Rational points on symmetric varieties

Yves Benoist
joint work with Hee Oh

www.dma.ens.fr/˜benoist

Abstract

Let Z be a symmetric variety defined over $\mathbb{Q}$ and p a prime number. (For instance Z may be a quadric)

I will describe equidistribution results for the rational points of Z with denominator a power of p.

This will rely on a polar decomposition of p-adic symmetric spaces.

1. An old example
2. Integral points on symmetric varieties
3. Rational points on symmetric varieties
4. Well-roundedness, mixing and wavefront

1. An old example

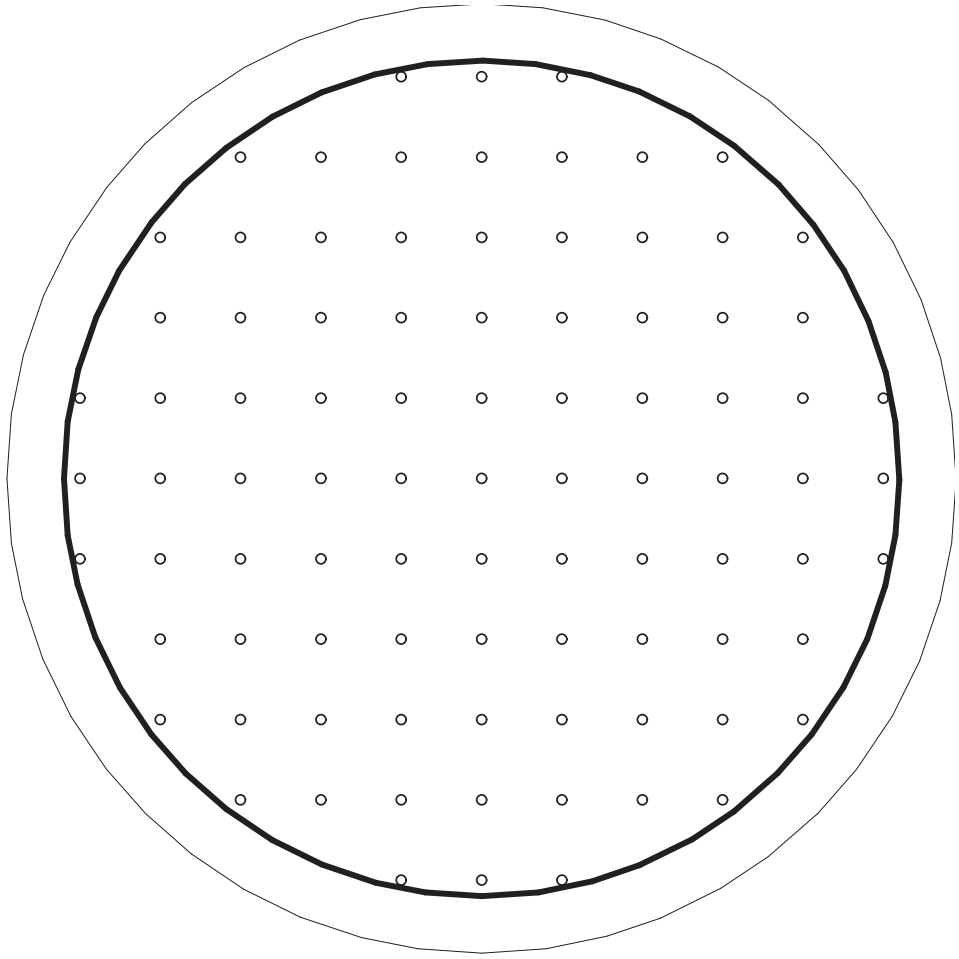
Set $N_R = \#(\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 \leq R^2\})$**.**

