Indian J. pure appl. Math., 23(5): 321-324, May 1992

Srinivasa Ramanujan Medal Lecture – 1991

VALUES OF QUADRATIC FORMS*

M. S. RAGHUNATHAN, F.N.A.

School of Mathematics, Tata Institue of Fundamental Research
Homi Bhabha Road, Bombay

Many of you will be familiar with Kronecker's theorem; if α is irrational, the set of numbers $m\alpha+n, m,n \in \mathbf{Z}$ is dense in the set of real numbers. This can be reformulated in the following fashion: If $f : \mathbf{R}^2 \to \mathbf{R}$ is the linear form

$$f(x, y) = x\alpha + y$$

on the 2-dimensional vector space $\mathbf{R}^2$, then the values of f on the (discrete) set of lattice points $\mathbf{Z}^2 = \{(x, y) \in \mathbf{R}^2 \mid x, y \in \mathbf{Z}\}$ from a dense subset of $\mathbf{R}^2$ whenever α is irrational. And this can be generalised in the following fashion: let $f : \mathbf{R}^n \to \mathbf{R} (n > 1)$ be a linear form on $\mathbf{R}^n$ such that if $\alpha_1,\ldots\alpha_i,\ldots,\alpha_n$ are defined by

$$f(x_1,\ldots,x_n) = \sum x_i\alpha_i,\ 1 \leq i \leq n,\ x_i \in \mathbf{R}$$

atleast one of the ratios $\alpha_i|\alpha_j$ $(\neq 0)$ is irrational; then $f(\mathbf{Z}_n)$ is dense in R. There are more refined generalisations but we will not go into it now. One way of looking at the problem is as follows: Let L be the kernel of $f : L = \{w \in \mathbf{R}^n) \mid f(w) = 0\}$. Then one has for any $v \in \mathbf{R}^n$ and $w \in L$,

$$f(v + w) = f(v) + f(w) = f(v)$$

i.e. f is invariant under the translation action of L on $\mathbf{R}^n$. Thus the values of f on $\mathbf{Z}^n$ are the same as those of f on the much larger set $L + L^n = \{v + \gamma | v \in L, \gamma \in \mathbf{Z}^n\}$; and if we can show that $L + \mathbf{Z}^n$ is dense in $\mathbf{R}^n$ $f(\mathbf{Z}^n)$ would be dense in $\mathbf{R}^n$. Replacing $\mathbf{R}^n$ by a suitable dimension 2 subspace spanned by lattice vectors one can reduce the question to the case of dimension 2 and thus one has to show that if L is a line in $\mathbf{R}^2$ containing no lattice point, then $L + \mathbf{Z}^2$ is dense in $\mathbf{R}^2$. Finally passing to the quotient by L we are reduced to the problem formulated at the outset. The discussion above is not to suggest an alternative proof but to draw attention to the fact that linear forms are tractable because of the availability of a large group of symmetries. If f is a linear form with kernel L,

$$f \circ (T_v x) = f(x) \ (T_v = \text{translation by } v)$$

for all $x \in \mathbf{R}^n$ and $v \in L$; and the presence of this large group of symmetrics can be exploited when we want to understand this function, in particular its value set.

---

*Lecture delievered at the Physical Research Laboratory, Ahmedabad on 30 December 1991.

The simplest function one can think of on $\mathbf{R}^n$ beyond constants and linear functions are quadratic forms. Recall that a quadratic form on $\mathbf{R}^n$ is a function f of the form

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{n} a_i x_i^2 + \sum_{1\le i\le j\le n} b_{ij} x_i x_j$$

$x_i \in \mathbf{R}$, $1 \le i \le n$. It is a homogeneous polynomial of degree 2. It is natural to ask what can be said of values of quadratic forms on the set of lattice points. Natural, because after having settled the question for linear forms, quadratic forms come to mind as the next least complex functions on R^n; also because quadratic forms turn up very naturally in several different contexts any way.

