NUMBER OF LATTICE POINTS IN SYMMETRIC CONVEX BODIES

Let $K$ be an open subset of $\mathbb{R}^d$. We say $K$ is symmetric if $K = -K$ and that $K$ is a convex body if $K + K + 2 \cdot K$. Many problems in number theory involve estimating $|K \cap \mathbb{Z}^d|$ for various choices of $K$. For instance, the famous Gauss circle problem is concerned with the case $K = R \cdot B_2$, where $B_2$ is the unit ball in $\mathbb{R}^2$ and $R > 0$ is large. Heuristically, we expect that $|K \cap \mathbb{Z}^d| \approx \text{Vol}(K)$, as the unit cube centered at a typical lattice point in $K$ should be entirely contained in $K$. Of course, this heuristic is not rigorous as lattice points near the boundary of $K$ do not satisfy this property.

Our goal is to classify when $|K \cap \mathbb{Z}^d| \geq CVol(K)$ for some constant $C$ much larger than 1. We prove the following.

**Theorem 0.1** Let $K \subset \mathbb{R}^d$ be a symmetric, convex body. Then there exists a $C > 1$ depending only on $d$ such that either

1. $|K \cap \mathbb{Z}^d| \leq CVol(K)$
2. $K \cap \mathbb{Z}^d$ is contained in some $d-1$ dimensional subspace $W$.

A key example is

$$L = \left\{ \sum_{i=1}^{d} \alpha_i e_i : |\alpha_1| < N, \ldots, |\alpha_{d-1}| < N, |\alpha_d| < N^{1-d} \right\}.$$ 

Then $L$ is a symmetric convex body and $\text{Vol}(L) = 1$, but $|L \cap \mathbb{Z}^d| \sim N^{d-1}$. Thus $L$ falls into case (2) of Theorem 0.1 but not case (1). We give a proof below. The idea is to efficiently contain $K$ in a box $B = [-M_1, M_1] \times \cdots \times [-M_d, M_d]$ and use the basic fact that

$$|K \cap \mathbb{Z}^d| \leq |B \cap \mathbb{Z}| = \prod_{j=1}^{d} 2|M_j| + 1 \lesssim M_1 \cdots M_d,$$

as long as $M_1, \ldots, M_d \geq 1$. Otherwise $M_j < 1$ for some $j$ and we conclude (2). We turn to the details.

**Proof.** Let $\lambda_1 \leq \ldots \leq \lambda_d$ be the successive minimum of $K$ with respect to $\mathbb{Z}^d$. Then by Minkowski’s second theorem there exists $b_1, \ldots, b_d \in \mathbb{Z}^d$ such that the following hold.

---

1. $A + B = \{a + b : a \in A, b \in B \}$ while $c \cdot K = \{ck : k \in K \}$
2. One can take $C = O(d)^d$
3. $\lambda_j = \inf\{\lambda > 0 : \lambda \cdot B \text{ contains } j \text{ linearly independent elements of } \mathbb{Z}^d\}$
4. such a statement can be found in Theorem 3.30 as well as exercise 3.5.5 in Tao and Vu’s book on additive combinatorics

---
(i) The vectors $b_1, \ldots, b_d$ are linearly independent.

(ii) Let $O$ be the octahedron with vertices $\pm b_i / \lambda_i$. \footnote{So $O = \{ \sum_{i=1}^d \alpha_i b_i / \lambda_i : \sum_{i=1}^d |\alpha_i| < 1 \}$} Then $O \subseteq K \subseteq r \cdot O$ where $r \lesssim d$.

(iii) Let $\Gamma := \langle b_1, \ldots, b_d \rangle \mathbb{Z}$. Then $|\mathbb{Z}^d / \Gamma| \lesssim d$.

(iv) The successive minimum satisfy $\lambda_1 \cdots \lambda_d \gtrsim d \text{Vol}(K)^{-1}$.

We let $B$ be the matrix whose columns are $b_1, \ldots, b_d$. Note by (iii), $\det(B) \gtrsim d$ and that $B$ is invertible. We have that

$$K \cap \mathbb{Z}^d \subseteq (r \cdot O) \cap \mathbb{Z}^d$$

$$= (r \cdot \{ \alpha_1 b_1 / \lambda_1 + \cdots + \alpha_d b_d / \lambda_d : \sum_{i=1}^d |\alpha_i| < 1 \}) \cap \mathbb{Z}^d$$

$$= \{ \tau_1 b_1 / \lambda_1 + \cdots + \tau_d b_d / \lambda_d : \sum_{i=1}^d \lambda_i |\tau_i| < r \} \cap \mathbb{Z}^d$$

$$= \{ \tau_1 b_1 + \cdots + \tau_d b_d : \lambda_i |\tau_i| < r, \forall i \} \cap \mathbb{Z}^d$$

$$\subseteq B (\{ \tau_1 e_1 + \cdots + \tau_d e_d : \lambda_i |\tau_i| < r, \forall i \} \cap B^{-1} \mathbb{Z}^d)$$

$$\subseteq B (\{ \tau_1 e_1 + \cdots + \tau_d e_d : \lambda_i |\tau_i| < r, \forall i \} \cap \det(B)^{-1} \mathbb{Z}^d)$$

$$= B / \det(B) (\{ \tau_1 e_1 + \cdots + \tau_d e_d : \lambda_i |\tau_i| < r \det(B), \forall i \} \cap \mathbb{Z}^d)$$

The first containment is (ii) from Minkwoski’s second theorem. The sixth line follows from Cramer’s rule. Thus $|K \cap \mathbb{Z}^d| \leq \prod_{i=1}^d 2^\left[ \frac{r \det(B)}{\lambda_i} \right] + 1 \lesssim d \prod_{i=1}^d \lambda_i^{-1} \lesssim d \text{Vol}(K)$, as long as $r \det(B) \lambda_i^{-1} \geq 1$.\footnote{Here we use the inequality $2[x] + 1 \leq 3x$ as long as $x \geq 1$} In this case, we conclude (1) of Theorem \ref{thm:main} so we may assume that $r \det(B) \lambda_i^{-1} < 1$. Thus the only choice for $\tau_d$ is zero, that is

$$K \cap \mathbb{Z}^d \subseteq \text{span}_\mathbb{R} \{ B e_1, \ldots, B e_{d-1} \}$$

and we conclude (2) of Theorem \ref{thm:main} with $W = \text{span}_\mathbb{R} \{ B e_1, \ldots, B e_{d-1} \}$.

$\square$