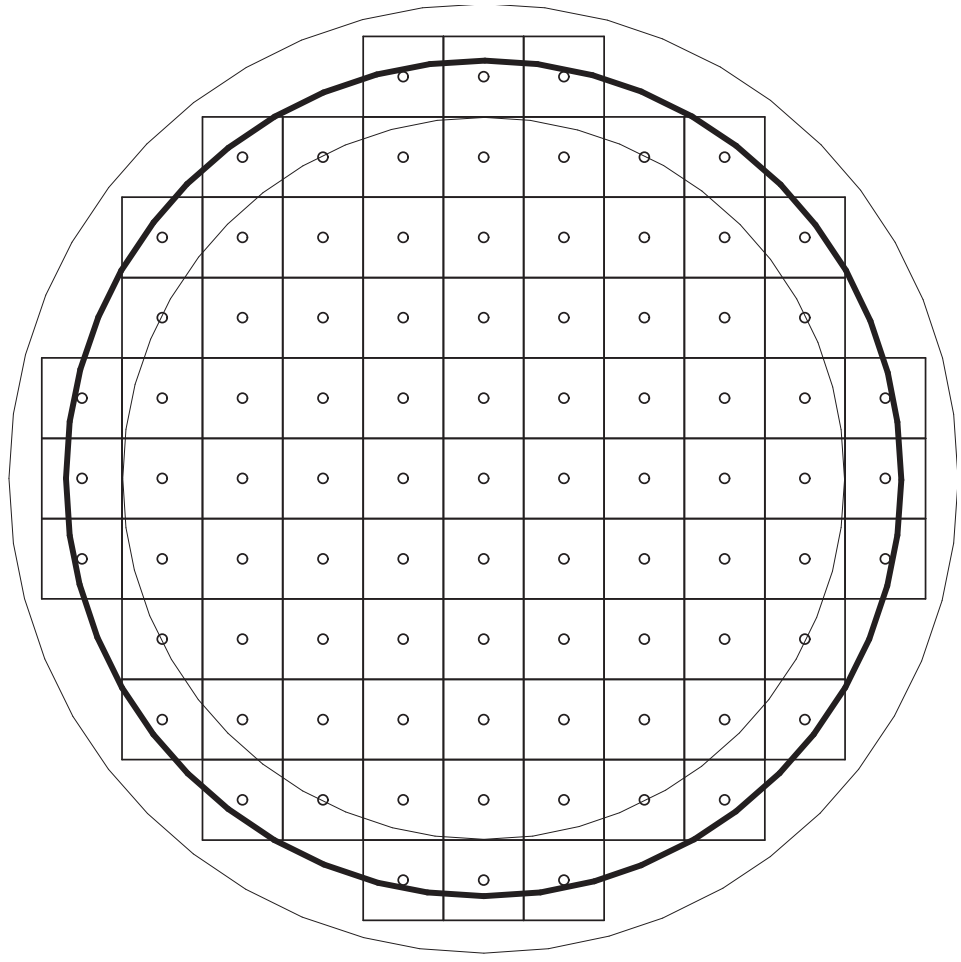
Theorem (Gauss) $N_R = \pi R^2 + O(R)$

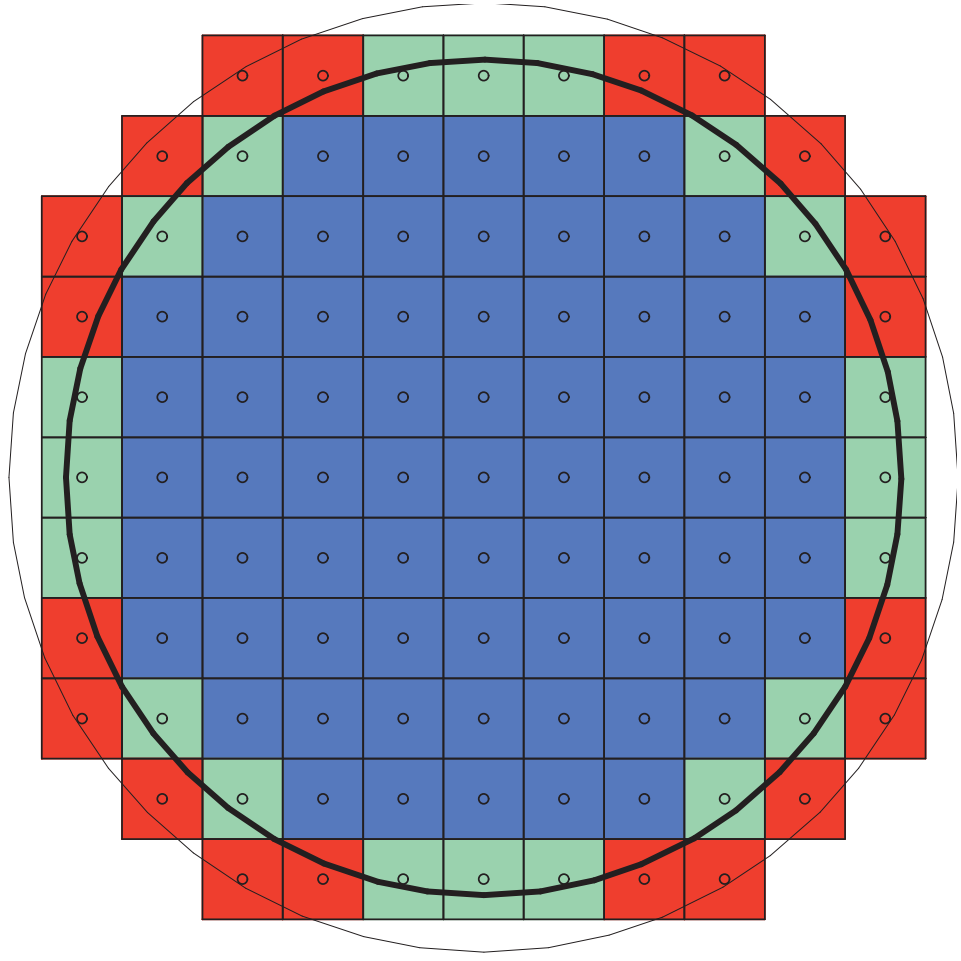
Proof $\pi\,(R - \frac{1}{\sqrt{2}})^2 \leq N_R \leq \pi\,(R + \frac{1}{\sqrt{2}})^2$**.**

