreteness.

Theorem 6.3 (Random walks on the Arakelov ray class group, ERH)**.** *Let $n = [K : \mathbb{Q}] \geq 2$, $s = 1/(1000 \cdot n^2)$ and let $\varepsilon > 0$ be an error parameter. There exists a bound $B = \widetilde{O}\Big(n^4[\log\log(1/\varepsilon)]^2 + n^2[\log(|\Delta_K|\mathcal{N}(\mathfrak{m}))]^2\Big)$ such that for $N = \lfloor 8n + \log\mathcal{N}(\mathfrak{m}) + \log|\Delta_K| + 2\log(1/\varepsilon)\rfloor$ the random walk distribution $[\mathcal{W}(B, N, s)]$ on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ is ε-close to uniform in $L_1(\mathrm{Pic}^0_{K^{\mathfrak{m}}})$, i.e.,*

$$\Big\|[\mathcal{W}(B, N, s)] - \mathcal{U}(\mathrm{Pic}^0_{K^{\mathfrak{m}}})\Big\|_1 \leq \varepsilon.$$

Proof. This formulation of the random walk theorem is obtained by instantiating Theorem 4.3 of Chapter 4 with $C = \Lambda_{K^{\mathfrak{m},1}}$, $s = 1/n^2$ and $k = 1$.

In that case, $B = \widetilde{O}\Big(n^4[\log\log(1/\varepsilon)]^2 + n^2[\log(|\Delta_K|\mathcal{N}(\mathfrak{m}))]^2\Big)$, by simply suppressing polylogarithmic factors. By using the bounds $\eta_1(\Lambda^*_{K^{\mathfrak{m},1}}) \leq \eta_1(\Lambda^*_K) \leq 2000 \cdot (\mathrm{r}+1) \cdot \log(\mathrm{r})^3 \leq 1000 \cdot n^2 = s^{-1}$ (see the proof of Proposition 5.10),

$\log \mathrm{Vol}(\mathrm{Pic}^0_{K^{\mathfrak{m}}})) \leq \log(\mathcal{N}(\mathfrak{m})) + \log \mathrm{Vol}(\mathrm{Pic}^0_{K^{\mathfrak{m}}}) \leq \log(\mathcal{N}(\mathfrak{m})) + \log|\Delta_K|$ (see Lemma 2.17) and $\mathbb{r} \leq n$ one obtains that Theorem 4.3 applies, with

$$\begin{aligned} N &= \lfloor 8n + \log \mathcal{N}(\mathfrak{m}) + \log|\Delta_K| + 2\log(1/\varepsilon) \rfloor \\ &\geq \frac{1}{2\log n} \cdot (n\log(1000n^2) + \log \mathcal{N}(\mathfrak{m}) + \log|\Delta_K| + 2\log(1/\varepsilon) + 2) \\ &\geq \frac{1}{2k\log n} \cdot (\mathbb{r} \cdot \log(1/\tilde{s}) + \log|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| + 2\log(1/\varepsilon) + 2). \end{aligned}$$

□

Remark 6.4. *One can simplify the bounds on B and N in the theorem above by putting $\varepsilon = 2^{-n}$. In that case $B = \widetilde{O}(n^2 \cdot (\log(|\Delta_K|\mathcal{N}(\mathfrak{m})))^2)$ and $N = \lfloor 12n + \log \mathcal{N}(\mathfrak{m}) + \log|\Delta_K| \rfloor$ is sufficient.*

6.4. Probability-density Correspondence

6.4.1. Result

For an ideal set $\mathcal{S} \subseteq \mathcal{I}_K$ consisting of integral ideals, we denote by $\mathcal{S}(t)$ the subset of $\mathcal{S}$ consisting of those integral ideals with norm bounded by $t \in \mathbb{R}_{>0}$, which is made precise in the following lemma. With this notation we will define the *local density* in Definition 6.6.

Definition 6.5. *Let $\mathcal{S}$ be an set of integral ideals of $\mathcal{O}_K$. Then we define $\mathcal{S}(t) := \{\mathfrak{b} \in \mathcal{S} \mid \mathcal{N}(\mathfrak{b}) \leq t\}$ and we define the counting function $|\mathcal{S}(\cdot)| : \mathbb{R}_{>0} \to \mathbb{N}$ of $\mathcal{S}$ by the following rule:*

$$|\mathcal{S}(t)| = |\{\mathfrak{b} \in \mathcal{S} \mid \mathcal{N}(\mathfrak{b}) \leq t\}|.$$

Definition 6.6 (Local density of an ideal set)**.** *Let $x > 0$ a positive real number, and let $\mathcal{S}$ be a set of integral ideals of K. We define the* local density[1]

[1] Note that this quantity tends to the 'natural density' of the ideal set $\mathcal{S}$ when x goes to infinity, since $|\{\mathfrak{a} \mid \mathcal{N}(\mathfrak{a}) < t\}| \sim \rho \cdot t$ [Ove14, §9.5].

of $\mathcal{S}$ at x as

$$\delta_{\mathcal{S}}[x] = \min_{t\in[x/e^n,x]} \frac{|\mathcal{S}(t)|}{\rho\cdot t} = \min_{t\in[x/e^n,x]} \frac{|\{\mathfrak{b}\in\mathcal{S} \mid \mathcal{N}(\mathfrak{b})\le t\}|}{\rho\cdot t}.$$

Definition 6.7 (Infinity ball)**.** *Let $r>0$ be a positive number, then we denote*

$$r\mathcal{B}_\infty = \{(x_\sigma)_\sigma \in K_{\mathbb{R}} \mid |x_\sigma|\le r, \text{ for all } \sigma\}.$$

Definition 6.8. *For a distribution $\mathcal{D}$ on $\mathrm{Div}^0_{K^{\mathfrak{m}}}$, we denote by $[\mathcal{D}] = \mathcal{D}|^{K^{\mathfrak{m},1}}$ the distribution on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ obtained by periodizing $\mathcal{D}$ with respect to the subgroup $K^{\mathfrak{m},1}\hookrightarrow \mathrm{Div}^0_{K^{\mathfrak{m}}}$ (see Definition 2.3).In other words,*

$$[\mathcal{D}] = \mathcal{D}|^{K^{\mathfrak{m},1}} = \sum_{\alpha\in K^{\mathfrak{m},1}} \mathcal{D}(\cdot + (\!|\alpha|\!)).$$

This distribution $[\mathcal{D}]$ describes exactly the distribution of the Arakelov ray class $[\mathbf{a}]$, where $\mathbf{a}\leftarrow\mathcal{D}$.

The main result of this section shows a close relationship between the *local density* of an ideal set $\mathcal{S}$ and the *probability* that the integral ideal $\beta\mathbf{a}^{-1}$ lies in $\mathcal{S}$ for β sampled appropriately from $\mathbf{a}$. Here, $\mathbf{a}$ is a Arakelov ray divisor whose Arakelov ray class is uniformly distributed.

Theorem 6.9. *Let $r\ge 8\cdot n\cdot|\Delta_K|^{\frac{3}{2n}}\cdot\mathcal{N}(\mathfrak{m})^{1/n}$, let $\tau\in(\mathcal{O}_K/\mathfrak{m})^*$ and let $\mathcal{S}^{\mathfrak{m}}$ be a set of integral ideals coprime to $\mathfrak{m}$ with local density $\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]$ at r^n. Let $\mathcal{D}$ be a distribution on $\mathrm{Div}^0_{K^{\mathfrak{m}}}$ such that $[\mathcal{D}]$ is uniform in $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$. Then*

$$\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})\in\mathcal{S}^{\mathfrak{m}} \;\middle|\; \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \ge \tfrac{1}{3}\cdot\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]. \tag{6.77}$$

where α is uniformly sampled from the finite set $\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty$.

Remark 6.10. *The $1/3$ occurring in Equation (6.77) can be made arbitrarily close to one by increasing the radius $r\in\mathbb{R}$ and slightly increasing the density interval $[x/e^n,x]$ in Definition 6.6. For sake of simplicity we just chose $r\in\mathbb{R}$ and the length of the interval $[x/e^n,x]$ to be minimal to achieve the optimal lower bound up to an explicit constant (i.e., Equation (6.77)).*

Remark 6.11. *Theorem 6.9 involves a* conditional probability*. It is possible, with essentially the same proof technique, to rephrase this theorem in such a way that it concerns the* intersection *of the events* $(\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) \in \mathcal{S}^{\mathfrak{m}}$ *and* $\alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1}$*. The probability then depends as well on the number* $\phi(\mathfrak{m}) = |(\mathcal{O}_K/\mathfrak{m})^*| = |K^{\mathfrak{m}}/K^{\mathfrak{m},1}|$ *of elements in* $(\mathcal{O}_K/\mathfrak{m})^*$*. More specifically, for a given* $\tau \in (\mathcal{O}_K/\mathfrak{m})^*$ *one can prove that, under the same conditions as in Theorem 6.9,*

$$\begin{aligned}
&\Pr_{\substack{\mathbf{a}\leftarrow\mathcal{D}\\ \alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})\in\mathcal{S}^{\mathfrak{m}} \text{ and } \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\\
&=\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})\in\mathcal{S}^{\mathfrak{m}} \text{ and } \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right]\\
&\geq\frac{1}{3\cdot\phi(\mathfrak{m})}\cdot\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]. \qquad (6.78)
\end{aligned}$$

6.4.2. Proof Overview of Theorem 6.9

In the following text we prove Theorem 6.9, leaving out details. In the later Section 6.5, which follows the exact same structure as this proof overview, a full proof is given, including all required lemmas.

Simplify the Probability by Fixing a Single Ideal $\mathfrak{c} \in \mathcal{S}^{\mathfrak{m}}$ and a Single Arakelov Divisor $\mathbf{a} \in \mathrm{Div}^0_{K^{\mathfrak{m}}}$

The statement Equation (6.77) of Theorem 6.9 involves two random processes: first the random sampling of $\mathbf{a} \leftarrow \mathcal{D}$, then the uniform sampling of an element $\alpha \in \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$. It is insightful to focus on the latter random process, that of the element α, for a *fixed* $\mathbf{a} \in \mathrm{Div}^0_{K^{\mathfrak{m}}}$.

Also, the probability in Equation (6.77) concerns an entire ideal set $\mathcal{S}^{\mathfrak{m}}$. In this part of the proof, we focus instead on a single ideal $\mathfrak{c} \in \mathcal{S}^{\mathfrak{m}}$. In other words, we estimate the following probability, for a *fixed* $\mathbf{a} \in \mathrm{Div}^0_{K^{\mathfrak{m}}}$ and a *single* integral ideal $\mathfrak{c} \in \mathcal{I}_K^{\mathfrak{m}}$,

$$\mathbb{p}_{\mathbf{a},\mathfrak{c}} = \Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})=\mathfrak{c} \mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right] \qquad (6.79)$$

where the sampling $\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ is uniform. In the notation above we leave the dependency on $r \in \mathbb{R}$, $\mathfrak{m} \subseteq \mathcal{O}_K$ and $\tau \in (\mathcal{O}_K/\mathfrak{m})^*$ implicit.

