Journal de Théorie des Nombres de Bordeaux **17** (2005), 301–322

Counting invertible matrices and uniform distribution

par CHRISTIAN ROETTGER

RÉSUMÉ. On considère le groupe $\mathrm{SL}_2(\mathbf{O}_K)$ sur l'anneau des entiers d'un corps de nombres K. La hauteur d'une matrice est définie comme le maximum de tous les conjugués de ses éléments en valeur absolue. Soit $\mathrm{SL}_2(\mathbf{O}_K, t)$ le nombre de matrices de $\mathrm{SL}_2(\mathbf{O}_K)$ dont la hauteur est inférieure à t. Nous déterminons le comportement asymptotique de $\mathrm{SL}_2(\mathbf{O}_K, t)$, ainsi qu'un terme d'erreur. Plus précisemment,

$$\mathrm{SL}_2(\mathbf{O}_K, t) = Ct^{2n} + O(t^{2n-\eta})$$

où n est le degré de K. La constante C dépend du discriminant de K, d'une intégrale ne dépendant que de la signature de K, et de la valeur de la fonction zêta de Dedekind relative à K pour $s = 2$. Nous faisons appel à la théorie de distribution uniforme et de la discrépance pour obtenir le terme d'erreur. Enfin, nous discuterons trois applications concernant le nombre asymptotique de matrices de $\mathrm{GL}_2(\mathbf{O}_K)$, d'unités dans certains anneaux de groupe entiers, et de bases normales intégrales.

ABSTRACT. Consider the group $\mathrm{SL}_2(\mathbf{O}_K)$ 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 $\mathrm{SL}_2(\mathbf{O}_K, t)$ be the number of matrices in $\mathrm{SL}_2(\mathbf{O}_K)$ with height bounded by t. We determine the asymptotic behaviour of $\mathrm{SL}_2(\mathbf{O}_K, t)$ as t goes to infinity including an error term,

$$\mathrm{SL}_2(\mathbf{O}_K, t) = Ct^{2n} + O(t^{2n-\eta})$$

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 discuss applications to counting problems concerning matrices in the general linear group, 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 in the special linear group with height less than t,

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

as t tends to infinity. We also ask the same question with the general linear group $\mathrm{GL}_m(\mathbf{O}_K)$ 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 [1]. The best known error term in this case is $O(t^{2/3+\varepsilon})$, due to A. Selberg, see [11]. Duke/Rudnick/Sarnak have proved a very general theorem (see [4]) which, as an 'application', answers the question in case $K = \mathbb{Q}$ for arbitrary m with the 2-norm instead of our height function.

Theorem 1.1 (Duke/Rudnick/Sarnak). *Write* $\|g\|_2$ *for the 2-norm of a matrix with real entries. For all* $m \geq 1$,

$$\#\{g \in \mathrm{SL}_m(\mathbb{Z}) : \ \|g\|_2 \leq t\} \sim c_m t^{m^2-m} \tag{1.1}$$

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 sharpens an asymptotic result of [16]. The thesis [16] is available on-line at

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

Theorem 1.2. *For any positive* $\eta < 1/(20n - 5)$,

$$\mathrm{SL}_2(\mathbf{O}_K, t) = 4E_K D_K t^{2n} + O(t^{2n-\eta}) \tag{1.2}$$

where D_K *depends only on the signature of* K *and*

$$E_K := \frac{1}{\zeta_K(2)|\mathrm{disc}(K)|^{3/2}}. \tag{1.3}$$

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

Remark 1.3.

(1) Theorem 1.2 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, although the implicit constant will depend on the coset.

(2) The constant D_K is given by

$$D_K = 2^{3s_K} \int_{\mathbb{B}} \mathrm{g}(x)\, dx, \tag{1.4}$$

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

$$\mathrm{g}(x) := 4^{r_K} \pi^{2s_K} \|x\|_\infty^n \prod_{i=1}^{r_K} \left(1 + \log\left(\frac{\|x\|_\infty}{|x_i|}\right)\right)$$
$$\prod_{i=r_K+1}^{r_K+s_K} \left(\frac{\|x\|_\infty}{|x_i|} + 2\log\left(\frac{\|x\|_\infty}{|x_i|}\right)\right) \tag{1.5}$$

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 1.1 and 1.2. This is no surprise, 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 [18].

2. Notation and Basic Definitions

Order the complex embeddings $\sigma : K \to \mathbb{C}$ so that σ_i is real for $1 \leq i \leq r_K$ and complex for $r_K < i \leq r_K + s_K$. Write $k := r_K + s_K$. With V defined as above, we get a one-to-one algebra homomorphism $\Sigma : K \to V$,

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

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 $t > 0$. Given a lattice L in $\mathbb{R}^s$, the *covolume* $\mathrm{cov}(L)$ is the volume of a fundamental parallelotope for L.

