Journal de Théorie des Nombres
de Bordeaux **16** (2004), 197–214

The distribution of powers of integers in algebraic number fields

par Werner Georg NOWAK et Johannes SCHOISSENGEIER

Résumé. Pour tout corps de nombres K (non totalement réel), se pose la question de déterminer le nombre de puissances p-ièmes d'entiers algébriques γ de K, vérifiant $\mu(\tau(\gamma^p)) \leq X$, ceci pour tout plongement τ de K dans le corps des nombres complexes. Ici, X est un paramètre réel grand, p est un entier fixé ≥ 2 et $\mu(z) = \max(|\mathrm{Re}(z)|, |\mathrm{Im}(z)|)$ (z, nombre complexe). Ce nombre est évalué asymptotiquement sous la forme $c_{p,K}X^{n/p}+R_{p,K}(X)$, avec des estimations précises sur le reste $R_{p,K}(X)$. La démonstration utilise des techniques issues de la théorie des réseaux, dont en particulier la généralisation multidimensionnelle, donnée par W. Schmidt, du théorème de K.F. Roth sur l'approximation des nombres algébriques par les nombres rationnels.

Abstract. For an arbitrary (not totally real) number field K of degree ≥ 3, we ask how many perfect powers γ^p of algebraic integers γ in K exist, such that $\mu(\tau(\gamma^p)) \leq X$ for each embedding τ of K into the complex field. (X a large real parameter, $p \geq 2$ a fixed integer, and $\mu(z) = \max(|\mathrm{Re}(z)|, |\mathrm{Im}(z)|)$ for any complex z.) This quantity is evaluated asymptotically in the form $c_{p,K}X^{n/p} + R_{p,K}(X)$, with sharp estimates for the remainder $R_{p,K}(X)$. The argument uses techniques from lattice point theory along with W. Schmidt's multivariate extension of K.F. Roth's result on the approximation of algebraic numbers by rationals.

1. Introduction and statement of results

In the context of computer calculations on Catalañ's problem in $\mathbb{Z}[i]$, Opfer and Ripken [18] raised questions about the distribution of p-th powers of Gaussian integers ($p \geq 2, p \in \mathbb{Z}$ fixed). In particular, they asked for their number $\mathcal{M}_p(X)$ in a square $\{z \in \mathbb{C} \,:\, \mu(z) \leq X\}$, where

$$\mu(z) := \max\{|\mathrm{Re}(z)|, |\mathrm{Im}(z)|\}, \tag{1.1}$$

Manuscrit reçu le 7 octobre 2002.

X a large real parameter. While Opfer and Ripken gave only the crude bound $\mathcal{M}_p(X) \ll X^{2/p}$, H. Müller and the first named author [14] undertook a thorough analysis of the problem. They reduced it to the task to evaluate the number $A_p(X)$ of lattice points (of the standard lattice $\mathbb{Z}^2$) in the linearly dilated copy $X^{1/p}\mathcal{D}_p$ of the planar domain

$$\mathcal{D}_p := \{(\xi,\eta) \in \mathbb{R}^2 : \ \mu((\xi+\eta i)^p) \le 1\}. \tag{1.2}$$

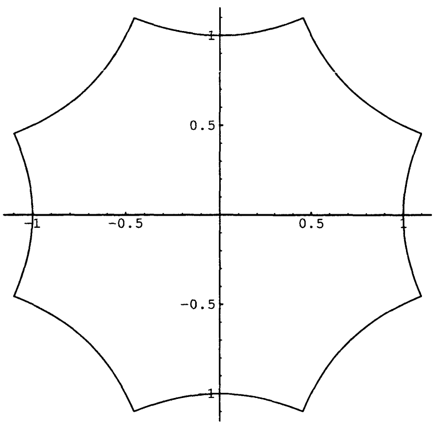

FIG. 1 : The domain $\mathcal{D}_2$

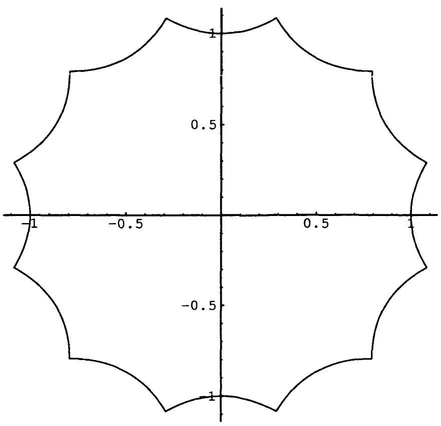

FIG. 2 : The domain $\mathcal{D}_3$

In fact,

$$\mathcal{M}_p(X) = \frac{1}{\gcd(4,p)}\left(A_p(X^{1/p}) - 1\right) + 1 = \frac{\operatorname{area}(\mathcal{D}_p)}{\gcd(4,p)} X^{2/p} + \mathcal{R}_p(X), \tag{1.3}$$

where $\mathcal{R}_p(X)$ is a certain error term. The area of $\mathcal{D}_p$ is readily computed (supported, e.g., by *Mathematica* [22]) as

$$\begin{aligned}\operatorname{area}(\mathcal{D}_p) &= 4\int_0^{\frac{\pi}{4}} (\cos(w))^{-2/p}\,\mathrm{d}w \\ &= \frac{4p\sqrt{\pi}\,\Gamma(\frac{3}{2}-\frac{1}{p})}{(p-2)\Gamma(1-\frac{1}{p})} - \frac{2^{2+1/p}p}{p-2}\,{}_2F_1\left(\frac{1}{2},1;\frac{3}{2}-\frac{1}{p};-1\right)\end{aligned}$$

for $p > 2$, resp., $\operatorname{area}(\mathcal{D}_2) = 4\log(1+\sqrt{2}) = 3.52549\ldots$. Here ${}_2F_1$ denotes the *hypergeometric function*

$${}_2F_1(a_1,a_2;b;z) = \sum_{k=0}^{\infty} \frac{(a_1)_k(a_2)_k}{(b)_k}\frac{z^k}{k!}, \qquad (a)_k = \prod_{1\le j\le k}(a-1+j).$$

Using deep tools from the theory of lattice points[1], in particular those due to Huxley [3], [4], it was proved in [14] that

$$\mathcal{R}_p(X) \ll X^{\frac{1}{p}\frac{46}{73}} (\log X)^{315/146}\,, \tag{1.4}$$

and

$$\limsup_{X\to\infty} \left(\frac{\mathcal{R}_p(X)}{X^{1/(2p)}(\log X)^{1/4}} \right) > 0\,. \tag{1.5}$$

Furthermore,

$$\mathcal{R}_p(X) \ll X^{1/(2p)} \qquad \textit{in mean}-\textit{square}\,, \tag{1.6}$$

as was discussed in detail in [17].

Kuba [7] – [11] generalized the question to squares of integer elements in hypercomplex number systems like quarternions, octaves, etc.

In this paper we consider the – apparently natural – analogue of the problem in an algebraic number field K, not totally real, of degree $[K:\mathbb{Q}] = n \geq 3$. (The case of an arbitrary *imaginary quadratic* field K can be dealt with in the same way as that of the Gaussian field, as far as the O-estimate (1.4) is concerned.) Again for a fixed exponent $p \geq 2$ and large real X, let $\mathcal{M}_{p,K}(X)$ denote the number of $z \in K$ with the following properties:

(i) There exists some algebraic integer $\gamma \in K$ with $\gamma^p = z$,

(ii) For each embedding τ of K into $\mathbb{C}$,

$$\mu(\tau(z)) \leq X\,.$$

Our objective will be to establish an asymptotic formula for $\mathcal{M}_{p,K}(X)$.

Theorem. *For any fixed exponent $p \geq 2$, and any not totally real number field K of degree $[K:\mathbb{Q}] = n \geq 3$,*

$$\mathcal{M}_{p,K}(X) = \frac{2^{r+s}(\mathrm{area}(\mathcal{D}_p))^s}{\gcd(p, w_K)\sqrt{|\mathrm{disc}(K)|}} X^{n/p} + \mathcal{R}_{p,K}(X)\,,$$

where w_K is the number of roots of unity in K, r the number of real embeddings $K \to \mathbb{R}$, $s = \frac{1}{2}(n-r)$, and disc(K) *the discriminant of K. The error term $\mathcal{R}_{p,K}(X)$ can be estimated as follows:*

If K is ”totally complex”, i.e., $r = 0$,

$$\mathcal{R}_{p,K}(X) \ll \begin{cases} X^{\frac{1}{p}\left(n-1-\frac{3}{2n-5}\right)+\epsilon} & \text{for } n \leq 6, \\ X^{\frac{1}{p}\left(n-\frac{4}{3}\right)} & \text{for } n > 6. \end{cases}$$

If $r \geq 1$,

$$\mathcal{R}_{p,K}(X) \ll X^{\frac{1}{p}\left(n-1-\frac{1}{n-2}\right)+\epsilon}\,,$$

[1] For an enlightening presentation of the whole topic the reader is recommended to the monographs of Krätzel [5] and [6].

where throughout $\epsilon > 0$ is arbitrary but fixed. The constants implied in the $\ll$-symbol may depend on p, K and ϵ.

