Counting Invertible Matrices and Uniform Distribution

Christian GJ Roettger
Iowa State University
400 Carver Hall, 50011 Ames, IA

January 19, 2004

Abstract

Consider the group $SL(2)$ over the ring of algebraic integers of a number field K. Define the height of a matrix to be the maximum over all the conjugates of its entries in absolute value. Let $N(t)$ be the number of matrices in $SL(2)$ with height bounded by t. We determine the asymptotic behaviour of N(t) as t goes to infinity including an error term,

$$N(t) = Ct^{2n} + O(t^{2n-\eta})$$

with n being the degree of K. The constant C involves the discriminant of K, an integral depending only on the signature of K and the value of the Dedekind zeta function of K at s=2. We use the theory of uniform distribution and discrepancy to obtain the error term. Then we will make connections to counting problems concerning units in certain integral group rings and integral normal bases.

1 Introduction and Background

Let K be a number field of degree n over $\mathbb{Q}$. For $a \in K$ define the *height of a* by

$$\mathrm{ht}(a) := \max_{\sigma} |\sigma(a)|,$$

where σ runs over all n complex embeddings of K. For any matrix A with entries in K, let $\mathrm{ht}(A)$ be the maximum of the heights of its entries. It is an old problem to estimate the number of matrices

$$N(t) := \{A \in \mathrm{SL}_m(\mathbf{O}_K) : \ \mathrm{ht}(A) \leq t\}$$

as t tends to infinity. We also ask the same question with $\mathrm{GL}_m(\mathbf{O}_K)$ in place of $\mathrm{SL}_m(\mathbf{O}_K)$.
For $m = 2$ and $K = \mathbb{Q}$, this is known as the 'hyperbolic circle problem' because it has a beautiful interpretation in hyperbolic geometry, see Beardon (1983). The best known error term in this case is $O(t^{2/3+\varepsilon})$, due to A. Selberg, see Lax and Phillips (1982).
Duke/Rudnick/Sarnak have proved a very general theorem (see Duke et al. (1993)) which, as an 'application', answers the question in case $K = \mathbb{Q}$ for arbitrary m.

Theorem 1 (Duke/Rudnick/Sarnak)
Write $\|g\|_2$ for the usual 2-norm of a matrix with real entries. For all $m \geq 1$,

$$\#\{g \in \mathrm{SL}_m(\mathbb{Z}) : \ \|g\|_2 \leq t\} \sim c_m t^{m^2-m} \tag{1}$$

where

$$c_m = \frac{\pi^{m^2/2}}{\Gamma\left(\frac{m^2-m+2}{2}\right)\Gamma\left(\frac{m}{2}\right)\zeta(2)\cdots\zeta(m)}.$$

The following theorem is the main result of this paper, valid for arbitrary number fields, but only in case $m = 2$. It is a strenghtening of an asymptotic result in Roettger (2000). This thesis is available on-line at

http://www.mth.uea.ac.uk/admissions/graduate/phds.html

Theorem 2
Let $m = 2$. For any positive $\eta < 1/(20n - 5)$,

$$N(t) = 4E_K D_K t^{2n} + O(t^{2n-\eta}) \tag{2}$$

where D_K depends only on the signature of K and

$$E_K := \frac{1}{\zeta_K(2)|\mathrm{disc}(K)|^{3/2}}. \tag{3}$$

Here, ζ_K denotes the *Dedekind zeta function of* K and $\mathrm{disc}(K)$ the *discriminant of* K.

Remark 3

1. Theorem 2 holds for arbitrary cosets of $\mathrm{SL}_2(\mathbf{O}_K)$ in $\mathrm{GL}_2(\mathbf{O}_K)$ with the same limit and error term.

2. The constant D_K is given by

$$D_K = 2^{3s_K} \int_{\mathbb{B}} \mathrm{g}(x)\, dx, \tag{4}$$

where s_K, $\mathbb{B}$ and the function g are defined as follows. Let K have r_K real and $2s_K$ complex embeddings into $\mathbb{C}$. Let $V = \mathbb{R}^{r_K} \oplus \mathbb{C}^{s_K}$ and define for $x = (x_i) \in V$ the 'height' $\|x\|_\infty = \max |x_i|$. Now $\mathbb{B}$ is the unit ball corresponding to $\|.\|_\infty$ in V, and

$$\begin{aligned} \mathrm{g}(x) \quad := \quad & 4^{r_K} \pi^{2s_K} \|x\|_\infty^n \prod_{i=1}^{r_K} \left(1 + \log\left(\frac{\|x\|_\infty}{|x_i|}\right)\right) \\ & \prod_{i=r_K+1}^{r_K+s_K} \left(\frac{\|x\|_\infty}{|x_i|} + 2\log\left(\frac{\|x\|_\infty}{|x_i|}\right)\right) \end{aligned} \tag{5}$$

for those $x \in V$ such that all coordinates x_i are nonzero. Note that g has singularities!

3. Note the appearance of the zeta function in the denominator in both Theorems 1 and 2. This is not unexpected, since $\zeta(2)...\zeta(m)$ is the volume of the quotient space $\mathrm{SL}_m(\mathbb{R})/\mathrm{SL}_m(\mathbb{Z})$ for all $m \geq 2$, see Siegel (1989).

2 Notation and Basic Definitions

The embeddings $\sigma : K \to \mathbb{C}$ can be grouped together to give an one-to-one algebra homomorphism $\Sigma : K \to V$,

$$\Sigma(a) := (\sigma_1(a), \ldots, \sigma_k(a))$$

Here, we have ordered the embeddings so that σ_i is real for $1 \leq i \leq r_K$ and complex for $r_K < i \leq r_K + s_K$. We write $k := r_K + s_K$. In the rest of this paper, we will always identify K and $\Sigma(K)$, that is we will consider K as a subset of V. Thus, we may say that K is dense in V and $\mathbf{O}_K$ is a full lattice in V. All the usual maps $N_{K/\mathbb{Q}}$, $\mathrm{Tr}_{K/\mathbb{Q}}$ and indeed σ_i have unique continuous extensions from K to V, which we will denote by the same name as the original. We also extend the height function to V. When we want to emphasize that this extension is a Euclidean norm on V, we will denote it by $\|x\|_\infty$. The height of a vector is defined as the maximum of the heights of its entries. We use the Vinogradov notation $f(t) \ll g(t)$ and $f(t) = O(g(t))$ both in the sense that there is an implicit constant C such that $f(t) \leq Cg(t)$ for all $t > 0$.

We will need the notion of covolume. Given a lattice L in $\mathbb{R}^s$, the *covolume* $\mathrm{cov}(L)$ is the volume of a fundamental parallelotope F for L. As an example, the lattice $\mathbf{O}_K$ in V has covolume

$$\mathrm{cov}(\mathbf{O}_K) = \frac{|\mathrm{disc}(K)|^{1/2}}{2^{s_K}} \tag{6}$$

(for a proof, see a textbook like eg Samuel (1970)). We will always use a, b for elements of $\mathbf{O}_K$ and u, v, x, y, z for elements of V. A matrix $A \in \mathrm{SL}_2(\mathbf{O}_K)$ is always understood to have entries a, b, c, d.

3 Strategy of the Proof

We will emphasize the role of uniform distribution and discrepancy in the proof, since this is the part which goes beyond the thesis Roettger (2000). These concepts are used in sections 5 and 6, respectively, to derive estimates which are needed for the first counting method as outlined in subsection 3.1. Section 4 contains the results about lattice point counting needed for both counting methods, and section 7 is about an estimate of a crucial volume.

