UNIPOTENT FLOWS AND QUADRATIC FORMS (AFTER LINNIK)

AKSHAY VENKATESH

Suppose $Q(x, y, z)$ is a positive definite quadratic form, e.g. $x^2 + 5y^2 + 10z^2$.

Question. Which values does Q take? I.e. $Q(\mathbb{Z}^3)$.

Answer (Duke, Schulze-Pillot)**.** *For N (square-free) and large enough we can solve $Q(x, y, z) = N$ if and only if it is solvable modulo m for all integers m. This cuts out a finite number of congruence classes)*

Linnik proved a slightly weaker statement where he imposed an auxiliary congruence condition on N. He also showed that as $N \to \infty$ the set of solutions to $Q(x, y, z) = n$ becomes uniformly distributed, and similarly, as $N \to \infty$ the set of solutions to $Q(x, y, z)$ becomes uniformly distributed when reduced modulo a fixed q (i.e. fix q, e.g. $q = 7$, then $\{(x, y, z) \in \mathbb{Z}^3 \mid Q = N\} \xrightarrow[\text{reduce} \mod q]{} \{(x, y, z) \in (\mathbb{Z}/q\mathbb{Z})^3 \mid Q = N\}$).

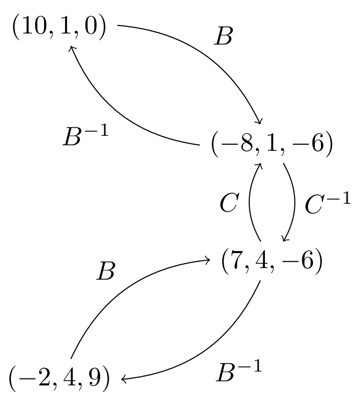
We will show that for $Q = x^2 + y^2 + z^2$, $\{x^2 + y^2 + z^2 = N\} \xrightarrow[\text{reduce} \mod 7]{} \{x^2 + y^2 + z^2 = N \mod 7\}$ if $(N, 6) = 1$, and $N \equiv 1 \mod 5$ (this is Linnik's auxiliary prime condition, the 5 is arbitrary), then as $N \to \infty$ this become uniformly distributed.

1. Explicit proof following Linnik due to Ellenberg, Michel, Venkatesh

Let $A = \frac{1}{5}\begin{pmatrix} 5 & & \\ & -4 & 3 \\ & -3 & -4 \end{pmatrix} \in \mathrm{SO}(3)$, and B, C be the same rotation about the y and the z axes respectively. Set $S(N) = \{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + y^2 + z^2 = N\}$

Fact 1. *If $\underline{x} = (x, y, z) \in S(N)$, then exactly 2 of $A\underline{x}, A^{-1}\underline{x}, B\underline{x}, B^{-1}\underline{x}, C\underline{x}, C^{-1}\underline{x}$ belong to $\mathbb{Z}^1$ (i.e., to $S(N)$).*

Example 1. Let $N = 101$, $\underline{x} = (10, 1, 0))$. Then



So from each $\underline{x} \in SN$ you get a string in A, B, C and their inverses, e.g $\xleftarrow{B}\xleftarrow{C} \underline{x} \xrightarrow{A}\xrightarrow{B}\xrightarrow{A^{-1}}$.

Fact 2. *$\underline{x}, \underline{x}' \in S(N)$ correspond to the same string of ℓ steps in either direction if and only if $\underline{x} \equiv \pm\underline{x}'$* mod 5^ℓ.

Example 2. $\xleftarrow{C}\xleftarrow{A^{-1}}\xleftarrow{B} \underline{x} \xrightarrow{A}\xrightarrow{B}\xrightarrow{C}$ and $\xleftarrow{C}\xleftarrow{A^{-1}}\xleftarrow{B} \underline{x}' \xrightarrow{A}\xrightarrow{B}\xrightarrow{C}$ if an only if $\underline{x} \equiv \underline{x}' \mod 5^3$.

Date: February 05, 2015.

Fact 3 (Linnik's basic lemma)**.** *The number of pairs* $\underline{x}, \underline{x}' \in S(N)^2$ *where* $\underline{x} \equiv \underline{x}' \mod M$ *is "not much more than expected", precisely this means it is*

$$\ll |S(N)| + (NM)^{\varepsilon}\left(1 + \frac{|S(N)|^2}{M^2}\right)$$

Recall that we are taking the set $S(N)$ and reducing modulo M which leaves a set of size M^2. Consider the setting where $M = 7$. Give the set of solutions the structure of a 6-valent graph, $G(N)$, where $\underline{\mathrm{x}}$ is joined to $A\underline{\mathrm{x}}, A^{-1}\underline{\mathrm{x}}, B\underline{\mathrm{x}}, B^{-1}\underline{\mathrm{x}}, C\underline{\mathrm{x}}, C^{-1}\underline{\mathrm{x}}$. Each $\underline{\mathrm{x}}$ gives a path in the graph. Now, suppose that the reduction is not uniformly distributed. Then there exists a subset $X \subseteq G(N)$ such that most paths spend more than $\frac{|X|}{|G(N)|}$ time inside X.