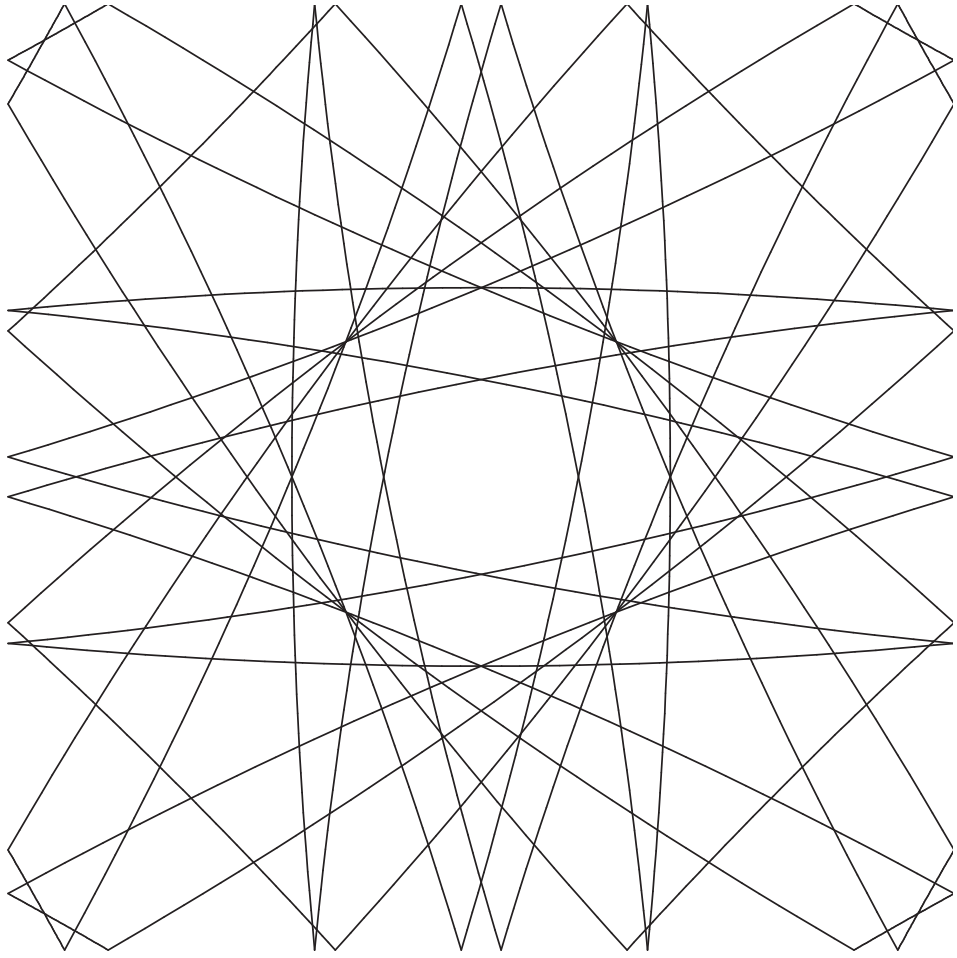
Best hoped error term: $O(R^{\frac{1}{2}+\varepsilon})$**.**