Remarks. Our method of proof uses techniques from the theory of lattice points in domains with boundaries of nonzero curvature[2], along with tools from Diophantine approximation. It works best for $n = 3$ and for $n = 4$, K totally complex. The bounds achieved in these two cases read $X^{\frac{1}{p}+\epsilon}$, resp., $X^{\frac{2}{p}+\epsilon}$. The first one significantly improves upon the estimate $O\left(X^{\frac{1}{p}\frac{11}{7}+\epsilon}\right)$ which had been established in [12]. The result for $r = 0$, $n > 6$ is somewhat crude (and, by the way, independent of our Diophantine approximation techniques). Using a more geometric argument and plugging in Huxley's method, this most likely can be refined to $X^{\frac{1}{p}(n-\frac{100}{73})+\epsilon}$.

2. Auxiliary results and other preliminaries

First of all, we reduce our task to a lattice point problem. To this end, we have to take care of multiple solutions of the equation $\gamma^p = z$. Since, as is well-known (cf., e.g., Narkiewicz [16], p. 100), the set of *all* roots of unity in an algebraic number field K forms a cyclic group (of order w_K, say), it is simple to see that K contains just $\gcd(p, w_K)$ p-th roots of unity, for any fixed $p \geq 2$. Therefore, if we define $A_{p,K}(X)$ as the number of algebraic integers in $\gamma \in K$ with the property that $\mu(\tau(\gamma^p)) \leq X$ for each embedding $\tau : K \to \mathbb{C}$, it readily follows that

$$\mathcal{M}_{p,K}(X) = \frac{1}{\gcd(p, w_K)} \left(A_{p,K}(X) - 1\right) + 1 . \tag{2.1}$$

Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ the complex embeddings of K into $\mathbb{C}$. Further, let $\Gamma = (\alpha_1, \ldots, \alpha_n)$ be a fixed (ordered) integral basis of K. For $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{R}^n$, we define linear forms

$$\Lambda_j(\mathbf{u}) = \sum_{k=1}^{n} \sigma_j(\alpha_k) u_k , \qquad j = 1, \ldots, r+s ,$$

and

$$\Phi_j(\mathbf{u}) = \operatorname{Re} \Lambda_j(\mathbf{u}) , \quad \Psi_j(\mathbf{u}) = \operatorname{Im} \Lambda_j(\mathbf{u}) , \qquad j = r+1, \ldots, r+s .$$

Obviously, $A_{p,K}(X)$ is the number of lattice points (of the standard lattice $\mathbb{Z}^n$) in the linearly dilated copy $X^{1/p}\mathcal{B}_p$ of the body

$$\begin{aligned}\mathcal{B}_p &= \{\mathbf{u} \in \mathbb{R}^n : \ \mu(\Lambda_j(\mathbf{u})^p) \leq 1 , \ j = 1, \ldots, r+s \,\} \\ &= \left\{\mathbf{u} \in \mathbb{R}^n : \begin{array}{ll} |\Lambda_j(\mathbf{u})| \leq 1 , & 1 \leq j \leq r \\ (\Phi_j(\mathbf{u}), \Psi_j(\mathbf{u})) \in \mathcal{D}_p , & r+1 \leq j \leq r+s \end{array}\right\} .\end{aligned}$$

[2] Cf. again the books of Krätzel [5], [6].

In our argument, we shall need the linear transformations[3]

$$\mathbf{u} \mapsto \mathbf{v} = (\Lambda_1(\mathbf{u}), \dots, \Lambda_r(\mathbf{u}), \Phi_{r+1}(\mathbf{u}), \Psi_{r+1}(\mathbf{u}), \dots, \Phi_{r+s}(\mathbf{u}), \Psi_{r+s}(\mathbf{u})) =: \mathbf{Mu} \tag{2.2}$$

and

$$\mathbf{u} \mapsto \mathbf{v} = (\Lambda_1(\mathbf{u}), \dots, \Lambda_r(\mathbf{u}), \Lambda_{r+1}(\mathbf{u}), \overline{\Lambda_{r+1}}(\mathbf{u}), \dots, \Lambda_{r+s}(\mathbf{u}), \overline{\Lambda_{r+s}}(\mathbf{u})) =: \mathbf{Cu}\,. \tag{2.3}$$

Let $\mathbf{P} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}$, and define an $(n \times n)$-matrix $\mathbf{P}_{r,s}$ as follows: Along the main diagonal, there are first r 1's, then s blocks $\mathbf{P}$, and all other entries are 0. Then it is simple to see that

$$\mathbf{M} = \mathbf{P}_{r,s}\,\mathbf{C}$$

where $\mathbf{M}, \mathbf{C}$, are defined by (2.2), (2.3), respectively. Since $|\det \mathbf{P}| = \frac{1}{2}$, it is clear that

$$|\det \mathbf{M}| = 2^{-s}\,|\det \mathbf{C}| = 2^{-s}\,\sqrt{|\mathrm{disc}(K)|}\,. \tag{2.4}$$

For any matrix $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$, we shall write $\mathbf{A}^* = {}^t\mathbf{A}^{-1}$ for the *contragradient* matrix. Of course,

$$\mathbf{M}^* = \mathbf{P}^*_{r,s}\mathbf{C}^*\,, \tag{2.5}$$

where $\mathbf{P}^*_{r,s}$ is quite similar to $\mathbf{P}_{r,s}$, only with $\mathbf{P}$ replaced by $\mathbf{P}^* = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$. From this it is easy to verify that the first r rows of $\mathbf{C}^*$ are real and that its $(r+2k)$-th row is the complex conjugate of the $(r+2k-1)$-th row, $k = 1, \dots, s$. Moreover, if we define linear forms $L_j(\mathbf{w})$, $j = 1, \dots, r+s$, and $F_{r+k}(\mathbf{w}), G_{r+k}(\mathbf{w})$, $k = 1, \dots, s$, $\mathbf{w} \in \mathbb{R}^n$, by

$$\begin{aligned}(L_1(\mathbf{w}), \dots, L_r(\mathbf{w}), F_{r+1}(\mathbf{w}), G_{r+1}(\mathbf{w}), \dots, F_{r+s}(\mathbf{w}), G_{r+s}(\mathbf{w})) &:= \mathbf{M}^*\mathbf{w}\,,\\ (L_1(\mathbf{w}), \dots, L_r(\mathbf{w}), L_{r+1}(\mathbf{w}), \overline{L_{r+1}}(\mathbf{w}), \dots, L_{r+s}(\mathbf{w}), \overline{L_{r+s}}(\mathbf{w})) &:= \mathbf{C}^*\mathbf{w}\,,\end{aligned} \tag{2.6}$$

it readily follows from (2.5) that $L_1, \dots, L_r$ are real and, for $j = r+1, \dots, r+s$,

$$F_j(\mathbf{w}) = 2\,\mathrm{Re}\,L_j(\mathbf{w})\,, \qquad G_j(\mathbf{w}) = 2\,\mathrm{Im}\,L_j(\mathbf{w})\,. \tag{2.7}$$

Moreover, since the linear transformation $\mathbf{w} \mapsto \mathbf{C}^*\mathbf{w}$ is non-singular, $\|\mathbf{C}^*\mathbf{w}\|_2$ attains a positive minimum on $\|\mathbf{w}\|_2 = 1$. By homogeneity, for all $\mathbf{w} \in \mathbb{R}^n \setminus \{(0, \dots, 0)\}$,

$$\left(\sum_{j=1}^{r+s} |L_j(\mathbf{w})|^2\right)^{1/2} \gg \|\mathbf{C}^*\mathbf{w}\|_2 \gg \|\mathbf{w}\|_2\,. \tag{2.8}$$

[3] Vectors are always meant as *column vectors* although we write them – for convenience of print – as n-tuples in one line.

A salient point in our argument will be to estimate from below absolute values of the linear forms $L_j(\mathbf{m})$, $\mathbf{m} \in \mathbb{Z}^n$. For this purpose, we need first some information about the linear independence (over the rationals) of their coefficients.