As an example, the lattice $\mathbf{O}_K$ in V has covolume

$$\mathrm{cov}(\mathbf{O}_K) = \frac{|\mathrm{disc}(K)|^{1/2}}{2^{s_K}} \tag{2.1}$$

(for a proof, see eg [17] - V is identified with $\mathbb{R}^{2n}$ here). 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 use two different counting methods, outlined in subsections 3.1 and 3.2, respectively. The first method relies on uniform error terms for lattice point counting (section 4) and on the theory of uniform distribution and discrepancy (sections 5 and 6).

The second method relies also on section 4 and on an estimate for certain volumes (section 7). It is tailored to give an upper bound for those matrices where the first method fails. Since the statement in case $K = \mathbb{Q}$ is well-known, we exclude this case from now on. This will give us simpler error terms in Theorems 4.3 and 4.4.

3.1. Counting Matrices With One Fixed Entry.

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

$$M_a := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ \mathrm{ht}(b,c,d) \leq \mathrm{ht}(a) \right\} \tag{3.1}$$

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

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

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

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

We will show in Proposition 4.9 that the accumulated differences between $\#Q_a$ and $\#P_a$ can be estimated by

$$\sum_{\mathrm{ht}(a) \leq t} |\#Q_a - \#P_a| = O(t^{2n-\eta}) \tag{3.2}$$

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

$$H_x := \left\{ (y,z) : \ y, z, yz \in \frac{\mathrm{ht}(x)}{x} \mathbb{B} \right\}. \tag{3.3}$$

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 well-defined. Using H_a, we get

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

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.

$$m_a(f) := \frac{\mathrm{cov}(\mathbf{O}_K)^2}{\phi(a)} \sum_{bc \equiv 1 \pmod{a}} f\left(\frac{b}{a}, \frac{c}{a}\right). \tag{3.4}$$

The summation is over all $b, c \in \mathbf{O}_K$ such that $bc \equiv 1 \pmod{a}$, and $\phi(a) = \#(\mathbf{O}_K/a)^*$ is the generalized Euler totient function. This functional is defined for all functions with compact support in V^2. Obviously,

$$\#P_a = \frac{\phi(a)}{\mathrm{cov}(\mathbf{O}_K)^2} m_a(\mathbf{1}_{H_a}). \tag{3.5}$$

We will prove in Theorem 5.4 that for all Riemann-integrable sets H in V^2

$$\lim_{\phi(a) \to \infty} m_a(\mathbf{1}_H) = \mathrm{Vol}(H) \tag{3.6}$$

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 5.4, 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 (3.6) seems to suggest

$$m_a(\mathbf{1}_{Ha}) \approx \mathrm{Vol}(H_a). \tag{3.7}$$

However, the 'target' H in (3.6) 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 (3.7). The classical theory of discrepancy comes into play here. Writing $r(a)$ for the diameter of H_a and using (3.5), we get an error bound from Theorem 6.3,

$$\left| \#P_a - \frac{\phi(a)}{\mathrm{cov}(\mathbf{O}_K)^2} \mathrm{Vol}(H_a) \right| \ll \phi(a) r(a)^{2n-1} |N_{K/\mathbb{Q}}(a)|^{-\delta} \tag{3.8}$$

for the error in equation (3.7), 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

$$K_e(t) := \{x \in V : \ |N_{K/\mathbb{Q}}(x)| \geq \mathrm{ht}(x)^{n-e}, \ \mathrm{ht}(x) \leq t\}. \tag{3.9}$$

We want to sum the error bound (3.8) over all $a \in K_e(t)$. Replacing $\phi(a)$ by $|N_{K/\mathbb{Q}}(a)|$, we have for the sum over these 'nice' elements a

$$\sum_a |N_{K/\mathbb{Q}}(a)|^{1-\delta} \mathrm{ht}(a)^{(2n-1)e} = O(t^{2n-n\delta+(2n-1)e}). \tag{3.10}$$

For the main term, we get from Theorem 4.5 for all $\gamma < e/2$

$$\frac{1}{\mathrm{cov}(\mathbf{O}_K)^2} \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a) = C_K t^{2n} + O(t^{2n-\gamma}) \tag{3.11}$$

where

$$C_K := \frac{2^{3s_K}}{\zeta_K(2)|\mathrm{disc}(K)|^{3/2}} \int_{\mathbb{B}} |N_{K/\mathbb{Q}}(x)|\mathrm{Vol}(H_x)\, dx. \tag{3.12}$$