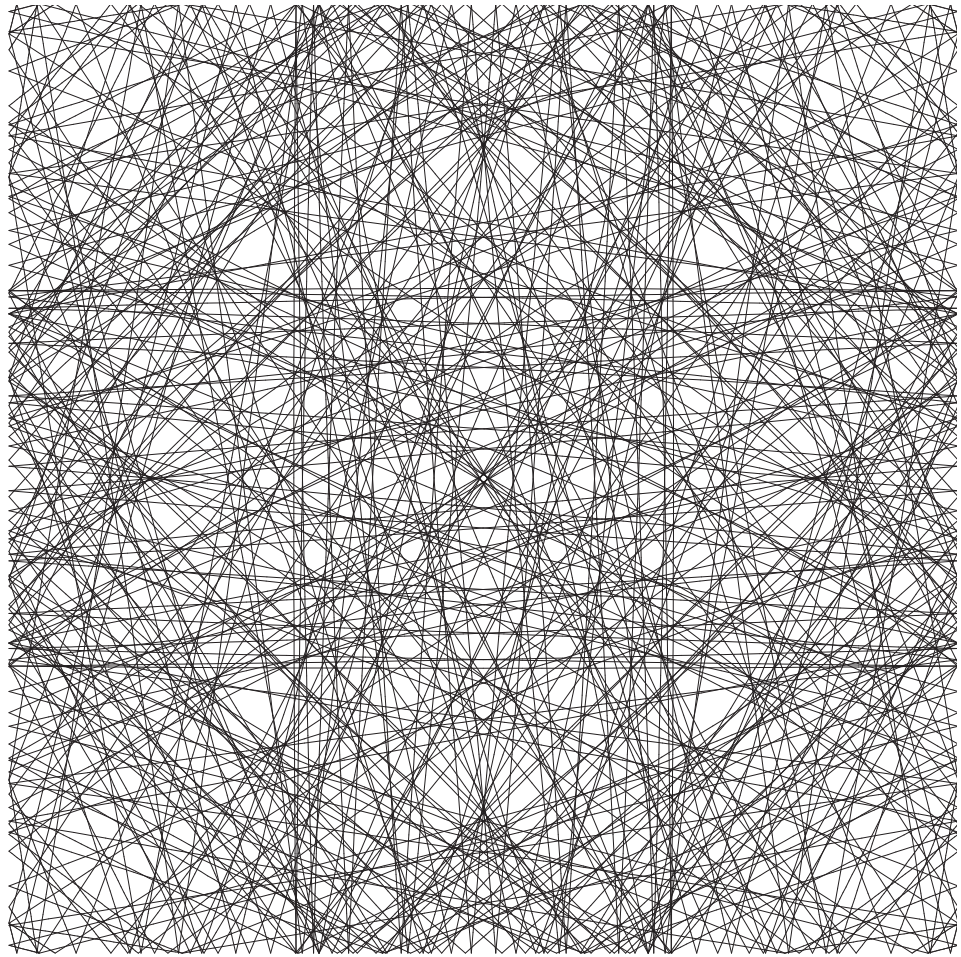
It is related to the equidistribution speed of the image of a great circle in $\mathbb{R}^2/\mathbb{Z}^2$











The hyperbolic plane

Set $N_R = \#(\{(x,y,z) \in \mathbb{Z}^3 \mid z^2 = x^2 + y^2 + 1 \quad x^2 + y^2 + z^2 \leq R^2\})$**.**

Theorem (Huber) $N_R \sim 4\sqrt{2}R$

Since the length of the circle is comparable to the area of the disk, one has, already for the main term, to understand equidistribution properties of the image of the circle.