By the law of conditional probability, we have that Equation (6.79) equals

$$\mathbb{P}_{\mathbf{a},\mathfrak{c}} = \frac{\Pr\limits_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[\begin{array}{c} (\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \\ \text{and} \\ \alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \end{array} \right]}{\Pr\limits_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} [\alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1}]} \tag{6.80}$$

Focusing on the numerator first, we will prove later, in Lemma 6.12, that

$$\Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[\begin{array}{c} (\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \\ \text{and} \\ \alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \end{array} \right] = \frac{|\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|}{|\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty|} \tag{6.81}$$

Here, $|\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|$ is the number of *generators* of the ideal lattice $\mathrm{Exp}(\mathbf{a})\mathfrak{c}$ that are equivalent to τ modulo $\mathfrak{m}$ (see Definition 6.2) lying in the box $r\mathcal{B}_\infty$. So, essentially, Equation (6.81) counts how many of the $|\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty|$ elements in the sampling space $r\mathcal{B}_\infty$ actually generate the ideal lattice $\mathrm{Exp}(\mathbf{a})\mathfrak{c}$ and are equivalent to τ modulo $\mathfrak{m}$.

For the denominator we will prove (see Lemma 6.12) that there exists $\tilde{\tau} \in K_\mathbb{R}$ such that

$$\Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[\alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \right] = \frac{|(\mathrm{Exp}(\mathbf{a})\mathfrak{m} + \tilde{\tau}) \cap r\mathcal{B}_\infty|}{|\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty|} \tag{6.82}$$

where the sampling $\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ is uniform. This equation can be intuitively derived by ignoring the $\mathbf{a}_\infty$-part. Any element $\alpha \in \mathrm{Exp}(\mathbf{a})$ that satisfies $\alpha \equiv \tau$ modulo $\mathfrak{m}$ must lie in $\mathrm{Exp}(\mathbf{a}) \cap (\mathfrak{m} + \tau)$, which can indeed by rewritten to $\mathrm{Exp}(\mathbf{a})\mathfrak{m} + \tilde{\tau}$ by choosing an $\tilde{\tau} \in \mathrm{Exp}(\mathbf{a})$ that satisfies $\tilde{\tau} \equiv \tau$ modulo $\mathfrak{m}$.

By combining Equations (6.80) to (6.82) and scratching terms that occur both in the numerator and denominator, one concludes that there exists

$\tilde{\tau} \in \mathrm{Exp}(\mathbf{a})$ such that

$$\mathbb{p}_{\mathbf{a},\mathfrak{c}} = \Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[(\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \mid \alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \right] = \frac{|\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|}{|(\mathrm{Exp}(\mathbf{a})\mathfrak{m} + \tilde{\tau}) \cap r\mathcal{B}_\infty|}. \quad (6.83)$$

Using the estimate $|(\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}) \cap r\mathcal{B}_\infty| \approx r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}} / (e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|})$

When the radius r is quite large compared to the lattice $\mathrm{Exp}(\mathbf{a}) \subseteq K_\mathbb{R}$, one can deduce that for $\mathbf{a} \in \mathrm{Div}_{K^\mathfrak{m}}$ the number of points in $(\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}) \cap r\mathcal{B}_\infty$ is approximately $\mathrm{Vol}(r\mathcal{B}_\infty)/e^{\deg(\mathbf{a})}$, where $\deg(\cdot)$ is defined in Equation (2.12). More specifically, in Lemma 6.13 we prove that for all $\mathbf{a} \in \mathrm{Div}^0_{K^\mathfrak{m}}$ and $\tilde{\tau} \in K_\mathbb{R}$,

$$|(\mathrm{Exp}(\mathbf{a})\mathfrak{m} + \tilde{\tau}) \cap r\mathcal{B}_\infty| \in [e^{-1/4}, e^{1/4}] \cdot r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}} / (\mathcal{N}(\mathfrak{m}) \cdot \sqrt{|\Delta_K|}).$$

Applying this to the denominator of Equation (6.83), we directly deduce that

$$\mathbb{p}_{\mathbf{a},\mathfrak{c}} = \Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[(\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \mid \alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \right] \in [e^{-1/4}, e^{1/4}] \cdot \frac{\sqrt{|\Delta_K|} \cdot \mathcal{N}(\mathfrak{m})}{r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}} \cdot |\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty| \quad (6.84)$$

Estimating the probability of sampling a single fixed ideal for a *random* Arakelov divisor

As already mentioned, Equation (6.77) of Theorem 6.9 involves two random processes, where the first process samples the Arakelov ray divisor $\mathbf{a} \leftarrow \mathcal{D}$ and the second process samples $\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ uniformly. Therefore,

for a fixed integral ideal $\mathfrak{c} \in \mathcal{I}_K^{\mathfrak{m}}$, using Equation (6.84), we have

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\mathbb{p}_{\mathbf{a},\mathfrak{c}}\right] \\
=&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})=\mathfrak{c}\mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \\
\in&[e^{-1/4},e^{1/4}]\cdot\frac{\sqrt{|\Delta_K|}\cdot\mathcal{N}(\mathfrak{m})}{r^n\cdot 2^{n_{\mathbb{R}}}\cdot(2\pi)^{n_{\mathbb{C}}}}\cdot\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\left|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty\right|\right]. \qquad (6.85)
\end{aligned}$$

The number $|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty|$ only depends on the Arakelov ray *class* of $\mathbf{a}\in\mathrm{Div}_{K^{\mathfrak{m}}}^0$

By quite a technical argument (see Lemma 6.14(iii)) one can show that the number of 'good' α's, $|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty|$, only depends on the real number $r\in\mathbb{R}_{>0}$, the Arakelov ray *class* of the divisor $\mathbf{a}$ and $\tau\in(\mathcal{O}_K/\mathfrak{m})^*$.

Since the distribution $\mathcal{D}$ is assumed to be uniform when projected to the Arakelov ray class group $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$, we can deduce that, for any fundamental domain F of $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$ in $\mathrm{Div}_{K^{\mathfrak{m}}}^0$,

$$\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}[|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty|]=\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F)}[|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty|] \qquad (6.86)$$

where $\mathcal{U}(F)$ is the uniform distribution on the fundamental domain F.

By scaling, one can show that $|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty|=|\mathrm{Exp}(\mathbf{a}+d^0(\mathfrak{c}))_\tau^\times\cap r\mathcal{N}(\mathfrak{c})^{-1/n}\mathcal{B}_\infty|$. By another technical argument (see Lemma 6.14(i)) one can show that this quantity is non-zero only if $[\mathbf{a}+d^0(\mathfrak{c})]\in[(\!|\tau^{-1}|\!)]T^{\mathfrak{m}}\subseteq\mathrm{Pic}_{K^{\mathfrak{m}}}^0$, i.e., if the Arakelov ray class of $\mathbf{a}+d^0(\mathfrak{c})$ lies in a specific coset of the ray unit torus in $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$. We can then deduce that for any fundamental domain $F_{T^{\mathfrak{m}}}$ of $T^{\mathfrak{m}}$ in H,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F)}[|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times\cap r\mathcal{B}_\infty|] \\
=&\frac{1}{|\mathrm{Cl}_K^{\mathfrak{m}}|}\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F_{T^{\mathfrak{m}}})}[|\mathrm{Exp}(\mathbf{a})_\tau^\times\cap r\,\mathcal{N}(\mathfrak{c})^{-1/n}\mathcal{B}_\infty|]. \qquad (6.87)
\end{aligned}$$

where $\mathcal{U}(F_{T^{\mathfrak{m}}})$ is the uniform distribution on the fundamental domain $F_{T^{\mathfrak{m}}}$.

Taking the logarithmic map into $H = \operatorname{Log} K_{\mathbb{R}}^0$

Applying the logarithmic map on the set $\operatorname{Exp}(\mathbf{a})_\tau^\times \cap r \cdot \mathcal{N}(\mathfrak{c})^{-1/n}\mathcal{B}_\infty$, sends $\operatorname{Exp}(\mathbf{a})_\tau^\times$ to a shift of the logarithmic ray unit lattice $\Lambda_{K^{\mathfrak{m},1}} = \operatorname{Log}(\mathcal{O}_{K^{\mathfrak{m},1}}^\times)$ and $r \cdot \mathcal{N}(\mathfrak{c})^{-1/n}\mathcal{B}_\infty$ to a simplex $S_{n \log r - \log \mathcal{N}(\mathfrak{c})}$ of volume $C(r, \mathcal{N}(\mathfrak{c}))$, where $S_x = \operatorname{Log}(x\mathcal{B}_\infty) \subseteq \operatorname{Log} K_{\mathbb{R}}$ as in Lemma A.1.

The expected value as in Equation (6.87) then equals the average number of points of a randomly shifted logarithmic ray unit lattice into this simplex, which equals $C(r, \mathcal{N}(\mathfrak{c}))/\operatorname{Vol}(T^{\mathfrak{m}})$. The precise value is as follows.

$$\frac{1}{|\operatorname{Cl}_K^{\mathfrak{m}}|} \mathop{\mathbb{E}}_{\mathbf{a} \leftarrow \mathcal{U}(F_{T^{\mathfrak{m}}})} [|\operatorname{Exp}(\mathbf{a})_\tau^\times \cap r\,\mathcal{N}(\mathfrak{c})^{-1/n}\mathcal{B}_\infty|] = \frac{|\mu_K| \cdot C(r, \mathcal{N}(\mathfrak{c}))}{\phi(\mathfrak{m}) \cdot h_K \cdot R_K} \tag{6.88}$$

Applying the Abel summation formula to get the probability for the ideal set $\mathcal{S}^{\mathfrak{m}}$

By combining Equations (6.85) to (6.88), using the class number formula (see Equation (2.11)) and by the fact that $\frac{\mathcal{N}(\mathfrak{m})}{\phi(\mathfrak{m})} = \frac{|\mathcal{O}_K/\mathfrak{m}|}{|(\mathcal{O}_K/\mathfrak{m})^*|} \geq 1$, one obtains,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a} \leftarrow \mathcal{D}} [\mathbb{p}_{\mathbf{a},\mathfrak{c}}] \\
&= \mathop{\mathbb{E}}_{\mathbf{a} \leftarrow \mathcal{D}} \left[\Pr_{\alpha \leftarrow \operatorname{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[(\alpha) \cdot \operatorname{Exp}(-\mathbf{a}) = \mathfrak{c} \mid \alpha \cdot \operatorname{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \right] \right] \\
&\geq e^{-1/4} \cdot \frac{\sqrt{|\Delta_K|} \cdot \mathcal{N}(\mathfrak{m})}{r^n \cdot 2^{n_{\mathbb{R}}} \cdot (2\pi)^{n_{\mathbb{C}}}} \cdot \frac{|\mu_K| \cdot C(r, \mathcal{N}(\mathfrak{c}))}{\phi(\mathfrak{m}) \cdot h_K \cdot R_K} = e^{-1/4} \cdot \frac{C(r, \mathcal{N}(\mathfrak{c}))}{r^n \cdot \rho_K} \cdot \frac{\mathcal{N}(\mathfrak{m})}{\phi(\mathfrak{m})} \\
&\geq e^{-1/4} \cdot \frac{C(r, \mathcal{N}(\mathfrak{c}))}{r^n \cdot \rho_K},
\end{aligned} \tag{6.89}$$

By taking the sum over all $\mathfrak{c} \in \mathcal{S}^{\mathfrak{m}}$, using linearity of the expected value operator, one can achieve the following lower bound.