3.1 Counting Matrices With One Fixed Entry

Fix some nonzero $a \in \mathbf{O}_K$ and count the set of matrices in $\mathrm{SL}_2(\mathbf{O}_K)$

$$M_a := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ \mathrm{ht}(b,c,d) \le \mathrm{ht}(a) \right\} \tag{7}$$

which have this fixed entry a in top left position. Writing

$$Q_a \ := \ \left\{ (b,c) : \ \begin{array}{l} -bc \equiv 1(a), \\ \mathrm{ht}(b,c,\frac{1+bc}{a}) \le \mathrm{ht}(a) \end{array} \right\},$$

we have $\#M_a = \#Q_a$. Rather than summing $\#Q_a$, we will deal with

$$P_a := \{(b,c) : \ bc \equiv 1(a), \ \mathrm{ht}(b,c,bc/a) \le \mathrm{ht}(a)\}.$$

We will show in Proposition 12 that the difference between $\#Q_a$ and $\#P_a$ can be estimated by

$$\sum_{\mathrm{ht}(a) \le t} |\#Q_a - \#P_a| = O(t^{n-\eta}) \tag{8}$$

and so we can deal with the sets P_a from now on. Rewrite the conditions defining P_a geometrically. Define for all units $x \in V$ a subset H_x of V^2 by

$$H_x := \left\{ (y,z) : \ y, z, yz \in \frac{\mathrm{ht}(x)}{x} \mathbb{B} \right\} \tag{9}$$

There is some sloppiness in the notation. Real numbers like $\mathrm{ht}(x)$ act by multiplication on V in the obvious way, whereas multiplication by x^{-1} means multiplication by different factors in each coordinate, namely by x_i^{-1}. Note that all $0 \neq a \in K$ are units of V, so H_a is defined. Using H_a, we can write

$$P_a = \left\{ (b,c) : \ bc \equiv 1(a), \ \left(\frac{b}{a}, \frac{c}{a}\right) \in H_a \right\}.$$

The points $\left(\frac{b}{a}, \frac{c}{a}\right)$ are spread around H_a irregularly, but 'on average' uniformly. The concept of *uniform distribution* makes this precise. Define for every nonzero $a \in \mathbf{O}_K$ a *sampling functional* m_a as follows.

$$m_a(f) := \frac{\mathrm{cov}(\mathbf{O}_K)^2}{\phi(a)} \sum_{bc \equiv 1(a)} f\left(\frac{b}{a}, \frac{c}{a}\right) \tag{10}$$

The summation is over all $b, c \in \mathbf{O}_K$ such that $bc \equiv 1 \pmod{a}$. This functional is defined for all functions with compact support in V^2. Obviously,

$$\#P_a = \frac{\phi(a)}{\mathrm{cov}(\mathbf{O}_K)^2} m_a(\mathbf{1}_{H_a}) \tag{11}$$

We will prove in Theorem 17 that for all Riemann-integrable sets H in V^2

$$\lim_{\phi(a) \to \infty} m_a(\mathbf{1}_H) = \mathrm{Vol}(H) \tag{12}$$

where $\lim_{\phi(a)}$ means a limit for all sequences of elements $a \in \mathbf{O}_K$ such that $\phi(a)$ tends to infinity. To prove Theorem 17, we use the Weyl criterion. This leads us to estimating 'Fourier coefficients' which turn out to be very natural generalizations of the classical Kloosterman sums. See section 5 for more details. Equation (12) seems to suggest

$$m_a(\mathbf{1}_{H\,a}) \approx \mathrm{Vol}(H_a) \tag{13}$$

However, the 'target' H in (12) is supposed to be fixed, independent of a, which is the parameter of the sampling functional. We aim for a 'moving target' H_a, and so we need an estimate for the error in the approximation (13). The classical theory of discrepancy comes into play here. Writing $r(a)$ for the diameter of H_a and using (11), we get an error bound from Theorem 20.

$$\left| \#P_a - \frac{\phi(a)}{\mathrm{cov}(\mathbf{O}_K)} \mathrm{Vol}(H_a) \right| \ll \phi(a) r(a)^{2n-1} |N_{K/\mathbb{Q}}(a)|^{-\delta} \tag{14}$$

for the error in equation (13), valid for all $\delta < 1/(5n)$. This bound is too crude to be summed over all a of height less than t. However, if we choose a small exponent e and consider only those elements a such that $|N_{K/\mathbb{Q}}(a)| \geq \mathrm{ht}(a)^{n-e}$, the strategy still works. For these elements, $\min_\sigma |\sigma(a)| \geq \mathrm{ht}(a)^{1-e}$ and

$$r(a) = \frac{2\mathrm{ht}(a)}{\min_\sigma |\sigma(a)|} \leq 2\mathrm{ht}(a)^e$$

So we define

$$K_e(t) := \{x \in V : \ |N_{K/\mathbb{Q}}(x)| \geq \mathrm{ht}(x)^{n-e}, \ \mathrm{ht}(x) \leq t\} \tag{15}$$

We want to sum the error bound (14) over all $0 \neq a \in K_e(t)$. Replacing $\phi(a)$ by $|N_{K/\mathbb{Q}}(a)|$, we have for the sum over these 'nice' elements a

$$\sum_a |N_{K/\mathbb{Q}}(a)|^{1-\delta} \mathrm{ht}(a)^{(2n-1)e} = O(t^{2n-n\delta+(2n-1)e}). \tag{16}$$

In Theorem 8, we will prove for all $\gamma < 1/2$

$$\frac{1}{\mathrm{cov}(\mathbf{O}_K)^2} \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a) = C_K t^{2n} + O(t^{2n-\gamma}) \tag{17}$$

where

$$C_K := \frac{2^{3s_K}}{\zeta_K(2)|\mathrm{disc}(K)|^{3/2}} \int_{\mathbb{B}} |N_{K/\mathbb{Q}}(x)|\mathrm{Vol}(H_x)\, dx \tag{18}$$

It is not hard to calculate $|N_{K/\mathbb{Q}}(x)|\mathrm{Vol}(H_x) = g(x)$ with the function g defined in (5). Therefore $C_K = D_K E_K$ with the constants D_K, E_K defined in (4) and (3). Together with the error estimate (16), this shows

$$\sum_{a \in K_e(t)} \#M_a = C_K t^{2n} + O(t^{2n-\gamma} + t^{2n-n\delta+(2n-1)e}) \tag{19}$$

The factor 4 in equation (2) comes from the four possibilities for the position of the maximal entry of a matrix. By Proposition 13, the number of matrices where two or more entries have maximal height is $O(t^{2n-\eta})$ and goes into the error term.
Now we have to deal with the elements $a \notin K_e(t)$ such that $|N_{K/\mathbb{Q}}(a)|$ is very small in comparison to $\mathrm{ht}(a)$, eg units of $\mathbf{O}_K$. We will employ an entirely different counting strategy.

3.2 Counting Matrices With Two Fixed Entries

Given $a, b \in \mathbf{O}_K$ such that $\mathrm{ht}(b) \leq \mathrm{ht}(a)$ and $a\mathbf{O}_K + b\mathbf{O}_K = \mathbf{O}_K$, let

$$R(a,b) := \{(c,d) \in \mathbf{O}_K^2 : \ ad - bc = 1, \ \mathrm{ht}(c,d) \leq \mathrm{ht}(a,b)\} \tag{20}$$

If we sum $\#R(a,b)$ over all b such that $a\mathbf{O}_K + b\mathbf{O}_K = \mathbf{O}_K$ and $\mathrm{ht}(b) \leq \mathrm{ht}(a)$, we get $\sum_b \#R(a,b) = \#M_a$, with the set of matrices M_a defined in (7). This is the connection between the two counting strategies. Consider the lattice $(a,b)\mathbf{O}_K$ of rank n inside V^2. Let $\mathrm{cov}(a,b)$ be its covolume. We will prove in Proposition 5 that

$$\#R(a,b) = O\left(\frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)}\right) \tag{21}$$

with an implicit constant independent of a and b. From Proposition 4 follows that there exists a constant factor C so that $\mathrm{cov}(a,b) \leq C\mathrm{ht}(a,b)^n$ for all a, b.