It is not hard to calculate $|N_{K/\mathbb{Q}}(x)|\mathrm{Vol}(H_x) = \mathrm{g}(x)$ with the function g defined in (1.5). Therefore $C_K = D_K E_K$ with the constants D_K, E_K defined in (1.4) and (1.3). Together with the error estimate (3.10), this shows

$$\sum_{a \in K_e(t)} \#M_a = C_K t^{2n} + O(t^{2n-\gamma} + t^{2n-n\delta+(2n-1)e}). \tag{3.13}$$

The factor 4 in equation (1.2) comes from the four possibilities for the position of the maximal entry of a matrix. By Proposition 4.10, the number of matrices where two or more entries have maximal height is $O(t^{2n-\eta})$ and goes into the error term. We still have to deal with the elements $a \notin K_e(t)$, meaning that $|N_{K/\mathbb{Q}}(a)|$ is very small in comparison to $\mathrm{ht}(a)$. For example units of $\mathbf{O}_K$ are such elements. 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 $\mathrm{ht}(b) \leq \mathrm{ht}(a)$, let

$$R(a,b) := \{(c,d) \in \mathbf{O}_K^2 : \ ad - bc = 1, \ \mathrm{ht}(c,d) \leq \mathrm{ht}(a,b)\}. \tag{3.14}$$

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 (3.1). This is the connection between the two counting strategies. Consider the

lattice $\mathbf{O}_K(a,b)$ of rank n inside V^2. Let $\mathrm{cov}(a,b)$ be its covolume. We will prove in Proposition 4.2 that

$$\#R(a,b) = O\left(\frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)}\right) \tag{3.15}$$

with an implicit constant independent of a and b. From Proposition 4.1 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

$$K_\mu(t) := \left\{(x,y) \in V^2 : \frac{1}{\mu+1} < \frac{\mathrm{cov}(x,y)}{\mathrm{ht}(x,y)^n} \leq \frac{1}{\mu},\ \mathrm{ht}(y) \leq \mathrm{ht}(x) \leq t\right\},$$

$$K_{\mu\nu}(t) := \left\{(x,y) \in K_\mu(t) : \frac{1}{\nu+1} < \frac{|N_{K/\mathbb{Q}}(x)|}{\mathrm{ht}(x)^n} \leq \frac{1}{\nu}\right\}.$$

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

$$\sum_{a,b} \#R(a,b) = S_1(t) + S_2(t) + S_3(t) \qquad \text{with} \tag{3.16}$$

$$S_1(t) = \sum_{\mu \leq t^e} \sum_{\nu \leq t^e} \sum_{(a,b) \in K_{\mu\nu}(t)} \#R(a,b),$$

$$S_2(t) = \sum_{\mu \leq t^e} \sum_{\nu > t^e} \sum_{(a,b) \in K_{\mu\nu}(t)} \#R(a,b),$$

$$S_3(t) = \sum_{\mu > t^e} \sum_{(a,b) \in K_\mu(t)} \#R(a,b).$$

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 (3.15) and Theorem 4.3. This gives

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

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 $S_2(t)$, use Theorem 7.1 with $\varepsilon = 1/\mu$, $\varepsilon = 1/(\mu+1)$ and $\delta = t^{-e}$. Note that this covers the whole union 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 7.1 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 7.1 implies

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

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

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

For $S_3(t)$, use first the estimate (3.15) and then Proposition 4.8 to count the summands. This gives

$$S_3(t) \ll \sum_{\mu>t^e} \sum_{(a,b)\in K_\mu(t)} \frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)} = O(t^{2n-e/2}\log^{n-1}(t)). \tag{3.17}$$

The summand $S_1(t)$ agrees with the sum in equation (3.13) except that it does not count the pairs (a,b) in $K_\mu(t)$ for $\mu > t^e$. These exceptions went into $S_3(t)$ and can be subsumed into 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 1.2.

4. Counting Lattice Points

4.1. Homogeneous Counting Problems.

Proposition 4.1. *Let* $\mathrm{cov}(a,b)$ *be the covolume of the lattice* $L = \mathbf{O}_K(a,b)$ *as before and write* $e_i = 1$ *if* σ_i *is real,* $e_i = 2$ *otherwise. 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 constant C *independent of* (a,b) *such that* L *has a fundamental domain with diameter less than* $C\mathrm{cov}(a,b)^{1/n}$.

