APOLLONIAN CIRCLE PACKINGS: DYNAMICS AND NUMBER THEORY

HEE OH

Abstract. We give an overview of various counting problems for Apollonian circle packings, which turn out to be related to problems in dynamics and number theory for thin groups. This survey article is an expanded version of my lecture notes prepared for the 13th Takagi lectures given at RIMS, Kyoto in the fall of 2013.

Contents

1. Counting problems for Apollonian circle packings

An Apollonian circle packing is one of the most of beautiful circle packings whose construction can be described in a very simple manner based on an old theorem of Apollonius of Perga:

Theorem 1.1 (Apollonius of Perga, 262-190 BC)**.** *Given* 3 *mutually tangent circles in the plane, there exist exactly two circles tangent to all three.*

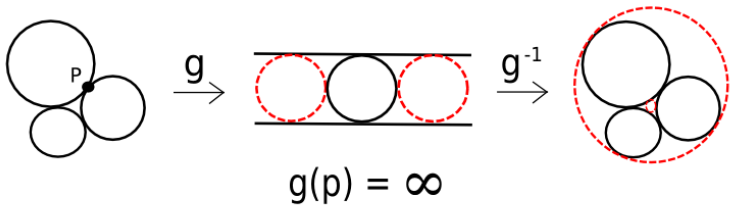


Figure 1. Pictorial proof of the Apollonius theorem

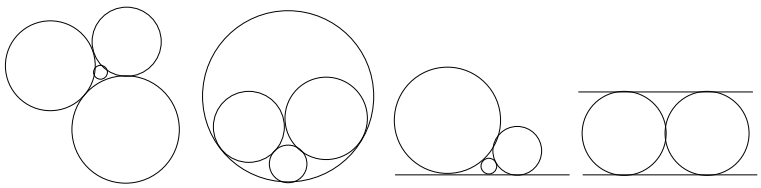


FIGURE 2. Possible configurations of four mutually tangent circles

Proof. We give a modern proof, using the linear fractional transformations of $\mathrm{PSL}_2(\mathbb{C})$ on the extended complex plane $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, known as Möbius transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d},$$

where $a, b, c, d \in \mathbb{C}$ with $ad - bc = 1$ and $z \in \mathbb{C} \cup \{\infty\}$. As is well known, a Möbius transformation maps circles in $\hat{\mathbb{C}}$ to circles in $\hat{\mathbb{C}}$, preserving angles between them. (In the whole article, a line in $\mathbb{C}$ is treated as a circle in $\hat{\mathbb{C}}$). In particular, it maps tangent circles to tangent circles.

For given three mutually tangent circles C_1, C_2, C_3 in the plane, denote by p the tangent point between C_1 and C_2, and let $g \in \mathrm{PSL}_2(\mathbb{C})$ be an element which maps p to ∞. Then g maps C_1 and C_2 to two circles tangent at ∞, that is, two parallel lines, and $g(C_3)$ is a circle tangent to these parallel lines. In the configuration of $g(C_1)$, $g(C_2)$, $g(C_3)$ (see Fig. 1), it is clear that there are precisely two circles, say, D and D' tangent to all three $g(C_i)$, $1 \le i \le 3$. Using g^{-1}, which is again a Möbius transformation, it follows that $g^{-1}(D)$ and $g^{-1}(D')$ are precisely those two circles tangent to C_1,C_2,C_3. □

In order to construct an Apollonian circle packing, we begin with four mutually tangent circles in the plane (see Figure 2 for possible configurations) and keep adding newer circles tangent to three of the previous circles provided by Theorem 1.1. Continuing this process indefinitely, we arrive at an infinite circle packing, called an *Apollonian circle packing*.

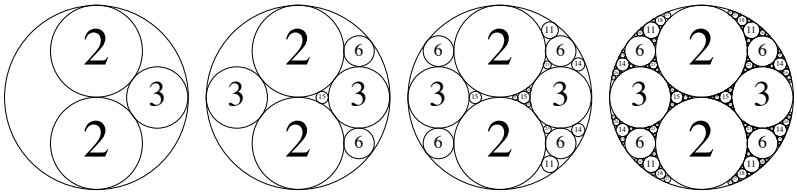


FIGURE 3. First few generations

FIGURE 4. Unbounded Apollonian circle packing

Figure 3 shows the first few generations of this process, where each circle is labeled with its curvature (= the reciprocal of its radius) with the normalization that the greatest circle has radius one.