For convenience, suppose $\mathrm{cov}(a,b) \leq \mathrm{ht}(a,b)^n$ for all a, b - one could also redefine $\mathrm{ht}(a,b)$ or $\mathrm{cov}(a,b)$, but a constant factor never affects the magnitude of our error bounds. Define for positive integers μ, ν

$$\begin{aligned} K_\mu(t) &:= \left\{(x,y) \in V^2 : \ \frac{1}{\mu+1} \leq \frac{\mathrm{cov}(x,y)}{\mathrm{ht}(x,y)^n} \leq \frac{1}{\mu}, \ \mathrm{ht}(y) \leq \mathrm{ht}(x) \leq t\right\} \\ K_{\mu\nu}(t) &:= \left\{(x,y) \in K_\mu(t) : \ \frac{1}{\nu+1} \leq \frac{|N_{K/\mathbb{Q}}(x)|}{\mathrm{ht}(x)^n} \leq \frac{1}{\nu}\right\} \end{aligned} \tag{22}$$

Then we split the sum over $\#R(a,b)$ according to the values of $\mathrm{cov}(a,b)$ and $|N_{K/\mathbb{Q}}(a)|$.

$$\begin{aligned} \sum_{a,b} \#R(a,b) &= S_1(t) + S_2(t) + S_3(t) \qquad \text{with} \\ S_1(t) &= \sum_{\mu \leq t^e} \sum_{\nu \leq t^e} \sum_{(a,b) \in K_{\mu\nu}(t)} \#R(a,b) \\ S_2(t) &= \sum_{\mu \leq t^e} \sum_{\nu > t^e}^{\infty} \sum_{(a,b) \in K_{\mu\nu}(t)} \#R(a,b) \\ S_3(t) &= \sum_{\mu > t^e} \sum_{(a,b) \in K_\mu(t)} \#R(a,b) \end{aligned} \tag{23}$$

We will show that $S_1(t)$ has the stated asymptotic behavior and that $S_2(t), S_3(t)$ go into the error term.
For $S_2(t)$, use (21) and Theorem 6. This says

$$S_2(t) \ll \sum_{\mu \leq t^e} \mu \left[\mathrm{Vol}_{2n}(K_{\mu\nu}(1)) t^{2n} + O(t^{2n-1/2})\right]$$

with an implicit constant independent of μ. Therefore the sum over the terms $O(t^{2n-1})$ can be bounded by summing t^{2n-1+e} over $\mu \leq t^e$, giving a term of size $O(t^{2n-1+2e})$. For the main term of $S_2(t)$, we want to use Theorem 21 with $\varepsilon = 1/\mu$, $\varepsilon = 1/(\mu+1)$ and $\delta = 1/\nu$. Note that this covers all the summands in the summation over ν. For the definition of $K_{\mu\nu}(t)$, we used the height function and for the definition of $K(\varepsilon, \delta, \underline{e})$ in Theorem 21, a different Euclidean norm. Since these are bounded in terms of each other, there is no change in the order of magnitude of the given bounds. Theorem 21 implies

$$\mathrm{Vol}_{2n}(K_{\mu\nu}(1)) \ll \left(\frac{1}{\mu} - \frac{1}{\mu+1}\right) \frac{1}{\nu} \log(\nu)^m$$

and so the whole sum $S_2(t)$ is bounded by

$$S_2(t) \ll O(t^{2n-1+2e}) + \sum_{\mu \leq t^e} \frac{1}{\mu} t^{2n-e} \log(t)^m = O(t^{2n-1+2e} + t^{2n-e} \log(t)^{m+1})$$

For $S_3(t)$, use first the estimate (21) and then Proposition 11 to count the summands. This gives

$$S_3(t) \ll \sum_{\mu > t^e} \sum_{(a,b) \in K_\mu(t)} \frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)} = O(t^{2n-e/2} \log^{k-1}(t)) \tag{24}$$

The summand $S_1(t)$ agrees with the sum in equation (19) except that it does not run over any pairs (a,b) in $K_\mu(t)$ for $\mu > t^e$. These exceptions went into $S_3(t)$, and therefore their contribution can be subsumed in the error term. The exponent e can be chosen to be any number less than $2/(20n-5)$ to give an error term as stated in Theorem 2.

4 Counting Lattice Points

4.1 Homogeneous Counting Problems

Proposition 4
Let $\mathrm{cov}(a,b)$ be the covolume of the lattice $L = (a,b)\mathbf{O}_K$ as before. Then

$$\mathrm{cov}(a,b) = \mathrm{cov}(\mathbf{O}_K) \prod_{i=1}^{k} (|\sigma_i(a)|^2 + |\sigma_i(b)|^2)^{e_i/2}$$

and there exists a fundamental domain F for L with diameter less than $C\mathrm{cov}(a,b)^{1/n}$ for some constant C independent of (a,b).

Proof of Proposition 4. The evaluation of $\mathrm{cov}(a,b)$ is fairly straightforward and we omit it here. For details, see Roettger (2000). For the second assertion, start with the fact that there exists a constant $C' > 0$, independent of L, and at least one nonzero vector $v \in L$ such that $\mathrm{ht}(v) \leq C'\mathrm{cov}(a,b)^{1/n}$. This follows for example from Theorem 29 in Siegel (1989) and the commensurability of ht(.) with the maximum norm on V. By definition of L, there exists $r \in \mathbf{O}_K$ such that $v = (ar, br)$. For any fixed $\mathbb{Z}$-basis $v_1, \ldots, v_n$ of $\mathbf{O}_K$, the vectors

$$(arv_1, brv_1), \ldots, (arv_n, brv_n)$$

form a $\mathbb{Z}$-basis for the sublattice rL of L. The height of each of these vectors is $O(\mathrm{cov}(a,b)^{1/n})$. Hence they define a fundamental parallelotope for rL of diameter $O(\mathrm{cov}(a,b)^{1/n})$, and it contains at least one fundamental parallelotope for L. □

Proposition 5
Given $a, b \in \mathbf{O}_K$ such that $a\mathbf{O}_K + b\mathbf{O}_K = \mathbf{O}_K$, let $R(a,b)$ be the set of all pairs $(c,d) \in \mathbf{O}_K^2$ such that $ad - bc = 1$. Then

$$\#\{(c,d) \in R(a,b) : \ \mathrm{ht}(c,d) \leq \mathrm{ht}(a,b)\} = O\left(\frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)}\right),$$

with an implicit constant independent of a, b.

Proof of Proposition 5. Since $a\mathbf{O}_K + b\mathbf{O}_K = \mathbf{O}_K$, there exist c_0 and d_0 in $\mathbf{O}_K$ such that $ad_0 - bc_0 = 1$. It is then easy to see that

$$R(a,b) = (c_0, d_0) + (a,b)\mathbf{O}_K.$$

This is a coset of the lattice $L = (a,b)\mathbf{O}_K$ considered in Proposition 4. Let U be the subspace of V^2 spanned by L, and let $\mathbb{B}$ be the unit cube in V^2. Define the number $N(t)$ by

$$N(t) := \#\{(c,d) \in R(a,b) : \ \mathrm{ht}(c,d) \leq t\}.$$

This number can be rewritten as the number of points in L lying in $(t\mathbb{B} - (c_0,d_0) \cap U$. Since L has rank n, U is an n-dimensional subspace of V^2. It is not hard to prove that

$$\mathrm{Vol}_n((t\mathbb{B} - (c_0,d_0) \cap U) = t^n \mathrm{Vol}_n((\mathbb{B} - t^{-1}(c_0,d_0) \cap U) = O(t^n) \tag{25}$$

with an implicit constant independent of (c_0,d_0) and U, i. e. independent of a and b. Choose a fundamental domain F for L in U with $\mathrm{diam}(F) \leq C\mathrm{cov}(L)^{1/n}$. By Proposition 4, it is possible to do this with a constant C independent of (a,b). From Proposition 4, we also get

$$\mathrm{cov}(L) \leq \mathrm{cov}(\mathbf{O}_K)(\mathrm{ht}(a)^2 + \mathrm{ht}(b)^2)^{n/2},$$

and this allows us to bound $\mathrm{diam}(F)$.

$$\begin{aligned} \mathrm{diam}(F) &\leq C\mathrm{cov}(L)^{\frac{1}{n}} \leq C\mathrm{cov}(\mathbf{O}_K)^{\frac{1}{n}} \sqrt{\mathrm{ht}(a)^2 + \mathrm{ht}(b)^2} \\ &= O(\mathrm{ht}(a,b)) \end{aligned} \tag{26}$$

Now compare the number $N(t)$ to the volume of $(t\mathbb{B} - (c_0,d_0)) \cap U$. Using (25) and (26),

$$N(t)\mathrm{Vol}_n(F) \leq \mathrm{Vol}_n(((t+\mathrm{diam}(F))\mathbb{B} - (c_0,d_0)) \cap U) = O((t+\mathrm{ht}(a,b))^n). \tag{27}$$

From $\mathrm{Vol}_n(F) = \mathrm{cov}(L)$ follows $N(t) = O((t + \mathrm{ht}(a,b))^n / \mathrm{cov}(L))$, with an implicit constant independent of t, (c_0,d_0) and (a,b). Finally, put $t = \mathrm{ht}(a,b)$ to complete the proof of proposition 5. □

Note that finding a fundamental domain F of diameter bounded by $C\mathrm{cov}(L)^{1/n}$ with a uniform constant C is not possible for arbitrary families of lattices.