Proof. The evaluation of $\mathrm{cov}(a,b)$ is fairly straightforward and we omit it here. For details, see [16]. For the second assertion, start with the fact that there exists a constant $C' > 0$, independent of L, and at least one nonzero vector $\mathbf{v} \in L$ such that $\mathrm{ht}(\mathbf{v}) \le C'\mathrm{cov}(a,b)^{1/n}$. This follows for example from Theorem 29 in [18] and the commensurability of $\mathrm{ht}(.)$ with the maximum norm on V. By definition of L, there exists $r \in \mathbf{O}_K$ such that $\mathbf{v} = r(a,b)$. For any fixed $\mathbb{Z}$-basis $c_1,\dots,c_n$ of $\mathbf{O}_K$, the vectors

$$c_i\mathbf{v} = c_i r(a,b) \qquad \text{for } i = 1,\dots,n$$

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 $O(\mathrm{cov}(a,b)^{1/n})$, containing at least one fundamental parallelotope for L. □

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

Proposition 4.2. *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. Since $a\mathbf{O}_K + b\mathbf{O}_K = \mathbf{O}_K$, there It is

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

This is a Proposition Let U be the subspace of V^2 spanned by L, and the unit cube in V^2. Define the

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

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

$$\mathrm{Vol}_n((t\mathbb{B} - (c_0,d_0)) \cap U) = t^n \mathrm{Vol}_n((\mathbb{B} - t^{-1}(c_0,d_0)) \cap U) = O(t^n) \tag{4.1}$$

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 4.1, it is possible to do this with a constant C independent of (a,b). From Proposition 4.1, 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 $\mathrm{diam}(F)$.

$$\begin{aligned} \mathrm{diam}(F) &\leq C\mathrm{cov}(L)^{\frac{1}{n}} \leq C\mathrm{cov}(\mathbf{O}_K)^{\frac{1}{n}} \sqrt{\mathrm{ht}(a)^2 + \mathrm{ht}(b)^2} \\ &= O(\mathrm{ht}(a,b)). \end{aligned} \tag{4.2}$$

Now compare the number $N(t)$ to the volume of $(t\mathbb{B} - (c_0,d_0)) \cap U$. From (4.1) and (4.2) follows

$$\begin{aligned} N(t)\mathrm{Vol}_n(F) &\leq \mathrm{Vol}_n(((t + \mathrm{diam}(F))\mathbb{B} - (c_0,d_0)) \cap U) \\ &= O((t + \mathrm{ht}(a,b))^n). \end{aligned} \tag{4.3}$$

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 4.2. □

Theorem 4.3. *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

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

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

For a proof, see [16]. 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 4.4. *For every $\varepsilon > 0$, let*

$$C_{K,\varepsilon} := \frac{1}{\zeta_K(2)\mathrm{cov}(\mathbf{O}_K)^3} \int_{\mathbb{B}\cap N_\varepsilon} \mathrm{g}(x)\, dx \tag{4.4}$$

with the set H_x as defined in (3.3), $\mathrm{g}(x) := |N_{K/\mathbb{Q}}(x)|\mathrm{Vol}(H_x)$ 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 $\gamma < 1$

$$\frac{1}{\mathrm{cov}(\mathbf{O}_K)^2} \sum_{a\in N_\varepsilon} \phi(a)\mathrm{Vol}(H_a) = C_{K,\varepsilon} t^{2n} + O\left(t^{2n-\gamma}\right) \tag{4.5}$$

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 $\mathbb{Z}$, μ_K helps to write $\phi(a)$ as a sum over all ideals I dividing (a),

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

Insert this into (4.5) and use that $N_{K/\mathbb{Q}}(.)$ is strongly multiplicative. Reverse the order of summation. An analogue of Theorem 4.3 gives

$$\begin{aligned} \sum_{a\in I\cap N_\varepsilon} \mathrm{g}(a) = {} & \frac{t^{2n}}{N_{K/\mathbb{Q}}(I)\mathrm{cov}(\mathbf{O}_K)} \int_{\mathbb{B}\cap N_\varepsilon} \mathrm{g}(x)\, dx \\ & + O(N_{K/\mathbb{Q}}(I)^{1-\eta} t^{2n-\gamma}) \end{aligned} \tag{4.6}$$

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 4.1. See [16] for details. Finally, multiplying (4.6) by $\mu_K(I)/N_{K/\mathbb{Q}}(I)$ and summing it over all ideals I produces equation (4.5) and in particular the factor $1/\zeta_K(2)$. □