If we had started with a configuration containing two parallel lines, we would have arrived at an unbounded Apollonian circle packing as in Figure 4. There are also other unbounded Apollonian packings containing either only one line or no line at all; but it will be hard to draw them in a paper with finite size, as circles will get enormously large only after a few generations.

For a bounded Apollonian packing $\mathcal{P}$, there are only finitely many circles of radius bigger than a given number. Hence the following counting function is well-defined for any $T > 0$:

$$N_{\mathcal{P}}(T) := \#\{C \in \mathcal{P} : \mathrm{curv}(C) \leq T\}.$$

Question 1.2.
- *Is there an asymptotic formula of $N_{\mathcal{P}}(T)$ as $T \to \infty$?*
- *If so, can we compute?*

The study of this question involves notions related to metric properties of the underlying fractal set called a *residual set*:

$$\mathrm{Res}(\mathcal{P}) := \overline{\cup_{C \in \mathcal{P}} C},$$

i.e., the residual set of $\mathcal{P}$ is the closure in $\mathbb{C}$ of the union of all circles in $\mathcal{P}$.

The Hausdorff dimension of the residual set of $\mathcal{P}$ is called the *residual dimension of* $\mathcal{P}$, which we denote by α. The notion of the Hausdorff dimension was first given by Hausdorff in 1918. To explain its definition, we first recall the notion of the Hausdorff measure (cf. [36]):

Definition 1.3. *Let $s \geq 0$ and F be any subset of $\mathbb{R}^n$. The s-dimensional Hausdorff measure of F is defined by*

$$\mathcal{H}^s(F) := \lim_{\epsilon \to 0} \Big(\inf\{ \sum d(B_i)^s : F \subset \cup_i B_i, d(B_i) < \epsilon \} \Big)$$

where $d(B_i)$ is the diameter of B_i.

For $s = n$, it is the usual Lebesgue measure of $\mathbb{R}^n$, up to a constant multiple. It can be shown that as s increases, the s-dimensional Hausdorff measure of F will be ∞ up to a certain value and then jumps down to 0. The Hausdorff dimension of F is this critical value of s:

$$\dim_{\mathcal{H}}(F) = \sup\{s : \mathcal{H}^s(F) = \infty\} = \inf\{s : \mathcal{H}^s(F) = 0\}.$$

In fractal geometry, there are other notions of dimensions which often have different values. But for the residual set of an Apollonian circle packing, the Hausdorff dimension, the packing dimension and the box dimension are all equal to each other [55].

We observe

- $1 \leq \alpha \leq 2$.
- α is independent of $\mathcal{P}$: any two Apollonian packings are equivalent to each other by a Möbius transformation which maps three tangent points of one packing to three tangent points of the other packing.
- The precise value of α is unknown, but approximately, $\alpha = 1.30568(8)$ due to McMullen [37].

In particular, $\mathrm{Res}(\mathcal{P})$ is much bigger than a countable union of circles (as $\alpha > 1$), but not too big in the sense that its Lebesgue area is zero (as $\alpha < 2$).

The first counting result for Apollonian packings is due to Boyd in 1982 [7]:

Theorem 1.4 (Boyd)**.**

$$\lim_{T \to \infty} \frac{\log N_{\mathcal{P}}(T)}{\log T} = \alpha.$$

Boyd asked in [7] whether $N_{\mathcal{P}}(T) \sim c \cdot T^{\alpha}$ as $T \to \infty$, and wrote that his numerical experiments suggest this may be false and perhaps

$$N_{\mathcal{P}}(T) \sim c \cdot T^{\alpha} (\log T)^{\beta}$$

might be more appropriate.

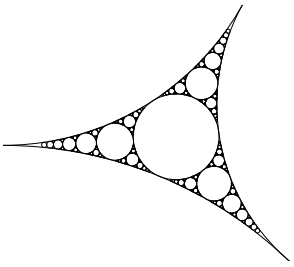
However it turns out that there is no extra logarithmic term:

Theorem 1.5 (Kontorovich-O. [30])**.** *For a bounded Apollonian packing $\mathcal{P}$, there exists a constant $c_{\mathcal{P}} > 0$ such that*

$$N_{\mathcal{P}}(T) \sim c_{\mathcal{P}} \cdot T^{\alpha} \quad \text{as } T \to \infty.$$

Theorem 1.6 (Lee-O. [32])**.** *There exists $\eta > 0$ such that for any bounded Apollonian packing $\mathcal{P}$,*

$$N_{\mathcal{P}}(T) = c_{\mathcal{P}} \cdot T^{\alpha} + O(T^{\alpha - \eta}).$$



Vinogradov [58] has also independently obtained Theorem 1.6 with a weaker error term.