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a} \leftarrow \mathcal{D}} \left[\Pr_{\alpha \leftarrow \operatorname{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[(\alpha) \cdot \operatorname{Exp}(-\mathbf{a}) \in \mathcal{S}^{\mathfrak{m}} \;\middle|\; \alpha \cdot \operatorname{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \right] \right] \\
&= \mathop{\mathbb{E}}_{\mathbf{a} \leftarrow \mathcal{D}} \left[\sum_{\mathfrak{c} \in \mathcal{S}^{\mathfrak{m}}} \mathbb{p}_{\mathbf{a},\mathfrak{c}} \right] = \sum_{\mathfrak{c} \in \mathcal{S}^{\mathfrak{m}}} \mathop{\mathbb{E}}_{\mathbf{a} \leftarrow \mathcal{D}} [\mathbb{p}_{\mathbf{a},\mathfrak{c}}] \geq e^{-1/4} \sum_{\mathfrak{c} \in \mathcal{S}^{\mathfrak{m}}} \frac{C(r, \mathcal{N}(\mathfrak{c}))}{\rho_K \cdot r^n}
\end{aligned} \tag{6.90}$$

By an application of the Abel summation formula, one can relate the sum $\sum_{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}} C(r,\mathcal{N}(\mathfrak{c}))$ with an integral involving the counting function $|\mathcal{S}^{\mathfrak{m}}(t)| = |\{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}} \mid \mathcal{N}(\mathfrak{a})\leq t\}|$ of the ideal set $\mathcal{S}^{\mathfrak{m}}$. In fact, we will show that, for some function $f:\mathbb{R}\to\mathbb{R}$,

$$\sum_{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}} \frac{C(r,\mathcal{N}(\mathfrak{c}))}{\rho_K\cdot r^n} = \int_{t=1}^{r^n} \frac{|\mathcal{S}^{\mathfrak{m}}(t)|}{\rho_K\cdot t}\cdot f(t)dt \geq \delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]/2 \tag{6.91}$$

where the last inequality is due to the function $f(t)$ having most of his weight in the interval $[r^n/e^n, r^n]$; precisely the relevant interval for the local density $\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]$ (see Definition 6.6). By combining Equations (6.90) and (6.91), we obtain

$$\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})\in\mathcal{S}^{\mathfrak{m}} \mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \geq \delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]/3.$$

which finishes the proof.

6.5. Extended Proof of Theorem 6.9

6.5.1. Simplify the Probability by Fixing a Single Ideal $\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}$ and a single Arakelov divisor $\mathbf{a}\in\mathrm{Div}^0_{K^{\mathfrak{m}}}$

In this part of the proof we focus on a fixed $\mathbf{a}\leftarrow\mathrm{Div}^0_{K^{\mathfrak{m}}}$ in the probabilistic process of Equation (6.77) in Theorem 6.9, leaving the remaining randomness to be the uniform sampling of $\alpha\in\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty$. Furthermore, we concentrate on a fixed ideal $\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}$ as well. By the law of conditional probability, we have

$$\begin{aligned}\mathbb{p}_{\mathbf{a},\mathfrak{c}} &= \Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})=\mathfrak{c} \mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\\ &= \frac{\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[\begin{array}{c}(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})=\mathfrak{c}\\ \text{and}\\ \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\end{array}\right]}{\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[\alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]}.\end{aligned} \tag{6.92}$$

In the following lemma we compute the exact values of these probabilities.

Lemma 6.12. *Let $\mathfrak{m} \subseteq \mathcal{O}_K$ be a modulus, let $\tau \in (\mathcal{O}_K/\mathfrak{m})^*$, let $\mathbf{a} \in \mathrm{Div}^0_{K^{\mathfrak{m}}}$ be a fixed Arakelov ray divisor, and let $\mathfrak{c} \in \mathcal{I}_K^{\mathfrak{m}}$ be an integral ideal. Then*

$$\Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \begin{bmatrix} (\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \\ \textit{and} \\ \alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \end{bmatrix} = \frac{|\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|}{|\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty|}, \tag{6.93}$$

and, there exists some $\tilde{\tau} \in K_{\mathbb{R}}$ such that

$$\Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty} \left[\alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1}\right] = \frac{|(\mathrm{Exp}(\mathbf{a})\mathfrak{m} + \tilde{\tau}) \cap r\mathcal{B}_\infty|}{|\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty|}, \tag{6.94}$$

where the sampling $\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ is uniform in both expressions.

Proof. By examining Definition 6.2 closely, noting that $\mathrm{Exp}((\mathbf{a} + d(\mathfrak{c}))_{\mathrm{f}}) = \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) \cdot \mathfrak{c} \in \mathcal{I}_K^{\mathfrak{m}}$, we see that for all $\alpha \in \mathrm{Exp}(\mathbf{a})$,

$$(\alpha) \cdot \mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \text{ and } \alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1} \iff \alpha \in \mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times.$$

As the number of choices for $\alpha \in \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ equals $|\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty|$, the number of good choices equals $|\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|$ and since the sampling procedure is uniform, we arrive at the first probability claim. For the second probability claim, write $\mathfrak{a} = \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) \in \mathcal{I}_K^{\mathfrak{m}}$, for conciseness. We note that for $\alpha \in \mathrm{Exp}(\mathbf{a})$, $\alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1}$ is equivalent to

$$\alpha \cdot \mathrm{Exp}(-\mathbf{a}_\infty) \in \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) \cap \tau K^{\mathfrak{m},1} = \mathfrak{a} \cap \tau K^{\mathfrak{m},1} = \mathfrak{a}\mathfrak{m} + \tau',$$

where $\tau' \in \mathfrak{a}$ is such that $\tau' \equiv \tau$ modulo $\mathfrak{m}$ (note that $\mathfrak{a}$ and $\mathfrak{m}$ are coprime). This, in turn, is equivalent to

$$\alpha \in \mathrm{Exp}(\mathbf{a}_\infty)(\mathfrak{a}\mathfrak{m} + \tau') = \mathrm{Exp}(\mathbf{a})\mathfrak{m} + \tilde{\tau}$$

where $\tilde{\tau} = \mathrm{Exp}(\mathbf{a}_\infty)\tau' \in K_{\mathbb{R}}$, which proves the claim. □

6.5.2. Estimating the Number of Shifted Lattice Points in a Box

Both Equations (6.93) and (6.94) involve the number of shifted lattice points in the volume $r\mathcal{B}_\infty$. For large enough radius r, we can reasonably estimate

this quantity to be $|(\mathrm{Exp}(\mathbf{a})+\tilde{\tau})\cap r\mathcal{B}_\infty| \approx r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}/(e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|})$.

Lemma 6.13. *Let $x \geq 1$. For any Arakelov ray divisor $\mathbf{a} \in \mathrm{Div}_{K^\mathfrak{m}}$, any $r > x \cdot n^2 \cdot |\Delta_K|^{\frac{3}{2n}} \cdot e^{\deg(\mathbf{a})/n}$ and any $\tilde{\tau} \in K_\mathbb{R}$, we have*

$$|(\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}) \cap r\mathcal{B}_\infty| \in [e^{-1/x}, e^{1/x}] \cdot \frac{r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}}{e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|}},$$

where we note that for $\mathbf{a} \in \mathrm{Div}^0_{K^\mathfrak{m}}$, i.e., degree-one Arakelov ray divisors, we have $\deg(\mathbf{a}) = 0$.

Proof. Let us write $\mathcal{V}_\infty$ for the Voronoi cell of $\mathrm{Exp}(\mathbf{a})$ around 0 with respect to the infinity norm, i.e., $\mathcal{V}_\infty = \{x \in K_\mathbb{R} \mid \|x\|_\infty < \|x - v\|_\infty \text{ for all } v \in \mathrm{Exp}(\mathbf{a})\}$. This is well-known to be a fundamental domain for the lattice $\mathrm{Exp}(\mathbf{a})$ (up to a set of 'faces' of measure zero), thus having volume $\det(\mathrm{Exp}(\mathbf{a})) = e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|}$. Denote $\mathrm{cov}_\infty = \mathrm{cov}_\infty(\mathrm{Exp}(\mathbf{a})) = \max\{\|x\|_\infty \mid x \in \mathcal{V}_\infty\}$ for the covering radius of the lattice $\mathrm{Exp}(\mathbf{a})$ with respect to the infinity norm. Furthermore, denote $\tilde{\tau}_0 \in \mathcal{V}_\infty$ for the unique representative of $\tilde{\tau} + \mathrm{Exp}(\mathbf{a})$ in $\mathcal{V}_\infty$, implying $\mathrm{Exp}(\mathbf{a}) + \tilde{\tau} = \mathrm{Exp}(\mathbf{a}) + \tilde{\tau}_0$.

The sets $v + \mathcal{V}_\infty$ for $v \in (\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}_0) \cap r\mathcal{B}_\infty$ are disjoint and are included in $K_\mathbb{R} \cap (r + 2 \cdot \mathrm{cov}_\infty)\mathcal{B}_\infty$. Hence, by computing the volume of $\cup_{v \in (\mathrm{Exp}(\mathbf{a})+\tilde{\tau}_0)\cap r\mathcal{B}_\infty}(v + \mathcal{V}_\infty)$ in $K_\mathbb{R}$, we obtain

$$\begin{aligned} |(\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}_0) \cap r\mathcal{B}_\infty| \cdot e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|} &\leq (r + 2 \cdot \mathrm{cov}_\infty)^n \cdot \mathrm{Vol}(K_\mathbb{R} \cap \mathcal{B}_\infty) \\ &\leq (r + 2 \cdot \mathrm{cov}_\infty)^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}, \end{aligned}$$

where we used the fact that $\mathrm{Vol}(\mathcal{V}_\infty) = \det(\mathrm{Exp}(\mathbf{a})) = e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|}$. Observe also that $K_\mathbb{R} \cap \mathcal{B}_\infty$ contains some coordinates that are real and other that are complex. Hence, its volume is $2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}$ and not 2^n (the 2-dimensional volume of $\{(x, \overline{x}) \in \mathbb{C}^2 | \ |x| \leq 1\}$ is 2π).

