A further omega result for the ellipsoid problem in algebraic number fields

by

ULRICH RAUSCH (Marburg)

The classical ellipsoid problem, i.e., the problem of evaluating asymptotically the number of lattice points in a multidimensional ellipsoid, was generalized in [2] to algebraic number fields, and upper and lower estimates for the pertinent lattice rest were proved (^{1}).

While the O-result obtained there holds generally, the Ω-theorems impose several restrictions on the parameters involved. For instance, the ellipsoids under consideration are supposed to be centered at lattice points. Also, the arithmetic nature of the underlying Hermitian forms plays a significant role.

In the present paper I give a somewhat weaker Ω-estimate valid in the general case, which fits well into what is known for the rational field.

We begin by formulating the problem. Let K be an algebraic number field of degree $[K : \mathbb{Q}] = n = r_1 + 2r_2$ (in the standard notation), d its discriminant, and $r = r_1 + r_2 - 1$. Let $e_p = 1$ for $p = 1, \ldots, r_1$ and $e_p = 2$ for $p = r_1 + 1, \ldots, n$.

For a fixed rational integer $k \geq 2$, consider the set $\mathcal{T}$ of all column vectors

$$\boldsymbol{\nu} = (\nu_1^{(1)}, \ldots, \nu_k^{(1)}, \nu_1^{(2)}, \ldots, \nu_k^{(2)}, \ldots, \nu_1^{(n)}, \ldots, \nu_k^{(n)})^T \in \mathbb{C}^{kn}$$

such that

$$\nu_j^{(p)} \in \mathbb{R} \quad (j = 1, \ldots, k; \ p = 1, \ldots, r_1),$$

$$\nu_j^{(p+r_2)} = \overline{\nu_j^{(p)}} \quad (j = 1, \ldots, k; \ p = r_1 + 1, \ldots, r + 1);$$

let $\boldsymbol{0} \in \mathcal{T}$ denote the zero vector, and

$$\boldsymbol{\nu}^{(p)} = (\nu_1^{(p)}, \ldots, \nu_k^{(p)})^T \quad \text{for } \boldsymbol{\nu} \in \mathcal{T}.$$

(^{1}) There is a misprint on p. 330, line -10, of [2]: For "endlichen Grad über $\boldsymbol{Q}$" read "endlichen Grad über $\mathbb{Q}$".

We call $\boldsymbol{\nu}, \boldsymbol{\alpha} \in \mathcal{T}$ *congruent* with respect to a given system $\mathfrak{a} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ of non-zero ideals $\mathfrak{a}_j \subseteq K$, in symbols

$$\boldsymbol{\nu} \equiv \boldsymbol{\alpha} \ (\mathfrak{a}) \,,$$

if there exist numbers $\mu_j \in \mathfrak{a}_j \ (j = 1, \ldots, k)$ such that

$$\nu_j^{(p)} - \alpha_j^{(p)} = \mu_j^{(p)} \quad (p = 1, \ldots, n; \ j = 1, \ldots, k) \,,$$

where $\mu_j^{(p)}$ denotes the pth conjugate of μ_j.

For $p = 1, \ldots, r + 1$, let $\boldsymbol{Q}^{(p)} \in \mathbb{C}^{k \times k}$ be a positive definite Hermitian matrix, real for $p = 1, \ldots, r_1$, and let $Q^{(p)}$ be the Hermitian form in k variables arising from it; we write briefly Q for the system of these forms.

Further, let $x = (x_1, \ldots, x_{r+1}) \in \mathbb{R}_+^{r+1}$, $\mathbb{R}_+$ denoting the set of positive real numbers.