4.2. Non-Homogeneous Counting Problems.

The goal of the subsection is to prove Theorem 4.5 and Proposition 4.8. 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 4.5. *Recall the set $K_e(t)$ defined in (3.9) and the constant C_K defined in (3.12). For all $0 < e < 1$ and all $\gamma < e/2$,*

$$\frac{1}{\mathrm{cov}(\mathbf{O}_K)^2} \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a) = C_K t^{2n} + O(t^{2n-\gamma}). \tag{4.7}$$

Proof. Since the implicit constant in the error term of Theorem 4.4 does not depend on ε, we may substitute $\varepsilon = t^{-e}$. For this value of ε, $K_e(t)$ is contained in the set N_ε defined in Theorem 4.4. 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 $|N_{K/\mathbb{Q}}(x)| \geq t^{-e/2}\mathrm{ht}(x)^n$, the latter 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

$$\begin{aligned} S(t,e) &\geq \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a), \\ S(t,e/2) &\leq O(t^{n+e/2}) + \sum_{a \in K_e(t)} \phi(a)\mathrm{Vol}(H_a). \end{aligned} \tag{4.8}$$

The O-term in the second inequality comes from summing $\phi(a)\mathrm{Vol}(H_a)$ over those $a \in N_\varepsilon$ of small height which are not in $K_e(t)$, using

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

From Theorem 4.4, we get the asymptotic behavior of $S(t,e)$ as

$$S(t,e) = \mathrm{cov}(\mathbf{O}_K)^3 C_{K,\varepsilon} t^{2n} + O(t^{2n-\gamma}) \quad \text{with } \varepsilon = t^{-e} \tag{4.9}$$

and similarly for $S(t,e/2)$. The last ingredient is

$$0 \leq C_K - C_{K,\varepsilon} \ll \varepsilon |\log^n(\varepsilon)|. \tag{4.10}$$

This is a tedious, but elementary calculation which requires transforming the integrals involved using polar and then logarithmic coordinates. The estimates (4.8)-(4.10) together complete the proof of Theorem 4.5. □

Note that by establishing the inequality (4.10) we have shown that C_K is actually finite, even though it is defined by an improper integral.

Lemma 4.6. *Let K be a number field of degree n and let $0 \leq \alpha < n$ be fixed. Then*

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

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 $N_{K/\mathbb{Q}}(I) \leq t^\alpha$ 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 4.7. *Let K be a number field of degree n and $\mathrm{cov}(a,b)$ the covolume of the lattice $\mathbf{O}_K(a,b)$ as before. We claim that for any $0 \leq \alpha < n$ and any $C > 0$*

$$\#\{(a,b) \in \mathbf{O}_K^2 : \ \mathrm{cov}(a,b) \leq Ct^\alpha, \ \mathrm{ht}(a,b) \leq t\} = O(t^{2\alpha} \log^{n-1}(t)). \tag{4.11}$$

Proof. 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 $C_1 > 0$,

$$\left|\sigma_i(a) \pm \sigma_i(b)\sqrt{-p}\right| \leq |\sigma_i(a)| + \sqrt{p}|\sigma_i(b)| \leq C_1\sqrt{|\sigma_i(a)|^2 + |\sigma_i(b)|^2} \tag{4.12}$$

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

$$|N_{L/\mathbb{Q}}(x)| = |N_{L/\mathbb{Q}}(a + b\sqrt{-p})| \leq C_1^{2n}\mathrm{cov}(a,b)^2. \tag{4.13}$$

Now $\mathrm{ht}(a,b) \leq t$ implies $\mathrm{ht}(x) \leq (1+\sqrt{p})t$. In view of inequality (4.13), $\mathrm{cov}(a,b) \leq Ct^\alpha$ implies $|N_{L/\mathbb{Q}}(x)| \leq C_2 t^{2\alpha}$ 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 4.6 with L, C_2 and 2α in place of K, C and α, respectively. This gives the required estimate. □

Proposition 4.8. *Let* $\mathrm{cov}(a,b)$ *be the covolume of* $\mathbf{O}_K(a,b)$ *as in Proposition 4.1. For any given* $e > 0$,

$$\sum_{\substack{\mathrm{ht}(a,b) \le t \\ \mathrm{cov}(a,b) \le t^{n-e}}} \frac{\mathrm{ht}(a,b)^n}{\mathrm{cov}(a,b)} = O(t^{2n-e/2} \log^{n-1}(t)) \tag{4.14}$$

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

Proof. For any $0 \le \alpha < \beta < n$, consider the subsum $S_{\alpha,\beta}$ of the one in equation (4.14), ranging only over those summands satisfying