For an unbounded Apollonian packing $\mathcal{P}$, we have $N_{\mathcal{P}}(T) = \infty$ in general; however we can modify our counting question so that we count only those circles contained in a fixed curvilinear triangle $\mathcal{R}$ whose sides are given by three mutually tangent circles.

Setting

$$N_{\mathcal{R}}(T) := \#\{C \in \mathcal{R} : \mathrm{curv}(C) \leq T\} < \infty,$$

we have shown:

Theorem 1.7 (O.-Shah [45])**.** *For a curvilinear triangle $\mathcal{R}$ of any Apollonian packing $\mathcal{P}$, there exists a constant $c_{\mathcal{R}} > 0$ such that*

$$N_{\mathcal{R}}(T) \sim c_{\mathcal{R}} \cdot T^{\alpha} \quad \text{as } T \to \infty.$$

Going even further, we may ask if we can describe the asymptotic distribution of circles in $\mathcal{P}$ of curvature at most T as $T \to \infty$. To formulate this question precisely, for any bounded region $E \subset \mathbb{C}$, we set

$$N_{\mathcal{P}}(T, E) := \#\{C \in \mathcal{P} : C \cap E \neq \emptyset, \mathrm{curv}(C) \leq T\}.$$

Then the question on the asymptotic distribution of circles in $\mathcal{P}$ amounts to searching for a locally finite Borel measure $\omega_{\mathcal{P}}$ on the plane $\mathbb{C}$ satisfying that

$$\lim_{T \to \infty} \frac{N_T(\mathcal{P}, E)}{T^{\alpha}} = \omega_{\mathcal{P}}(E)$$

for any bounded Borel subset $E \subset \mathbb{C}$ with negligible boundary.

Noting that all the circles in $\mathcal{P}$ lie on the residual set of $\mathcal{P}$, any Borel measure describing the asymptotic distribution of circles of $\mathcal{P}$ must be supported on $\mathrm{Res}(\mathcal{P})$.

Theorem 1.8 (O.-Shah [45])**.** *For any bounded Borel $E \subset \mathbb{C}$ with smooth boundary,*

$$N_{\mathcal{P}}(T, E) \sim c_A \cdot \mathcal{H}^{\alpha}_{\mathcal{P}}(E) \cdot T^{\alpha} \quad \text{as } T \to \infty$$

where $\mathcal{H}^{\alpha}_{\mathcal{P}}$ denotes the α-dimensional Hausdorff measure of the set $\mathrm{Res}(\mathcal{P})$ *and $0 < c_A < \infty$ is a constant independent of $\mathcal{P}$.*

In general, $\dim_{\mathcal{H}}(F) = s$ does not mean that the s-dimensional Hausdorff measure $\mathcal{H}^s(F)$ is non-trivial (it could be 0 or ∞). But on the residual set $\mathrm{Res}(\mathcal{P})$ of an Apollonian packing, $\mathcal{H}^{\alpha}_{\mathcal{P}}$ is known to be locally finite and

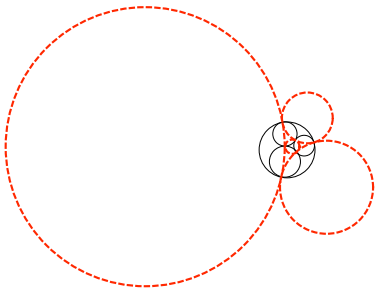


FIGURE 5. Dual circles

its support is precisely $\mathrm{Res}(\mathcal{P})$ by Sullivan [57]; hence $\mathcal{H}^\alpha_{\mathcal{P}}(E) < \infty$ for E bounded and $0 < \mathcal{H}^\alpha_{\mathcal{P}}(E)$ if $E^\circ \cap \mathrm{Res}(\mathcal{P}) \neq \emptyset$.

Though the Hausdorff dimension and the packing dimension are equal to each other for $\mathrm{Res}(\mathcal{P})$, the packing measure is locally infinite ([57], [39]) which indicates that the metric properties of $\mathrm{Res}(\mathcal{P})$ are subtle.