For convenience we supplement x_p, $\boldsymbol{Q}^{(p)}$ (and thus $Q^{(p)}$) for $r + 1 < p \leq n$ by setting

$$x_{p+r_2} = x_p, \quad \boldsymbol{Q}^{(p+r_2)} = \overline{\boldsymbol{Q}^{(p)}} \quad \text{for } p = r_1 + 1, \ldots, r + 1 \,.$$

The counting function

$$A_k(x) = A_k(x; Q, \mathfrak{a}, \boldsymbol{\alpha})$$

is now defined as the number of vectors $\boldsymbol{\nu} \in \mathcal{T}$ satisfying $\boldsymbol{\nu} \equiv \boldsymbol{\alpha} \ (\mathfrak{a})$ and

$$Q^{(p)}(\boldsymbol{\nu}^{(p)}) \leq x_p \quad \text{for } p = 1, \ldots, r + 1$$

(or, equivalently, for $p = 1, \ldots, n$). The lattice rest in question is

$$P_k(x) = P_k(x; Q, \mathfrak{a}, \boldsymbol{\alpha}) = A_k(x) - C_0 X^{k/2}$$

with

$$X = x_1 \ldots x_n = \prod_{p=1}^{r+1} x_p^{e_p} \,, \quad C_0 = \frac{2^{kr_2} \omega_k^{r_1} \omega_{2k}^{r_2}}{|d|^{k/2} N(\mathfrak{a}_1 \ldots \mathfrak{a}_k) \sqrt{D}} \,,$$

where

$$D = \prod_{p=1}^{n} \det \boldsymbol{Q}^{(p)} \,, \quad \omega_l = \pi^{l/2} / \Gamma(\tfrac{1}{2} l + 1) \,,$$

and N denotes the ideal norm in K. Then we have the following result.

THEOREM. *Always (i.e., for all choices of k, Q, $\mathfrak{a}$, $\boldsymbol{\alpha}$)*

$$P_k(x) = \Omega_\pm(X^{(k - \frac{r+1}{n})/4}) \quad \text{as } X \to \infty \,.$$

P r o o f. We shall use extensively the contents of [2]. By $\widetilde{Q}^{(p)}$ we denote the Hermitian form associated with the matrix $(\overline{\boldsymbol{Q}^{(p)}})^{-1}$, and $\mathfrak{c}$ stands for the system of ideals $\mathfrak{c}_j = (\mathfrak{a}_j \mathfrak{d})^{-1} \ (j = 1, \ldots, k)$, where $\mathfrak{d}$ is the different of K. $c_1, \ldots, c_{17}$ are positive constants which, as well as all O-, $\ll$-, and $\gg$-constants, may depend on K, k, Q, $\mathfrak{a}$, and $\boldsymbol{\alpha}$.

For $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{R}_+^n$, $\lambda_{p+r_2} = \lambda_p$ $(p = r_1 + 1, \ldots, r+1)$, let

(1)
$$a(\lambda) := \sum_{\boldsymbol{\nu} \equiv \mathbf{0}(\mathfrak{c}), \, \widetilde{Q}(\boldsymbol{\nu}) = \lambda} e^{-2\pi i \boldsymbol{\alpha} \cdot \boldsymbol{\nu}},$$

where $\widetilde{Q}(\boldsymbol{\nu}) = \lambda$ means $\widetilde{Q}^{(p)}(\boldsymbol{\nu}^{(p)}) = \lambda_p$ for $p = 1, \ldots, n$, and $\boldsymbol{\alpha} \cdot \boldsymbol{\nu}$ denotes the real number

$$\sum_{j=1}^{k} \sum_{p=1}^{n} \alpha_j^{(p)} \nu_j^{(p)}.$$

Since $\boldsymbol{\nu}$ and $-\boldsymbol{\nu}$ occur together in (1), $a(\lambda)$ is real.

If $a(\lambda)$ were always zero, the series

$$\Theta\left(\frac{\pi e_1 x_1}{u_1}, \ldots, \frac{\pi e_n x_n}{u_n}; \widetilde{Q}, \mathfrak{c}, \mathbf{0}, -\boldsymbol{\alpha}\right)$$

in the proof of [2, Hilfssatz 6.1] would reduce to its constant term 1, and it would follow that

$$\mathcal{J}_\varepsilon(P_k(x)) := (4\pi\varepsilon)^{-(r+1)/2} \int_{\mathbb{R}^{r+1}} P_k(x_1 e^{v_1}, \ldots, x_{r+1} e^{v_{r+1}}) \exp\left(-\frac{1}{4\varepsilon} \sum_{p=1}^{r+1} v_p^2\right) dv$$

$$= 0 \quad \text{for all } x \in \mathbb{R}_+^{r+1} \text{ and all } \varepsilon > 0.$$