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

In view of Lemma 4.7,

$$S_{\alpha,\beta} = O(t^{2\beta+n-\alpha} \log^{n-1}(t)). \tag{4.15}$$

Now cover the interval $[0, n-e]$ by finitely many intervals $[\alpha_j, \beta_j]$ of length at most $e/2$. The maximum of all β_j is therefore $n-e$. For each corresponding subsum S_{α_j,β_j}, the exponent in equation (4.15) 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 4.8. □

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 (3.2). Using the fact that the function ht(.) satisfies the triangle inequality, we get for these matrices

$$|\mathrm{ht}(bc/a) - \mathrm{ht}(a)| \le \mathrm{ht}(1/a). \tag{4.16}$$

Proposition 4.9. *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 1.2.*

Proof. 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 1.2. For $a \notin K_e(t)$, look again at the proof of Theorem 4.5. 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 1.2. □

Proposition 4.10. *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 1.2.*

Proof. Consider first all matrices $A \in \mathrm{SL}_2(\mathbf{O}_K)$ 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 (3.3). The same argument as before gives a main term involving the volume of this boundary, namely zero, and an error term as before. Then consider all matrices such that $\mathrm{ht}(a) = \mathrm{ht}(d) > \mathrm{ht}(b), \mathrm{ht}(c)$. This leads to inequality (4.16), and matrices satisfying (4.16) have already been dealt with in Proposition 4.9. □

5. Uniform Distribution

The statement of Theorem 5.4 means that *the set of pairs $(b/a, c/a)$ used to define m_a in (3.4) 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 5.4, we will need certain *generalized Kloosterman sums.*

The bound for these sums given in Corollary 5.3 will not only be used for proving Theorem 5.4. We will rely directly on this bound rather than Theorem 5.4 to obtain the error term in equation (3.13). Now let us define the aforementioned Kloosterman sums.

Definition 5.1. Consider the symmetric bilinear form $\langle .,. \rangle$ on V defined by

$$\langle u, v \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(uv). \tag{5.1}$$

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 5.2. *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 is a fractional ideal with bounded denominator).

A proof may be found in [2, section 5]. In fact, [2] makes a far more precise statement. In related work, [12] gives a more general uniform distribution result about rational functions in arbitrarily many variables, and [14] studies the angular distribution of $K(u,v;a)$. The hypothesis in Theorem 5.2 that both of u,v 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 [13]. For fixed $u,v \in \widehat{\mathbf{O}}_K$, we have therefore the corollary

Corollary 5.3. *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 5.4. *Recall the sampling functional m_a defined in (3.4). It satisfies for all Riemann-integrable functions f on V^2 with compact support*

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

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,

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

Proof. Use the *Weyl criterion*, see [9] or [10]. 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 factor $\mathrm{cov}(\mathbf{O}_K)^2/\phi(a)$, the value of the sampling functional m_a at this character is precisely the Kloosterman sum $K(u,v;a)$. Corollary 5.3, together with the Weyl criterion implies the statement of Theorem 5.4. □

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 (3.4), maximized over all cubes inside the fundamental domain F^2 for $V^2/\mathbf{O}_K^2$.

The following theorem of [8] has been adapted to our situation. It shows how the discrepancy gives a bound on the approximation error in (3.7) which depends only mildly on H_a.

Theorem 6.1 (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*

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

In order to apply Theorem 6.1 to all sets H_a defined in (3.3) simultaneously, we need a uniform bound on the number h.

Proposition 6.2. *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. 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 estimate for Kloosterman sums quoted in Corollary 5.3 and the famous inequality of Erdös/Turán/Koksma. 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 $(\mathbb{R}/\mathbb{Z})^s$.

$$D(A) \leq \frac{2^s \cdot 300}{M} + 30^s \sum_{0 \neq |h| \leq M} m_A(\chi_h) R(h)^{-1} \tag{6.1}$$

where we have written

$$h = (h_1, \ldots, h_s) \in \mathbb{Z}^s,$$
$$|h| = \max(|h_1|, \ldots, |h_s|),$$
$$R(h) = \prod_{j=1}^{s} \max(1, |h_j|),$$

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 $bc \equiv 1 \pmod{a}$. Then the sum $m_a(\chi_h)$ is just $K(u, v; a)/\phi(a)$. Estimate the second summation in (6.1) by taking the absolute value of each summand and use the bound from Corollary (5.3) 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

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

$$\ll \frac{1}{M} + M^{2n+n/2-1} |N_{K/\mathbb{Q}}(a)|^{-1/2+\varepsilon}. \tag{6.2}$$

The optimal choice for M balances the two summands of the right-hand side of (6.2), so put $M = [|N_{K/\mathbb{Q}}(a)|^{(1-2\varepsilon)/(5n)}]$. Rewriting this, we get for every $\delta < 1/(5n)$

$$D(a) = O\left(|N_{K/\mathbb{Q}}(a)|^{-\delta}\right). \tag{6.3}$$

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 6.1 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 6.3. *For all $0 \neq a \in \mathbf{O}_K$, the error in equation (3.7) is bounded by*

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

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

7. Calculation of a Volume

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 define

$$\|x, y\|_2 := \max_i \{|x_i|^2 + |y_i|^2\}.$$

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.

