# AN APPLICATION OF ERGODIC THEORY TO A CLASSICAL PROBLEM IN NUMBER THEORY 

ROBERT C. RHOADES


#### Abstract

These are the notes from the colloquium talk given by Jordan Ellenberg on December 9, 2005 a the University of Wisconsin. (joint work with Akshay Venkatesh) A famous theorem of Langrange asserts that every positive integer is the sum of four squares. One can ask many more general questions about representations of integers by quadratic forms, or quadratic forms by quadratic forms. We will describe a theorem " of Lagrange type" whose proof relies on ideas from ergodic theory. No prior knowledge of quadratic forms or ergodic theory will be assumed.


## 1. Introduction

A classical result is concerned with the following question about the sum of squares: Which integers are the sum of two squares? Lagrange proved every integer is the sum of four squares and it is completely understood which are the sum of two squares.
Question. So the natural question to ask is how do we push this question forward?
(1) We can ask how many ways can a number be represented as the sum of four squares? This question was considered by Jacobi and is classical.
(2) More generally, we define a quadratic form is a function $Q: \mathbb{Z}^{n} \rightarrow \mathbb{Z}$ given by a homogenous of degree 2 and we write $\operatorname{rank}(Q)=n$. Then we can ask if every integer is represented by $Q$.
For example, $x^{2}+x y+y^{2}+z^{2}$ is a quadratic form of rank 3 .
Definition 1.1. We say that $Q$ represents an integer $N$ if there exists $x_{1}, \ldots, x_{n} \in \mathbb{Z}$ such that $Q\left(x_{1}, \ldots, x_{n}\right)=N$.

Even more generally we are led to the following problem.

## 2. General Problem

Given two quadratic forms $Q, Q^{\prime}$ with ranks $n$ and $m$ with $m<n$. Can we find linear forms $L_{1}, \ldots, L_{n}$ in $m$ variables such that $Q\left(L_{1}, \ldots, L_{n}\right)=Q^{\prime}$. If so we say $Q^{\prime}$ is represented by $Q$ over $\mathbb{Z}$.

I ask the following question:
Question. What can we say when $n=m$ ? I suspect the problem is not difficult.

Remark. Representation of integers by $Q$ is the case when $m=1$.
It is natural to ask what is so special about Quadratic forms? Why don't we consider equations of the form $x^{3}+y^{3}=n$ ? People certainly have done these, but for our purposes it is too high to do higher degree equations then degree 2 , and doing degree 1 is trivial.

In the end this reduces to finding integral points on certain algebraic varieties.

## 3. Local Arguments

It is easy to use local arguments to show $Q$ does not represent $Q^{\prime}$. For example $x^{2}+y^{2}$ does not represent -5 over $\mathbb{Z}$ or over $\mathbb{Q}$ or over $\mathbb{R}$. In this case it is easy to check you can't do it over $\mathbb{R}$ thus you can't do it over $\mathbb{Z}$.

As another example $x^{2}+y^{2}$ does not represent 7 over $\mathbb{Q}$. It is easy to check over $\mathbb{Z}$ just by plugging in enough numbers. Over $\mathbb{Q}$ we may rewrite this equation as $a^{2}+b^{2}=$ $7 c^{2}$ for $a, b, c \in \mathbb{Z}$. So this problem is more like representing a rank 1 quadratic form by a rank 2 quadratic form. Reducing modulo 7 we obtain a contradiction, which shows there are no solutions over $\mathbb{Q}$ to our original problem.

Here we only used that we could reduce modulo 7. This only shows that $x^{2}+y^{2}$ does not represent over $\mathbb{Q}_{7}$ and $\mathbb{Q}_{7}$ is a local field of $\mathbb{Q}$.

The moral here is that you should always check that you have solutions in local fields, because if you don't then you would have them in the field you are interested in. The upshot is that if $Q$ represents $Q^{\prime}$ over $\mathbb{Z}$ (resp. $\mathbb{Q}$ ) it represents $Q^{\prime}$ over $\mathbb{R}$ and all $\mathbb{Z}_{p}$ for all $p$ (resp. $\mathbb{Q}_{p}$ ).

What about the converse? The converse are called local-to-global principals.
Theorem 3.1 (Hasse-Minkowski). If $Q$ represents $Q^{\prime}$ over all $\mathbb{Q}_{p}$ and over $\mathbb{R}$ then $Q$ represents $Q^{\prime}$ over $\mathbb{Q}$.

But our goal are not representing things over $\mathbb{Q}$ but over $\mathbb{Z}$. So do we have the same theorem in our case with $\mathbb{Q}_{p}$ replaced by $\mathbb{Z}_{p}$. It would be great if we had this theorem, but it does not hold in general. That is to say in general, we cannot pass from local solutions to a global solution.

For a nice survey see "On the passage from local to global in number theory" by B. Mazur in the Bulletin of the AMS in 1992.