Lemma 1. *For nonnegative integers p, n, denote by*

$$s_p^{(n)} := \sum_{\substack{H\subseteq\{1,\dots,n\}\\ |H|=p}} \prod_{i\in H} X_i$$

the symmetric basic polynomial of index p in the n indeterminates $X_1, \dots, X_n$ (in particular, $s_0^{(n)} = 1$ and $s_p^{(n)} = 0$ for $p > n$). Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field of degree $[K : \mathbb{Q}] = n$, and σ_j, $j = 1, \dots, n$, its embeddings into $\mathbb{C}$. Then the set $\{s_i^{(n-1)}(\sigma_2(\alpha), \dots, \sigma_n(\alpha)) : 0 \le i < n\}$ is linearly independent over $\mathbb{Q}$.

Proof. Choose $x_0, \dots, x_{n-1} \in \mathbb{Q}$ so that

$$(*) \qquad \sum_{i=0}^{n-1} x_i s_i^{(n-1)}(\sigma_2(\alpha), \dots, \sigma_n(\alpha)) = 0.$$

We construct a finite sequence $(p_k)_{k=0}^n$ of polynomials $p_k \in \mathbb{Q}[X]$, by the recursion

$$p_0 = 0, \qquad p_k = \sum_{i=0}^{n-k} x_i s_{i+k}^{(n)}(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) - X p_{k-1} \qquad \text{for } k \ge 1.$$

The sum on the right hand side is always a rational number, and obviously the degree of p_k is $< k$ throughout. We shall show that for $0 \le k \le n$,

$$(**) \qquad \sum_{i=0}^{n-k-1} x_i s_{i+k}^{(n-1)}(\sigma_2(\alpha), \dots, \sigma_n(\alpha)) = p_k(\sigma_1(\alpha)).$$

We use induction on k. For $k = 0$ we simply appeal to $(*)$. Supposing that

$$\sum_{i=0}^{n-k} x_i s_{i+k-1}^{(n-1)}(\sigma_2(\alpha), \dots, \sigma_n(\alpha)) = p_{k-1}(\sigma_1(\alpha))$$

has already been established, we multiply this identity by $\sigma_1(\alpha)$ and use

$$s_{j+1}^{(n)}(X_1, \dots, X_n) - s_{j+1}^{(n-1)}(X_2, \dots, X_n) = X_1 s_j^{(n-1)}(X_2, \dots, X_n)$$

to obtain

$$\sigma_1(\alpha) p_{k-1}(\sigma_1(\alpha)) =$$
$$\sum_{i=0}^{n-k} x_i (s_{i+k}^{(n)}(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) - s_{i+k}^{(n-1)}(\sigma_2(\alpha), \dots, \sigma_n(\alpha)))$$

or, in other terms,

$$\sum_{i=0}^{n-k-1} x_i s_{i+k}^{(n-1)}(\sigma_2(\alpha), ..., \sigma_n(\alpha)) =$$
$$\sum_{i=0}^{n-k} x_i s_{i+k}^{(n)}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) - \sigma_1(\alpha) p_{k-1}(\sigma_1(\alpha)),$$

which, by our recursion formula, yields just $(**)$.Putting $k = n$ in $(**)$ gives $p_n(\sigma_1(\alpha)) = 0$. As $\sigma_1(\alpha)$ has degree n over $\mathbb{Q}$, it follows that $p_n = 0$. By our recursive construction, all p_j vanish identically, $j = 0, \ldots, n$. Let I be the minimal index such that $x_I \neq 0$ in $(*)$. Applying $(**)$ with $k = n-I-1$, we infer that $x_I s_{n-1}^{(n-1)}(\sigma_2(\alpha), \ldots, \sigma_n(\alpha)) = x_I \sigma_2(\alpha) \cdots \sigma_n(\alpha) = 0$, thus $x_I = 0$, hence the assertion of Lemma 1. □

Lemma 2. *Let* $\Gamma = (\alpha_1, \ldots, \alpha_n)$ *be a basis of the number field* K *as a vector space over* $\mathbb{Q}$. *Let the matrix* $\mathbf{A}$ *be defined as* $\mathbf{A} = (a_{j,k})_{1 \leq j,k \leq n} = (\sigma_j(\alpha_k))_{1 \leq j,k \leq n}$, σ_j *the embeddings of* K *into* $\mathbb{C}$. *Then for each row of* $\mathbf{A}^*$, *the* n *elements are linearly independent over* $\mathbb{Q}$.

Proof. W.l.o.g. we may choose notation so that the assertion will be established for the *first* row of $\mathbf{A}^*$. We start with the special case that the basis has the special form $\Gamma_0 = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Then $\mathbf{A}_0 = \left((\sigma_j(\alpha))^{k-1}\right)_{1 \leq j,k \leq n}$ is a Vandermonde matrix, and a little reflection shows[4] that the first row of $\mathbf{A}_0^*$ (which is the first column of $\mathbf{A}_0^{-1}$) is proportional to the vector

$$\left((-1)^k s_{n-k}^{(n-1)}(\sigma_2(\alpha), \ldots, \sigma_n(\alpha))\right)_{1 \leq k \leq n}.$$

By Lemma 1, this is actually linearly independent over $\mathbb{Q}$. If Γ is arbitrary, and $K = \mathbb{Q}(\alpha)$, there exists a nonsingular $(n \times n)$-matrix $\mathbf{R} = (r_{j,k})_{1 \leq j,k \leq n}$, with rational entries, so that $\mathbf{A} = \mathbf{A}_0 \mathbf{R}$, hence also $\mathbf{A}^* = \mathbf{A}_0^* \mathbf{R}^*$. Let us write $\mathbf{A}^* = (a_{j,k}^*)_{1 \leq j,k \leq n}$, $\mathbf{A}_0^* = (\beta_{j,k}^*)_{1 \leq j,k \leq n}$, $\mathbf{R}^* = (r_{j,k}^*)_{1 \leq j,k \leq n}$. Assume that $x_1, \ldots, x_n$ are rational numbers with

$$\sum_{k=1}^{n} x_k a_{1,k}^* = 0.$$

Then

$$0 = \sum_{k=1}^{n} x_k \left(\sum_{j=1}^{n} \beta_{1,j}^* \, r_{j,k}^*\right) = \sum_{j=1}^{n} \beta_{1,j}^* \left(\sum_{k=1}^{n} x_k \, r_{j,k}^*\right).$$

[4] In fact, it is plain to see that, for $j \geq 2$, the j-th row of $\mathbf{A}_0$ is orthogonal to this vector.

Since we have already shown the linear independence of $(\beta^*_{1,1},\dots,\beta^*_{1,n})$, each of the last inner sums must vanish. As $\det(\mathbf{R}^*)\neq 0$, this implies that $x_1=\dots=x_n=0$. □

Lemma 3. *Let $L(\mathbf{m})=c_1m_1+\dots+c_nm_n$ be a linear form whose coefficients are algebraic numbers and linearly independent over $\mathbb{Q}$. Let further $\gamma\geq 1$, $\epsilon>0$ and $c>0$ be fixed, and let Y and M be large real parameters.*
(i) *If L is a real form, it follows that*

$$\sum_{0<\|\mathbf{m}\|_\infty\leq M}\min\left(Y^\gamma,|L(\mathbf{m})|^{-\gamma}\right)\ll Y^{\gamma-1}M^{n-1+\epsilon}.$$

(ii) *If L is not proportional to a real form, then*

$$\sum_{\substack{0<\|\mathbf{m}\|_\infty\leq M,\\ |L(\mathbf{m})|\leq c}}\min\left(Y^\gamma,|L(\mathbf{m})|^{-\gamma}\right)\ll Y^{\gamma-1}M^{n-2+\epsilon}.$$

(iii) *Furthermore, in that latter case,*

$$\sum_{\substack{0<\|\mathbf{m}\|_\infty\leq M,\\ |L(\mathbf{m})|>c}}|L(\mathbf{m})|^{-\gamma}\ll M^{n-\min(\gamma,2)+\epsilon}.$$

Proof. (i) We split up the sum in question as

$$Y^\gamma\sum_{\substack{0<\|\mathbf{m}\|_\infty\leq M,\\ |L(\mathbf{m})|\leq 1/Y}}1+\sum_{\substack{0<\|\mathbf{m}\|_\infty\leq M,\\ |L(\mathbf{m})|>1/Y}}|L(\mathbf{m})|^{-\gamma}=:S_1+S_2.$$