Theorem 7.1. *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. Write out the conditions defining $K(\varepsilon, \delta, \underline{e})$ in coordinates. These are

$$\begin{aligned} \prod_{i=1}^{k} (|x_i|^2 + |y_i|^2)^{e_i/2} &\leq \varepsilon \|x,y\|_2^n, \\ \prod_{i=1}^{k} |x_i|^{e_i} &\leq \delta \|x,y\|_2^n, \\ \|x,y\|_2 &\leq 1. \end{aligned} \tag{7.1}$$

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

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

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

$$C(\varepsilon, \delta, \underline{e}) := \left\{(x,y) : \ 0 < x_i, y_i < 1, \ \begin{array}{r} \prod_{i=1}^k (x_i^2 + y_i^2)^{e_i/2} \leq \varepsilon \|x,y\|_2^n, \\ \prod_{i=1}^k x_i^{e_i} \leq \delta \|x,y\|_2^n \end{array} \right\}. \tag{7.2}$$

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

$$E := \left\{ (s, \theta) \in \mathbb{R}^{2k} : \begin{array}{c} 0 \le s_k \le \ldots \le s_1 \le 1,\ 0 \le \theta_i \le \pi/2, \\ \prod_{i=1}^{k} s_i^{e_i} < \varepsilon,\ \prod_{i=1}^{k} (s_i \cos(\theta_i))^{e_i} \le \delta \end{array} \right\},$$

$$g(\varepsilon, \delta) := g_{\underline{e}}(\varepsilon, \delta) := \int_E \prod_{i=1}^{k} s_i^{2e_i - 1} (\cos(\theta_i) \sin(\theta_i))^{e_i - 1} \, dV.$$

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

$$\frac{1}{ck!} \mathrm{Vol}_{2n}(K(\varepsilon, \delta, \underline{e})) = g(\varepsilon, \delta). \tag{7.3}$$

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

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 $(e_2, \ldots, e_k)$ (the 'tail' of $\underline{e}$), so that $\tilde{g}$ has two fewer variables than g. There is an obvious recurrence relation between g and $\tilde{g}$,

$$g(\varepsilon, \delta) = \int_0^1 \int_0^{\pi/2} s^{2e_1 - 1} (\cos(\theta) \sin(\theta))^{e_1 - 1} \tilde{g}\left(\frac{\varepsilon}{s^{e_1}}, \frac{\delta}{s \cos(\theta))^{e_1}} \right) d\theta \, ds. \tag{7.4}$$

Write $\tilde{h}$ for the partial derivative of $\tilde{g}$ with respect to ε, h for that of g. From (7.4) 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 $\tilde{h}$,

(7.5)
$$h(\varepsilon,\delta) = \int_0^1 \int_0^{\pi/2} s^{e_1-1}(\cos(\theta)\sin(\theta))^{e_1-1}\tilde{h}\left(\varepsilon/s^{e_1}, \delta/(s\cos(\theta))^{e_1}\right) d\theta\, ds$$

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

(7.6)
$$\tilde{h}(\varepsilon,\delta) = O(\min\{1, \delta\log_+(1/\delta)^m\})$$

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 (7.5) to

(7.7)
$$h(\varepsilon,\delta) = \int_0^1 \int_0^1 su\,\tilde{h}(\varepsilon/s^2, \delta/(su)^2)\, du\, ds.$$

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 (7.7), 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 (7.6), 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

The following problems are closely related to the one treated in this paper.

(1) Counting elements of $\mathrm{GL}_2(\mathbf{O}_K)$
In [16], we show for the number $\mathrm{GL}_2(\mathbf{O}_K, t)$ of matrices in $\mathrm{GL}_2(\mathbf{O}_K)$ with height less than t

(8.1)
$$t^{2n}\log^r(t) \ll \mathrm{GL}_2(\mathbf{O}_K, t) \ll t^{2n}\log^r(t)$$

with $r = r_K + s_K - 1$ being the $\mathbb{Z}$-rank of the group of units ${\mathbf{O}_K}^*$.