In a similar fashion, we can deduce that the set $K_\mathbb{R} \cap (r - 2 \cdot \mathrm{cov}_\infty)\mathcal{B}_\infty$ is included in $\cup_{v \in (\mathrm{Exp}(\mathbf{a})+\tilde{\tau}_0)\cap r\mathcal{B}_\infty}(v + \overline{\mathcal{V}}_\infty)$, where $\overline{\mathcal{V}}_\infty$ is the topological closure

of $\mathcal{V}_\infty$. The sets $v + \overline{\mathcal{V}}_\infty$ for $v \in (\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}_0) \cap r\mathcal{B}_\infty$ are disjoint up to sets of measure zero, and therefore, by computing volumes, we obtain

$$\begin{aligned}(r - 2 \cdot \mathrm{cov}_\infty)^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}} &= (r - 2 \cdot \mathrm{cov}_\infty)^n \cdot \mathrm{Vol}(K_\mathbb{R} \cap \mathcal{B}_\infty) \\ &\leq |(\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}_0) \cap r\mathcal{B}_\infty| \cdot e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|}\end{aligned}$$

Combining the two bounds, one obtains

$$\begin{aligned}\left(1 - \frac{2 \cdot \mathrm{cov}_\infty}{r}\right)^n \cdot \frac{r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}}{e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|}} &\leq |(\mathrm{Exp}(\mathbf{a}) + \tilde{\tau}_0) \cap r\mathcal{B}_\infty| \\ &\leq \left(1 + \frac{2 \cdot \mathrm{cov}_\infty}{r}\right)^n \cdot \frac{r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}}{e^{\deg(\mathbf{a})} \cdot \sqrt{|\Delta_K|}}.\end{aligned}$$

From Lemma 2.22, we know that $\mathrm{cov}_\infty(\mathrm{Exp}(\mathbf{a})) \leq n/2 \cdot |\Delta_K|^{\frac{3}{2n}} \cdot e^{\deg(\mathbf{a})/n}$; so, by assumption, $r \geq 2 \cdot x \cdot n \cdot \mathrm{cov}_\infty$. We obtain the final claim by substituting r and using the inequality $(1 + y/n)^n \leq e^y$ for all $y \in (-1, 1)$. □

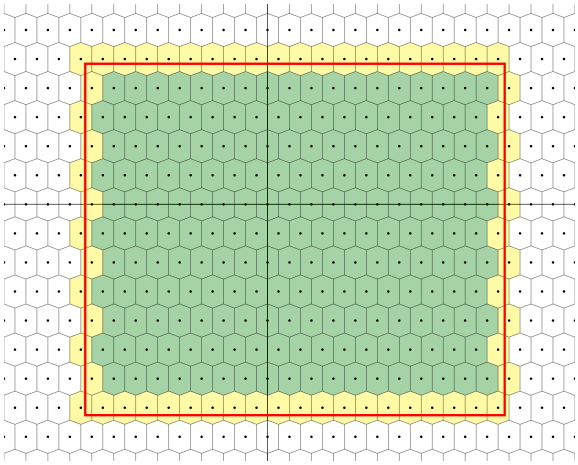

Figure 6.1.: The number of lattice points in the red box is clearly sandwiched by the number of green cells and the number of green and yellow cells together.

Applying above lemma with $x = 4$ and thus $r = 4 \cdot n^2 \cdot |\Delta_K|^{\frac{3}{2n}} \cdot \mathcal{N}(\mathfrak{m})^{1/n}$, to Equations (6.93) and (6.94) and substituting them into Equation (6.92),

one obtains,

$$\begin{aligned}\mathbb{p}_{\mathbf{a},\mathfrak{c}} &= \Pr_{\alpha \leftarrow \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty) \in \tau K^{\mathfrak{m},1}\right] \\ &= \frac{|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|}{|(\mathrm{Exp}(\mathbf{a})\mathfrak{m}+\tilde{\tau}) \cap r\mathcal{B}_\infty|} \\ &\in [e^{-1/4}, e^{1/4}] \cdot \frac{\sqrt{|\Delta_K|}\cdot\mathcal{N}(\mathfrak{m})}{r^n \cdot 2^{n_\mathbb{R}} \cdot (2\pi)^{n_\mathbb{C}}} \cdot |\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty| \qquad (6.95)\end{aligned}$$

Here, we use that $\det(\mathrm{Exp}(\mathbf{a})\mathfrak{m}) = e^{\deg(\mathbf{a})}\cdot\sqrt{|\Delta_K|} = \mathcal{N}(\mathfrak{m})\cdot\sqrt{|\Delta_K|}$, and thus $|(\mathrm{Exp}(\mathbf{a})\mathfrak{m}+\tilde{\tau}) \cap r\mathcal{B}_\infty| \in [e^{-1/4}, e^{1/4}] \cdot \frac{r^n\cdot 2^{n_\mathbb{R}}\cdot(2\pi)^{n_\mathbb{C}}}{\sqrt{|\Delta_K|}\cdot\mathcal{N}(\mathfrak{m})}$.

6.5.3. Estimating the Probability of Sampling a Single Fixed Ideal for a *Random* Arakelov Divisor

To obtain the probability of sampling a fixed ideal for a *random* Arakelov divisor, one needs to take the weighted sum over the probabilities of sampling a fixed ideal for a fixed Arakelov divisor, where the weights are given by the density $\mathcal{D}$ on $\mathrm{Div}^0_{K^\mathfrak{m}}$. In other words, one needs to take the *expected value*. So, for a fixed integral ideal $\mathfrak{c} \in \mathcal{I}_K^\mathfrak{m}$, we have

$$\begin{aligned}&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\mathbb{p}_{\mathbf{a},\mathfrak{c}}\right] \\ &= \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a}) = \mathfrak{c} \mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \\ &\in [e^{-1/4}, e^{1/4}] \cdot \frac{\sqrt{|\Delta_K|}\cdot\mathcal{N}(\mathfrak{m})}{r^n\cdot 2^{n_\mathbb{R}}\cdot(2\pi)^{n_\mathbb{C}}} \cdot \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|\right]. \qquad (6.96)\end{aligned}$$

where the last approximate equality follows from the linearity of the expectation and Equation (6.95).

6.5.4. The Number $|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|$ Only Depends on the Arakelov Ray *Class* of $\mathbf{a} \in \mathrm{Div}^0_{K^\mathfrak{m}}$

It thus remains to focus on the expected value

$$\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|\right]. \qquad (6.97)$$

In the following rather technical lemma we will – among other things – prove that the number of elements in $\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty$ only depends on the Arakelov ray *class* of $\mathbf{a}$, meaning that we might take the expected value over the uniform distribution over a fundamental domain of $\mathrm{Pic}^0_{K^\mathfrak{m}}$ in $\mathrm{Div}^0_{K^\mathfrak{m}}$ in Equation (6.97), as $[\mathcal{D}]$ is uniform over $\mathrm{Pic}^0_{K^\mathfrak{m}}$, per assumption (see Definition 6.8).

Lemma 6.14. *For all ray divisors $\mathbf{a} \in \mathrm{Div}^0_{K^\mathfrak{m}}$, elements $\tau, \tau' \in K^\mathfrak{m}$, ideals $\mathfrak{c} \in \mathcal{I}_K^\mathfrak{m}$ and real numbers $r > 0$ we have the following list of facts.*

(i) $|\mathrm{Exp}(\mathbf{a})_\tau^\times \cap r\mathcal{B}_\infty| = |\mathrm{Exp}(\mathbf{a}+(\!|\tau'|\!))_{\tau\tau'}^\times \cap r\mathcal{B}_\infty|$, *i.e., the number of τ-equivalent ray generators of $\mathbf{a}$ in a fixed box of radius r is equal to the number of $\tau\tau'$-equivalent ray generators of $\mathbf{a}+(\!|\tau'|\!)$ in the same box.*

(ii) $|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty| = |\mathrm{Exp}(\mathbf{a}+d^0(\mathfrak{c}))_\tau^\times \cap \frac{r}{\mathcal{N}(\mathfrak{c})^{1/n}}\mathcal{B}_\infty|$, *so the only difference between the maps d^0 and d is just some appropriate scaling.*

(iii) Writing $\mathbf{a}_\infty = \sum_\nu a_\nu \cdot (\!|\nu|\!) \in H \subseteq \mathrm{Div}^0_{K^\mathfrak{m}}$, we have

$$|\mathrm{Exp}(\mathbf{a}_\infty)_1^\times \cap r\mathcal{B}_\infty| = |\mu_{K^\mathfrak{m},1}| \cdot |(\Lambda_{K^\mathfrak{m},1} + (a_{\nu_\sigma})_\sigma) \ \cap \ S_{\log(r)}|, \quad (6.98)$$

where $S_{\log r} = \{x \in \mathrm{Log}\, K_\mathbb{R} \mid x_\sigma \leq \log(r)\,,\ \sum_\sigma x_\sigma = 0\}$ is a simplex as in Lemma A.1.

Proof. For part (i), observe that multiplying by $\left(\frac{\sigma(\tau')}{|\sigma(\tau')|}\right)_\sigma \in K_\mathbb{R}$ yields a bijection from $\mathrm{Exp}(\mathbf{a})$ to $\mathrm{Exp}(\mathbf{a}+(\!|\tau'|\!))$, preserving the maximum norm. It remains to show that this bijection sends $\mathrm{Exp}(\mathbf{a})_\tau^\times$ to $\mathrm{Exp}(\mathbf{a}+(\!|\tau'|\!))_{\tau'\tau}^\times$. Using Definition 6.2 and assuming $\mathrm{Exp}(\mathbf{a}_\mathrm{f}) = \kappa\mathcal{O}_K$ (and therefore $\mathrm{Exp}([\mathbf{a}+(\!|\tau'|\!)]_\mathrm{f}) = \tau'\kappa\mathcal{O}_K$), we have

$$\left(\frac{\sigma(\tau')}{|\sigma(\tau')|}\right)_\sigma \cdot \mathrm{Exp}(\mathbf{a})_\tau^\times = \left(\frac{1}{|\sigma(\tau')|}\right)_\sigma \cdot (\tau') \cdot \underbrace{\mathrm{Exp}(\mathbf{a}_\infty) \cdot (\kappa\mathcal{O}_K^\times \cap \tau K^{\mathfrak{m},1})}_{\mathrm{Exp}(\mathbf{a})_\tau^\times}$$

$$= \underbrace{\left(\frac{1}{|\sigma(\tau')|}\right)_\sigma \cdot \mathrm{Exp}(\mathbf{a}_\infty)}_{\mathrm{Exp}((\mathbf{a}+(\!|\tau'|\!))_\infty)} \cdot (\tau'\kappa\mathcal{O}_K^\times \cap \tau'\tau K^{\mathfrak{m},1}) = \mathrm{Exp}(\mathbf{a}+(\!|\tau|\!))_{\tau'\tau}^\times$$

For part (ii), recall that multiplying the ideal lattice $\mathrm{Exp}(d(\mathfrak{c})) = \mathfrak{c} \subseteq K_{\mathbb{R}}$ by the scalar $\mathcal{N}(\mathfrak{c})^{-1/n}$ results in the ideal lattice $\mathrm{Exp}(d^0(\mathfrak{c}))$. Applying this scalar multiplication to the set $\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c})) \cap r\mathcal{B}_\infty$ yields a bijective correspondence with $\mathrm{Exp}(\mathbf{a} + d^0(\mathfrak{c})) \cap \frac{r}{\mathcal{N}(\mathfrak{c})^{1/n}}\mathcal{B}_\infty$.