By a celebrated result of W. Schmidt [20] and [21], p. 152, $|L(\mathbf{m})|\gg M^{-(n-1)-\epsilon'}$, under the conditions stated. For $\mathbf{m},\mathbf{m}'\in\mathbb{Z}^n$, $\mathbf{m}\neq\pm\mathbf{m}'$, $\|\mathbf{m}\|_\infty,\|\mathbf{m}'\|_\infty\leq M$, it thus follows that

$$\big||L(\mathbf{m})|-|L(\mathbf{m}')|\big|=\min_{\pm}|L(\mathbf{m}\pm\mathbf{m}')|\geq c'M^{-(n-1)-\epsilon'}=:z$$

for short. (Here we mimick an idea which may be found, e.g., in the book of Kuipers and Niederreiter [13], p. 123.) Hence the real numbers $|L(\mathbf{m})|$, with $\mathbf{m}\in\mathbb{Z}^n$, $0<\|\mathbf{m}\|_\infty\leq M$, have distances $\geq z$ from each other (apart from the fact that $|L(\mathbf{m})|=|L(-\mathbf{m})|$, which does not affect the $\ll$-estimates which follow) and also from $0=|L(0,\dots,0)|$. Therefore,

$$\#\{\mathbf{m}\in\mathbb{Z}^n:\ 0<\|\mathbf{m}\|_\infty\leq M,\ |L(\mathbf{m})|\leq\frac{1}{Y}\}\ll(Yz)^{-1},$$

thus

$$S_1\ll Y^\gamma(Yz)^{-1}\ll Y^{\gamma-1}M^{n-1+\epsilon}.$$

(Note that $S_1 = 0$ if $1/Y < z$.) Furthermore,

$$S_2 \le \sum_{1\le k\ll M^C} \left(\frac{1}{Y}+kz\right)^{-\gamma} \ll z^{-\gamma} \sum_{\substack{1\le \ell\ll M^C,\\ \ell>[(Yz)^{-1}]}} \ell^{-\gamma}$$
$$\ll z^{-1}M^{\epsilon'}Y^{\gamma-1} \ll Y^{\gamma-1}M^{n-1+\epsilon},$$

which gives just the assertion (i). Slightly more general (and useful for what follows), we readily derive the following conclusion: If q is a fixed rational number, $\langle w\rangle$ denotes the distance of the real w from the nearest integer, and $c_1',\dots,c_{n-1}'$ are real algebraic numbers such that $1, c_1',\dots,c_{n-1}'$ are linearly independent over $\mathbb{Q}$, then (with Y, M as before),

$$\sum_{0<|m_j|\le M} \min\left(Y^\gamma, \langle q+c_1'm_1+\dots+c_{n-1}'m_{n-1}\rangle^{-\gamma}\right) \ll Y^{\gamma-1}M^{n-1+\epsilon}. \tag{2.9}$$

(ii) Dealing with the complex case, we put $\nu = n-2$, and may assume w.l.o.g. that $c_{\nu+2} = 1$ and $c_{\nu+1} \notin \mathbb{R}$. For $j = 1,\dots,\nu+1$, we set $a_j = \operatorname{Re} c_j$, $b_j = \operatorname{Im} c_j$, and[5] $\underline{a} = (a_1,\dots,a_\nu)$, $\underline{b} = (b_1,\dots,b_\nu)$, $\underline{m} = (m_1,\dots,m_\nu)$. We notice that

$$|L(\mathbf{m})|^2 = (\underline{a}\cdot\underline{m} + a_{\nu+1}m_{\nu+1} + m_{\nu+2})^2 + (\underline{b}\cdot\underline{m} + b_{\nu+1}m_{\nu+1})^2. \tag{2.10}$$

For $\underline{m} \in \mathbb{Z}^\nu$, we thus choose $m_{\nu+1}^*(\underline{m})$ the nearest integer to $-\underline{b}\cdot\underline{m}/b_{\nu+1}$, then $m_{\nu+2}^*(\underline{m})$ the nearest integer to $-m_{\nu+1}^*(\underline{m})\,a_{\nu+1} - \underline{a}\cdot\underline{m}$. (To be quite precise, the nearest integer to $x \in \mathbb{R}$ is meant to be $[x+\frac{1}{2}]$. Throughout, $\cdot$ denotes the standard inner product.) Accordingly, we define

$$\mathcal{S}_L := \{(m_1,\dots,m_\nu, m_{\nu+1}^*(\underline{m}), m_{\nu+2}^*(\underline{m})) : \underline{m} = (m_1,\dots,m_\nu) \in \mathbb{Z}^\nu\}.$$

The sum to be estimated is therefore

$$\sum_{\substack{0<\|\mathbf{m}\|_\infty\le M,\\ |L(\mathbf{m})|\le c}} \min\left(Y^\gamma, |L(\mathbf{m})|^{-\gamma}\right) \ll \sum_{\substack{0<\|\mathbf{m}\|_\infty\le M,\\ \mathbf{m}\in\mathcal{S}_L}} \min\left(Y^\gamma, |L(\mathbf{m})|^{-\gamma}\right). \tag{2.11}$$

Now consider the group $G := \{\underline{m} \in \mathbb{Z}^\nu : \underline{b}\cdot\underline{m}/b_{\nu+1} \in \mathbb{Z}\}$, and let R denote its rank, $0 \le R \le \nu$. According to Bourbaki [2], chap. VII, § 4, No. 3, p. 18, Theorem 1, there exist a basis $(\underline{e}_1,\dots,\underline{e}_\nu)$ of $\mathbb{Z}^\nu$ and positive integers $g_1,\dots,g_R$, so that $(g_1\,\underline{e}_1,\dots,g_R\,\underline{e}_R)$ is a basis of G, i.e., $G = g_1\,\underline{e}_1\,\mathbb{Z} + \dots + g_R\,\underline{e}_R\,\mathbb{Z}$. Furthermore, each $\underline{m} \in \mathbb{Z}^\nu$ has a (unique) representation

$$\underline{m} = \sum_{j=1}^{R}(h_j + g_jq_j)\underline{e}_j + \sum_{j=R+1}^{\nu} t_j\underline{e}_j, \tag{2.12}$$

[5] Only for the rest of this proof, vectors have less than n components. We symbolize this by writing $\underline{m}$ instead of $\mathbf{m}$, and so on.

where $\underline{h} = (h_1, \dots, h_R) \in \mathbb{Z}^R$, $\underline{q} = (q_1, \dots, q_R) \in \mathbb{Z}^R$, $0 \le h_j < g_j$ for $j = 1, \dots, R$, and $\underline{t} = (t_{R+1}, \dots, t_\nu) \in \mathbb{Z}^{\nu-R}$. Obviously, $\underline{m} \in G$ iff all h_j and t_j vanish. By Cramer's rule, $\|\underline{m}\|_\infty \le M$ implies that also $\left\|\underline{q}\right\|_\infty \ll M$ and $\|\underline{t}\|_\infty \ll M$. As a further simple consequence of (2.12), the numbers 1, $\underline{e}_{R+1} \cdot \underline{b}/b_{\nu+1}, \dots, \underline{e}_\nu \cdot \underline{b}/b_{\nu+1}$ are linearly independent over $\mathbb{Q}$. Since $\sum\limits_{j=1}^{R} h_j\, \underline{e}_j \cdot \underline{b}/b_{\nu+1}$ is rational, we infer from (2.9) (with $n-1$ replaced by $\nu - R$, the t_j taking over the rôle of the m_j in (2.9)), (2.10) (and $|\mathrm{Im}\, z| \le |z|$) that the portion of the right hand side of (2.11) which corresponds to $\underline{m} \notin G$ is

$$\begin{aligned}
&\ll \sum_{\substack{\|\underline{m}\|_\infty \le M,\\ \underline{m} \notin G}} \min\left(Y^\gamma, \left|L(m_1, \dots, m_\nu, m^*_{\nu+1}(\underline{m}),\, m^*_{\nu+2}(\underline{m}))\right|^{-\gamma}\right) \\
&\ll \sum_{\substack{\|\underline{m}\|_\infty \le M,\\ \underline{m} \notin G}} \min\left(Y^\gamma, \langle \underline{b} \cdot \underline{m}\, / b_{\nu+1} \rangle^{-\gamma}\right) \\
&\ll \sum_{\substack{\underline{h} \in \mathbb{Z}^R:\\ 0 \le h_j < g_j}} \sum_{\substack{\|\underline{q}\|_\infty, \|\underline{t}\|_\infty \ll M\\ (\underline{h}, \underline{t}) \ne (0, \dots, 0)}} \min\left(Y^\gamma, \begin{array}{r} \langle \sum_{j=1}^R h_j\, \underline{e}_j \cdot \underline{b}/b_{\nu+1} + \\ \sum_{j=R+1}^\nu t_j\, \underline{e}_j \cdot \underline{b}/b_{\nu+1} \rangle^{-\gamma} \end{array}\right) \\
&\ll Y^{\gamma-1} M^{\nu+\epsilon}, \qquad (2.13)
\end{aligned}$$

since $g_1, \dots, g_R \ll 1$. It remains to deal with the $\underline{m} \in G$. Here (2.12) simplifies to $\underline{m} = \sum\limits_{j=1}^{R} g_j q_j \underline{e}_j$, with $\underline{q}$ unique. Hence, in this case,

$$m^*_{\nu+1}(\underline{m}) = -\underline{b} \cdot \underline{m}/b_{\nu+1} = -\sum_{j=1}^{R} g_j q_j \underline{b} \cdot \underline{e}_j \frac{1}{b_{\nu+1}}\,.$$