Theorem 1.8 says that circles in an Apollonian packing $\mathcal{P}$ are uniformly distributed with respect to the α-dimensional Hausdorff measure on $\mathrm{Res}(\mathcal{P})$: for any bounded Borel subsets $E_1, E_2 \subset \mathbb{C}$ with smooth boundaries and with $E_2^\circ \cap \mathrm{Res}(\mathcal{P}) \neq \emptyset$,

$$\lim_{T\to\infty} \frac{N_{\mathcal{P}}(T, E_1)}{N_{\mathcal{P}}(T, E_2)} = \frac{\mathcal{H}^\alpha_{\mathcal{P}}(E_1)}{\mathcal{H}^\alpha_{\mathcal{P}}(E_2)}.$$

Apollonian constant. Observe that the constant c_A in Theorem 1.8 is given by

$$c_A = \lim_{T\to\infty} \frac{N_{\mathcal{P}}(T, E)}{T^\alpha \cdot \mathcal{H}^\alpha_{\mathcal{P}}(E)}$$

for *any* Apollonian circle packing $\mathcal{P}$ and any E with $E^\circ \cap \mathrm{Res}(\mathcal{P}) \neq \emptyset$. In particular,

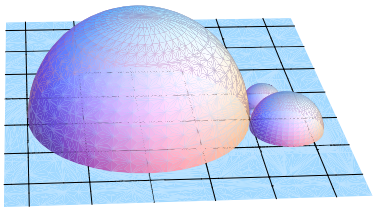
$$c_A = \lim_{T\to\infty} \frac{N_{\mathcal{P}}(T)}{T^\alpha \cdot \mathcal{H}^\alpha_{\mathcal{P}}(\mathrm{Res}(\mathcal{P}))}$$

for any bounded Apollonian circle packing $\mathcal{P}$.

Definition 1.9. We propose to call $0 < c_A < \infty$ the *Apollonian constant*.

Problem 1.10. What is c_A? (even approximation?)

Whereas all other terms in the asymptotic formula of Theorem 1.7 can be described using the metric notions of Euclidean plane, our exact formula of c_A involves certain singular measures of an infinite-volume hyperbolic 3 manifold, indicating the intricacy of the precise counting problem.



2. Hidden symmetries and Orbital counting problem

Hidden symmetries. The key to our approach of counting circles in an Apollonian packing lies in the fact that

An Apollonian circle packing has lots of hidden symmetries.

Explaining these hidden symmetries will lead us to explain the relevance of the packing with a Kleinian group, called the (geometric) Apollonian group.

Fix 4 mutually tangent circles C_1, C_2, C_3, C_4 in $\mathcal{P}$ and consider their dual circles $\hat{C}_1, \cdots, \hat{C}_4$, that is, $\hat{C}_i$ is the unique circle passing through the three tangent points among C_j's for $j \neq i$. In Figure 5, the solid circles represent C_i's and the dotted circles are their dual circles. Observe that inverting with respect to a dual circle preserves the three circles that it meets perpendicularly and interchanges the two circles which are tangent to those three circles.

Definition 2.1. The inversion with respect to a circle of radius r centered at a maps x to $a + \frac{r^2}{|x-a|^2}(x-a)$. The group $\mathrm{M\ddot{o}b}(\hat{\mathbb{C}})$ of Möbis transformations in $\hat{\mathbb{C}}$ is generated by inversions with respect to all circles in $\hat{\mathbb{C}}$.

The geometric Apollonian group $\mathcal{A} := \mathcal{A}_{\mathcal{P}}$ associated to $\mathcal{P}$ is generated by the four inversions with respect to the dual circles:

$$\mathcal{A} = \langle \tau_1, \tau_2, \tau_3, \tau_4 \rangle < \mathrm{M\ddot{o}b}(\hat{\mathbb{C}})$$

where τ_i denotes the inversion with respect to $\hat{C}_i$. Note that $\mathrm{PSL}_2(\mathbb{C})$ is a subgroup of $\mathrm{M\ddot{o}b}(\hat{\mathbb{C}})$ of index two; we will write $\mathrm{M\ddot{o}b}(\hat{\mathbb{C}}) = \mathrm{PSL}_2(\mathbb{C})^{\pm}$. The Apollonian group $\mathcal{A}$ is a Kleinian group (= a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})^{\pm}$) and satisfies

- $\mathcal{P} = \cup_{i=1}^4 \mathcal{A}(C_i)$, that is, inverting the initial four circles in $\mathcal{P}$ with respect to their dual circles generates the whole packing $\mathcal{P}$;
- $\mathrm{Res}(\mathcal{P}) = \Lambda(\mathcal{A})$ where $\Lambda(\mathcal{A})$ denotes the limit set of $\mathcal{A}$, which is the set of all accumulation points of an orbit $\mathcal{A}(z)$ for $z \in \hat{\mathbb{C}}$.