Theorem 6
Let $\mathbb{D}$ be a Riemann-integrable conical domain in V^2. Let $\partial\mathbb{D}$ be the boundary of $\mathbb{D}$ and $U_\varepsilon(\partial\mathbb{D})$ an ε-neighbourhood of it. Define the number $S(t)$ by

$$S(t) := \left\{(a,b) \in \mathbf{O}_K^2 : \ (a,b) \in \mathbb{D}, \ \mathrm{ht}(a,b) \leq t\right\}$$

If $\mathrm{Vol}_{2n}(U_\varepsilon(\partial\mathbb{D}) \cap \mathbb{B}^2) \leq C_1\varepsilon$ for all $\varepsilon > 0$ sufficiently small, then

$$S(t) = \frac{\mathrm{Vol}(\mathbb{D} \cap \mathbb{B}^2)}{\mathrm{cov}(\mathbf{O}_K)^2} t^{2n} + O(t^{2n-1/2})$$

with an implicit constant depending only on C_1, not on $\mathbb{D}$.

For a proof, see Roettger (2000). The shape of the main term is to be expected, the intricacy lies in getting an error term which depends only loosely on $\mathbb{D}$.

Theorem 7
For every $\varepsilon > 0$, let

$$C_{K,\varepsilon} := \frac{2^{3s_K}}{\zeta_K(2)\mathrm{cov}(\mathbf{O}_K)^3} \int_{\mathbb{B}\cap N_\varepsilon} |N_{K/\mathbb{Q}}(x)| \mathrm{Vol}(H_x)\, dx \tag{28}$$

with the set H_x as defined in (9) and

$$N_\varepsilon := \left\{ x \in V : \ |N_{K/\mathbb{Q}}(x)| \geq \varepsilon \mathrm{ht}(x)^n, \ \mathrm{ht}(x) \leq t \right\}$$

Then for all $\gamma < 1/2$

$$\frac{1}{\mathrm{cov}(\mathbf{O}_K)^2} \sum_{a \in N_\varepsilon} \phi(a) \mathrm{Vol}(H_a) = C_{K,\varepsilon} t^{2n} + O\left(t^{2n-\gamma}\right) \tag{29}$$

with an implicit constant independent of t and ε.

Sketch of proof. Use the Möbius function μ_K of K. Just as the well-known Möbius function for $\mathbb{Z}$, it satisfies

$$\phi(a) = \sum_{I|(a)} \mu_K(I) N_{K/\mathbb{Q}}(I^{-1}a)$$

Insert this into (29) and use that $N_{K/\mathbb{Q}}(.)$ is strongly multiplicative. Invert the order of summation. An analogue of Theorem 6 gives

$$\begin{aligned} \sum_{a \in I \cap N_\varepsilon} |N_{K/\mathbb{Q}}(a)| \mathrm{Vol}(H_a) &= \frac{t^{2n}}{N_{K/\mathbb{Q}}(I)\mathrm{cov}(\mathbf{O}_K)} \int_{\mathbb{B}\cap N_\varepsilon} |N_{K/\mathbb{Q}}(x)| \mathrm{Vol}(H_x) dx \\ &\quad + O(N_{K/\mathbb{Q}}(I)^{1-\eta} t^{2n-\gamma}). \end{aligned} \tag{30, 31}$$

for some $\eta > 0$. The general shape of this asymptotic behaviour is to be expected, the crucial fact is that the implicit constant can be chosen independent of I and ε. This can be proven using elementary arguments similar to and including Proposition 4. See Roettger (2000) for details. Finally, dividing (30) by $N_{K/\mathbb{Q}}I$ and summing it over all ideals I produces equation (29) and in particular the factor $1/\zeta_K(2)$. □

4.2 Non-Homogeneous Counting Problems

The goal of the subsection is to prove Propositions 8 and 11. The counting problems in the previous sections involve homogeneous functions like $|N_{K/\mathbb{Q}}|$ and $\mathrm{Vol}(H_x)$ and lattice points in conical sets. The problems in this subsection do not fit this pattern. This means that we have to employ different techniques. However, the classical geometry of numbers again provides elegant answers.

Theorem 8
Recall the set $K_e(t)$ defined in (15) and the constant C_K defined in (18). For all $0 < e < 1$ and all $\gamma < e/2$,

$$\frac{1}{\mathrm{cov}(\mathbf{O}_K)^2} \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a) = C_K t^{2n} + O(t^{2n-\gamma}) \tag{32}$$

Proof of Theorem 8. Since the implicit constant in the error term of Theorem 7 does not depend on ε, we may substitute $\varepsilon = t^{-e}$ with e as in section 3. For this value of ε, $K_e(t)$ is contained in N_ε. We may also substitute $\varepsilon = t^{-e/2}$. Suppose $x \in N_\varepsilon$ for this second value of ε. Then either $x \in K_e(t)$ or $|N_{K/\mathbb{Q}}(x)| < \mathrm{ht}(x)^{n-e}$. Together with $|N_{K/\mathbb{Q}}(x)| \geq t^{-e/2}\mathrm{ht}(x)^n$, this implies

$$\mathrm{ht}(x) < t^{1/2}$$

meaning N_ε is contained in $K_e(t)$ except for some x of small height. Compare the sum of $\phi(a)\mathrm{Vol}(H_a)$ over $K_e(t)$ with the corresponding sums over N_ε for $\varepsilon = t^{-e}$ and $\varepsilon = t^{-e/2}$. Writing $S(t,e)$ and $S(t,e/2)$ for the latter two, we can summarize

$$\begin{aligned} S(t,e) &\geq \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a) && (33)\\ S(t,e) &= C_{K,\varepsilon} t^{2n} + O(t^{2n-\gamma}) \quad \text{with } \varepsilon = t^{-e} && (34)\\ S(t,e/2) &\leq O(t^{n+e/2}) + \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a) \end{aligned}$$

The $O(t^{n+e/2})$-term in the last inequality comes from summing $\phi(a)\mathrm{Vol}(H_a)$ over those $a \in N_\varepsilon$ which are not in $K_e(t)$, using

$$\mathrm{Vol}(H_a) \leq \mathrm{Vol}\left(\frac{\mathrm{ht}(a)}{a}\mathbb{B}^2\right) = \frac{\mathrm{ht}(a)^{2n}}{(|N_{K/\mathbb{Q}}(a)|)^2}\mathrm{Vol}(\mathbb{B})^2$$

The last ingredient is

$$0 \leq C_K - C_{K,\varepsilon} \ll \varepsilon |\log^n(\varepsilon)| \tag{35}$$

This is best seen by considering $C_{K,\varepsilon}$ as a function of ε. This function is differentiable, and the derivative is the surface integral

$$\frac{d}{d\varepsilon} C_{K,\varepsilon} = \frac{2^{3s_K}}{\zeta_K(2)\mathrm{cov}(\mathbf{O}_K)^3} \int_{\partial N_\varepsilon \cap \mathbb{B}} |N_{K/\mathbb{Q}}(x)|\mathrm{Vol}(H_x)\, dS(x)$$

which is a $O(|\log^n(\varepsilon)|)$ by looking at (28) and (5). The estimates (33)-(35) together complete the proof of Theorem 8. □

Note that after establishing the inequality (35), we can be sure that C_K is actually finite, even though it is defined by an improper integral.