Therefore (motivated by a look at (2.10)), we infer that

$$\langle m^*_{\nu+1}(\underline{m}) a_{\nu+1} + \underline{a} \cdot \underline{m} \rangle = \left\langle \sum_{j=1}^{R} g_j q_j \underline{e}_j \cdot \left(\underline{a} - \frac{a_{\nu+1}}{b_{\nu+1}} \underline{b}\right) \right\rangle. \qquad (2.14)$$

We claim that the numbers $\eta_0 := 1\,, \eta_j := \underline{e}_j \cdot \left(\underline{a} - \frac{a_{\nu+1}}{b_{\nu+1}} \underline{b}\right)$ for $1 \le j \le R$, are linearly independent over $\mathbb{Q}$. Write $\underline{e}_j =: (e_{j,1}, \dots, e_{j,R})$ for $1 \le j \le R$. Suppose that $k_0\eta_0 + \dots + k_R\eta_R = 0$ for certain integers $k_0, \dots, k_R$. This is just the real part of the equality

$$k_0 + \sum_{\ell=1}^{\nu} \left(\sum_{j=1}^{R} k_j e_{j,\ell}\right) c_\ell - c_{\nu+1} \sum_{j=1}^{R} k_j \underline{b} \cdot \underline{e}_j \frac{1}{b_{\nu+1}} = 0\,,$$

whose imaginary part is trivial. The last sum is again a rational number. Since $1, c_1, \dots, c_\nu, c_{\nu+1}$ are linearly independent over $\mathbb{Q}$, it follows that $\sum_{j=1}^{R} k_j e_{j,\ell} = 0$ for $\ell = 1, \dots, \nu$, hence $k_1 = \cdots = k_R = 0$, and also $k_0 = 0$.

Therefore, by (2.9) (with R instead of $n-1$), (2.10), and the fact that $|\operatorname{Re} z| \le |z|$, the relevant part of the right hand side sum in (2.11) is

$$\begin{aligned}
&\ll \sum_{\substack{0<\|\underline{\mathrm{m}}\|_\infty \le M,\\ \underline{\mathrm{m}}\in G}} \min\left(Y^\gamma, \left|L(m_1,\dots,m_\nu, m^*_{\nu+1}(\underline{\mathrm{m}}),\, m^*_{\nu+2}(\underline{\mathrm{m}}))\right|^{-\gamma}\right)\\
&\ll \sum_{\substack{0<\|\underline{\mathrm{m}}\|_\infty \le M,\\ \underline{\mathrm{m}}\in G}} \min\left(Y^\gamma, \left\langle m^*_{\nu+1}(\underline{\mathrm{m}}) a_{\nu+1} + \underline{\mathrm{a}}\cdot\underline{\mathrm{m}}\right\rangle^{-\gamma}\right)\\
&= \sum_{0<\|\underline{\mathrm{q}}\|_\infty \ll M} \min\left(Y^\gamma, \left\langle \sum_{j=1}^{R} g_j q_j \underline{\mathrm{e}}_j \cdot \left(\underline{\mathrm{a}} - \frac{a_{\nu+1}}{b_{\nu+1}}\underline{\mathrm{b}}\right)\right\rangle^{-\gamma}\right)\\
&\ll Y^{\gamma-1} M^{R+\epsilon}\,. \qquad (2.15)
\end{aligned}$$

Combining the bounds (2.13) and (2.15), we complete the proof of clause (ii).

(iii) For a further parameter $1 \ll M_1 \ll M$, consider the body

$$W(M, M_1) = \{\mathbf{w} \in \mathbb{R}^n : \ \|\mathbf{w}\|_\infty \le M,\ \tfrac{1}{2}M_1 \le |L(\mathbf{w})| \le M_1\}\,.$$

It is easy to see[6] that $\operatorname{vol}(W(M, M_1)) \ll M_1^2 M^{n-2}$, hence also

$$\#\,(\mathbb{Z}^n \cap W(M, M_1)) \ll M_1^2 M^{n-2}\,.$$

Therefore,

$$\sum_{\mathbf{m}\in W(M,M_1)} |L(\mathbf{m})|^{-\gamma} \ll M_1^{-\gamma}\,\#\,(\mathbb{Z}^n \cap W(M, M_1)) \ll M_1^{2-\gamma} M^{n-2}\,.$$

Finally, we let M_1 range over a dyadic sequence, $1 \ll M_1 \ll M$, and sum up to complete the proof of Lemma 3. □

Lemma 4. *There exist positive constants C_1, C_2, depending only on p and on the integral basis Γ of the number field K, so that for $0 < \omega \le C_1$ the following holds true: For arbitrary points $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ such that $\mathbf{u} \in \mathcal{B}_p$, $\mathbf{v} \notin (1+\omega)\mathcal{B}_p$, it follows that $\|\mathbf{u}-\mathbf{v}\|_2 > C_2\omega$.*

Proof. By definition of $\mathcal{B}_p$, there are two possible cases: Either $|\Lambda_j(\mathbf{v})| > 1 + \omega$ for some $j \in \{1, \dots, r\}$, then

$$|\Lambda_j(\mathbf{u})| + \omega \le 1 + \omega < |\Lambda_j(\mathbf{u}) + \Lambda_j(\mathbf{v}-\mathbf{u})| \le |\Lambda_j(\mathbf{u})| + |\Lambda_j(\mathbf{v}-\mathbf{u})|\,,$$

[6] E.g., by a change of the coordinate system, using a basis of $\mathbb{R}^n$ which contains $(a_1, \dots, a_{\nu+1}, 1)$, $(b_1, \dots, b_{\nu+1}, 0)$, with L as in (2.10).

hence $|\Lambda_j(\mathbf{v}-\mathbf{u})| \geq \omega$, and by Cauchy's inequality

$$\omega \leq \left(\sum_{k=1}^{n} \sigma_j(\alpha_k)^2\right)^{1/2} \|\mathbf{u}-\mathbf{v}\|_2$$

as desired. Or, $\mu(\Lambda_j(\mathbf{v})^p) > 1+\omega$ for some $j \in \{r+1,\dots,r+s\}$, i.e., $(\Phi_j(\mathbf{v}),\Psi_j(\mathbf{v})) \notin (1+\omega)\mathcal{D}_p$. By Lemma D in [17], therefore the Euclidean distance of $(\Phi_j(\mathbf{u}),\Psi_j(\mathbf{u}))$ and $(\Phi_j(\mathbf{v}),\Psi_j(\mathbf{v}))$ is $\geq C\omega$, for appropriate $C>0$. Therefore,

$$C\omega \leq \|(\Phi_j(\mathbf{u}-\mathbf{v}),\Psi_j(\mathbf{u}-\mathbf{v}))\|_2 \leq \left(\sum_{k=1}^{n} |\sigma_j(\alpha_k)|^2\right)^{1/2} \|\mathbf{u}-\mathbf{v}\|_2 \,.$$

□

Lemma 5. *For the region $\mathcal{D}_p$ and arbitrary real numbers T_1, T_2, not both* 0,

$$\iint_{\mathcal{D}_p} e(T_1x+T_2y)\,\mathrm{d}(x,y) \ll (T_1^2+T_2^2)^{-3/4},$$

with $e(w) := e^{2\pi i w}$ as usual.

Proof. This is just (a special case of) Lemma 1 in [12]. □

3. Proof of the Theorem

Like in [12], we employ a method of W. Müller [15], ch. 3, to evaluate the number of lattice points $A_{p,K}(X)$ in the body $X^{1/p}\mathcal{B}_p$. For any fixed positive real N there exists[7] a continuous function $\delta_1 : \mathbb{R}^n \to [0,\infty[$ with the following properties:

(i) The support of δ_1 is contained in the n-dimensional unit ball $\|\mathbf{u}\|_2 \leq 1$.