Understanding quadratic forms is naturally more difficult than understanding linear forms. There is a complete classification over real numbers. The classification theorem says the following. If f is a quadratic form on $\mathbf{R}^n$,

$$f(x) = \sum_{1\le i\le n} a_i x_i^2 + \sum_{1\le i<j\le n} b_{ij} x_i x_j$$

where $x = (x_1,\ldots, z_n)$, one can find a basis $e_1,\ldots,e_n$ of $\mathbf{R}^n$ such that refered to the new basis one has

$$f(y) = \sum_{i=1}^{n} \epsilon_i y_i^2, \quad y = \sum y_i e_i$$

where $\epsilon_i = 0$, 1 or -1. If $p(f) = \#\{i \mid \epsilon_i = 1\}$ $q(f) = \#\{i \mid \epsilon_i = -1\}$ and $n(f) = \#\{i \mid \epsilon_i = 0\}$ then $p(f)$ $q(f)$ and $n(f)$ determine the quadratic form upto equivalence over $\mathbf{R}$ i.e. if f, f' are quadratic forms on $\mathbf{R}^n$ such that $p(f) = p(f')$, $q(f) = q(f')$ and $n(f) = n(f')$, then there is a vector space isomorphism $u : \mathbf{R}^n \to \mathbf{R}^n$ such that

$$f'(x) = f(u(x)).$$

The quadratic form f is positive (resp. negative) definite if $q(f)$ (resp. $p(f)$) $= n(f) = 0$; it is nondegenerate if $n(f) = 0$. It is indefinite if $p(f) \neq 0$ as also $n(f) \neq 0$. f is a rational form if

$$f(x) = \sum_{1\le i,j\le n} a_i x_i^2 + \sum_{1\le i<j\le n} b_{ij} x_i x_j$$

with a_i, $b_{ij} \in \mathbf{Q}$. Suppose now that f is positive (resp. negative) definite. Then one can find a constant $C > 0$ such that

$$f(x) \text{ (resp. } -f(x)) \ge C \sum_{0=1}^{n} x_i^2.$$

This is because f is determined by its values on the unit sphere S^{n-1} - $f(\lambda v) = \lambda^2 f(v)$ and being positive (resp negative definite) definite, f (resp $-f$) is no where zero on S^{n-1} and hence has a minimum $C > 0$, say. Since

$$f(x)(\text{resp. } -f(x))(\Sigma x_i^2)\, f\left(\frac{x}{(\Sigma x_i^2)^{1/2}}\right)\left(\text{resp.}\left(\sum x_i^2\right)\left(-f\left(\frac{x}{(\Sigma x_i^2)^{1/2}}\right)\right)\right) \ge (\Sigma x_i^2)\, C.$$

our contention follows. Thus for a positive (resp. negative) definite quadratic form we have for any non-zero integral point

$$\underline{x} = (x_1 \ldots x_n),\ f(\underline{x}) \text{ (resp. } -f(\underline{x})) \geq C \sum x_i^2 \geq C$$

if $\underline{x} \neq 0$. The values in fact will evidently form a discrete set. Next suppose f is a quadratic form such that $f(\underline{x}) = \lambda(\Sigma\, a_i x_i^2 + \Sigma\, b_{ij} x_{ij})$ with $a_i,\ b_{ij} \in \mathbf{Q}$ and $\lambda \in \mathbf{R}$, then if $N = lcm$ of the denominators of the b_{ij}, we see that $N.\lambda^{-1} f(\underline{x})$ is an integer for $\underline{x} \in \mathbf{Z}^n$. It is clear from this that the set of values in this case is also discrete. So if one is looking for a generalisation of the Kronecker theorem to quadratic forms we need to make the following assumption:

f is not positive or negative definite and f is not a real multiple of a rational form. It turns out that this is not adequate either. There are indefinite quadratic forms in 2 variables such that their set of values on integer points are bounded away from zero. However, when the number of variables is at least 3, the picture changes. It turns out that one has the following theorem:

If $f(\underline{x}) = \sum_{1 \leq i < j \leq n} b_{ij} x_i x_j + \sum_{1 \leq i \leq n} a_i x_i^2$ is a quadratic form such that $n \geq 3$, $n(f) = 0$, $p(f) \neq 0$ and $q(f) \neq 0$ and f is not of the form λg where g has all coefficients in $\mathbf{Q}$, then $f(\mathbf{Z}^n \backslash \{0\})$ is dense in $\mathbf{R}$.