Lemma 9
Let K be a number field of degree n and let $0 \le \alpha < n$ be fixed. Then

$$\#\{a \in \mathbf{O}_K : \ |N_{K/\mathbb{Q}}(a)| \le t^\alpha, \ \mathrm{ht}(a) \le t\} = O(t^\alpha \log^{k-1}(t)),$$

where $k-1$ is the $\mathbb{Z}$-rank of the unit group of $\mathbf{O}_K$.

Proof. It is well known that the number of ideals I of norm $N_{K/\mathbb{Q}}(I) \le t^\alpha$ is of order $O(t^\alpha)$. For each principal ideal $I = (a)$, there are $O(\log^{k-1}(t))$ generators of height less than t. To see this, use the Dirichlet map D from K^* to $\mathbb{R}^k$ defined by

$$\mathrm{D}(a) := (\log|\sigma_1(a)|, \ldots, \log|\sigma_k(a)|)$$

with the notation of section 2. □

Lemma 10
Let K be a number field of degree n and $\mathrm{cov}(a,b)$ the covolume of the lattice $(a,b)\mathbf{O}_K$ as before. We claim that for any $0 \le \alpha < n$ and any $C > 0$ holds

$$\#\{(a,b) \in \mathbf{O}_K^2 : \ \mathrm{cov}(a,b) \le Ct^\alpha, \ \mathrm{ht}(a,b) \le t\} = O(t^{2\alpha} \log^{n-1}(t)). \qquad (36)$$

Proof of Lemma 10. Clearly, there exists a natural number $p > 0$ such that $-p$ has no square root in K. Consider the field $L := K(\sqrt{-p})$ and let $R := \mathbf{O}_K[\sqrt{-p}]$. Pairs $(a,b) \in \mathbf{O}_K^2$ correspond bijectively to elements $a + b\sqrt{-p}$ in the ring R. Also, R is contained in the ring $\mathbf{O}_L$ of integers of L. The degree of L is $2n$, and Galois theory tells us that every embedding $\sigma_i : \ K \to \mathbb{C}$ can be extended to L in exactly two ways, characterised by the value on $\sqrt{-p}$. The conjugates of $x := a + b\sqrt{-p}$ in $\mathbb{C}$ are given by

$$\sigma_i(a) \pm \sigma_i(b)\sqrt{-p}, \qquad i = 1, \ldots, n.$$

With a suitably chosen constant $C_1 > 0$,

$$\left|\sigma_i(a) \pm \sigma_i(b)\sqrt{-p}\right| \le |\sigma_i(a)| + \sqrt{p}|\sigma_i(b)| \le C_1\sqrt{|\sigma_i(a)|^2 + |\sigma_i(b)|^2} \qquad (37)$$

for all $a, b \in \mathbf{O}_K$ and for all $i = 1, \ldots, n$. Multiply this inequality over all i with both $+$ and $-$ on the left-hand side. This gives

$$|N_{L/\mathbb{Q}}(x)| = |N_{L/\mathbb{Q}}(a + b\sqrt{-p})| \le C_1^{2n}\mathrm{cov}(a,b)^2. \qquad (38)$$

Now $\mathrm{ht}(a,b) \le t$ implies $\mathrm{ht}(x) \le (1+\sqrt{p})t$. In view of inequality (38), $\mathrm{cov}(a,b) \le Ct^\alpha$ implies $|N_{L/\mathbb{Q}}(x)| \le C_2 t^{2\alpha}$ with a suitable constant C_2. Finally the unit rank of L is $n-1$, since L is totally complex. We are ready to apply Lemma 9 with L, C_2 and 2α in place of K, C and α, respectively. This gives the required estimate. □

Proposition 11
Let $\mathrm{cov}(a,b)$ be the function defined in Proposition 4. For any given $e>0$,

$$\sum_{\substack{\mathrm{ht}(a,b)\le t\\ \mathrm{cov}(a,b)\le t^{n-e}}} \frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)} = O(t^{2n-e/2}\log^{n-1}(t)) \tag{39}$$

where the implicit constant depends only on e. The pair $(a,b)=(0,0)$ should be omitted from the summation.

Proof of Proposition 11. For any $0\le\alpha<\beta<n$, consider the subsum $S_{\alpha,\beta}$ of the one in equation (39), ranging only over those summands satisfying

$$t^\alpha < \mathrm{cov}(a,b) \le t^\beta.$$

In view of Lemma 10,

$$S_{\alpha,\beta} = O(t^{2\beta+n-\alpha}\log^{n-1}(t)). \tag{40}$$

Now cover the interval $[0,n-e]$ by finitely many intervals $[\alpha_j,\beta_j]$ of length $e/2$. The maximum of all β_j is therefore $n-e$. For each corresponding subsum S_{α_j,β_j}, the exponent in equation (40) is

$$2\beta_j+n-\alpha_j = \beta_j+n+\frac{e}{2} \le 2n-\frac{e}{2}.$$

Summing over all j will give a $O(t^{2n-e/2}\log^{n-1}(t))$. This completes the proof of Proposition 11. □

The following proposition gives an upper bound on the number of matrices which are in P_a, but not in Q_a or vice versa as claimed in equation (8). For these matrices, use the fact that the function ht(.) satisfies the triangle inequality. This gives

$$|\mathrm{ht}(bc/a)-\mathrm{ht}(a)| \le \mathrm{ht}(1/a) \tag{41}$$

Proposition 12
Define a set of matrices in $\mathrm{SL}_2(\mathbf{O}_K)$ by

$$R_a := \{A\in \mathrm{SL}_2(\mathbf{O}_K):\ \mathrm{ht}(A)=\mathrm{ht}(a), |\mathrm{ht}(bc/a)-\mathrm{ht}(a)|\le \mathrm{ht}(1/a)\}$$

Then $\sum_{\mathrm{ht}(a)\le t}\#R_a = O(t^{2n-\eta})$ with η as in Theorem 2.

Proof of Proposition 12. Pursuing the first counting strategy as in subsection 3.1, one arrives at a subset G_a of V^2 such that $(b/a,c/a)\in G_a$ if and only if it stems from a matrix $A\in R_a$. For all $a\in K_e(t)$, the height $\mathrm{ht}(1/a)$ tends to zero as $\mathrm{ht}(a)$ tends to infinity, therefore $\mathrm{Vol}(G_a)$ tends to zero. The same uniform distribution argument as before shows that the sum over $\#R_a$ goes into the error term of Theorem 2. For $a\notin K_e(t)$, look again at the proof of Theorem 8.

There we have actually proved that the total number of matrices in $\mathrm{SL}_2(\mathbf{O}_K)$ of height less than t with maximal entry $a \notin K_e(t)$ goes into the error term of Theorem 2. $\square$

Proposition 13
The number of matrices $A \in \mathrm{SL}_2(\mathbf{O}_K)$ such that two entries have maximal height is $O(t^{2n-\eta})$ with η as in Theorem 2.

Proof of Proposition 13. Consider only matrices $A \in \mathrm{SL}_2(\mathbf{O}_K)$ is such that $\mathrm{ht}(A) = \mathrm{ht}(a) = \mathrm{ht}(b)$. Pursuing the first counting strategy as in subsection 3.1, we see that $(b/a, c/a)$ is then in the boundary ∂H_a for H_a as defined in (9). The same argument as before gives a main term involving the volume of this boundary, namely zero, and an error term as before. The second possibility is $\mathrm{ht}(a) = \mathrm{ht}(d) > \mathrm{ht}(b), \mathrm{ht}(c)$. This leads to inequality (41), and matrices satisfying (41) have already been dealt with in Proposition 12. $\square$

5 Uniform Distribution

The statement of Theorem 17 means that *the set of pairs* $(b/a, c/a)$ *used in defining* m_a *in (10) is uniformly distributed in* F^2 (more precisely, this is a sequence of sets, and the distribution becomes more and more uniform). To prove Theorem 17, we will need certain *generalized Kloosterman sums.*
The bound for these sums given in Corollary 16 will not only be used for proving Theorem 17. We will rely directly on this bound rather than Theorem 17 to obtain the error term in equation (19). Now let us define the aforementioned Kloosterman sums.