In order to explain how the hyperbolic geometry comes into the picture, it is most convenient to use the upper-half space model for hyperbolic 3

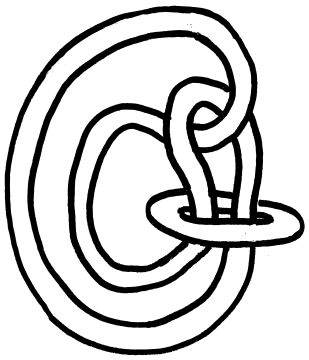


FIGURE 6. Whitehead Link

space $\mathbb{H}^3$: $\mathbb{H}^3 = \{(x_1, x_2, y) : y > 0\}$. The hyperbolic metric is given by $ds = \frac{\sqrt{dx_1^2+dx_2^2+dy^2}}{y}$ and the geometric boundary $\partial_\infty(\mathbb{H}^3)$ is naturally identified with $\hat{\mathbb{C}}$. Totally geodesic subspaces in $\mathbb{H}^3$ are vertical lines, vertical circles, vertical planes, and vertical hemispheres.

The Poincare extension theorem gives an identification $\mathrm{M\ddot{o}b}(\hat{\mathbb{C}})$ with the isometry group $\mathrm{Isom}(\mathbb{H}^3)$. Since $\mathrm{M\ddot{o}b}(\hat{\mathbb{C}})$ is generated by inversions with respect to circles in $\hat{\mathbb{C}}$, the Poincare extension theorem is determined by the correspondence which assigns to an inversion with respect to a circle C in $\hat{\mathbb{C}}$ the inversion with respect to the vertical hemisphere in $\mathbb{H}^3$ above C. An inversion with respect to a vertical hemisphere preserves the upper half space, as well as the hyperbolic metric, and hence gives rise to an isometry of $\mathbb{H}^3$.

The Apollonian group $\mathcal{A} = \mathcal{A}_{\mathcal{P}}$, now considered as a discrete subgroup of $\mathrm{Isom}(\mathbb{H}^3)$, has a fundamental domain in $\mathbb{H}^3$, given by the exterior of the hemispheres above the dual circles to $\mathcal{P}$. In particular, $\mathcal{A}\backslash\mathbb{H}^3$ is an infinite volume hyperbolic 3-manifold and has a fundamental domain with finitely many sides; such a manifold is called a geometrically finite manifold.

Connection with the Whitehead link. The Apollonian manifold $\mathcal{A}\backslash\mathbb{H}^3$ can also be constructed from the Whitehead link complement. To explain the connection, consider the group, say, $\mathcal{A}^*$ generated by 8 inversions with respect to four mutually tangent circles as well as their four dual circles. Then the group $\mathcal{A}^*$ has a regular ideal hyperbolic octahedron as a fundamental domain in $\mathbb{H}^3$, and is commensurable to the Picard group $\mathrm{PSL}_2(\mathbb{Z}[i])$, up to a conjugation, which is a lattice in $\mathrm{PSL}_2(\mathbb{C})$. The quotient orbifold $\mathcal{A}^*\backslash\mathbb{H}^3$ is commensurable to the Whitehead link complement $S^3 - W$ (see Figure 6). In this finite volume 3-manifold $S^3 - W$, we have a triply punctured sphere (corresponding a disk in S^3 spanning one component of W and pierced twice by the other component), which is totally geodesic and whose fundamental group is conjugate to the congruence subgroup $\Gamma(2)$ of

$\mathrm{PSL}_2(\mathbb{Z})$ of level 2. If we cut the manifold $S^3 - W$ open along this totally geodesic surface $\Gamma(2)\backslash\mathbb{H}^2$, we get a finite volume hyperbolic manifold with totally geodesic boundary, whose fundamental group is the Apollonian group $\mathcal{A}$. We thank Curt McMullen for bringing this beautiful relation with the Whitehead link to our attention.

