# Reading: ...

The statement is a bit technical that the "full [counting] measure" is close to the "joint measure". These terms don't mean anything until we at least provide a definition. That doesn't mean we've looked at them ...ever.

**Thm 1.1** [AES 16a] Let $d \geq 3$ and for any integer $D$ define

$$Q_D = \left\{ \left( \frac{v}{||v||}, [\Lambda_v] \right) : v \in \hat{\mathbb{Z}}^d, ||v||^2 = D \right\} \subset S^{d-1} \times \mathcal{X}_{d-1}$$

Then the normalized counting measure $m_D$ on $\mathcal{Q}_D$ converges to $m_{S^{d-1}} \times m_{\chi_{d-1}}$ in the weak* topology as $D \to \infty$, provided that the set $\mathcal{Q}_D$ is non-empty and that in addition one has the following conditions on the number $D$

- $d = 3$ ...
- $d = 4$ ...

For $d \geq 4$ a stronger claim is given. They remove a "congruence condition" and instead of the "shape of the lattice" they look at a "grid". These terms might deserve enunciation.

**Thm 1.2** Let $d = 4$ or $d = 5$ for any positive integer $D$, let $m_{Q_D}$ denote the normalized counting measure

$$|m_{Q_D}(f) - m_S^{d-1} \times m_{\mathcal{X}}| < D^{-\kappa} S_\infty(f)$$

(provided that $Q_D$ is non-empty).

How we can read this as an elementary problem? Since $f \in C_c^\infty(S^{d-1} \times \mathcal{X}_{d-1})$ could be any **smooth** and **compactly supported** function on the space of [sphere] $\times$ [space of lattices].

How do we decide about elements of $Q_D$ ? Maybe this set is empty? Counting measure suggests we locate the object exactly at the point. That's unlikely we might try to find equidistribution, we

The theorem clearly says that something "nearly factors" and our solutions is "nearly symmetric":

$$[\text{counting measure}] \approx [\text{sphere measure}] \times [\text{lattice measure}]$$

We are unlikely to solve these problem explicitly as $D \to \infty$. How can we write $v^2 = v_1^2 + v_2^2 + v_3^2 + v_4^2 = D$ with $D \gg 10^{100}$? Maybe there are appoximate algorithms for budgeting space and time resources?

Finally smooth functions can be really arbitrary, we could try to construct a smooth function that vanishes on a dense set of the sphere (as $D \to \infty$) or with other properties, and our equidistribution result should old. Indeed, these are left as exercises.

Around 1959, there's interest in writing as an integer as sums of four squares. First of all:

- $\widehat{\mathbb{Z}}^d$ is the set of "primitive" vectors in $\mathbb{Z}^d$
- If we have any four numbers $\vec{v} = (v_1, v_2, v_3, v_4) \in \mathbb{Z}^4$ the vector has a radius $v^2 = v_1^2 + v_2^2 + v_3^2 + v_4^2 = D = \text{radius}^2$.
- One more computation we can do is the orhogonal lattice:

$$\Lambda_v = v^\perp \cap \mathbb{Z}^4$$

  These exercises in 4-dimesional geomtry might be done formally using Linear Algebra (in fact module theory it's over $\mathbb{Z}$) yet ...

So we can study the joint equidistribution problem:

$$\frac{1}{\sqrt{D}} v \in [\text{diretion}] \times [\text{shape of the lattice}]$$

The very notion of **vector** took centuries to develop to describe quantities in geometry and physics.[1]

## References


[1] ...

[2] ...


[1] Euclid's elements had a notion of "line" or of "rectangle" not a notion of "physics". Wikipedia credits the term "vector" to dissions clarifying Electricity and Magnetism in 1860's.

Actually *using* these formulas is another story. Let's try to read the instructions. Set $d = 4$ so we are trying to solve:

$$v^2 = v_1^2 + v_2^2 + v_3^2 + v_4^2 = D \in \mathbb{Z}$$

we are looking for integer solutions $(v_1, v_2, v_3, v_4) \in \mathbb{Z}$. So that's the statement "Let $v \in S^3(D)$ be a primitive point." This is the equation we would like to solve and we're assuming it's already there.

For each vector $v \in S^3(D)$ we can find a group orbit $v \mapsto \mathbb{H}_v(\mathbb{Q}_S)\mathbb{G}_1(\mathbb{Z}^S)$ dense in $\mathcal{Y}_1^S$ with $S \in \{\infty, p\}$. There's a lot of notation. If we rotate the sphere $\mathsf{SO}_3(\mathbb{Z})$ has only 8 elements.

- $\mathbb{Q}_S = \prod_v \mathbb{Q}_v = \mathbb{Q}_\infty \times \mathbb{Q}_p = \mathbb{R} \times \mathbb{Q}_p$
- $\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p}]$ (we adjoined the fraction $\frac{1}{p}$ standard move in **commutative algebra**).
- $\mathbb{H}_v := \mathsf{Stab}_{\mathbb{G}_1}(v)$ is the **stabilizer** of $v$ in the quaternion algebra $\mathbb{H}$.
- $\mathcal{Y}_S = \big(\mathsf{ASL}_3(\mathbb{R}) \times \mathsf{SO}_3(\mathbb{R})\big) \times \big(\mathsf{ASL}_3(\mathbb{Q}_p) \times \mathsf{SO}_3(\mathbb{Q}_p)\big)$ this is a rather complicated homogeneous space since it insolves both the real part $\mathbb{R}$ and the $p$-adic part $\mathbb{Q}_p$.