From this we would easily conclude, either with the aid of [2, Hilfssatz 4.3] (= [1, Theorem 3.1]) or directly (cf. the remark at the beginning of [1, Sect. 3]), that $P_k(x) = 0$ for all $x \in \mathbb{R}_+^{r+1}$. But this is impossible since $A_k(x)$ is certainly not continuous. Thus

$$M := \{\lambda : a(\lambda) \neq 0\} \neq \emptyset.$$

By [2, Hilfssatz 6.1] (with $\delta = 1/(4n)$) we have for $x \in \mathbb{R}_+^{r+1}$, $0 < \varepsilon \leq 1/2$

(2)
$$\mathcal{J}_\varepsilon(P_k(x)) = S_k(x, \varepsilon) + O(\varepsilon^{-(nk-r-1)/4} X^{-1/(4n)}),$$

where

$$S_k(x, \varepsilon) = c_1 X^{k/2} \sum_{\lambda \in M} a(\lambda)$$

$$\times \prod_{p=1}^{r+1} \left\{ \frac{e^{-\varepsilon\pi^2 e_p^2 \lambda_p x_p}}{(\pi^2 e_p^2 \lambda_p x_p)^{(e_p k + 1)/4}} \cos(2\pi\sqrt{e_p^2 \lambda_p x_p} - \tfrac{1}{4}(e_p k + 1)\pi) \right\}.$$

We proceed to select one dominant term from $S_k(x, \varepsilon)$.

Let $\boldsymbol{\nu} \equiv \mathbf{0}$ ($\mathfrak{c}$), $\lambda = \widetilde{Q}(\boldsymbol{\nu})$, such that $\lambda_1 \ldots \lambda_n =: \Lambda \leq \Lambda_0$. The vector $\boldsymbol{\nu}$ is made up of the conjugates of numbers $\nu_j \in \mathfrak{c}_j$ $(j = 1, \ldots, k)$. Multiplying all of these by the same suitably chosen unit, we can obtain a $\boldsymbol{\mu} \equiv \mathbf{0}$ ($\mathfrak{c}$) such that $\lambda' := \widetilde{Q}(\boldsymbol{\mu})$ satisfies

$$\lambda_1' \ldots \lambda_n' = \Lambda \quad \text{and} \quad \lambda_p' \leq c_2 \Lambda^{1/n} \quad (p = 1, \ldots, n),$$

hence

$$\sum_{j=1}^{k} |\mu_j^{(p)}|^2 \leq c_3 \Lambda_0^{1/n} \quad (p = 1, \ldots, n)$$

by [2, Hilfssatz 5.1]. Since these inequalities have only finitely many solutions $\boldsymbol{\mu} \equiv \boldsymbol{0}$ (c), it follows that Λ belongs to some discrete subset of $\mathbb{R}_+$. Consequently, we may choose from M a $\lambda^* = (\lambda_1^*, \ldots, \lambda_n^*)$ (c-constants!) such that

$$\lambda_1^* \ldots \lambda_n^* = \min\{\lambda_1 \ldots \lambda_n : \lambda \in M\}.$$

The inequality between arithmetic and geometric means yields for $\lambda \in M$

$$\sum_{p=1}^{r+1} e_p \frac{\lambda_p}{\lambda_p^*} = \sum_{p=1}^{n} \frac{\lambda_p}{\lambda_p^*} \geq n$$

with equality only for $\lambda = \lambda^*$, hence

$$(3) \qquad \sum_{p=1}^{r+1} e_p \frac{\lambda_p}{\lambda_p^*} \geq n + 2c_4 \quad \text{for } \lambda \in M, \ \lambda \neq \lambda^*,$$

since the left-hand member attains only discrete values.