Best hoped error term: $O(R^{\frac{1}{2}+\varepsilon})$**.**

Motivation

Let V be the n-dimensional affine space,
$F_i \in \mathbb{Z}[X_1, \ldots, X_n]$**,**
$\mathbf{Z} = \{z \in \mathbf{V} \mid F_i(z) = 0 \ \forall i\}$.

General question

Study rational points on Z.

- **Do they exist?**
- **Are they dense in $\mathbf{Z}_{\mathbb{R}}$?**
- **Are they equidistributed in $\mathbf{Z}_{\mathbb{R}}$?**
- **What is the speed of equidistribution?**

2. Integral points

A symmetric variety Z is a variety which is an orbit
$Z = Gz_0 = G/H \subset V$ where
G is a semisimple algebraic group
G acts linearly on V, $z_0 \in V$,
$H \subset G^\sigma = \{g \in G \mid g^\sigma = g\}$ is of finite index,
for some involution σ of G.

We assume
- Everything is defined over $\mathbb{Q}$
- G is quasisimple and simplyconnected
- H has no $\mathbb{Q}$-characters.

Examples of symmetric varieties Z

$$\mathbf{Z}_1 = \{(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) \mid \sum x_i^2 - \sum y_j^2 = 1\}$$

$$\mathbf{Z}_2 = \{M,\ d \times d \textbf{ matrix} \mid \det M = k\}$$

$$\mathbf{Z}_3 = \{\pi,\ d \times d \textbf{ matrix} \mid {}^t\pi = \pi = \pi^2 \ \ tr(\pi) = d'\}$$

$$\mathbf{Z}_4 = \{S,\ d \times d \textbf{ symmetric matrix} \mid \det S = k\}$$

with $n_1, n_2 > 0$**,** $(n_1, n_2) \neq (2, 1)$**,**
$d \geq 3$**,** $k \neq 0$ **and** $0 < d' < d$**.**

Set $B_R = \mathbf{Z}_{\mathbb{R}} \cap B(0,R)$ and $v_R = \mu_{\mathbf{Z}_{\mathbb{R}}}(B_R)$.
Assume $\mathbf{Z}_{\mathbb{R}}$ is non compact.

Theorem **(Duke, Rudnick, Sarnak; Eskin, McMullen)**

$$\exists\, c > 0 \quad \#\,(\mathbf{Z}_{\mathbb{Z}} \cap B_R) \;\sim\; c\, v_R.$$

Examples

$$\#\{z = (x,y) \in \mathbb{Z}^{n_1+n_2} \mid \textstyle\sum x_i^2 - \sum y_j^2 = 1\ ,\ \|z\| \le R\}$$
$$\sim\; c_{n_1,n_2}\, R^{n_1+n_2-2}$$

$$\#\{M \in \mathcal{M}(d,\mathbb{Z}) \mid \det M = k\ ,\ \|M\| \le R\} \;\sim\; c_{d,k}\, R^{d^2-d}$$

3. Rational points **Assume $\mathbf{Z}_{\mathbb{Q}_p}$ is non compact.**

Theorem **(Be-Oh) The rational points on Z with denominator p^n become equidistributed on $\mathbf{Z}_{\mathbb{R}}$ when $n \mapsto \infty$ with exponential speed.**

In other words

Theorem **(Be-Oh)** $\exists \alpha > 0, \omega_n > 0 \mid$ **for all compact** $\Omega \subset \mathbf{Z}_{\mathbb{R}}$ **with smooth boundary**

$$\#\{z \in \Omega \mid p^n z \in \mathbf{V}_{\mathbb{Z}}\} = \omega_n \, \mu_{\mathbf{Z}_{\mathbb{R}}}(\Omega)\,(1 + O(p^{-\alpha n}))$$

- $\omega_n = \mu_{\mathbf{Z}_{\mathbb{Q}_p}}(\{z \in \mathbf{Z}_{\mathbb{Q}_p} \mid p^n z \in \mathbf{V}_{\mathbb{Z}_p}\})$
- $\exists a > 0, b \geq 0, c_1, c_2 > 0 \mid c_1 p^{an} n^b \leq \omega_n \leq c_2 p^{an} n^b$