In part (iii) it is enough to show that the logarithm $\mathrm{Log} : K_{\mathbb{R}} \to \mathrm{Log}(K_{\mathbb{R}})$ takes $\mathrm{Exp}(\mathbf{a}_\infty)_1^\times$ to the shifted lattice $\mathrm{Log}(\mathcal{O}_{K^{\mathfrak{m},1}}^\times) + (a_{\nu_\sigma})_\sigma \subset H$ and takes $r\mathcal{B}_\infty$ to the simplex $S_{\log(r)} \subset H$. This logarithmic map is $|\mu_{K^{\mathfrak{m},1}}|$-to-one on $\mathrm{Exp}(\mathbf{a}_\infty)_1^\times$, as it sends roots of unity to the all-one vector in $K_{\mathbb{R}}$, yielding the extra factor $|\mu_{K^{\mathfrak{m},1}}|$ in Equation (6.98). Here, $\mu_{K^{\mathfrak{m},1}} = \mu_K \cap K^{\mathfrak{m},1}$, i.e., the roots of unity in $K^{\mathfrak{m},1}$. □

As a corollary of Lemma 6.14(i) we deduce that

$$|\mathrm{Exp}(\mathbf{a})_\tau^\times \cap r\mathcal{B}_\infty| = |\mathrm{Exp}(\mathbf{a} + (\!|\kappa|\!))_\tau^\times \cap r\mathcal{B}_\infty|$$

for $\kappa \in K^{\mathfrak{m},1}$, i.e., the number of elements $|\mathrm{Exp}(\mathbf{a})_\tau^\times \cap r\mathcal{B}_\infty|$ only depends on the Arakelov ray class of $\mathbf{a}$ (next to $r \in \mathbb{R}$, $\mathfrak{m}$ and $\tau \in K^{\mathfrak{m}}$). Choose a (measurable) fundamental domain $F \subseteq \mathrm{Div}_{K^{\mathfrak{m}}}^0$ of the quotient group $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$, and put $F_{T^{\mathfrak{m}}} = \{\mathbf{a} \in F \mid [\mathbf{a}] \in T^{\mathfrak{m}}\}$, a fundamental domain of $T^{\mathfrak{m}}$ in $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$. Then, by the assumption that $[\mathcal{D}]$ is uniform on $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$, and writing $\tilde{r} = r\,\mathcal{N}(\mathfrak{c})^{-1/n}$ we deduce

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[|\mathrm{Exp}(\mathbf{a} + d(\mathfrak{c}))_\tau^\times \cap r\mathcal{B}_\infty|\right] = \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[|\mathrm{Exp}(\mathbf{a} + d^0(\mathfrak{c}))_\tau^\times \cap \tilde{r}\mathcal{B}_\infty|\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F)}\left[|\mathrm{Exp}(\mathbf{a} + d^0(\mathfrak{c}))_\tau^\times \cap \tilde{r}\mathcal{B}_\infty|\right] = \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F)}\left[|\mathrm{Exp}(\mathbf{a} + (\!|\tau|\!))_\tau^\times \cap \tilde{r}\mathcal{B}_\infty|\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F)}\left[|\mathrm{Exp}(\mathbf{a})_1^\times \cap \tilde{r}\mathcal{B}_\infty|\right] = \frac{1}{|\mathrm{Cl}_K^{\mathfrak{m}}|}\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F_{T^{\mathfrak{m}}})}\left[|\mathrm{Exp}(\mathbf{a})_1^\times \cap \tilde{r}\mathcal{B}_\infty|\right] \quad (6.99)
\end{aligned}$$

where the first equality follows from scaling (Lemma 6.14(ii)) and the second one by the fact that the random variable is an Arakelov ray class invariant (Lemma 6.14(i)) and that $[\mathcal{D}]$ is uniform on $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$. The third equality holds because $F + d^0(\mathfrak{c}) - (\!|\tau|\!)$ is a fundamental domain of $\mathrm{Pic}_{K^{\mathfrak{m}}}^0$ in $\mathrm{Div}_{K^{\mathfrak{m}}}^0$ if F is. The fourth equality follows directly from Lemma 6.14(i), and the last equality follows from Definition 6.2. Namely, an Arakelov divisor $\mathbf{a}$ can only have generators if the ideal class of $\mathrm{Exp}(\mathbf{a}_{\mathrm{f}})$ is trivial, i.e., if $[\mathbf{a}] \in T^{\mathfrak{m}}$. So,

instead, $\mathbf{a}$ can be chosen uniformly from a fundamental domain $F_{T^{\mathfrak{m}}}$ of $T^{\mathfrak{m}}$ in $\mathrm{Div}^0_{K^{\mathfrak{m}}}$, with a correction factor of $\frac{1}{|\mathrm{Cl}^{\mathfrak{m}}_K|}$ in the expected value.

6.5.5. Taking the Logarithmic Map into $H = \mathrm{Log}\, K^0_{\mathbb{R}}$

By taking the Logarithmic image, we find, by Lemma 6.14(iii), that Equation (6.99) equals

$$\frac{|\mu_{K^{\mathfrak{m},1}}|}{|\,\mathrm{Cl}^{\mathfrak{m}}_K\,|} \cdot \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{U}(F_{T^{\mathfrak{m}}})} \left[\left|\Lambda_{K^{\mathfrak{m},1}} + (a_{\nu_\sigma})_\sigma \cap S_{\log(r)-\log\mathcal{N}(\mathfrak{c})/n}\right|\right] \tag{6.100}$$

$$= \frac{|\mu_{K^{\mathfrak{m},1}}|}{|\,\mathrm{Cl}^{\mathfrak{m}}_K\,|} \frac{\mathrm{Vol}(S_{\log(r)-\log\mathcal{N}(\mathfrak{c})/n})}{\mathrm{Vol}(F_{T^{\mathfrak{m}}})} \tag{6.101}$$

$$= \frac{|\mu_K| \cdot C(r,\mathcal{N}(\mathfrak{c}))}{|\,\mathrm{Cl}^{\mathfrak{m}}_K\,| \cdot [\mathcal{O}^\times_K : \mathcal{O}^\times_{K^{\mathfrak{m},1}}] \cdot R_K} = \frac{|\mu_K| \cdot C(r,\mathcal{N}(\mathfrak{c}))}{\phi(\mathfrak{m}) \cdot h_K \cdot R_K}. \tag{6.102}$$

where $C(r,\mathcal{N}(\mathfrak{c})) = \mathrm{Vol}(S_{\log(r)-\log\mathcal{N}(\mathfrak{c})/n}) = (n\log r - \log\mathcal{N}(\mathfrak{c}))^{\mathbb{r}}/\mathbb{r}!$ whenever $\mathcal{N}(\mathfrak{c}) \leq r^n$ and zero otherwise; and where $\phi(\mathfrak{m}) = |(\mathcal{O}_K/\mathfrak{m})^*|$. The first inequality of Equation (6.101) follows from Lemma 6.1, the second equality follows from Lemmas A.1 and A.2 and the fact that $\mathrm{Vol}(F_{T^{\mathfrak{m}}}) = \mathrm{Vol}(T^{\mathfrak{m}}) = [\mathcal{O}^\times_K : \mathcal{O}^\times_{K^{\mathfrak{m},1}}] \cdot |\mu_{K^{\mathfrak{m},1}}| \cdot |\mu_K|^{-1} \cdot \mathrm{Vol}(T)$ (see Lemma 2.16). The third inequality (Equation (6.102)) uses the fact that $|\,\mathrm{Cl}^{\mathfrak{m}}_K\,| \cdot [\mathcal{O}^\times_K : \mathcal{O}^\times_{K^{\mathfrak{m},1}}] = \phi(\mathfrak{m}) \cdot h_K$ (see Lemma 2.15).

Remark 6.15. *Note that all number-theoretic quantities in Equation (6.102) make sense intuitively: one out of h_K random ideal lattices is expected to be principal, the density of units (including roots of unity) is $|\mu_K|/R_K$ and one out of $\phi(\mathfrak{m})$ random elements coprime to $\mathfrak{m}$ equals τ mod $\mathfrak{m}$*

Combining Equations (6.96), (6.99) and (6.100) and the class number formula

(see Equation (2.11)), we have

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}[\mathbb{p}_{\mathbf{a},\mathfrak{c}}] \\
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\cdot\mathrm{Exp}(-\mathbf{a})=\mathfrak{c}\mid \alpha\cdot\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \\
&\in [e^{-1/4},e^{1/4}]\cdot\frac{\sqrt{|\Delta_K|}\cdot\mathcal{N}(\mathfrak{m})}{r^n\cdot 2^{n_\mathbb{R}}\cdot(2\pi)^{n_\mathbb{C}}}\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[|\mathrm{Exp}(\mathbf{a}+d(\mathfrak{c}))^\times_\tau\cap r\mathcal{B}_\infty|\right] \\
&= [e^{-1/4},e^{1/4}]\cdot\frac{\sqrt{|\Delta_K|}\cdot\mathcal{N}(\mathfrak{m})}{r^n\cdot 2^{n_\mathbb{R}}\cdot(2\pi)^{n_\mathbb{C}}}\cdot\frac{|\mu_K|\cdot C(r,\mathcal{N}(\mathfrak{c}))}{\phi(\mathfrak{m})\cdot h_K\cdot R_K} \\
&= [e^{-1/4},e^{1/4}]\cdot\frac{C(r,\mathcal{N}(\mathfrak{c}))}{r^n\cdot\rho_K}\cdot\frac{\mathcal{N}(\mathfrak{m})}{\phi(\mathfrak{m})}\geq e^{-1/4}\cdot\frac{C(r,\mathcal{N}(\mathfrak{c}))}{r^n\cdot\rho_K}. \qquad (6.103)
\end{aligned}$$

where $C(r,\mathcal{N}(\mathfrak{c}))=(n\log r-\log\mathcal{N}(\mathfrak{c}))^{\mathbb{r}}/\mathbb{r}!$ whenever $\mathcal{N}(\mathfrak{c})\leq r^n$ and zero otherwise.