(ii) $\displaystyle\int_{\mathbb{R}^n} \delta_1(\mathbf{u})\,\mathbf{du} = 1\,.$

(iii) The Fourier transform satisfies

$$\widehat{\delta_1}(\mathbf{w}) := \int_{\mathbb{R}^n} \delta_1(\mathbf{u})e(\mathbf{u}\cdot\mathbf{w})\,\mathbf{du} \ll \min\left(1, \|\mathbf{w}\|_2^{-N}\right) \qquad (\mathbf{w}\in\mathbb{R}^n),$$

where $\mathbf{u}\cdot\mathbf{w}$ denotes the standard inner product. For a small parameter $\omega>0$, we put $\delta_\omega(\mathbf{u}) = \omega^{-n}\delta_1(\omega^{-1}\mathbf{u})$. Then the support of δ_ω is contained in the ball $\|\mathbf{u}\|_2 \leq \omega$, and it follows that

$$\widehat{\delta_\omega}(\mathbf{w}) = \widehat{\delta_1}(\omega\mathbf{w}) \ll \min\left(1, (\omega\,\|\mathbf{w}\|_2)^{-N}\right),$$

[7] For an explicit construction of such a δ_1, one can start from the normalized indicator function of a smaller ball and apply repeated convolution with itself. See also [12] for further details and references.

$$\widehat{\delta_\omega}(0,\dots,0)=1\,. \tag{3.1}$$

Denote by I_S the indicator function of any set $S\subseteq\mathbb{R}^n$. We shall use convolution by δ_ω to smoothen indicator functions:

$$(I_S*\delta_\omega)(\mathbf{v})=\int\limits_{\mathbb{R}^n} I_S(\mathbf{u})\delta_\omega(\mathbf{v}-\mathbf{u})\,\mathrm{d}\mathbf{u}\,,\qquad \mathbf{v}\in\mathbb{R}^n\,.$$

We put $Y_\pm:=X^{1/p}\pm C_2^{-1}\omega$, with C_2 as in Lemma 4, and claim:

(a) $I_{Y_-\mathcal{B}_p}*\delta_\omega=0$ on $\mathbb{R}^n\setminus(X^{1/p}\mathcal{B}_p)$,

(b) $I_{Y_+\mathcal{B}_p}*\delta_\omega=1$ on $X^{1/p}\mathcal{B}_p$.

To verify (a), let $\mathbf{u}\in Y_-\mathcal{B}_p$, $\mathbf{v}\in\mathbb{R}^n\setminus(X^{1/p}\mathcal{B}_p)$. Then there exist $\mathbf{u}_*\in\mathcal{B}_p$, $\mathbf{v}_*\in\mathbb{R}^n\setminus\mathcal{B}_p$, with $\mathbf{u}=Y_-\mathbf{u}_*$, $\mathbf{v}=X^{1/p}\mathbf{v}_*$. By Lemma 4,

$$\|\mathbf{v}-\mathbf{u}\|_2=Y_-\left\|\mathbf{v}_*\left(1+\frac{\omega}{C_2Y_-}\right)-\mathbf{u}_*\right\|_2>\omega\,,$$

hence $I_{Y_-\mathcal{B}_p}(\mathbf{u})\delta_\omega(\mathbf{v}-\mathbf{u})=0$ for all $\mathbf{u}\in\mathbb{R}^n$, therefore (a) is true. Similarly, let $\mathbf{u}\in\mathbb{R}^n\setminus(Y_+\mathcal{B}_p)$, $\mathbf{v}\in X^{1/p}\mathcal{B}_p$. There exist $\mathbf{u}_*\in\mathbb{R}^n\setminus\mathcal{B}_p$, $\mathbf{v}_*\in\mathcal{B}_p$, with $\mathbf{u}=Y_+\mathbf{u}_*$, $\mathbf{v}=X^{1/p}\mathbf{v}_*$. Again by Lemma 4,

$$\|\mathbf{u}-\mathbf{v}\|_2=X^{1/p}\left\|\mathbf{u}_*\left(1+\frac{\omega}{C_2X^{1/p}}\right)-\mathbf{v}_*\right\|_2>\omega\,,$$

thus $I_{\mathbb{R}^n\setminus(Y_+\mathcal{B}_p)}(\mathbf{u})\delta_\omega(\mathbf{v}-\mathbf{u})=0$ for all $\mathbf{u}\in\mathbb{R}^n$, hence $I_{\mathbb{R}^n\setminus(Y_+\mathcal{B}_p)}*\delta_\omega=0$ on $X^{1/p}\mathcal{B}_p$, which is equivalent to (b). Since $0\le I_{Y_\pm\mathcal{B}_p}*\delta_\omega\le 1$ throughout, (a) and (b) imply that

$$I_{Y_-\mathcal{B}_p}*\delta_\omega\le I_{X^{1/p}\mathcal{B}_p}\le I_{Y_+\mathcal{B}_p}*\delta_\omega\,.$$

Therefore,

$$\sum_{\mathbf{k}\in\mathbb{Z}^n}(I_{Y_-\mathcal{B}_p}*\delta_\omega)(\mathbf{k})\le A_{p,K}(X)\le\sum_{\mathbf{k}\in\mathbb{Z}^n}(I_{Y_+\mathcal{B}_p}*\delta_\omega)(\mathbf{k})\,.$$

By Poisson's formula in $\mathbb{R}^n$ (see Bochner [1]), we thus infer that

$$\sum_{\mathbf{m}\in\mathbb{Z}^n}\widehat{I_{Y_-\mathcal{B}_p}}(\mathbf{m})\,\widehat{\delta_\omega}(\mathbf{m})\le A_{p,K}(X)\le\sum_{\mathbf{m}\in\mathbb{Z}^n}\widehat{I_{Y_+\mathcal{B}_p}}(\mathbf{m})\,\widehat{\delta_\omega}(\mathbf{m})\,. \tag{3.2}$$

Since $\widehat{\delta_\omega}(0,\dots,0)=1$ and

$$\widehat{I_{Y_\pm\mathcal{B}_p}}(0,\dots,0)=\mathrm{vol}(\mathcal{B}_p)Y_\pm^n=\mathrm{vol}(\mathcal{B}_p)X^{n/p}+O\left(X^{(n-1)/p}\omega\right)\,,$$

we obtain from (3.1) and (3.2)

$$\left|A_{p,K}(X)-\mathrm{vol}(\mathcal{B}_p)X^{n/p}\right|\ll\max_{\pm}\sum_{\mathbf{m}\in\mathbb{Z}_*^n}\left|\widehat{I_{Y_\pm\mathcal{B}_p}}(\mathbf{m})\right|\left|\widehat{\delta_\omega}(\mathbf{m})\right|+X^{(n-1)/p}\omega$$

$$\ll \max_{\pm} \sum_{\mathbf{m}\in\mathbb{Z}_*^n} \left|\widehat{I_{Y_\pm \mathcal{B}_p}}(\mathbf{m})\right| \min\left(1, (\omega\,\|\mathbf{m}\|_2)^{-N}\right) + X^{(n-1)/p}\omega \tag{3.3}$$

with $\mathbb{Z}_*^n := \mathbb{Z}^n \setminus \{(0,\dots,0)\}$. Writing Y instead of $Y_\pm$ for short (thus $Y \asymp X^{1/p}$), we have to estimate

$$\widehat{I_{Y\mathcal{B}_p}}(\mathbf{m}) = \int\limits_{Y\mathcal{B}_p} e(\mathbf{m}\cdot\mathbf{u})\,\mathrm{d}\mathbf{u} = Y^n \int\limits_{\mathcal{B}_p} e(Y\mathbf{m}\cdot\mathbf{u})\,\mathrm{d}\mathbf{u}\,. \tag{3.4}$$

To this integral we apply the linear transformation $\mathbf{u} \mapsto \mathbf{v} = \mathbf{M}\mathbf{u}$ defined in (2.2). Thus

$$\begin{aligned}\widehat{I_{Y\mathcal{B}_p}}(\mathbf{m}) &= \frac{Y^n}{|\det\mathbf{M}|}\int\limits_{\mathcal{B}_p^*} e(Y\mathbf{m}\cdot(\mathbf{M}^{-1}\mathbf{v}))\,\mathrm{d}\mathbf{v} \\ &= \frac{Y^n}{|\det\mathbf{M}|}\int\limits_{\mathcal{B}_p^*} e(Y({}^t\mathbf{M}^{-1}\mathbf{m})\cdot\mathbf{v})\,\mathrm{d}\mathbf{v}\,,\end{aligned}$$

where

$$\mathcal{B}_p^* := \left\{\mathbf{v} = (v_1,\dots,v_n) : \begin{array}{ll} |v_j| \le 1, & 1 \le j \le r, \\ (v_{r+2k-1}, v_{r+2k}) \in \mathcal{D}_p, & 1 \le k \le s. \end{array}\right\}$$