Theorem **(Be-Oh)**

$$\frac{\#\{z \in \Omega_1 \mid p^n z \in \mathbf{V}_{\mathbb{Z}}\}}{\#\{z \in \Omega_2 \mid p^n z \in \mathbf{V}_{\mathbb{Z}}\}} = \frac{\mu_{\mathbf{Z}_{\mathbb{R}}}(\Omega_1)}{\mu_{\mathbf{Z}_{\mathbb{R}}}(\Omega_2)}\,(1 + O(p^{-\alpha n}))$$

Strategy **We use an ergodic method.**
A few people have already worked on related counting problems using various ergodic methods:

L. Clozel, W. Duke, A. Eskin, A. Gorodnik, A. Guilloux, F. Ledrappier, Y. Linnik, G. Margulis, F. Maucourant, P. Michel, S. Mozes, H. Oh, J.F. Quint, M. Ratner, Z. Rudnick, P. Sarnak, N. Shah, Y. Tschinkel, E. Ullmo, A. Venkatesh, ...

Starting point

Let S be a finite set of primes and $\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p}, p \in S]$.
When $S = \emptyset$ then $\mathbb{Z}_S = \mathbb{Z}$.

Theorem (Borel, Harish-Chandra)

- **$\mathbf{G}_{\mathbb{Z}_S} \hookrightarrow \mathbf{G}_{\mathbb{R}} \times \prod_{p \in S} \mathbf{G}_{\mathbb{Q}_p}$ is a lattice.**
- **$\mathbf{G}_{\mathbb{Z}_S}$ has finitely many orbits in $\mathbf{Z}_{\mathbb{Z}_S}$.**

Set $G := \mathbf{G}_{\mathbb{R}} \times \prod_{p \in S} \mathbf{G}_{\mathbb{Q}_p}$, $\Gamma := \mathbf{G}_{\mathbb{Z}_S}$,
$H := \mathbf{H}_{\mathbb{R}} \times \prod_{p \in S} \mathbf{H}_{\mathbb{Q}_p}$, $Z = Gz_0 = G/H$,
μ_Z **the normalized** G**-invariant measure on** Z,
$B_n = \Omega \times \prod_{p \in S} \{z \in \mathbf{Z}_{\mathbb{Q}_p} \mid \|z\|_p \leq p^n\}$, $v_n := \mu_Z(B_n)$.

Theorem **(Be-Oh) Assume** $v_n \to \infty$**. Then,** $\exists\, \delta > 0$ **st.**

$$\#\left(\Gamma z_0 \cap B_n\right) = v_n \left(1 + O(v_n^{-\delta})\right).$$

POLAR DECOMPOSITION $G = KAH$

Example 1 : $G/H = SL(p+q,\mathbb{R})/SO(p,q)$ **:**
Every non-degenerate quadratic form on $\mathbb{R}^n$ **is diagonalizable in an orthogonal basis.**
(here $K = SO(n)$ **and** $A = \{$**diagonal matrices**$\}$**)**

Theorem **For k** $= \mathbb{R}$**, one has** $\mathbf{G}_{\mathbb{R}} = KA\mathbf{H}_{\mathbb{R}}$ **with** K **maximal compact subgroup of** $\mathbf{G}_{\mathbb{R}}$ **and** A **a maximal split abelian subgroup.**

POLAR DECOMPOSITION $G = KAH$

Example 2 : $G/H = SL(n, \mathbb{Q}_p)/SO(Q) \quad p \neq 2$ **:**
Every non-degenerate quadratic form Q **on** $\mathbb{Q}_p^n$ **is diagonalizable with base change in** $SL(n, \mathbb{Z}_p)$**.**

Theorem (Be-Oh, Delorme-Sécherre)
For $\mathbf{k} = \mathbb{Q}_\mathbf{p}$**, one has** $\mathbf{G_k} = KA\mathbf{H_k}$ **with** K **compact and** A **a finite union of split abelian groups.**

4. **Let G be a locally compact group, Γ a lattice in G, $H \subset G$ closed subgroup st $H \cap \Gamma$ is a lattice in H, μ_Z the normalized G-invariant measure on $Z := G/H$, $B_n \subset Z$, $v_n := \mu_Z(B_n)$. Assume $v_n \to \infty$.**