Example. This local-to-global is not true over $\mathbb{Z}$. We define $Q_{1}: x^{2}+55 y^{2}$ and $Q_{2}: 11 x^{2}+5 y^{2}$ are isomorphic over $\mathbb{Z}_{p}$ for all $p$ and $\mathbb{R}$. But $Q_{2}$ represents 5 over $\mathbb{Q}$ and $Q_{1}$ does not.

## 4. Fixing Local-to-Global

Instead of a single $Q$ consider $Q_{1}, Q_{2}, \ldots, Q_{h}$ the set of forms isomorphic to $Q$ over every $\mathbb{Z}_{p}$ and $\mathbb{R}$. This set is the genus of $Q$. It is not clear, but is true, that the genus is finite. For us, isomorphic means a linear change of variables.

Theorem 4.1 (Siegel-Mass Formula). If $r_{Q}\left(Q^{\prime}\right)$ is the number of representations of $Q^{\prime}$ by $Q$. Then

$$
r_{Q_{1}}+\cdots+r_{Q_{h}}
$$

has a precise asymptotic expression. (asymptotic means something about the size of the matrix which represents $Q^{\prime}$ which is measured by the size of the eigenvalues)

But how do we separate out one of these $r_{Q_{j}}$ from another. Well if $h=1$ then we win!

Letting $Q^{\prime}$ be "sufficiently large" we have the following results:
(1) Kloosterman (1924-thesis) if $n \geq 5$ and $m=1$ then every sufficiently large $n$ which is locally represented by $Q$ is globally represented by $Q$.
(2) For $n=4$ and $m=1$ Kloosterman-Tarkatovski prove the same thing
(3) For $n=3$ and $m=1$ Duke-Schulzer-Pillat make some huge advances.

Definition 4.2. Denote the property $L G(n, m)$ to hold if for all $Q$ of rank $n$ then there exists a positive integer $c(Q) \in \mathbb{Z}$ such that if $Q^{\prime}$ has rank $m$ and we have the following properties
(1) $Q^{\prime}$ represents no integer less than $c(Q)$
(2) $Q^{\prime}$ locally represented by $Q$
then $Q^{\prime}$ is represented by $Q$ over $\mathbb{Z}$.
Example. $L_{1}^{2}+L_{2}^{2}+10 L_{3}^{2}=x^{2}+2 y^{2}$ has no solutions in linear forms.
Question. For what values of $n, m$ do we have $L G(n, m)$ ? We may as well just consider $m \leq n-2$. This is because there exists easy examples for $m=n-1$ that show that we cannot have $L G(n, m)$.
(1) $L G(n, 1)$ for $n \geq 4$ is due to Kloosterman
(2) $L G(3,1)$ by D-S-P
(3) $L G(n, m)$ when $n \geq 2 m+3$ is due to Chsia, Kitav, Knesar in 1978
(4) $L G(6,2)$ is due to Jöcher

Theorem 4.3 (E, Venkantesh 2005). $L G(n, m)$ for $n \geq m+7$.
We notice that the best we could hope for is $n \geq m+2$.
The following group theory puzzle is at the heart of this result. Any improvement in this result could lead to a stronger version of this theorem.
Question. Suppose $V / K$ is a vector space (in our case we have $K=\mathbb{Q}_{p}$ or a nonarchimedean local field). Let $T_{1}, T_{2}, \ldots$ be a sequence of subspaces of codimension $d$ so that no infinite subsequence is contained in a proper subspace of $V$. Given $Q$ a quadratic form and let $O(V)$ be the orthogonal group, $O\left(T_{j}\right) \subset O(V)$ be a group fixing $T_{j}$ element-wise. We want to show that for $d \geq 2$ (but the best we have is $d \geq 7)$ then $O\left(T_{j}\right)$ generate $O(V)$.

## 5. Idea of the Proof

Set $\operatorname{Hom}\left(Q^{\prime}, Q\right)$ over the representations of $Q^{\prime}$ by $Q$ to be a variety $X$. We can act by the orthogonal group $G:=S O_{Q}$. We are interested in $X(\mathbb{Z})$. We think of $Q$ as a vector space with a quadratic form then we want a homomorphism between vector spaces that respect the quadratic form.

To begin with Siegel-Maass says there is a isomorphic form with an $x_{0} \in \tilde{X}(\mathbb{Z})$ where $\tilde{X}=\operatorname{Hom}\left(Q^{\prime}, Q_{1}\right)$ for some $Q_{1}$ in the genus of $Q$. We show that all other forms that have the same genus will have a point in $\mathbb{Z}$.

The proof then rests on ergodic theory and a very general theorem of Raftner gives us what we want.

Jordan believes there is probably a measure theoretic version of this theorem that might tell you each of the forms in the genus represent the chosen $Q^{\prime}$ an equal number of times. This is open but it might be painful to work out, but should be within reach of the method.

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: rhoades@math.wisc.edu