Definition 14
Consider the symmetric bilinear form $\langle ., . \rangle$ on V defined by

$$\langle u, v \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(uv). \tag{42}$$

It is well-known that $\langle ., . \rangle$ is non-degenerate. Let $\widehat{\mathbf{O}}_K$ be the lattice dual to $\mathbf{O}_K$ with respect to $\langle ., . \rangle$. The lattice $\widehat{\mathbf{O}}_K$ is a fractional ideal in K. Its inverse is an integral ideal, known as the *different* of K. For all $0 \neq a \in \mathbf{O}_K$ and $u, v \in \widehat{\mathbf{O}}_K$ define the *Kloosterman sum*

$$K(u, v; a) := \sum_{b,c} \exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}((bu + cv)/a)).$$

Here the summation is over all residue classes b, c modulo a such that $bc \equiv 1 \pmod{a}$.

Theorem 15
There exists a constant $C > 0$, depending only on the number field K, such that for all nonzero $u, v \in \widehat{\mathbf{O}}_K$ and all nonzero $a \in \mathbf{O}_K$

$$|K(u, v; a)| \leq C\, 2^{\omega(a)} \sqrt{|N_{K/\mathbb{Q}}((u, v, a))|} \sqrt{|N_{K/\mathbb{Q}}(a)|}.$$

Here, $\omega(a)$ denotes the number of prime ideals dividing $a\mathbf{O}_K$ and $(u, v, a) = u\mathbf{O}_K + v\mathbf{O}_K + a\mathbf{O}_K$ (this a fractional ideal with bounded denominator).

A proof may be found in (Bruggeman and Miatello, 1995, section 5). In fact, Bruggeman and Miatello give a far more precise statement. Odoni and Spain (1995) prove a more general uniform distribution result about rational functions of arbitrarily many variables. Patterson (1997) studies the angular distribution of $K(x, y; a)$ and more general sums. Theorem 15 can be derived from Proposition 2.1 of that article (let $n = 1$ and S be the set of all infinite places of K).
The hypothesis in Theorem 15 that both of x, y are non-zero can be relaxed to at least one of them being non-zero. The sums $K(u, 0; a)$ are equal to the Möbius function of K except for a finite number of cases. For this and a discussion of algebraic properties of Kloosterman sums, see Pacharoni (1998). For fixed $u, v \in \widehat{\mathbf{O}}_K$, we have therefore the corollary

Corollary 16
For all $\varepsilon > 0$ and $u, v \in \widehat{\mathbf{O}}_K$ not both zero, there is a constant $C_{u,v,\varepsilon}$ such that

$$|K(u, v; a)| \leq C_{u,v,\varepsilon} |N_{K/\mathbb{Q}}(a)|^{1/2+\varepsilon}$$

for all $0 \neq a \in \mathbf{O}_K$.

Theorem 17
Recall the sampling functional m_a defined in (10). It satisfies for all Riemann-integrable functions f on V^2 with compact support

$$\lim_{\phi(a)} m_a(f) = \int_{V^2} f(x, y)\, dx\, dy$$

where $\lim_{\phi(a)}$ means a limit for all sequences of elements $a \in \mathbf{O}_K$ such that $\phi(a)$ tends to infinity. In particular, for every Riemann-integrable subset H of V^2,

$$\lim_{\phi(a)} m_a(\mathbf{1}_H) = \mathrm{Vol}(H)$$

Proof of Theorem 17. Use the *Weyl criterion*, see Hlawka (1979) or Kuipers and Niederreiter (1974). To test for the phenomenon of uniform distribution, it is enough to consider as test functions f all characters of the compact abelian group $V^2/\mathbf{O}_K^2$, restricted to some fixed fundamental domain F^2 for $\mathbf{O}_K^2$ in V^2. Every such character can be written as $\exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(xu + yv))$ for some $u, v \in \widehat{\mathbf{O}}_K$.
Up to the normalizing factor $\mathrm{cov}(\mathbf{O}_K)^2$, the value of the sampling functional m_a at this character is precisely the Kloosterman sum $K(u, v; a)$. Corollary 16, together with the Weyl criterion implies the statement of Theorem 17. □

6 Discrepancy

In our setting, the discrepancy $D(a)$ is the error when approximating the volume of a cube by the sampling functional m_a as defined in (7), maximized over all cubes inside the fundamental domain F^2 for $V^2/\mathbf{O}_K^2$.
The following theorem of Hlawka (1961) has been adapted to our situation. It shows how the discrepancy gives a bound on the approximation error in (13) which depends only mildly on H_a.

Theorem 18 (HLAWKA)
Let H be a Riemann–integrable subset of F^2 such that for any straight line L in V^2, $L \cap H$ consists of at most h intervals and the same is true for all orthogonal projections of H. Then

$$|m_a(\mathbf{1}_H) - \mathrm{Vol}(H)| \leq (12h)^{2n} D(a)^{1/(2n)}.$$

For the sets H_a defined in (9), the number h is uniformly bounded by Proposition 19.

Proposition 19
For all $0 \neq a \in \mathbf{O}_K$ and all straight lines L in V^2, $L \cap H_a$ consists of at most $12k-1$ intervals. The same is true for all orthogonal projections of H_a.

Proof of Proposition 19. Consider x_i, y_i and $x_i y_i$ as real or complex-valued functions on a straight line L in V^2. They are linear or quadratic functions of one real parameter. The sets H_a are defined by bounds on the absolute value of these functions. Since an inequality on the absolute value of a quadratic function can be tight for at most four values of the parameter, the line L can hit the boundary of H_a at most $12k$ times. This proves that $L \cap H_a$ consists of at most $12k-1$ intervals.
Now let π be an orthogonal projection of V^2 onto a ρ-dimensional subspace. After a suitable linear coordinate change, π projects any point onto its last ρ coordinates. The inequalities defining H_a are still linear and quadratic after changing coordinates. So even if more of them than before might become tight on a given line L through πH_a, there are still at most $3k$ inequalities defining πH_a, and each of them becomes sharp at most 4 times. Therefore $12k-1$ is a uniform bound for the number of intervals in $L \cap \pi(H_a)$. □

It is usually hard to calculate $D(a)$ exactly, but we get an upper bound on it from the famous inequality of Erdös/Turán/Koksma and the estimate for Kloosterman sums quoted in Theorem 16. This inequality states the following. For every integer $M > 300$ and any finite set of points A in $X = [0,1[^s$, the discrepancy D_A for the corresponding sampling functional m_A is bounded in terms of the values of m_A at characters of $(\mathbb{R}/\mathbb{Z})^s$.

$$D(A) \leq \frac{2^s \cdot 300}{M} + 30^s \sum_{0 \neq |h| \leq M} m_A(\chi_h) R(h)^{-1} \tag{43}$$

where $h = (h_1, \ldots, h_s) \in \mathbb{Z}^s$, $|h| = \max(|h_1|, \ldots, |h_s|)$, $R(h) = \prod_{j=1}^{s} \max(1, |h_j|)$ and $\chi_h = \exp(2\pi i \langle h, . \rangle)$ runs through the characters of $(\mathbb{R}/\mathbb{Z})^s$.
To apply this to our setting, we identify $\mathbf{O}_K^2$ with $\mathbb{Z}^{2n}$ by choosing a basis B. The dual lattice $\widehat{\mathbf{O}}_K{}^2$ is spanned by the basis B' dual to B with respect to $\mathrm{Tr}_{K/\mathbb{Q}}(.,.)$. Characters may be parametrized by $\chi_h = \exp(2\pi i \mathrm{Tr}_{K/\mathbb{Q}}(ux + vy))$ where (u, v) has the coordinate vector h with respect to B'. The compact group $V^2/\mathbf{O}_K{}^2$ is identified with X and the dimension $s = 2n$. The volume is normalized so that $\mathrm{Vol}(F) = 1$, and our set A is the set of pairs $(b/a, c/a)$ where (b, c) runs through those residue classes modulo a where $bc \equiv 1 \pm a$. Then the sum $m_a(\chi_h)$ is just the Kloosterman sum $K(u, v; a)$. Estimate the second term by taking the absolute value of each summand and use the bound (15) for the Kloosterman sums. Estimate $|N_{K/\mathbb{Q}}((u, v, a))|$ simply by $|N_{K/\mathbb{Q}}(u)| = O(|h|^n)$, replace $R(h)^{-1}$ by $|h|^{-1}$. This gives

$$\begin{aligned} D(a) &\ll \frac{1}{M} + \frac{1}{\phi(a)} \sum_{0 \neq |h| \leq M} 2^{\omega(a)} |h|^{n/2-1} \sqrt{|N_{K/\mathbb{Q}}(a)|} \\ &\ll \frac{1}{M} + M^{2n+n/2-1} |N_{K/\mathbb{Q}}(a)|^{-1/2+\varepsilon} \end{aligned} \tag{44}$$