But, in a fixed finite regular graph G, the fraction of paths of length ℓ that spend more than $\frac{|X|}{|G(N)|} + \delta$ time inside X is at most $e^{-c\ell}$, where c is a function of G, X, δ. Therefore, there must be "unusually many" pairs $(\underline{\mathrm{x}}, \underline{\mathrm{x}}')$ giving rise to some path of length ℓ on $G(N)$. By Fact 2, we get that $\underline{\mathrm{x}} \equiv \pm\underline{\mathrm{x}}' \mod 5^{\ell}$, which contradicts Fact 3.

2. Reinterpretation

We can instead examine what happens if we fix a vector and move the lattice instead. Take the set of lattices in $\mathbb{Q}^3$ and consider the action of $\mathrm{GL}(3, \mathbb{Q}^3)$. Given a lattice L and $g \in \mathrm{GL}(3, \mathbb{Q}^3)$, we have that gL and L differ only at p. Let L_p be the closure of L in $\mathbb{Q}_p^3$, then $(gL)_p = g(L_p)$. Therefore, $\mathrm{GL}(3, \mathbb{A})f)$, where $\mathbb{A}_f = \prod_p \mathbb{Q}_p$ is the finite adeles, acts on the set of lattices in $\mathbb{Q}^3$. Let $\mathcal{G}$ denote the orbit of $\mathbb{Z}^3$ under $\mathrm{SO}(3, \mathbb{A}_f$.

$$\begin{array}{ccc}
\{(x,y,z) \in \mathbb{Z}^3 \mid x^2+y^2+z^2 = N\}/\mathrm{SO}(3,\mathbb{S}) & \longrightarrow & \{L \in \mathcal{G}, \underline{\mathrm{x}} \in L \mid \underline{\mathrm{x}} \cdot \underline{\mathrm{x}} = N\}/\mathrm{SO}(3,\mathbb{Q}) \\
\downarrow & & \downarrow \\
\{(x,y,x) \in \mathbb{Z}/7\mathbb{Z} \mid x^2+y^2+z^2 = N \mod 7\}/\mathrm{SO}(3,\mathbb{Z}) & \longrightarrow & \{L \in \mathcal{G}, \underline{\mathrm{x}} \in L/7L \mid \underline{\mathrm{x}} \cdot \underline{\mathrm{x}} = N \mod 7\}/\mathrm{SO}(3,\mathbb{Q})
\end{array}$$

Fact. *Both horizontal maps are bijections*

Let U be an open compact subgroup of $\mathrm{SO}(3, \mathbb{A}_f)$. Then there is a left action of $\mathrm{SO}(3, \mathbb{A}_f)/U$ on the space $\{L \in \mathcal{G}, \underline{\mathrm{x}} \in L/7L \mid \underline{\mathrm{x}} \cdot \underline{\mathrm{x}} = N \mod 7\}/\mathrm{SO}(3, \mathbb{Q})$ so that

$$\{L \in \mathcal{G}, \underline{\mathrm{x}} \in L/7L \mid \underline{\mathrm{x}} \cdot \underline{\mathrm{x}} = N \mod 7\}/\mathrm{SO}(3,\mathbb{Q}) \simeq \mathrm{SO}(3,\mathbb{Q})\backslash\mathrm{SO}(3,\mathbb{A}_f)/U$$

Note that any two solutions $\underline{\mathrm{x}}, \underline{\mathrm{x}}' \in \mathbb{Q}^3$ to $\underline{\mathrm{x}} \cdot \underline{\mathrm{x}} = \underline{\mathrm{x}}' \cdot \underline{\mathrm{x}}' = N$ are in the same $\mathrm{SO}(3, \mathbb{Q}$ orbit. So fix an $\underline{\mathrm{x}}_0 \in \mathbb{Q}^3$ with $\underline{\mathrm{x}}_0 \cdot \underline{\mathrm{x}}_0 = N$, then

$$\{L \in \mathcal{G}, \underline{\mathrm{x}} \in L \mid \underline{\mathrm{x}} \cdot \underline{\mathrm{x}} = N\}/\mathrm{SO}(3,\mathbb{Q}) = \{L \in \mathcal{G}, \underline{\mathrm{x}}_0 \in L \mid \underline{\mathrm{x}}_0 \cdot \underline{\mathrm{x}}_0 = N\}/\mathrm{Stab}_{\mathrm{SO}(3,\mathbb{Q})}(\underline{\mathrm{x}}_0)$$

But, the stabilizer is $\mathrm{SO}(2, \mathbb{Q})$. Therefore we get an action of $\mathrm{SO}(2, \mathbb{A}_f)$ on the set $\{L \in \mathcal{G}, \underline{\mathrm{x}}_0 \in L\}$ which in turn gives an action $\mathrm{SO}(2, \mathbb{A}_f)$ on $\{x^2 + y^2 + z^2 = N\}/\mathrm{SO}(3, \mathbb{Z})$.