**Q** Do we understand how to compute stabilizers in this setting. This object maps a vector to an entire group, and then we are letting $v \in S^3(D)$ vary over all the lattice points of the $3$-sphere.

We can try to solve for appoximate group *orbits*:

Given $g_\infty \in \mathsf{SO}_3(\mathbb{R})$ we can find some "rotations" $(h_\infty, h_p) \in \mathbb{H}_v(\mathbb{Q}_p \times \mathbb{R})$ (the subgroup that stabilizes the vector $v \in S^3(D)$).

$$[g_\infty \in \mathsf{SO}_3(\mathbb{R})] \to [(h_\infty, h_p) \in \mathbb{H}_v(\mathbb{Q}_p \times \mathbb{R})]$$

A perfect equation is too much we need just approximate identity of group orbits:

$$(h_\infty, h_p)\,\mathsf{SO}_3(\mathbb{Z}[\tfrac{1}{p}]) \approx (g_\infty, e)\mathsf{SO}_3(\mathbb{Z}[\tfrac{1}{p}])$$

This might be difficult because the rotations $(h_\infty, h_p)$ stabilize the previous solution $v \in S^3(D)$. For group elemeents we get an approxiate identity of the $3 \times 3$ matrices:

$$(h_\infty, h_p)(\gamma, \gamma) \approx (g_\infty, e)$$

We claim that with $\gamma \in \mathsf{SO}_3[\frac{1}{p}]$ and we can solve $w = \gamma^{-1}v$ (observe $\gamma$ has an inverse rotation $\gamma^{-1}$, so that $\gamma^{-1}v \in \mathbb{Z}^4$, solves our sum-of-four-squares in the direction arbitrarily close to $v$.

We have both that $\mathbb{Z}[\frac{1}{p}] \subseteq \mathbb{R}$ and $\mathbb{Z}[\frac{1}{p}] \subseteq \mathbb{Q}_p$ (with two different nototions of topology "closeness" either $|\frac{1}{p}| = \frac{1}{p} < 1$ or that $|\frac{1}{p}| = p$) so that maybe $\mathbb{Z}[\frac{1}{p}] \subseteq \mathbb{Q}_p \cap \mathbb{R}$.

Group theory exercise:

- over the real numbers $\gamma^{-1}v = \gamma^{-1}h_\infty^{-1}v \approx g_\infty^{-1}v \in \mathbb{R}^4$.
- over modular arithmetic $\gamma^{-1}v = \gamma^{-1}h_p^{\infty}v \approx v \in \mathbb{Q}_p^4$.
- conclude that $\gamma^{-1}v \in \mathbb{Z}^4$ .

**10/20** Here at least we just get told the answer to the exercise:

$$\begin{aligned} G_S = G_\infty \times G_p &= \mathbb{G}(\mathbb{R}) \times \mathbb{G}(\mathbb{Q}_p) \\ &= \big(\mathbb{G}_1(\mathbb{R}) \times \mathbb{G}_1(\mathbb{Q}_p)\big) \times \big(\mathbb{G}_2(\mathbb{R}) \times \mathbb{G}_2(\mathbb{Q}_p)\big) \\ &= \big(\text{rotations} \times \text{lattices}\big)_\infty \times \big(\text{rotations} \times \text{lattices}\big)_p \\ &= \big(\mathsf{SO}_4(\mathbb{R}) \times \mathsf{SL}_3(\mathbb{R})\big) \times \big(\mathsf{SO}_4(\mathbb{Q}_p) \times \mathsf{SL}_3(\mathbb{Q}_p)\big) \end{aligned}$$

So whatever problem we are trying to solve (in this case sum of four squares or sum of five squares) this is just our strategy of moving between solving the distance equations over congruences and with "Euclidean" distances.

$$\Gamma = \mathbb{G}(\mathbb{Z}[1/p]) \text{ is a lattice in } \mathbb{G}(\mathbb{R}) \times \mathbb{G}(\mathbb{Q}_p)$$

Abstractly this equation looks great even if our original question is getting further and further lost. There is isomorphism

$$\Gamma\mathbb{G}(\mathbb{Q}_S) \simeq \mathbb{G}(\mathbb{Z}[1/p])\backslash\mathbb{G}(\mathbb{Q}_S)$$

There's a group action:

$$g \cdot x = xg^{-1} \text{ with } x \in \Gamma\backslash\mathbb{G}(\mathbb{Q}_S) \text{ and } g \in \mathbb{G}(\mathbb{Q}_S)$$

At least theoretically we can write this freshman number theory problem as the comparison of two different Haar measures over algebraic groups.

The symmetry group of this problem seems to be:

$$\mathsf{SO}_3(\mathbb{R}) \times \mathbb{H}_v(\mathbb{Q}_p)$$

The second copy is also the rotation group (stabilizing $v$) over the finite place, $\mathbb{Q}_p$.

Just a reminder:

- Fermat theorem $p = x^2 + y^2$
- Lagrange Theorem $n = a^2 + b^2 + c^2 + d^2$

- Legendre Theorem $n = a^2 + b^2 + c^2$
- Ratner Theorem

$$\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$$