The optimal choice for M balances the two summands of the right-hand side of (44), so put $M = [|N_{K/\mathbb{Q}}(a)|^{(1-2\varepsilon)/(5n)}]$. Rewriting this, we get for every $\delta < 1/(5n)$

$$D(a) = O\left(|N_{K/\mathbb{Q}}(a)|^{-\delta}\right). \tag{45}$$

Unfortunately, our sets H_a are spread over more than one copy of F^2. This means we have to break H_a up into pieces $H_a \cap ((u, v) + F^2)$ and use Theorem 18 for those pieces which are neither empty nor entirely filled (in that case, the approximation error is zero). Writing $r(a)$ for the diameter of H_a, the number of such pieces is a $O(r(a)^{2n-1})$ (the order of magnitude of the surface of H_a). Thus, we have shown the following theorem.

Theorem 20
For all $0 \neq a \in \mathbf{O}_K$, the error in equation (13) is bounded by

$$|m_a(\mathbf{1}_{Ha}) - \mathrm{Vol}(H_a)| \ll r(a)^{2n-1} |N_{K/\mathbb{Q}}(a)|^{-\delta}$$

with an implicit constant depending on $\delta < 1/(5n)$, but independent of a.

7 Calculation of a Volume

Define the subset $K(\varepsilon, \delta, \underline{e})$ of V^2 by

$$K(\varepsilon, \delta, \underline{e}) := \left\{(x, y) : \ \mathrm{cov}(x, y) \leq \varepsilon \|x, y\|_2^n, \ |N_{K/\mathbb{Q}}(x)| \leq \delta \|x, y\|_2^n\right\}$$

where $\underline{e} = (e_1, ..., e_k)$ is a vector with $e_i = 1$ if the embedding σ_i of K into $\mathbb{C}$ is real and $e_i = 2$ otherwise. Recall $k = r_K + s_K$, $n = [K : \mathbb{Q}] = r_K + 2s_K$ with r_K being the number of real embeddings, s_K the number of complex embeddings of K and $\|x, y\|_2 := \max_i\{|x_i|^2 + |y_i|^2\}$.

Theorem 21
Write $\log_+(x) := \max\{\log(x), 0\}$. The volume of $K(\varepsilon, \delta, \underline{e})$ as a function of ε, δ is continuous and differentiable with respect to ε almost everywhere. Wherever its partial derivative exists, it is bounded for all $\varepsilon, \delta > 0$ and satisfies

$$\frac{\partial}{\partial \varepsilon} \mathrm{Vol}_{2n}(K(\varepsilon, \delta, \underline{e})) = O(\min\{1, \delta \log_+(1/\delta)^m\})$$

for some integer m. In particular, the volume of $K(\varepsilon, \delta, \underline{e})$ is Lipschitz-continuous in ε with a Lipschitz constant of order $O(\min\{1, \delta \log_+(1/\delta)^m\})$. The implicit constant in the O-term and the integer m only depend on the vector $\underline{e}$.

Proof of Theorem 21. Write out the conditions defining $K(\varepsilon, \delta, \underline{e})$ in coordinates. These are

$$\begin{aligned} \prod_{i=1}^{k} (|x_i|^2 + |y_i|^2)^{e_i/2} &\leq \varepsilon \|x, y\|_2^n \\ \prod_{i=1}^{k} |x_i|^{e_i} &\leq \delta \|x, y\|_2^n \\ \|x, y\|_2 &\leq 1 \end{aligned} \tag{46}$$

Reduce to $x_i, y_i > 0$ for all $1 \leq i \leq r_K$ and pass to polar coordinates $(x_i, y_i) \to (r_i, \theta_i, s_i, \phi_i)$ for all $r_K + 1 \leq i \leq k$. The angles θ_i and ϕ_i do not occur anywhere in the integral, so we can perform these integrations. Afterwards, we change r_i back to x_i and s_i to y_i for ease of notation. This gives

$$\mathrm{Vol}(K(\varepsilon, \delta, \underline{e})) = c \int_0^1 \ldots \int_0^1 \mathbf{1}_C(x, y) \prod_{i > r_K} x_i y_i \, dV$$

with $c = 4^{r_K} (2\pi)^{2s_K}$ and a domain $C = C(\varepsilon, \delta, \underline{e})$ in $\mathbb{R}^{2k}$ defined by

$$C(\varepsilon, \delta, \underline{e}) := \left\{ (x, y) : \ 0 < x_i, y_i < 1, \ \begin{array}{r} \prod_{i=1}^k (x_i^2 + y_i^2)^{e_i/2} \leq \varepsilon \|x, y\|_2^n, \\ \prod_{i=1}^k x_i^{e_i} \leq \delta \|x, y\|_2^n \end{array} \right\} \tag{47}$$

Define a subset E of $\mathbb{R}^{2k}$ and a function $g_{\underline{e}}(\varepsilon, \delta)$ by

$$\begin{aligned} E &:= \left\{ (s, \theta) \in \mathbb{R}^{2k} : \ \begin{array}{l} 0 \leq s_k \leq \ldots \leq s_1 \leq 1, \ 0 \leq \theta_i \leq \pi/2, \\ \prod_{i=1}^k s_i^{e_i} < \varepsilon, \ \prod_{i=1}^k (s_i \cos(\theta_i))^{e_i} \leq \delta \end{array} \right\} \\ g(\varepsilon, \delta) &:= g_{\underline{e}}(\varepsilon, \delta) := \int_E \prod_{i=1}^{k} s_i^{2e_i - 1} (\cos(\theta_i) \sin(\theta_i))^{e_i - 1} \, dV \end{aligned} \tag{48}$$

This is designed so that by changing to polar coordinates a second time,

$$\frac{1}{ck!} \mathrm{Vol}_{2n}(K(\varepsilon, \delta, \underline{e})) = g(\varepsilon, \delta) \tag{49}$$

The factor $k!$ comes in because we suppose the coordinates to be in descending order in E. From now on, we will deal with the function g instead of the original volume. In case $k = 1$, it is not hard to verify the following table, which serves to show that g is not simple to describe in general.