Using throughout the notation introduced in section 2, in particular (2.6), we can write this as

$$\widehat{I_{Y\mathcal{B}_p}}(\mathbf{m}) = \frac{Y^n}{|\det\mathbf{M}|}\prod_{j=1}^{r}\int\limits_{-1}^{1} e(YL_j(\mathbf{m})v_j)\,\mathrm{d}v_j \times$$

$$\times \prod_{k=1}^{s}\int\limits_{\mathcal{D}_p} e(Y(F_{r+k}(\mathbf{m})v_{r+2k-1} + G_{r+k}(\mathbf{m})v_{r+2k}))\,\mathrm{d}(v_{r+2k-1}, v_{r+2k})\,. \tag{3.5}$$

As an immediate by-result, we obtain, by an appeal to (2.4),

$$\mathrm{vol}(\mathcal{B}_p) = \widehat{I_{\mathcal{B}_p}}(0,\dots,0) = \frac{2^r(\mathrm{area}(\mathcal{D}_p))^s}{|\det\mathbf{M}|} = \frac{2^{r+s}(\mathrm{area}(\mathcal{D}_p))^s}{\sqrt{|\mathrm{disc}(K)|}}\,. \tag{3.6}$$

By Lemma 5, (3.5) implies (for $\mathbf{m} \ne (0,\dots,0)$)

$$\begin{aligned}\widehat{I_{Y\mathcal{B}_p}}(\mathbf{m}) \ll\ & Y^{n-r-3s/2}\prod_{j=1}^{r}\min\left(Y, |L_j(\mathbf{m})|^{-1}\right) \times \\ & \times \prod_{k=1}^{s}\min\left(Y^{3/2}, \left(F_{r+k}(\mathbf{m})^2 + G_{r+k}(\mathbf{m})^2\right)^{-3/4}\right) \\ \ll\ & Y^{s/2}\prod_{j=1}^{r}\min\left(Y, |L_j(\mathbf{m})|^{-1}\right)\prod_{j=r+1}^{r+s}\min\left(Y^{3/2}, |L_j(\mathbf{m})|^{-3/2}\right)\,,\end{aligned} \tag{3.7}$$

in view of (2.7). Combining this with (3.3), we arrive at

$$\begin{aligned}\left|A_{p,K}(X) - \mathrm{vol}(\mathcal{B}_p)X^{n/p}\right| &\ll \\ &\ll X^{(n-1)/p}\omega \;+\; X^{s/(2p)} \sum_{\mathbf{m}\in\mathbb{Z}_*^n} \min\left(1, (\omega\,\|\mathbf{m}\|_2)^{-N}\right) \times \\ &\times \prod_{j=1}^{r} \min\left(Y, |L_j(\mathbf{m})|^{-1}\right) \prod_{j=r+1}^{r+s} \min\left(Y^{3/2}, |L_j(\mathbf{m})|^{-3/2}\right). \qquad (3.8)\end{aligned}$$

We divide the range of summation of this sum into subsets

$$S(M,J) := \{\mathbf{m}\in\mathbb{Z}_*^n :\ \tfrac{1}{2}M < \|\mathbf{m}\|_\infty \le M,\ |L_J(\mathbf{m})| = \max_{1\le k\le r+s} |L_k(\mathbf{m})|\ \},$$

where $J \in \{1,\dots,r+s\}$, and M is large. By (2.8), always

$$\mathbf{m}\in S(M,J) \quad\Rightarrow\quad |L_J(\mathbf{m})| \asymp M\,. \qquad (3.9)$$

We have to distinguish two cases.
Case 1: $r = 0$, i.e., K is "totally complex". Let w.l.o.g. $J = 1$, then we conclude that

$$\begin{aligned}\sum_{\mathbf{m}\in S(M,1)} \prod_{k=1}^{s} \min\left(Y^{3/2}, |L_k(\mathbf{m})|^{-3/2}\right) &\ll \\ &\ll Y^{\frac{3}{2}(s-2)} M^{-3/2} \sum_{0<\|\mathbf{m}\|_\infty\le M} \min\left(Y^{3/2}, |L_2(\mathbf{m})|^{-3/2}\right) \\ &\ll Y^{\frac{3}{2}(s-2)+\frac{1}{2}} M^{2s-7/2+\epsilon'} + Y^{\frac{3}{2}(s-2)} M^{2s-3+\epsilon'}\,, \qquad (3.10)\end{aligned}$$

by (3.9) and an application of Lemma 3, (ii) and (iii). As a consequence, the corresponding portion of the sum in (3.8) can be estimated by

$$\begin{aligned}\sum_{\frac{1}{2}M<\|\mathbf{m}\|_\infty\le M} \min\left(1, (\omega\,\|\mathbf{m}\|_2)^{-N}\right) \prod_{k=1}^{s} \min\left(Y^{3/2}, |L_k(\mathbf{m})|^{-3/2}\right) &\ll \\ \ll \left(Y^{\frac{3}{2}(s-2)+\frac{1}{2}} M^{2s-7/2+\epsilon'} + Y^{\frac{3}{2}(s-2)} M^{2s-3+\epsilon'}\right) \min\left(1, (\omega M)^{-N}\right).\end{aligned}$$

We fix N sufficiently large and let M run through the powers of 2. It follows that

$$\begin{aligned}P_{p,K}(X) := A_{p,K}(X) - \mathrm{vol}(\mathcal{B}_p)X^{n/p} &\ll \\ \ll X^{(n-1)/p}\omega \;+ X^{s/(2p)} \left(Y^{\frac{3}{2}(s-2)+\frac{1}{2}}\omega^{-2s+7/2-\epsilon'} + Y^{\frac{3}{2}(s-2)}\omega^{-2s+3-\epsilon'}\right).\end{aligned}$$

Recalling that $Y \asymp X^{1/p}$, and balancing the remainder terms, we get $\omega = X^{-\frac{1}{p}\frac{3}{2n-5}}$ and thus

$$P_{p,K}(X) \ll X^{\frac{1}{p}\left(n-1-\frac{3}{2n-5}\right)+\epsilon}\,. \qquad (3.11)$$

For larger n, it is favorable to choose a different (actually somewhat cruder) approach. For any $U \in \{1, \dots, s\}$ and parameters $1 \ll T_1, \dots, T_U \ll M$, we consider the body

$$K_U(T_1, \dots, T_U) :=$$
$$\left\{ (x_1, \dots, x_n) \in \mathbb{R}^n : \begin{array}{ll} T_k^2 \le x_{2k-1}^2 + x_{2k}^2 \le 4T_k^2 & \text{for } 1 \le k \le U, \\ x_{2k-1}^2 + x_{2k}^2 \le 1 & \text{for } U+1 \le k \le s \end{array} \right\}.$$

It is plain to see that the number of points of the lattice $\mathbf{M}^* \, \mathbb{Z}^n$ (with $\mathbf{M}^*$ as in (2.2) through (2.6)) in $K_U(T_1, \dots, T_U)$ satisfies

$$\# \left(\mathbf{M}^* \, \mathbb{Z}^n \cap K_U(T_1, \dots, T_U)\right) \ll (T_1 \dots T_U)^2 .$$

Therefore[8],

$$\sum_{\substack{\frac{1}{2}M < \|\mathbf{m}\|_\infty \le M \\ \mathbf{M}^*\mathbf{m} \in K_U(T_1, \dots, T_U)}} \left| \widehat{I_{Y\mathcal{B}_p}}(\mathbf{m}) \right| \min\left(1, (\omega \, \|\mathbf{m}\|_2)^{-N}\right) \ll$$

$$\ll \min\left(1, (\omega M)^{-N}\right) Y^{s/2} \sum_{\mathbf{m}:\ \mathbf{M}^*\mathbf{m} \in K_U(T_1, \dots, T_U)} \prod_{k=1}^{s} \min\left(Y^{3/2}, |L_k(\mathbf{m})|^{-3/2}\right)$$

$$\ll \min\left(1, (\omega M)^{-N}\right) Y^{\frac{s}{2} + \frac{3}{2}(s-U)} \, (T_1 \dots T_U)^{-3/2} \sum_{\mathbf{m}:\ \mathbf{M}^*\mathbf{m} \in K_U(T_1, \dots, T_U)} 1$$

$$\ll \min\left(1, (\omega M)^{-N}\right) \, Y^{n - \frac{3}{2}U} \, (T_1 \dots T_U)^{1/2} .$$