This theorem is due to the Fields Medalist Margulis (1989). It was conjectured by Oppenheim and Davenport proved the theorem by analytic methods when $n \geq 10$. Margulis' approach was based on some observations I had made. The basic idea is as follows. Let $GL(n, \mathbf{Z})$ denote the group of invertible $(n \times n)$-matrices over $\mathbf{Z}$. Then for $A \in GL(n, \mathbf{Z})$ and $v \in \mathbf{Z}^n \backslash \{0\}$, $AV \in Z^n \backslash \{0\}$. Consequently $f(\mathbf{Z}^n) = f(GL(n, \mathbf{Z})\mathbf{Z}^n)$. On the other hand let $G \subset GL(n, \mathbf{R})$ denote the group of linear automorphism of $\mathbf{R}^n$ consisting of $T \in GL(n, \mathbf{R})$ with $f(T(\underline{x})) = f(\underline{x})$ for all $\underline{x} \in \mathbf{R}^n$ - G is the orthogonal group of $0(f)$ of the quadratic form f. Clearly then

$$\begin{aligned} f(\mathbf{Z}^n) &= f(0(f)GL(n, \mathbf{Z})\mathbf{Z}^n) \\ &= f(0(f)GL(n, \mathbf{Z})v_0) \end{aligned}$$

where $v_0 = (1, 0 \ldots, 0)$. Now $SL(n, \mathbf{R})\, v_0 = \mathbf{R}^n \backslash \{0\}$, so that if one can show that $SL(n, \mathbf{R})$ is contained in the closure of $0(f).GL(n, \mathbf{Z})$, i.e. if every element of $SL(n, \mathbf{R})$ is a limit of a sequence of the form $T_n A_n$ where $T_n \in 0(f)$, $A_n \in GL(n, \mathbf{Z})$, then every value of f on $\mathbf{R}^n - \{0\}$ is the limit of values of the form $f(T_n A_n v_0)$, $T_n \in 0(f)$, $A_n \in GL(n, \mathbf{Z})$ and $f(T_n A_n v_0) = T(A_n v_0)$; and $A_n v_0 \in Z^n - \{0\}$. We can thus conclude that every value $f(v)$, $v \in \mathbf{R}^n - \{0\}$ is the limit of values of f on non-zero lattice points. Since f is such that $n(f) = 0$ while $p(f)$, $q(f)$ are non-zero, from the well known facts about quadratic forms over $\mathbf{R}$, one knows that $f(\mathbf{R}^n - \{0\}) = \mathbf{R}$ and the theorem would be proved.

Margulis showed precisely what was exploited above viz. every matrix in $SL(n, \mathbf{R})$ can be approximated by matrices of the form $A.T, A \in 0(f)$, $T \in GL(n, \mathbf{Z})$ as closely as we want. This kind of result belongs in the domain of ergodic theory. The crucial properties of the form f that are exploited are

(i) $0(f)$ is not compact

(ii) $0(f)$ contains a matrix $T \neq \{1\}$ all of whose eigenvalues are 1.

(iii) $0(f) \cap GL(n, \mathbf{Z})$ is "sparse" in $0(f)$.

The first property is equivalent to the assumption that $p(f)$, $n(f)$ are non zero. The second property is true because of (i) and our assumption that $n \geq 3$. (If $n = 2$, there is no such T). The third property is equivalent to the assumption that f is not a multiple of a rational form. I will not go into the proof of the result which requires lot more background information. The point I want to emphasise here is the effectiveness of ideas from group theory in solving questions of this kind. We have exploited the fact that f has a large group of symmetries. So the set of values of f on lattice points is the same as the values of f on a much larger set viz. $0(f)(\mathbf{Z}^n \setminus \{0\})$ – and $0(f)$ is a continuous group with $n(n-1)/2$ parameters and as has already been remarked it is not compact. The right setting is to look at the quotient space $SL(n, \mathbf{R})/SL(n, \mathbf{Z})$ and study the orbits of various points of this space under the group $SO(f) = (0(f) \cap SL(n, \mathbf{R}))$. The space $SL(n, \mathbf{R})/SL(n, \mathbf{Z})$ is a locally compact space which carries a $SL(n, \mathbf{R})$ – invariant finite measure and it is the study of measure theoretic properties of the action of unipotent elements in $SL(n, \mathbf{R})$ acting by translations on this space that lead Margulis to his result. A more refined result settling a conjecture I made several years ago has been recently proved by Marina Ratner. The theorem of Margulis has been generalised to a result which says something about values in p-adic fields by A. Borel and Gopal Prasad.