6.5.6. Applying the Abel Summation Formula

We have, by Equation (6.103),

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\,\mathrm{Exp}(-\mathbf{a})\in\mathcal{S}^{\mathfrak{m}}\mid \alpha\,\mathrm{Exp}(\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \\
&=\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\sum_{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}}\mathbb{p}_{\mathbf{a},\mathfrak{c}}\right]=\sum_{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}}\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}[\mathbb{p}_{\mathbf{a},\mathfrak{c}}]\geq\frac{e^{-1/4}}{r^n\cdot\rho_K}\sum_{\substack{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}\\ \mathcal{N}(\mathfrak{c})\leq r^n}}C(r,\mathcal{N}(\mathfrak{c})). \qquad (6.104)
\end{aligned}$$

Lemma 6.16. *Let $\mathcal{S}^{\mathfrak{m}}\subseteq\mathcal{I}_K^{\mathfrak{m}}$ a set of integral ideals, let $r>e$, and denote $C(r,\mathcal{N}(\mathfrak{c}))=\frac{(n\log r-\log\mathcal{N}(\mathfrak{c}))^{\mathbb{r}}}{\mathbb{r}!}$. Then*

$$\frac{1}{r^n\cdot\rho_K}\sum_{\substack{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}\\ \mathcal{N}(\mathfrak{c})\leq r^n}}C(r,\mathcal{N}(\mathfrak{c}))\geq\tfrac{1}{2}\cdot\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]$$

Proof. We apply the Abel partial summation formula with $a_{N,\mathcal{S}^{\mathfrak{m}}}:=|\{\mathfrak{c}\in$

$\mathcal{S}^{\mathfrak{m}} \mid \mathcal{N}(\mathfrak{c}) = N\}|$ and $C(r,N) := \frac{(n\log r - \log N)^{\mathfrak{r}}}{\mathfrak{r}!}$, whose derivative equals

$$\begin{aligned}\tfrac{d}{dN}C(r,N)\Big|_t &= -\frac{(n\log r - \log t)^{\mathfrak{r}-1}}{t\cdot(\mathfrak{r}-1)!}\\ &= \frac{-r^n}{t\cdot(\mathfrak{r}-1)!}\cdot\left[\tfrac{d}{dN}\Gamma\big(\mathfrak{r}, n\log r - \log N\big)\right]\Big|_t,\end{aligned}$$

where $\Gamma(\mathfrak{r},x) = \int_x^\infty u^{\mathfrak{r}-1}e^{-u}du$ is the upper incomplete Gamma function. Recall that $|\mathcal{S}^{\mathfrak{m}}(t)| = \sum_{N\le t} a_{N,\mathcal{S}^{\mathfrak{m}}}$. A typical application of the Abel summation formula yields

$$\begin{aligned}&\frac{1}{r^n\cdot\rho_K}\sum_{\substack{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}\\ \mathcal{N}(\mathfrak{c})\le r^n}} C(r,\mathcal{N}(\mathfrak{c}))\\ &= \frac{1}{r^n\cdot\rho_K}\sum_{1\le N\le r^n} a_{N,\mathcal{S}^{\mathfrak{m}}}\cdot C(r,N)\\ &= -\int_{t=1}^{r^n}\frac{|\mathcal{S}^{\mathfrak{m}}(t)|}{\rho_K\cdot r^n}\cdot\left[\tfrac{d}{dN}C(r,N)\Big|_{N=t}\right]dt\\ &= \frac{1}{(\mathfrak{r}-1)!}\int_{t=1}^{r^n}\frac{|\mathcal{S}^{\mathfrak{m}}(t)|}{\rho_K\cdot t}\cdot\left[\tfrac{d}{dN}\Gamma\big(\mathfrak{r},n\log r-\log N\big)\Big|_{N=t}\right]dt, \qquad (6.105)\end{aligned}$$

Using Definition 6.6 about ideal density and the fact that the integrand is positive, Equation (6.105) is lower bounded by

$$\begin{aligned}&\frac{1}{(\mathfrak{r}-1)!}\int_{t=(r/e)^n}^{r^n}\frac{|\mathcal{S}^{\mathfrak{m}}(t)|}{\rho_K\cdot t}\cdot\left[\tfrac{d}{dN}\Gamma\big(\mathfrak{r},n\log r-\log N\big)\Big|_{N=t}\right]dt\\ \ge\ &\frac{\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]}{(\mathfrak{r}-1)!}\int_{t=(r/e)^n}^{r^n}\left[\tfrac{d}{dN}\Gamma\big(\mathfrak{r},n\log r-\log N\big)\Big|_{N=t}\right]dt \ge \tfrac{1}{2}\cdot\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n], \qquad (6.106)\end{aligned}$$

where the last inequality (Equation (6.106)) follows from the definition of the upper incomplete Gamma function,

$$\begin{aligned}&\frac{1}{(\mathfrak{r}-1)!}\int_{t=(r/e)^n}^{r^n}\left(\frac{d}{dt}\Gamma(\mathfrak{r},n\log r-\log N)\big|_{N=t}\right)dt\\ &= \frac{1}{(\mathfrak{r}-1)!}\cdot(\Gamma(\mathfrak{r},0)-\Gamma(\mathfrak{r},n)) = 1-e^{-n}\sum_{k=0}^{\mathfrak{r}-1}\frac{n^k}{k!}\ge 1/2,\end{aligned}$$

where we used the fact that $e^{-n}\sum_{k=0}^{\mathfrak{r}-1}\frac{n^k}{k!}$ equals the probability that a Poisson distribution with parameter n yields at most $\mathfrak{r}-1\le n-1$ occurrences, which is bounded by a half. □

We conclude that

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}[\mathbb{p}_{\mathbf{a},\mathfrak{c}}] \\
&= \mathop{\mathbb{E}}_{\mathbf{a}\leftarrow\mathcal{D}}\left[\Pr_{\alpha\leftarrow\mathrm{Exp}(\mathbf{a})\cap r\mathcal{B}_\infty}\left[(\alpha)\,\mathrm{Exp}(-\mathbf{a})\in\mathcal{S}^{\mathfrak{m}} \mid \alpha\,\mathrm{Exp}(-\mathbf{a}_\infty)\in\tau K^{\mathfrak{m},1}\right]\right] \\
&\geq \frac{e^{-1/4}}{r^n\cdot\rho_K}\sum_{\substack{\mathfrak{c}\in\mathcal{S}^{\mathfrak{m}}\\ \mathcal{N}(\mathfrak{c})\leq r^n}} C(r,\mathcal{N}(\mathfrak{c}))\geq \delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]/3.
\end{aligned}$$

This concludes the proof of Theorem 6.9.

Remark 6.17. *As already mentioned, the fraction* $\frac{1}{3}$ *before* $\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]$ *can be made arbitrarily close to* 1*. In order to achieve that, we need to enlarge the 'ideal density' interval in Definition 6.6 to* $[x/e^{2n}, x]$ *and we need to increase the radius* $r\in\mathbb{R}_{>0}$ *in Lemma 6.13.*

In the case of this larger density interval, the Poisson distribution in above proof changes into a Poisson distribution with parameter $2n$*, but with the same bound* $(\mathbb{r}-1\leq n-1)$ *on the occurrences. This yields an exponential instead of a constant bound. Increasing the radius* r *by an exponential factor* 2^n *also yields an exponential bound on the error. So, by implementing these changes, one can obtain a lower bound on the probability in Theorem 6.9 of* $(1-O(e^{-n}))\cdot\delta_{\mathcal{S}^{\mathfrak{m}}}[r^n]$*, which is exponentially close to optimal.*

6.6. Ideal Sampling

6.6.1. Sampling in a Box

In this section, we explain how one can efficiently sample in a (distorted) infinity box, provided that all the dimensions of the box are sufficiently large. More precisely, let $(r_\sigma)_\sigma\in K_{\mathbb{R}}$ be such that $r_\sigma>0$ for all coordinates. We let $(r_\sigma)_\sigma\mathcal{B}_\infty$ denote the distorted box

$$(r_\sigma)_\sigma\mathcal{B}_\infty := \{(x_\sigma)_\sigma\in K_{\mathbb{R}} \,|\, |x_\sigma|\leq r_\sigma,\ \forall\sigma\}.$$

Proposition 6.18. *Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal represented by a basis $M_\mathfrak{a}$, let $\beta \in \mathcal{O}_K$ be a shift and let $(r_\sigma)_\sigma \in K_\mathbb{R}$ be such that $r_\sigma > 0$ for all σ. Assume that for all embeddings σ, it holds that $r_\sigma \geq 4 \cdot 2^n \cdot n^{3/2} \cdot |\Delta_K|^{3/(2n)} \cdot \mathcal{N}(\mathfrak{a})^{1/n}$. Then, there exists an algorithm sampling uniformly in $(\mathfrak{a} + \beta) \cap (r_\sigma)_\sigma \mathcal{B}_\infty$ using time $O(n^6 \log(|M_\mathfrak{a}|)^3)$, where $|M_\mathfrak{a}|$ denotes the length of the longest basis vector of $M_\mathfrak{a}$.*

Remark 6.19. *This lemma can be seen as the 'algorithmization' of the ideas in the very similar Lemma 6.13. In that particular lemma (see also Figure 6.1), an estimation is made of the number of lattice points in a box, where Voronoi cells are used as the fundamental domain.*

In the proof of this lemma, we sample a random element in the ambient vector space of the lattice that also lies in the predescribed box $(r_\sigma)_\sigma \mathcal{B}_\infty$. Then, we use a 'rounding algorithm' to round this real vector to an actual lattice point in $\mathfrak{a}$. Such a rounding algorithm needs a fundamental domain of the lattice $\mathfrak{a}$, which can be computed by means of the LLL-algorithm. This might yield quite a skewed fundamental domain, hence the slightly worse requirements on the parameters, compared to Lemma 6.13.

Proof. The algorithm first computes (in polynomial time) an LLL reduced basis $(a_1, \cdots, a_n)$ of $\mathfrak{a}$ from $M_\mathfrak{a}$. This basis satisfies $\|a_i\| \leq 2^n \lambda_n(\mathfrak{a}) \leq 2^n \cdot \sqrt{n} \cdot |\Delta_K|^{3/(2n)} \cdot \mathcal{N}(\mathfrak{a})^{1/n}$ (using Lemma 2.22). After that, reduce $\beta \in \mathcal{O}_K$ modulo this LLL reduced basis $(a_1, \cdots, a_n)$ of $\mathfrak{a}$, yielding $\tilde{\beta} \in \beta + \mathfrak{a}$. That is, write $\beta = \sum_i t_i a_i$ and put $\tilde{\beta} = \sum_i (t_i - \lfloor t_i \rceil) a_i$.

Denoting $D := \sum_i \|a_i\|_\infty \leq 2^n \cdot \sqrt{n} \cdot |\Delta_K|^{3/(2n)} \cdot \mathcal{N}(\mathfrak{a})^{1/n}$ for the sum of the infinity norms of the basis vectors a_i, we have $\|\tilde{\beta}\|_\infty \leq D$. Also, by assumption on $(r_\sigma)_\sigma$, it holds that $r_\sigma \geq 4nD$ for every embedding σ.

To sample a uniform element $v \in \mathfrak{a} \cap (r_\sigma)_\sigma \mathcal{B}_\infty$, the algorithm goes through the following steps. It first samples a uniform element $t = (t_\sigma)_\sigma \in (r_\sigma + 2D)_\sigma \mathcal{B}_\infty$. This can be done in time $\mathsf{poly}(n, \log(\max_\sigma r_\sigma + 2D))$, by sampling every first $r_\mathbb{R} + r_\mathbb{C}$ coordinates of $t \in K_\mathbb{R}$ independently, and defining the last $r_\mathbb{C}$ ones appropriately in order to have $t \in K_\mathbb{R}$. The algorithm then writes $t = \sum_i t_i a_i$ with $t_i \in \mathbb{R}$ (the vector t lies in the real span of $\mathfrak{a}$) and puts

$v = \sum_i \lfloor t_i \rceil a_i + \tilde{\beta}$, which lies in $\beta + \mathfrak{a}$. Finally, the algorithm outputs v if $v \in (r_\sigma)_\sigma \mathcal{B}_\infty$, otherwise it restarts.

