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

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

(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] × [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":

[counting measure] ≈ [sphere measure] × [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 $v^2 = v_1^2 + v_2^2 + v_3^2 + v_4^2 = D = \mathsf{radius}^2$.

- 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:

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

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

References

[1] ...

[2] ...

[3]

[4] Matthew Tointon. **Approximate Groups** (London Mathematical Society Student Texts #94)

---

[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_∞, h_p) stabilize the previous solution $v \in S^3(D)$. For group elemeents we get an approxiate identity of the 3×3 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 γ has an inverse rotation γ^{-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

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

Example that the horocycle flow on $\mathsf{SL}(2, \mathbb{Z}) \backslash \mathsf{SL}(2, \mathbb{R})$ is ergodic and mixing. How do we illustrate the mixing here? That a neighborhood is going to spread out over the entire space.[2]

10/24 Here's a result I found on `arXiv:1808:01584` involving the Brauer-Manin obstrution.

Let X be a scheme over $\mathbb{Z}$ given by $x^2 + y^2 + z^2 - xyz = 4 + 2(lw)^2$ where w is an odd integer and l is a prime with $l = \pm 3 \pmod 8$.

If $lw = \pm 4 \pmod 9$ then $X(A_{\mathbb{Z}})^{Br} \neq \varnothing$. (There *is* an obstruction.)

X is an Affine scheme over $\mathbb{Z}$ and we write $X(A_{\mathbb{Z}}) = \prod_p X(\mathbb{Z}_p)$.

10/28 Let's do some "unpacking" – which menas just "reading". The theorem says $f \in C_c^\infty(\mathcal{Y})$ so there are two requisites:

- infinitely differentiable (e.g. no spikes like $f(x) = |x|$).

- "compact support" on the space

- $S^3 \times \mathsf{SL}_3(\mathbb{Z}) \backslash \mathsf{SL}_3(\mathbb{R}) / \mathsf{SO}_3(\mathbb{R} = \{\texttt{spheres}\} \times \{\texttt{lattices}\}$

How do we define smooth functions on these points? We're saying that the "average" of f supportd on the solutions to $n = a^2 + b^2 + c^2 + d^2$. Using Ratner theorem we might be able to traverse the entire space of lattices.

The acting group is the rotation group $\times$ the group of symmetries of the grid[3].

$$\left(\mathsf{SO}_3(\mathbb{R}) \times \mathsf{SL}_3(\mathbb{R})\right) \times \left(\mathsf{SO}_3(\mathbb{Q}_p) \times \mathsf{SL}_3(\mathbb{Q}_p)\right)$$

---

[2]Scholars spent a lot of time trying to prove or disprove Euclid's fifth postulate. Searching online, the term Hyperbolic geometry is coined around 1850 and discussions of special relativity around 1920. The connection to number theory and fractions during the 1980s or earlier.

[3]These were origially called the "Wallpaper groups". Certainly, the lawyer Pierre de Fermat didn't think of affine group symmetry in 1650. Over the next two centuries, his result would checked by serious and recteational mathematics. 1750 for a proof, we don't get the term **ring** or **ideal** until 1850, by Richard Dedekind. Emmy Noether and Emil Artin wouldn't revise algebra into an abstract subject until the turn of 20th century.

The lattice that we're setting to **1** is also larger. It's not just based on $\mathbb{Z}$ it's based on $\mathbb{Z}[\frac{1}{p}]$. This group will act on both the $\mathbb{R}$ component and the finite-place $\mathbb{Q}_p$.

$$\Gamma = \mathsf{SO}_3(\mathbb{Z}[\tfrac{1}{p}]) \times \mathsf{SL}_3(\mathbb{Z}[\tfrac{1}{p}])$$

They are writing $\Delta_H = \{(h,h) : h \in H\}$ for the **diagonal embedding**, here it just means we're going to do the same thing to both copies of our group.

$$\left(\mathbb{G}_1(\mathbb{Z}[\tfrac{1}{p}]) \times \mathbb{G}_2(\mathbb{Z}[\tfrac{1}{p}])\right) \cdot \left((k_v, e), (\theta_v, e)\right) \cdot \Delta_{\mathsf{SO}_3(\mathbb{R}) \times \mathbb{H}_v(\mathbb{Q}_p)}$$

The diagonal action could mean . Let's remind ourselves basic facts about matrix groups.

- $\mathsf{SO}_3(\mathbb{R}) \subseteq \mathsf{SL}_3(\mathbb{R})$
- $\mathbb{H}_v(\mathbb{Q}_p) \simeq \mathsf{SO}_3(\mathbb{Q}_p)$
- $k_v, \theta_v \in \mathsf{SO}_4(\mathbb{R})$

(rotations are part of the special linear group, they preserve lattices) (quaternions are 3D rotations) (these are 3D rotations we found in another computation) Using this diagonal group action we could try to infer one solution from another. We let the rotation vary and get a solution vector and lattice in random directions.

If we restruct to the rotation group the methods still work and get various sum-of-four-squares solutions:

$$\overline{\left(\mathbb{H}_v(\mathbb{R}) \times \mathbb{H}_v(\mathbb{Q}_p)\right)\mathsf{SO}_3(\mathbb{Z}[\tfrac{1}{p}])} = \mathsf{SO}_3(\mathbb{R}) \times \mathsf{SO}_3(\mathbb{Q}_p)$$

This leads to approximate equations (and approximate groups):

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

If we solve the equation in the ∞ place (over $\mathbb{R}$) and over the p-place (over $\mathbb{Q}_p$, e.g. using congruences or Hensel's Lemma) and it's a lattice point (in $\mathbb{Z}[\frac{1}{p}]$ then we have a solution over $\mathbb{Z}$.

OK. As usual, reading the "instruction manual" does little to help us reason about so-and-so's theoretical framework, or to help us "solve" equations in practical setting.[4]

---

[4] Maybe we "solve" the "equation" who care? Maybe solving is overrated.

The last point is worth repeating. We have that $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ is a lattice in $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$, as might be found in Wikipedia[5]

---

[5]https://en.wikipedia.org/wiki/Arithmetic_group