We let the T_k range over dyadic sequences $\ll M$, and sum also over $U = 1, \dots, s$ to arrive at

$$\sum_{\frac{1}{2}M < \|\mathbf{m}\|_\infty \le M} \left| \widehat{I_{Y\mathcal{B}_p}}(\mathbf{m}) \right| \min\left(1, (\omega \, \|\mathbf{m}\|_2)^{-N}\right) \ll$$

$$\ll \min\left(1, (\omega M)^{-N}\right) \max_{1 \le U \le s} \left(Y^{n - \frac{3}{2}U} M^{U/2} \right) .$$

With N fixed sufficiently large, we let again M range over the powers of 2 to obtain

$$P_{p,K}(X) \ll X^{(n-1)/p} \omega + \max_{1 \le U \le s} \left(X^{\frac{1}{p}(n - \frac{3}{2}U)} \omega^{-U/2} \right) .$$

Taking $\omega = X^{-1/(3p)}$, we thus get

$$P_{p,K}(X) \ll X^{\frac{1}{p}(n - \frac{4}{3})} + \max_{1 \le U \le s} \left(X^{\frac{1}{p}(n - \frac{4}{3}U)} \right) \ll X^{\frac{1}{p}(n - \frac{4}{3})} . \qquad (3.12)$$

[8] Note that, because of (3.9), this sum would be empty for $U = 0$, if M is sufficiently large.

Case 2: $r \geq 1$. Dealing again with the sum in (3.8), we consider first those domains $S(M,J)$ with $J \in \{r+1,\dots,r+s\}$, say, $J = r+s$. Similarly to (3.10),

$$\begin{aligned} &\sum_{\mathbf{m}\in S(M,r+s)} \prod_{j=1}^{r} \min\left(Y, |L_j(\mathbf{m})|^{-1}\right) \prod_{k=r+1}^{r+s} \min\left(Y^{3/2}, |L_k(\mathbf{m})|^{-3/2}\right) \ll \\ &\qquad \ll Y^{r-1+\frac{3}{2}(s-1)} M^{-3/2} \sum_{0<\|\mathbf{m}\|_\infty \leq M} \min\left(Y, |L_1(\mathbf{m})|^{-1}\right) \\ &\qquad \ll Y^{r+\frac{3}{2}s-\frac{5}{2}} M^{n-5/2+\epsilon'}, \end{aligned} \tag{3.13}$$

by an appeal to (3.9) and Lemma 3, part (i). Secondly, we deal with $S(M,J)$ where $J \in \{1,\dots,r\}$, say, $J=1$. The corresponding argument now reads

$$\begin{aligned} &\sum_{\mathbf{m}\in S(M,1)} \prod_{j=1}^{r} \min\left(Y, |L_j(\mathbf{m})|^{-1}\right) \prod_{k=r+1}^{r+s} \min\left(Y^{3/2}, |L_k(\mathbf{m})|^{-3/2}\right) \ll \\ &\qquad \ll Y^{r-1+\frac{3}{2}(s-1)} M^{-1} \sum_{0<\|\mathbf{m}\|_\infty \leq M} \min\left(Y^{3/2}, |L_{r+1}(\mathbf{m})|^{-3/2}\right) \\ &\qquad \ll Y^{r+\frac{3}{2}s-2} M^{n-3+\epsilon'} + Y^{r+\frac{3}{2}s-\frac{5}{2}} M^{n-5/2+\epsilon'}, \end{aligned} \tag{3.14}$$

again in view of (3.9) and Lemma 3, (ii) and (iii). Therefore, the part of the sum in (3.8) which corresponds to $\frac{1}{2}M < \|\mathbf{m}\|_\infty \leq M$ is

$$\ll \left(Y^{r+\frac{3}{2}s-2} M^{n-3+\epsilon'} + Y^{r+\frac{3}{2}s-\frac{5}{2}} M^{n-5/2+\epsilon'}\right) \min\left(1, (\omega M)^{-N}\right).$$

Again, with fixed N sufficiently large, we let M range through the powers of 2, and sum up to infer from (3.8) that

$$\begin{aligned} &P_{p,K}(X) \ll \\ &\quad \ll X^{(n-1)/p}\omega + X^{s/(2p)}\left(Y^{r+\frac{3}{2}s-2}\omega^{-n+3-\epsilon'} + Y^{r+\frac{3}{2}s-\frac{5}{2}}\omega^{-n+5/2-\epsilon'}\right). \end{aligned}$$

Recalling that $Y \asymp X^{1/p}$, and balancing the remainder terms, we choose $\omega = X^{-\frac{1}{p}\frac{1}{n-2}}$ and thus obtain

$$P_{p,K}(X) \ll X^{\frac{1}{p}\left(n-1-\frac{1}{n-2}\right)+\epsilon}. \tag{3.15}$$

Combining the estimates (3.11), (3.12), and (3.15), and recalling (3.6) and (2.1), we complete the proof of our Theorem. □

References

[1] S. Bochner, *Die Poissonsche Summenformel in mehreren Veränderlichen.* Math. Ann. **106** (1932), 55–63.

[2] N. Bourbaki, *Elements of mathematics, Algebra II.* Springer, Berlin 1990.

[3] M.N. HUXLEY, *Exponential sums and lattice points II.* Proc. London Math. Soc. **66** (1993), 279-301.

[4] M.N. HUXLEY, *Area, lattice points, and exponential sums.* LMS Monographs, New Ser. **13**, Oxford 1996.

[5] E. KRÄTZEL, *Lattice points.* Kluwer, Dordrecht 1988.

[6] E. KRÄTZEL, *Analytische Funktionen in der Zahlentheorie.* Teubner, Stuttgart 2000.

[7] G. KUBA, *On the distribution of squares of integral quaternions.* Acta Arithm. **93** (2000), 359–372.

[8] G. KUBA, *On the distribution of squares of integral quaternions II.* Acta Arithm. **101** (2002), 81–95.

[9] G. KUBA, *On the distribution of squares of hypercomplex integers.* J. Number Th. **88** (2001), 313–334.

[10] G. KUBA, *Zur Verteilung der Quadrate ganzer Zahlen in rationalen Quaternionenalgebren.* Abh. Math. Sem. Hamburg **72** (2002), 145–163.

[11] G. KUBA, *On the distribution of squares of integral Cayley numbers.* Acta Arithm. **108** (2003), 253–265.

[12] G. KUBA, H. MÜLLER, W.G. NOWAK and J. SCHOISSENGEIER, *Zur Verteilung der Potenzen ganzer Zahlen eines komplexen kubischen Zahlkörpers.* Abh. Math. Sem. Hamburg **70** (2000), 341–354.

[13] L. KUIPERS and H. NIEDERREITER, *Uniform distribution of sequences.* J. Wiley, New York 1974.

[14] H. MÜLLER and W.G. NOWAK, *Potenzen von Gaußschen ganzen Zahlen in Quadraten.* Mitt. Math. Ges. Hamburg **18** (1999), 119–126.

[15] W. MÜLLER, *On the average order of the lattice rest of a convex body.* Acta Arithm. **80** (1997), 89–100.

[16] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers.* 2$^{\text{nd}}$ ed., Springer, Berlin 1990.

[17] W.G. NOWAK, *Zur Verteilung der Potenzen Gaußscher ganzer Zahlen.* Abh. Math. Sem. Hamburg **73** (2003), 43–65.

[18] G. OPFER and W. RIPKEN, *Complex version of Catalań's problem.* Mitt. Math. Ges. Hamburg **17** (1998), 101–112.

[19] K.F. ROTH, *Rational approximations to algebraic numbers.* Mathematika **2** (1955), 1–20.

[20] W.M. SCHMIDT, *Simultaneous approximation to algebraic numbers by rationals.* Acta Math. **125** (1970), 189–201.

[21] W.M. SCHMIDT, *Diophantine approximation.* LNM **785**, Springer, Berlin 1980.

[22] WOLFRAM RESEARCH, Inc. *Mathematica*, Version 4.0. Wolfram Research, Inc. Champaign 1999.

Werner Georg NOWAK
Institute of Mathematics
Department of Integrative Biology
BOKU - University of Natural Resources and Applied Life Sciences
Peter Jordan-Straße 82
A-1190 Wien, Austria
E-mail : `nowak@mail.boku.ac.at`

Johannes SCHOISSENGEIER
Institut für Mathematik der Universität Wien
Nordbergstraße 15
A-1090 Wien, Austria
E-mail : `hannes.schoissengeier@univie.ac.at`