Let us first show that the distribution of v is indeed uniform in $(\mathfrak{a} + \beta) \cap (r_\sigma)_\sigma \mathcal{B}_\infty$. Let us define $\mathcal{P} = \{\sum_i x_i a_i \,,\, x_i \in [-1/2, 1/2]\}$ the fundamental parallelepiped associated to the basis $(a_1, \cdots, a_n)$. It holds that for all $x \in \mathcal{P}$, we have $\|x\|_\infty \leq D$.

The probability of sampling $v = \alpha + \tilde{\beta} \in (r_\sigma)_\sigma \mathcal{B}_\infty$ for $\alpha \in \mathfrak{a}$ via the above procedure is equal to the probability of sampling $t \in \alpha + \mathcal{P} \subseteq (r_\sigma + 2D)_\sigma \mathcal{B}_\infty$. This probability is equal to $\mathrm{Vol}(\mathcal{P}) / \mathrm{Vol}((r_\sigma + 2D)_\sigma \mathcal{B}_\infty \cap K_\mathbb{R})$, which does not depend on $\alpha \in \mathfrak{a}$. We conclude that above sampling procedure yields $v = \alpha + \tilde{\beta}$ that are uniformly distributed in $(\mathfrak{a} + \beta) \cap (r_\sigma)_\sigma \mathcal{B}_\infty$. The running time of the algorithm is dominated by the LLL-reduction of $M_\mathfrak{a}$, which takes time $O(n^6 \log(|M_\mathfrak{a}|)^3)$, where $|M_\mathfrak{a}|$ denotes the length of the longest basis vector of $M_\mathfrak{a}$.

To conclude the proof, we show that the success probability of the algorithm is constant. Indeed, observe that whenever $t = \sum_i t_i a_i \in (r_\sigma - 2D)_\sigma \mathcal{B}_\infty$, then we have $v = \sum_i \lfloor t_i \rceil a_i + \tilde{\beta} \in (r_\sigma)_\sigma \mathcal{B}_\infty$ (since $\|t - v\|_\infty \leq D$ and $\|\tilde{\beta}\| \leq D$), and so the algorithm succeeds. The success probability of the algorithm is then at least

$$\frac{\mathrm{Vol}((r_\sigma - 2D)_\sigma \mathcal{B}_\infty \cap K_\mathbb{R})}{\mathrm{Vol}((r_\sigma + 2D)_\sigma \mathcal{B}_\infty \cap K_\mathbb{R})} = \prod_\sigma \left(\frac{1 - 2D/r_\sigma}{1 + 2D/r_\sigma} \right) \geq \left(\frac{1 - \frac{1}{2n}}{1 + \frac{1}{2n}} \right)^n \geq 1/3,$$

where we used the fact that $2nD/r_\sigma \leq 1/(2n)$ for any σ. This concludes the proof. □

6.6.2. The Sampling Algorithm

Definition 6.20. *We denote by $\mathcal{S}_B$ the set of B-smooth ideals, i.e.,*

$$\mathcal{S}_B = \{\mathfrak{a} \text{ ideal of } \mathcal{O}_K \mid \text{ for any prime ideal } \mathfrak{p} \mid \mathfrak{a} \text{ holds } \mathcal{N}(\mathfrak{p}) \leq B\}$$

Algorithm 7: Sampling of $\beta \in \mathfrak{b}$ such that $\beta \equiv \tau$ modulo $\mathfrak{m}$

Require:

- A modulus $\mathfrak{m} \subseteq \mathcal{O}_K$.
- An ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ coprime with $\mathfrak{m}$,
- An element $\tau \in \mathcal{O}_K$ coprime with $\mathfrak{m}$,
- An error parameter $\varepsilon > 0$.

Ensure: An element $\beta \in \mathfrak{b}$ such that

- $\beta \equiv \tau$ modulo $\mathfrak{m}$,
- $|\mathcal{N}(\beta)| \leq \mathcal{N}(\mathfrak{b}) \cdot B^N \cdot r^n$, where $r = 4 \cdot 2^n \cdot n^{3/2} \cdot |\Delta_K|^{\frac{3}{2n}} \cdot \mathcal{N}(\mathfrak{m})^{\frac{1}{n}}$, where $B = \widetilde{O}\Big(n^4[\log\log(1/\varepsilon)]^2 + n^2[\log(|\Delta_K|\mathcal{N}(\mathfrak{m}))]^2\Big)$ and $N = \lfloor 8n + \log\mathcal{N}(\mathfrak{m}) + \log|\Delta_K| + 2\log(1/\varepsilon)\rfloor$ as in Theorem 6.3.

1: Multiply $\mathfrak{b}$ by N random prime ideals coprime with $\mathfrak{m}$ and that have a norm bounded by B, obtaining $\tilde{\mathfrak{b}} = \mathfrak{b} \cdot \prod_j \mathfrak{p}_j$.
2: Sample a Gaussian distortion $(x_\sigma)_\sigma \in H \subseteq \log K_{\mathbb{R}}$ with parameter $s = 1/n^2$ and define the $(e^{x_\sigma})_\sigma$-distorted box $\tilde{\mathcal{B}} = (e^{x_\sigma} \cdot r \cdot \mathcal{N}(\tilde{\mathfrak{b}})^{1/n})_\sigma \mathcal{B}_\infty$.
3: Compute $\tilde{\tau} \in \tilde{\mathfrak{b}}$ such that $\tilde{\tau} \equiv \tau$ modulo $\mathfrak{m}$.
4: Sample an element $\beta \in (\tilde{\mathfrak{b}}\mathfrak{m} + \tilde{\tau}) \cap \tilde{\mathcal{B}} = \tilde{\mathfrak{b}} \cap (\mathfrak{m} + \tau) \cap \tilde{\mathcal{B}}$ uniformly random following the algorithm from Proposition 6.18.
5: **return** β.

Theorem 6.21 (ERH)**.** *Let $\mathcal{S}$ be any set of integral ideals, let $\mathfrak{m} \subseteq \mathcal{O}_K$ be any ideal modulus, let $\mathfrak{b} \subseteq \mathcal{O}_K$ be an integral ideal coprime with $\mathfrak{m}$ and let $\tau \in (\mathcal{O}_K/\mathfrak{m})^*$ be any invertible element modulo $\mathfrak{m}$. Let, furthermore, $r \geq 4 \cdot 2^n \cdot n^{3/2} \cdot |\Delta_K|^{\frac{3}{2n}} \cdot \mathcal{N}(\mathfrak{m})^{\frac{1}{n}}$ and let $\varepsilon > 0$ be an error parameter. Then, assuming the Extended Riemann Hypothesis, Algorithm 7 outputs in time $T = \mathsf{poly}(\log|\Delta_K|, \mathrm{size}(\mathcal{N}(\mathfrak{b})), \log(1/\varepsilon), \log(\mathcal{N}(\mathfrak{m})))$ an element $\beta \in \mathfrak{b}$ such that*

- $(\beta)/\mathfrak{b} \in (\mathcal{S} \cdot \mathcal{S}_B) \cap \mathcal{I}_K^{\mathfrak{m}}$,
- $\beta \equiv \tau \ mod\ \mathfrak{m}$

with probability at least $\frac{1}{3}\delta_{\mathcal{S}}[r^n] - \varepsilon$.

Here, $B = \widetilde{O}\Big(n^2 \cdot \big[n^2 \cdot (\log\log(1/\varepsilon))^2 + (\log(|\Delta_K|\mathcal{N}(\mathfrak{m})))^2\big]\Big)$.

Proof. We split the proof into two parts. We start with the proof of correctness and the success probability and finish with the proof of the polynomial running time.

(Correctness and success probability). By Lemma 6.22, which we will treat later, the ideal-element pair $((\beta)/\tilde{\mathfrak{b}}, \beta) \in \mathcal{I}_K^{\mathfrak{m}} \times \mathcal{O}_K$ from Algorithm 7 is distributed as $((\alpha)\operatorname{Exp}(-\mathbf{a}), \alpha\operatorname{Exp}(-\mathbf{a}_\infty))$ with $\mathbf{a} \leftarrow \mathcal{W} = \mathcal{W}(N, B, s) + d^0(\mathfrak{b})$ and $\alpha \leftarrow \operatorname{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ uniformly. Here $\mathcal{W} = \mathcal{W}(N, B, s) + d^0(\mathfrak{b})$ is the random walk distribution starting on the point $d^0(\mathfrak{b}) \in \operatorname{Div}_{K^{\mathfrak{m}}}^0$ (see Definition 4.1).

For the random walk distribution $\mathcal{W} = \mathcal{W}(N, B, s) + d^0(\mathfrak{b})$ on $\operatorname{Div}_{K^{\mathfrak{m}}}^0$ with these parameters holds that $[\mathcal{W}]$ on $\operatorname{Pic}_{K^{\mathfrak{m}}}^0$ is ε-close to uniform in the total variation distance. So, allowing an error of ε we may as well assume that $\mathbf{a}$ instead comes from a distribution $\mathcal{D}$ on $\operatorname{Div}_{K^{\mathfrak{m}}}^0$ that satisfies $[\mathcal{D}] = \mathcal{U}(\operatorname{Pic}_{K^{\mathfrak{m}}}^0)$ (see Lemma 6.23).

By applying Theorem 6.9, one then obtains that the expected probability (over the randomness of $\mathbf{a} \in \operatorname{Div}_{K^{\mathfrak{m}}}^0$) that $(\beta)/\tilde{\mathfrak{b}} = (\alpha)\operatorname{Exp}(-\mathbf{a}) \in \mathcal{S} \cap \mathcal{I}_K^{\mathfrak{m}}$ given that $\beta = \alpha\operatorname{Exp}(-\mathbf{a}_\infty) \equiv \tau \bmod \mathfrak{m}$ is at least $\frac{1}{3}\delta_{\mathcal{S}}[r^n] - 2^{-n}$. From the fact that $\tilde{\mathfrak{b}} = \mathfrak{b} \cdot \prod_j \mathfrak{p}_j$ with $\mathfrak{p}_j \nmid \mathfrak{m}$ and $\mathcal{N}(\mathfrak{p}_j) \leq B$, we have that $(\beta)/\mathfrak{b} \in (\mathcal{S} \cdot \mathcal{S}_B) \cap \mathcal{I}_K^{\mathfrak{m}}$ in that case, and the result follows.

(Running time). Note that $\log B$ and N are $\mathsf{poly}(\log|\Delta_K|, \operatorname{size}(\mathcal{N}(\mathfrak{b})), \log(1/\varepsilon), \log(\mathcal{N}(\mathfrak{m})))$, so any complexity polynomially involving $\log B$ and N must be polynomial in the size of the input as well. In the following complexity analysis, any complexity that is within $\mathsf{poly}(\log|\Delta_K|, \operatorname{size}(\mathcal{N}(\mathfrak{b})), \log(1/\varepsilon), \log(\mathcal{N}(\mathfrak{m})))$ we will call 'polynomial in the size of the input'.