Theorem **(Eskin, McMullen)**
Assume
1. B_n **is** WELL-ROUNDED**,**
2. G **is** MIXING **on** $X = G/\Gamma$**,**
3. G **has the** WAVE-FRONT **property on** $Z = G/H$
Then

$$\#\left(\Gamma z_0 \cap B_n\right) \sim v_n.$$

To get the error term, we will need effective versions of WELL-ROUNDED, MIXING & WAVE-FRONT

1. B_n **is** WELL-ROUNDED **means,**

$\forall\, \varepsilon > 0$, $\exists\, U \subset G$ **neighborhood of** e **st** $\forall\, n$

$$(1-\varepsilon)\,\mu_Z(\bigcup_{u\in U} uB_n) \leq \mu_Z(B_n) \leq (1+\varepsilon)\,\mu_Z(\bigcap_{u\in U} uB_n)$$

To check effective WELL-ROUNDEDNESS **for our** Z**: use the asymptotic expansions for the volume of balls: Jeanquartier's theorem for real balls, Denef's theorem for** p**-adic balls.**

For $x = g\Gamma \in X$**, set** $F_n(x) = \frac{1}{v_n}\#\,(\Gamma g^{-1} z_0 \cap B_n)$**.**

Well-roundedness allows to replace pointwise convergence $F_n(x) \to 1$ **by weak convergence** $\int_X F_n\alpha \to \int_X \alpha \;\; \forall\, \alpha \in C_c(X)$**.**

2. G is MIXING on $X = G/\Gamma$, means

$\forall \varphi, \psi \in L^2(X)$, $\int_X \varphi(gx)\psi(x)d\mu_X \longrightarrow \int_X \varphi \int_X \psi$,

when $g \to \infty$ in G.

i.e. $g_\star(\varphi\mu_X) \longrightarrow (\int \varphi)\, \mu_X$.

or $\forall \varphi, \psi \in L^2_0(X)$, $\langle \pi(g)\varphi, \psi \rangle \longrightarrow 0$,

To check effective MIXING: use uniform decay of matrix coefficients for automorphic representations due to Clozel & Gorodnik, Maucourant, Oh :

3. G has the WAVE-FRONT **property on $Z = G/H$ means**

$\exists F \subset G$ **st** $G = FH$ **and** $\forall\ U \subset G$ **neighborhood of** e**,**
$\exists\ V \subset G$ **neighborhood of** e**, st**

$$\forall g \in F,\ gVH \subset UgH \quad (\star).$$

Set $Y = H/(H \cap \Gamma) \subset X = G/\Gamma$**. The wave-front property allows to deduce from mixing that**

$$g_\star \mu_Y \longrightarrow \mu_X \quad \textbf{when } g \to \infty \textbf{ in } G/H.$$

To check WAVE-FRONT**, for $Z = \mathbf{Z_k}$, one uses the** POLAR DECOMPOSITION **$\mathbf{G_k} = KA\mathbf{H_k}$ with K compact, A finite union of split abelian subgroups so that we only have to check $(\star)$ for $g \in A$.**

Proof of counting theorem **We know:**

$$g_\star \mu_Y \longrightarrow \mu_X, \quad \textbf{when } g \to \infty \textbf{ in } G/H$$

we want to show: $F_n \longrightarrow 1$ **weakly when** $n \to \infty$

Just compute, with $\alpha \in C_c(X)$**:**

$$\begin{aligned}
\int_X F_n \alpha &= \frac{1}{v_n} \int_{G/\Gamma} \sum_{\Gamma/(\Gamma \cap H)} \mathbf{1}_{B_n}(g\gamma H)\alpha(g\Gamma) \\
&= \frac{1}{v_n} \int_{G/(\Gamma \cap H)} \mathbf{1}_{B_n}(gH)\alpha(g\Gamma) \\
&= \frac{1}{v_n} \int_{G/H} \int_{H/(H \cap \Gamma)} \mathbf{1}_{B_n}(gH)\alpha(gh\Gamma) \\
&= \frac{1}{v_n} \int_{B_n} \left(\int_Y \alpha(gy) d\mu_Y(y) \right) \longrightarrow \int_X \alpha.
\end{aligned}$$

Rational points on symmetric varieties

Let Z be a symmetric variety defined over $\mathbb{Q}$ and p a prime number.

We have got equidistribution results for the rational points of Z with denominator a power of p.

This relied on a polar decomposition of p-adic symmetric spaces.