Now, for $t > 1$, let

$$x_p = \frac{1}{e_p \lambda_p^*}(t + \vartheta_p \sqrt{t}), \quad \text{where} \quad 0 \leq \vartheta_p \leq 3 \quad (p = 1, \ldots, r+1),$$

and

$$\varepsilon = T/t, \quad \text{where } T \geq 1;$$

the ϑ_p's and T will be chosen later. Then

$$(4) \qquad\qquad c_5 t \leq x_p \leq c_6 t \quad (p = 1, \ldots, r+1)$$

and, if $t \geq (3n/c_4)^2$,

$$(5) \qquad\qquad \varepsilon \pi^2 \sum_{p=1}^{r+1} e_p^2 \lambda_p^* x_p \leq T\pi^2(n + c_4) =: c_7 T,$$

while for $\lambda \neq \lambda^*$ we have by (3)

$$Y := \varepsilon \pi^2 \sum_{p=1}^{r+1} e_p^2 \lambda_p x_p \geq T\pi^2(n + 2c_4) =: \frac{c_7 + c_8}{1 - c_8} T,$$

say, so that

$$Y \geq (c_7 + c_8)T + c_8 Y.$$

Hence the terms with $\lambda \neq \lambda^*$ contribute to $S_k(x, \varepsilon)$ at most

$$c_1 e^{-(c_7+c_8)T} X^{k/2} \sum_{\lambda \in M} |a(\lambda)| \prod_{p=1}^{r+1} \frac{e^{-c_8 \varepsilon \pi^2 e_p^2 \lambda_p x_p}}{(\pi^2 e_p^2 \lambda_p x_p)^{(e_p k+1)/4}} \, ,$$

which, for $t \geq 2c_8 T$, is

$$\ll e^{-(c_7+c_8)T} \varepsilon^{-(nk-r-1)/4} \ll e^{-(c_7+c_8)T} X^{(k-(r+1)/n)/4}$$

by [2, Hilfssatz 5.6] and (4).

Regarding $\lambda = \lambda^*$, (4) and (5) yield

$$X^{k/2} |a(\lambda^*)| \prod_{p=1}^{r+1} \frac{e^{-\varepsilon \pi^2 e_p^2 \lambda_p^* x_p}}{(\pi^2 e_p^2 \lambda_p^* x_p)^{(e_p k+1)/4}} \gg e^{-c_7 T} X^{(k-(r+1)/n)/4} \, .$$

As $\vartheta_1, \ldots, \vartheta_{r+1}$ run independently through $[0, 3]$, the values of each term

$$2\pi \sqrt{e_p^2 \lambda_p^* x_p} = 2\pi \sqrt{e_p(t + \vartheta_p \sqrt{t})}$$

cover an interval of length $> 2\pi$; hence the product

$$\prod_{p=1}^{r+1} \cos \left(2\pi \sqrt{e_p^2 \lambda_p^* x_p} - \tfrac{1}{4}(e_p k + 1)\pi \right)$$

takes every value between -1 and $+1$. Thus, if ξ denotes either of the numbers $+1$ and -1, we can always find ϑ_p's such that

$$\xi S_k(x, \varepsilon) \geq e^{-c_7 T} \{ c_9 - c_{10} e^{-c_8 T} \} X^{(k-(r+1)/n)/4} \, ,$$

provided $t \geq c_{11} T$. Choosing here $T = c_{12}$ large enough to make the term in curly brackets positive, we obtain from (2) the following result:

There exist $x \in \mathbb{R}_+^{r+1}$ and $\varepsilon > 0$ such that X is arbitrarily large,

$$(6) \qquad\qquad c_{13} X^{-1/n} \leq \varepsilon \leq c_{14} X^{-1/n} \, ,$$

and

$$(7) \qquad\qquad \xi \mathcal{J}_\varepsilon(P_k(x)) \geq c_{15} X^{(k-(r+1)/n)/4} \, .$$

Now assume

$$\xi P_k(x) \leq \varrho X^{(k-(r+1)/n)/4} \quad \text{for } X \geq X_0 \, .$$

Then, as in [2, Hilfssatz 8.3], it follows that

$$\xi \mathcal{J}_\varepsilon(P_k(x)) \leq c_{16} \varrho X^{(k-(r+1)/n)/4} + O(1)$$

for $X \geq e^n X_0$ and every ε according to (6). Comparing this to (7) yields $\varrho \geq c_{17}$, hence the assertion. $\blacksquare$

References

[1] U. Rausch, *A summation formula in algebraic number fields and applications, I*, J. Number Theory 36 (1990), 46–79.

[2] —, *Zum Ellipsoidproblem in algebraischen Zahlkörpern*, Acta Arith. 58 (1991), 309–333.

KERSCHENSTEINERSTRASSE 18
D-W-3550 MARBURG
GERMANY