(2) Counting units in integral group rings
Given a finite group Γ, one can consider

$$\mathbb{Z}\Gamma^*(t) := \#\{u \in \mathbb{Z}\Gamma^* : \ \mathrm{ht}(u) \le t\}$$

where $\mathrm{ht}(u)$ is the maximum absolute value of the coefficients of u with respect to the basis of $\mathbb{Z}\Gamma$ consisting of the group elements. If the group Γ is 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

$$\bigoplus \mathrm{GL}_{m_i}(\mathbf{O}_{Ki}) \tag{8.2}$$

and the image has finite index. If at least one of $\mathbf{O}_{Ki} = \mathbb{Z}$ or $m_i = 2$ is true for all i then the result of [4] quoted here as theorem 1.1 and our result 8.1 imply immediately

$$t^N \log(t)^R \ll \mathbb{Z}\Gamma^*(t) \ll t^N \log(t)^R \tag{8.3}$$

where N, R are the sums of the numbers $(n_i^2 - n_i)m_i$ and $\mathrm{rk}(\mathbf{O}_{K_i}^*)$, respectively. A more precise result on $\mathrm{GL}_2(\mathbf{O}_K)$ would also mean progress with the problem of counting units in group rings.

(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 [3], [5], [7], and [6]. We have an asymptotic result for K not real, $\Gamma = S_3$, see [15]. The proof is based on the bijection with $\mathbb{Z}\Gamma^*$ and uses uniform distribution.

9. Conclusion

The methods presented here are certainly inferior to those of [4] 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.

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.

There is hope that our methods will give at least an asymptotic result for the group $\mathrm{GL}_2(\mathbf{O}_K)$. However, the natural approach - use Theorem 1.2 to count all matrices with a fixed determinant u and then sum the asymptotics - fails if there are infinitely many units u in $\mathbf{O}_K$.

10. Acknowledgements

I am much indebted to Professor S J Patterson, Goettingen, for support and helpful discussions, to Iowa State University for a reduced teaching

load and to Professor G R Everest, Norwich, who supervised my doctoral thesis.

References

[1] A. F. BEARDON, *The geometry of discrete groups.* Springer, 1983.
[2] R. W. BRUGGEMAN, R. J. MIATELLO, *Estimates of Kloosterman sums for groups of real rank one.* Duke Math. J. **80** (1995), 105–137.
[3] C. J. BUSHNELL, *Norm distribution in Galois orbits.* J. reine angew. Math. **310** (1979), 81–99.
[4] W. DUKE, Z RUDNICK. P. SARNAK, *Density of integer points on affine homogeneous varieties.* Duke Math. J. **71** (1993), 143–179.
[5] G. EVEREST, *Diophantine approximation and the distribution of normal integral generators.* J. London Math. Soc. **28** (1983), 227–237.
[6] G. EVEREST, *Counting generators of normal integral bases.* Amer. J. Math. **120** (1998), 1007–1018.
[7] G. EVEREST, K. GYÖRY, *Counting solutions of decomposable form equations.* Acta Arith. **79** (1997), 173–191.
[8] E. HLAWKA, *Funktionen von beschränkter Variation in der Theorie der Gleichverteilung (German).* Ann. Mat. Pura Appl., IV. Ser. (1961), 325–333.
[9] E. HLAWKA, *Theorie der Gleichverteilung.* Bibliographisches Institut, Mannheim 1979.
[10] L. KUIPERS AND H. NIEDERREITER, *Uniform distribution of sequences.* Wiley, New York 1974.
[11] P. LAX AND R. PHILLIPS, *The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces.* J. Funct. Anal. **46** (1982), 280–350.
[12] R. W. K. ODONI, P. G. SPAIN, *Equidistribution of values of rational functions* (mod p). Proc. R. Soc. Edinb. Sect. A **125** (1995), 911–929.
[13] I. PACHARONI, *Kloosterman sums on number fields of class number one.* Comm. Algebra **26** (1998), 2653–2667.
[14] S. J. PATTERSON, *The asymptotic distribution of Kloosterman sums.* Acta Arith. **79** (1997), 205–219.
[15] C. ROETTGER, *Counting normal integral bases in complex S_3-extensions of the rationals.* Tech. Rep. **416**, University of Augsburg, 1999.
[16] C. ROETTGER, *Counting problems in algebraic number theory.* PhD thesis, University of East Anglia, Norwich, 2000.
[17] P. SAMUEL, *Algebraic Number Theory.* Hermann, Paris 1970.
[18] C. L. SIEGEL, *Lectures on the geometry of numbers.* Springer, 1989.

Christian ROETTGER
Iowa State University
396 Carver Hall
50011 Ames, IA
E-mail : roettger@iastate.edu
URL: http://www.public.iastate.edu/~roettger