For the running time, we go through steps 1 to 4 of Algorithm 7. Step 1 involves the sampling of N primes, which, by Lemma 2.14 takes $O(N \cdot n^2 \log^2 B)$ time, clearly polynomial in the size of the input; the fact that

the primes need to be coprime with $\mathfrak{m}$ does not give a significant overhead[2]. Multiplication of two ideals can be done by LLL-reducing the $n^2 \times n$ matrix involving all products of the $\mathbb{Z}$-generators of the respective ideals, taking time at most $\tilde{O}(n^{8+\eta}\log(M)^{1+\eta})$ [NS16] for any $\eta > 0$, where M is the maximum entry of the matrix involved[3]. This multiplication is done with N ideals, which means that the total time of this ideal multiplication is polynomial in the size of the input. An alternative way to see this is by using the two-element representation of ideals (e.g., [CS08, §4.7]).

Step 2 requires to sample a Gaussian in $H = \operatorname{Log} K_{\mathbb{R}}^0$, which can be done by inverse transform sampling, without a significant running time. The estimation of the time required for sampling in the box $(e^{x_\sigma} \cdot r \cdot \mathcal{N}(\tilde{\mathfrak{b}})^{1/n})_\sigma \mathcal{B}_\infty$ is deferred to step 4.

In step 3 one only needs to compute $\beta \in \tilde{\mathfrak{b}}$ and $\mu \in \mathfrak{m}$ such that $\beta + \mu = 1$. In that case $\tilde{\tau} = \beta\tau$ suffices. Such a pair $(\beta, \mu) \in \tilde{\mathfrak{b}} \times \mathfrak{m}$ can be found by applying the Hermite normal form to the concatenated basis matrices of $\tilde{\mathfrak{b}}$ and $\mathfrak{m}$ [Coh99, Prop. 1.3.1]. This requires $\tilde{O}(n^5 \log(M)^2)$ time [SL96], where M is the maximum entry occurring in the basis matrices.

Step 4 requires the sampling-in-a-box algorithm described in Proposition 6.18 which requires $O(n^6 \log(|\Delta_K|\mathcal{N}(\mathfrak{m}\tilde{\mathfrak{b}}))^3) = O(n^6 \log(|\Delta_K|\mathcal{N}(\mathfrak{m})B^N)^3)$ time.

Clearly all steps require time at most polynomial in the size of the input, which proves the time complexity claim. □

Above proof needs the results of Lemma 6.22 and Lemma 6.23. The first proves the fact that Algorithm 7 mimics a random walk, and the second shows that the random walk distribution on $\operatorname{Div}_{K^{\mathfrak{m}}}^0$ is close to a distribution $\mathcal{D}$ for which $[\mathcal{D}]$ is uniform on $\operatorname{Pic}_{K^{\mathfrak{m}}}^0$. After these two lemmas, the proof is completed.

[2] In the sampling procedure in Lemma 2.14, the first step is sampling a random integer p in $[0, B]$. In this particular step one can avoid primes dividing $\mathfrak{m}$ by simply compute the greatest common divisor of p and $\mathcal{N}(\mathfrak{m})$. This only gives a non-significant overhead compared to the full algorithm in Lemma 2.14.

[3] This time estimate is from Neumaier and Stehlé [NS16], instantiated with $\beta = \log \max_i \|\mathbf{b}_i\| \leq \log(nM)$ and lattice dimension n^2.

Lemma 6.22 (Algorithm 7 mimicks a random walk)**.** *Let $\mathfrak{m} \subseteq \mathcal{O}_K$ a modulus, let N, B, s and r as in Algorithm 7 and let $\mathcal{W} = \mathcal{W}(N, B, s)$ be the random walk distribution on $\mathrm{Div}^0_{K^\mathfrak{m}}$ (see Definition 4.1). Let $\mathcal{W}_r$ be the distribution on $K_\mathbb{R} \times \mathrm{Div}^0_{K^\mathfrak{m}}$ obtained by sampling $\mathbf{a} \leftarrow \mathcal{W}(N, B, s) + d^0(\mathfrak{b})$ and subsequently sampling $\alpha \in \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ uniformly.*

Then the pair $((\beta)/\tilde{\mathfrak{b}}, \beta) \in \mathcal{I}_K^\mathfrak{m} \times \mathcal{O}_K$ obtained by running Algorithm 7 follows the exact same distribution as $((\alpha)\,\mathrm{Exp}(-\mathbf{a}), \alpha\,\mathrm{Exp}(-\mathbf{a}_\infty))$ with $(\alpha, \mathbf{a}) \leftarrow \mathcal{W}_r$.

Proof. The difference in the sampling procedure consists of where the disturbance of the 'infinite places' happens. In the case of the random walk, the disturbance happens on the the divisor, whereas in Algorithm 7 the disturbance happens on the box to be sampled in. We will show that this does not matter for the end distribution.

Both the distribution $\mathcal{W}$ and Algorithm 7 involve the following two random processes: picking N uniformly random primes from

$$\{\mathfrak{p} \in \mathcal{I}_K^\mathfrak{m} \text{ prime } \mid \mathcal{N}(\mathfrak{p}) \leq B\}$$

and sampling a Gaussian $(x_\sigma)_\sigma \in H$; both with the exact same parameters. Without loss of generality, we can therefore focus on one fixed sample $\{\mathfrak{p}_j \mid 1 \leq j \leq N\}$ of primes and one fixed vector $(x_\sigma)_\sigma \in H$.

This means that we consider the fixed $\mathbf{a} = \sum_{j=1}^N (\!|\mathfrak{p}_j|\!) + \sum_\nu x_{\sigma_\nu} (\!|\nu|\!) + d^0(\mathfrak{b}) \in \mathrm{Div}^0_{K^\mathfrak{m}}$ for the procedure involving $\mathcal{W}_r$ and the fixed ideal $\tilde{\mathfrak{b}} = \mathfrak{b}\prod_{j=1}^N \mathfrak{p}_j$ and distortion $(e^{-x_\sigma})_\sigma$ for the procedure involving Algorithm 7. Then, writing $\tilde{b} = \mathcal{N}(\tilde{\mathfrak{b}})^{1/n}$,

$$\mathrm{Exp}(\mathbf{a}) = (e^{x_\sigma})_\sigma \tilde{\mathfrak{b}}/\tilde{b}, \quad \mathrm{Exp}(\mathbf{a}_\mathrm{f}) = \tilde{\mathfrak{b}} \quad \text{and} \quad \mathrm{Exp}(\mathbf{a}_\infty) = (e^{x_\sigma})_\sigma/\tilde{b}$$

Thus, $\alpha\,\mathrm{Exp}(-\mathbf{a}_\infty)$ for uniformly random $\alpha \in \mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty$ is distributed as

$$\begin{aligned}\mathrm{Exp}(-\mathbf{a}_\infty) \cdot \mathcal{U}(\,\mathrm{Exp}(\mathbf{a}) \cap r\mathcal{B}_\infty) &= (e^{-x_\sigma})_\sigma \cdot \tilde{b} \cdot \mathcal{U}\Big((e^{x_\sigma})_\sigma \tilde{\mathfrak{b}}/\tilde{b} \cap r\mathcal{B}_\infty\Big) \\ &= \mathcal{U}\Big(\tilde{\mathfrak{b}} \cap (e^{-x_\sigma})_\sigma \cdot \tilde{b} \cdot r\mathcal{B}_\infty\Big)\end{aligned}$$

which is exactly the distribution of $\beta \in \tilde{\mathfrak{b}}$ in Algorithm 7 for fixed $\tilde{\mathfrak{b}}$. It follows that $(\alpha)\operatorname{Exp}(-\mathbf{a}) = (\alpha)\operatorname{Exp}(-\mathbf{a}_\infty)\operatorname{Exp}(-\mathbf{a}_\mathrm{f}) = (\alpha)\operatorname{Exp}(-\mathbf{a}_\infty)/\tilde{\mathfrak{b}}$ is distributed as $(\beta)/\mathfrak{b}$, which finishes the proof. □

Lemma 6.23 (Lifting property of distributions)**.** *Suppose that a distribution* $\mathcal{D} : \mathrm{Div}^0_{K^\mathfrak{m}} \to \mathbb{R}$ *satisfies* $\|[\mathcal{D}] - \mathcal{U}(\mathrm{Pic}^0_{K^\mathfrak{m}})\|_1 < \varepsilon$ *(see Definition 6.8). Then there exists a 'lifted' distribution* $\mathcal{D}_U : \mathrm{Div}^0_K \to \mathbb{R}^+$ *such that* $[\mathcal{D}_U] = \mathcal{U}(\mathrm{Pic}^0_{K^\mathfrak{m}})$ *and* $\|\mathcal{D} - \mathcal{D}_U\|_1 < \varepsilon$*.*

Proof. Put

$$\mathcal{D}_U(\mathbf{a}) = \begin{cases} \frac{1}{\mathrm{Vol}(\mathrm{Pic}^0_{K^\mathfrak{m}})} \cdot \frac{\mathcal{D}(\mathbf{a})}{[\mathcal{D}]([\mathbf{a}])} & \text{if } [\mathcal{D}]([\mathbf{a}]) \neq 0 \\ u & \text{otherwise} \end{cases},$$

for some $u : \mathrm{Div}^0_{K^\mathfrak{m}} \to \mathbb{R}^+$ that satisfies $[u] = \frac{1}{\mathrm{Vol}(\mathrm{Pic}^0_{K^\mathfrak{m}})}$. Then, one can check that $[\mathcal{D}_U] = \frac{1}{\mathrm{Vol}(\mathrm{Pic}^0_{K^\mathfrak{m}})}$ is uniform on $\mathrm{Pic}^0_{K^\mathfrak{m}}$. Furthermore, writing F for a fundamental domain in $\mathrm{Div}^0_{K^\mathfrak{m}}$ for $\mathrm{Pic}^0_{K^\mathfrak{m}}$, we have

$$\begin{aligned} \|\mathcal{D} - \mathcal{D}_U\|_1 &= \int_{\mathbf{a}\in F} \int_{\alpha \in K^*/\mu_K} |\mathcal{D}(\mathbf{a} + (\!|\alpha|\!)) - \mathcal{D}_U(\mathbf{a} + (\!|\alpha|\!))| d\alpha d\mathbf{a} \\ &= \int_{[\mathbf{a}]\in \mathrm{Pic}^0_{K^\mathfrak{m}}} \left| [\mathcal{D}]([\mathbf{a}]) - \frac{1}{\mathrm{Vol}(\mathrm{Pic}^0_{K^\mathfrak{m}})} \right| d([\mathbf{a}]) \\ &= \|[\mathcal{D}] - \mathcal{U}(\mathrm{Pic}^0_{K^\mathfrak{m}})\|_1 \leq \varepsilon. \end{aligned}$$

The first equation holds by definition, the second equation by the fact that the sign of $(\mathcal{D}(\mathbf{a} + (\!|\alpha|\!)) - \mathcal{D}_U(\mathbf{a} + (\!|\alpha|\!)))$ depends per construction solely on the coset $[\mathbf{a}]$. □