Conditions	$g(\varepsilon, \delta)$
Case $e_1 = 1$	
$\delta \geq 1, \varepsilon \geq 1$	$\pi/4$
$\delta \geq 1, \varepsilon \leq 1$	$\pi\varepsilon^2/4$
$\delta \leq 1, \varepsilon \geq 1$	$[\pi/2 - \arccos(\delta) + \delta\sqrt{1-\delta^2}]/2$
$\varepsilon \leq \delta \leq 1$	$\pi\varepsilon^2/4$
$\delta \leq \varepsilon \leq 1$	$[\pi\varepsilon^2/2 - \varepsilon^2 \arccos(\delta/\varepsilon) + \delta\sqrt{\varepsilon^2-\delta^2}]/2$
Case $e_1 = 2$	
$\delta \geq 1, \varepsilon \geq 1$	$1/8$
$\delta \geq 1, \varepsilon \leq 1$	$\varepsilon^2/8$
$\delta \leq 1, \varepsilon \geq 1$	$\delta(2-\delta)/8$
$\varepsilon \leq \delta \leq 1$	$\varepsilon^2/8$
$\delta \leq \varepsilon \leq 1$	$\delta(2\varepsilon - \delta)/8$

Note that this is a continuous function of ε and δ, differentiable almost everywhere. The partial derivative with respect to ε is $O(\delta)$ in all cases in the table, wherever it exists. Now use induction over k. Write $\tilde{g}$ for the function corresponding to g for the shorter parameter vector $(e_2, ..., e_k)$ (the 'tail' of $\underline{e}$), so that $\tilde{g}$ has two fewer variables than g. There is an obvious recurrence relation between g and $\tilde{g}$.

$$g(\varepsilon, \delta) = \int_0^1 \int_0^{\pi/2} s_1^{2e_1-1} (\cos(\theta_1)\sin(\theta_1))^{e_1-1} \tilde{g}\left(\varepsilon/s_1^{e_1}, \delta/(s_1\cos(\theta_1))^{e_1}\right) \, d\theta_1 \, ds_1 \tag{50}$$

Write $\tilde{h}$ for the partial derivative of $\tilde{g}$ with respect to ε, h for that of g. From (50) and the equality

$$\frac{\partial}{\partial\varepsilon}\tilde{g}(\varepsilon/s^{e_1}, \delta/(s\cos(\theta)^{e_1}) = \frac{1}{s^{e_1}}\tilde{h}(\varepsilon/s^{e_1}, \delta/(s\cos(\theta)^{e_1}),$$

valid almost everywhere, we get a corresponding recurrence relation for the functions h and $\tilde{h}$.

$$h(\varepsilon, \delta) = \int_0^1 \int_0^{\pi/2} s^{e_1-1} (\cos(\theta)\sin(\theta))^{e_1-1} \tilde{h}\left(\varepsilon/s_1^{e_1}, \delta/(s\cos(\theta))^{e_1}\right) \, d\theta \, ds \tag{51}$$

(hence for $k > 1$, g is in fact continously differentiable with respect to ε). Using the induction hypothesis for $\tilde{h}$,

$$\tilde{h}(\varepsilon, \delta) = O(\min\{1, \delta \log_+(1/\delta)^m)\}) \tag{52}$$

we get the desired upper bound for h. We will demonstrate this in case $e_1 = 2$. Without loss of generality, $0 < \delta < 1$. In this case, substituting $u = \cos(\theta)$

simplifies equation (51) to

$$h(\varepsilon,\delta)=\int_0^1\int_0^1 su\,\tilde{h}(\varepsilon/s^2,\delta/(su)^2)\,du\,ds \tag{53}$$

Split off the integrals $\int_0^{\sqrt{\delta}}\int_0^1 \ldots du\,ds$ and $\int_{\sqrt{\delta}}^1\int_0^{\sqrt{\delta}/s}\ldots du\,ds$ from (53), using that $\tilde{h}$ is bounded. Both integrals are $O(\delta\log(\delta))$ for $0<\delta<1$. The remaining integral

$$\int_{\sqrt{\delta}}^1\int_{\sqrt{\delta}/s}^1 su\,\tilde{h}(\varepsilon/s^2,\delta/(su)^2)\,du\,ds$$

can be bounded using the induction hypothesis (52), which gives a term of magnitude $O\left(\delta\log(\delta)^{m+2}\right)$. The calculations in case $e_1=1$ are more tedious, but entirely similar. □

8 Related Problems

We list three problems which are related to the one we treated in this paper.

1. Counting elements of $\mathrm{GL}_2(\mathbf{O}_K)$
   Our methods can be used to obtain

   $$t^{2n}\log^r(t)\ll \mathrm{GL}_2(\mathbf{O}_K)(t)\ll t^{2n}\log^r(t)$$

   with $r=r_K+s_K-1$ being the unit rank of $\mathbf{O}_K$.

2. Counting units in integral group rings
   For any finite group Γ such that all absolutely irreducible representations can be realized over the ring of integers in the field K_i generated by their character values, the group of units in $\mathbb{Z}\Gamma$ embeds into

   $$\bigoplus \mathrm{GL}_{n_i}(\mathbf{O}_{K\,i})$$

   such that the image has finite index. If $\mathbf{O}_{K\,i}=\mathbb{Z}$ or $n_i=2$, the theorem of [DRS] respectively theorem 2 can be used.

3. Counting integral normal bases
   Let $K/\mathbb{Q}$ be a Galois extension with Galois group Γ. If any integral normal basis exists, then the set of all integral normal bases is in 1-1 bijection with $\mathbb{Z}\Gamma^*$. Counting them with respect to a bound for their absolute norm requires results from diophantine approximation. Precise results are known for abelian Galois groups Γ, see Everest (1983), Everest and Győry (1997), Everest (1998),Bushnell (1979). We have an asymptotic result for K not real, $\Gamma=S_3$, see Roettger (1999).

9 Conclusion

The methods presented here are certainly inferior to those of Duke et al. since they are not capable of generalization beyond $\mathrm{SL}_2(\mathbf{O}_K)$. They do settle at least this case and give an error term which might still be improved. The group $\mathrm{GL}_2(\mathbf{O}_K)$ could possibly also be treated in this way. An additional feature is that these elementary methods provide a veritable showcase for beautiful concepts of classical number theory like higher-dimensional uniform distribution, discrepancy, geometry of lattices and Möbius inversion.
It seems odd that both counting methods should really be necessary - even if the first method is less robust with regard to error terms, the second one should be accessible to an analysis using uniform distribution etc. We have tried to do this without success.

10 Acknowledgements

I am much indebted to Professor S J Patterson, Goettingen, for support and helpful discussions, to Iowa State University for a reduction in teaching load and to Professor G R Everest, Norwich, who guided me through writing my doctoral thesis.

References

Beardon, A. F. (1983), *The geometry of discrete groups*, Springer.

Bruggeman, R. W. and Miatello, R. J. (1995), "Estimates of Kloosterman sums for groups of real rank one," *Duke Math. J.*, 80, 105–137.

Bushnell, C. J. (1979), "Norm distribution in Galois orbits," *J. reine angew. Math.*, 310, 81–99.

Duke, W., Rudnick, Z., and Sarnak, P. (1993), "Density of integer points on affine homogeneous varieties," *Duke Math. J.*, 71, 143–179.

Everest, G. (1983), "Diophantine approximation and the distribution of normal integral generators," *J. London Math. Soc.*, 28, 227–237.

— (1998), "Counting generators of normal integral bases," *Amer. J. Math.*, 120, 1007–1018.

Everest, G. and Győry, K. (1997), "Counting solutions of decomposable form equations," *Acta Arith.*, 79, 173–191.

Hlawka, E. (1961), "Funktionen von beschränkter Variation in der Theorie der Gleichverteilung (German)," *Ann. Mat. Pura Appl., IV. Ser.*, 325–333.

— (1979), *Theorie der Gleichverteilung*, Mannheim: Bibliographisches Institut.

Kuipers, L. and Niederreiter, H. (1974), *Uniform distribution of sequences*, New York: Wiley.

Lax, P. and Phillips, R. (1982), "The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces," *J. Funct. Anal.*, 46, 280–350.

Odoni, R. W. K. and Spain, P. G. (1995), "Equidistribution of values of rational functions $\pmod p$)," *Proc. R. Soc. Edinb. Sect. A*, 125, 911–929.

Pacharoni, I. (1998), "Kloosterman sums on number fields of class number one," *Comm. Algebra*, 26, 2653–2667.

Patterson, S. J. (1997), "The asymptotic distribution of Kloosterman sums," *Acta Arith.*, 79, 205–219.

Roettger, C. (1999), "Counting normal integral bases in complex S_3-extensions of the rationals," Tech. Rep. 416, University of Augsburg.

— (2000), "Counting problems in algebraic number theory," Ph.D. thesis, University of East Anglia, Norwich, UK.

Samuel, P. (1970), *Algebraic Number Theory*, Paris: Hermann.

Siegel, C. L. (1989), *Lectures on the geometry of numbers*, Springer.