COUNTING INTEGER POINTS ON VARIETIES

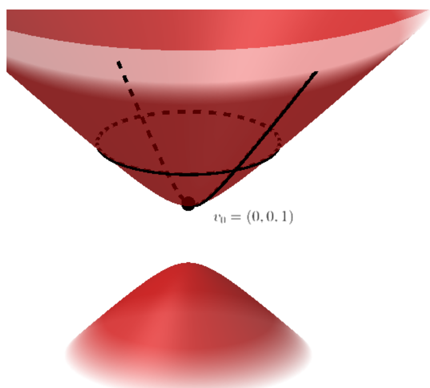
ANDREAS WIESER

1. Counting integer points on the hyperboloid

In the following we would like to count integer points not only in large balls, but also satisfying some side constraint. To keep everything very concrete, I would like to look at the following constraint

$$-x^2 - y^2 + z^2 = 1. \tag{1.1}$$

The set of points satisfying this equation is an example of an affine variety and looks as follows:



Denote by $Q(x, y, z) = -x^2 - y^2 + z^2$ the above quadratic form and let V be the set of points satisfying (1.1). Note that V is disconnected with connected components V^+, V^-, where V^+ contains $v_0 = (0, 0, 1)$. Define

$$V(\mathbb{Z}) = V \cap \mathbb{Z}^3.$$

Given a ball $B_R(0)$ we would like to understand the asymptotics of the number $|B_R(0) \cap V(\mathbb{Z})|$. First, we should as in the Gauss circle problem define a "natural" measure on the variety V.

Definition 1.1 (Cone measure)**.** For any Borel set $B \subset V$ define $m_V(B)$ as the Lebesgue measure of the "cone"

$$B \cdot [0, 1] = \{tb \mid t \in [0, 1], b \in B\}.$$

Note that it is not at all clear, why this measure should be a valid candidate for a measure concerning the counting problem at hand. One, very good reason will be given in a minute.

Theorem 1.2. *There is a constant $C > 0$ so that*

$$|B_R(0) \cap V(\mathbb{Z})| = Cm_V(B_R(0) \cap V) + o(m_V(B_R(0) \cap V))$$

Notice two things:

(a) The error rate is much worse than in the Gauss circle problem.
(b) On a not completely unrelated note, any similar attempt as in the naive approach to the Gauss circle problem is doomed to fail here. In fact, any small "tube" around the boundary of $B_R(0) \cap V$ will have approximately the same measure as $B_R(0) \cap V$ itself (which makes this a harder problem already).

To prove Theorem 1.2 we will use in a very strong fashion the fact that V is homogeneous, a notion we now explain. Consider the special orthogonal group

$$\mathrm{SO}_Q(\mathbb{R}) = \left\{ g \in \mathrm{SL}_3(\mathbb{R}) \mid Q(v) = Q(g.v) \text{ for all } v \in \mathbb{R}^3 \right\}.$$

for the quadratic form Q. By definition the group $\mathrm{SO}_Q(\mathbb{R})$ acts on V. In fact,

Lemma 1.3. $\mathrm{SO}_Q(\mathbb{R})$ *acts transitively on* V *and the stabilizer of* v_0 *is given by*

$$K := \mathrm{Stab}(v_0) = \left\{ \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} : k \in \mathrm{SO}(2) \right\}.$$

Furthermore, the action of $\mathrm{SO}_Q(\mathbb{R})$ *preserves the measure* m_V *i.e.*

$$m_V(g.B) = m_V(B)$$

for any $g \in \mathrm{SO}_Q(\mathbb{R})$ *and any Borel set* $B \subset V$.

You should consider the latter property as the reason why m_V was the right definition of a measure on V. Similarly, I would recommend the following exercise.

Exercise 1.4. *Show that the Lebesgue measure on* $\mathbb{R}^2$ *is the unique non-zero measure up to scalars which is invariant under* $\mathrm{SL}_2(\mathbb{R})$.

The study of invariant measures is central to homogeneous dynamics and indeed ergodic theory. We will return to this topic in greater generality at some point.

For convenience we now also introduce the subgroup

$$A = \left\{ a_t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cosh(t) & \sinh(t) \\ 0 & \sinh(t) & \cosh(t) \end{pmatrix} : t \in \mathbb{R} \right\}.$$

Check that this is indeed a subgroup.

Proof of the Lemma. We want to show that for any $v \in V$ there exists $g \in \mathrm{SO}_Q(\mathbb{R})$ with $g.v = v_0$. By applying

$$\mathrm{diag}(1, -1, -1) \in \mathrm{SO}_Q(\mathbb{R})$$

to v if necessary, we may assume that $v \in V^+$. Now notice that the action of K rotates V^+ around the z-axis, fixing in particular v_0. Using the right rotation on v we can therefore assume that the x-coordinate of v is zero i.e. v is of the form $v = (0, y, z)$ where $z^2 - y^2 = 1$. In particular, $z \geq 1$ so that there exists $t \in \mathbb{R}$ with $\cosh(t) = z$. Replacing t by $-t$ if necessary we obtain $y = \sinh(t)$ and therefore $a_t.v_0 = v$ or equivalently $a_{-t}.v = v_0$.

For the last claim in the lemma note that for any Borel set $B \subset V$ and any $g \in \mathrm{SO}_Q(\mathbb{R})$ we have $g(B \cdot [0,1]) = (g.B) \cdot [0,1]$ by linearity of g. Also, $g \in \mathrm{SO}_Q(\mathbb{R}) \subset \mathrm{SL}_3(\mathbb{R})$ preserves the measure on measurable subsets of $\mathbb{R}^3$ so that

$$m_V(g.B) = \mathcal{L}((g.B) \cdot [0,1]) = \mathcal{L}(g(B \cdot [0,1])) = \mathcal{L}(B \cdot [0,1]) = m_V(B),$$

where $\mathcal{L}$ is the Lebesgue measure on $\mathbb{R}^3$. This concludes the proof of the Lemma. $\square$

By the lemma we can in particular identify V with the quotient

$$\mathrm{SO}_Q(\mathbb{R}) \big/ K$$

via

$$gK \in \mathrm{SO}_Q(\mathbb{R}) \big/ K \mapsto g.v_0 \in V.$$

For the proof of Theorem 1.2 we would like to formulate the correct analogon of the equidistribution problem for large circles in this context. The details of this will be made clearer in the course of the seminar. Essentially the above shows further that we can identify $\mathrm{T}^1 V$ with $\mathrm{SO}_Q(\mathbb{R})$. Additionally, we would like to "glue" together the integer points in $V(\mathbb{Z})$. For this, notice that

$$\mathrm{SO}_Q(\mathbb{Z}) = \mathrm{SO}_Q(\mathbb{R}) \cap \mathrm{Mat}_3(\mathbb{Z})$$

acts on $V(\mathbb{Z})$.

Lemma 1.5 (A Borel-type result). *The action of* $\mathrm{SO}_Q(\mathbb{Z})$ *on* $V(\mathbb{Z})$ *has finitely many orbits.*

Proof. Later. □

As in the previously explained approach to the Gauss circle problem we will therefore consider the space

$$\mathrm{SO}_Q(\mathbb{Z}) \big\backslash \mathrm{SO}_Q(\mathbb{R})$$

and somewhat tautologically orbits under K in it. Geometrically you should think of this as considering a circle at a large height in V and then gluing it up under $\mathrm{SO}_Q(\mathbb{Z})$. The distributional properties of such circles (and also other shapes) will be central in this seminar (buzz word "equidistribution").