Orbital counting problem in $\mathrm{PSL}_2(\mathbb{R})\backslash\mathrm{PSL}_2(\mathbb{C})$. Observe that the number of circles in an Apollonian packing $\mathcal{P}$ of curvature at most T is same as the number of the vertical hemispheres above circles in $\mathcal{P}$ of Euclidean height at least T^{-1}. Moreover for a fixed bounded region E in $\mathbb{C}$, $N_{\mathcal{P}}(T, E)$ is same as the number of the vertical hemispheres above circles in $\mathcal{P}$ which intersects the cylindrical region

$$E_T := \{(x_1, x_2, y) \in \mathbb{H}^3 : x_1 + ix_2 \in E,\ \ T^{-1} \le y \le r_0\} \tag{2.2}$$

where $r_0 > 0$ is the radius of the largest circle in $\mathcal{P}$ intersecting E.

Since the vertical plane over the real line in $\mathbb{C}$ is preserved by $\mathrm{PSL}_2(\mathbb{R})$, and $\mathrm{PSL}_2(\mathbb{C})$ acts transitively on the space of all vertical hemispheres (including planes), the space of vertical hemispheres in $\mathbb{H}^3$ can be identified with the homogeneous space $\mathrm{PSL}_2(\mathbb{R})\backslash\mathrm{PSL}_2(\mathbb{C})$. Since $\mathcal{P}$ consists of finitely many $\mathcal{A}$-orbits of circles in $\mathbb{C}$, which corresponds to finitely many $\mathcal{A}$-orbits of points in $\mathrm{PSL}_2(\mathbb{R})\backslash\mathrm{PSL}_2(\mathbb{C})$, understanding the asymptotic formula of $N_{\mathcal{P}}(T, E)$ is a special case of the following more general counting problem: letting $G = \mathrm{PSL}_2(\mathbb{C})$ and $H = \mathrm{PSL}_2(\mathbb{R})$, for a given sequence of growing compact subsets $\mathcal{B}_T$ in $H\backslash G$ and a discrete $\mathcal{A}$-orbit $v_0\mathcal{A}$ in $H\backslash G$,

what is the asymptotic formula of the number $\#\mathcal{B}_T \cap v_0\mathcal{A}$?

If $\mathcal{A}$ were of finite co-volume in $\mathrm{PSL}_2(\mathbb{C})$, this type of question is well-understood due to the works of Duke-Rudnick-Sarnak [15] and Eskin-McMullen [17]. In the next section, we describe analogies/differences of this counting problem for discrete subgroups of infinite covolume.

3. Counting, Mixing, and the Bowen-Margulis-Sullivan measure

Euclidean lattice point counting We begin with a simple example of the lattice point counting problem in Euclidean space. Let $G = \mathbb{R}^3$, $\Gamma = \mathbb{Z}^3$ and let $B_T := \{x \in \mathbb{R}^3 : \|x\| \le T\}$ be the Euclidean ball of radius T centered at the origin. In showing the well-known fact

$$\#\mathbb{Z}^3 \cap B_T \sim \frac{4\pi}{3}T^3,$$

one way is to count the Γ-translates of a fundamental domain, say $\mathcal{F} := [-\frac{1}{2}, \frac{1}{2}) \times [-\frac{1}{2}, \frac{1}{2}) \times [-\frac{1}{2}, \frac{1}{2})$ contained in B_T, since each translate $\gamma + \mathcal{F}$ contains precisely one point, that is, γ, from Γ. We have

$$\begin{aligned}\frac{\mathrm{Vol}(B_{T-1})}{\mathrm{Vol}(\mathcal{F})} &\le \#\{\gamma + \mathcal{F} \subset B_{T-1} : \gamma \in \mathbb{Z}^3\} \\ &\le \#\mathbb{Z}^3 \cap B_T \le \#\{\gamma + \mathcal{F} \subset B_{T+1} : \gamma \in \mathbb{Z}^3\} \le \frac{\mathrm{Vol}(B_{T+1})}{\mathrm{Vol}(\mathcal{F})}, \end{aligned} \tag{3.1}$$

Since $\frac{\mathrm{Vol}(B_{T\pm 1})}{\mathrm{Vol}(\mathcal{F})} = \frac{4\pi}{3}(T\pm 1)^3$, we obtain that

$$\#\mathbb{Z}^3 \cap B_T = \frac{4\pi}{3}T^3 + O(T^2).$$

This easily generalizes to the following: for any discrete subgroup Γ in $\mathbb{R}^3$ and a sequence B_T of compact subsets in $\mathbb{R}^3$, we have

$$\#\Gamma \cap B_T = \frac{\mathrm{Vol}(B_T)}{\mathrm{Vol}(\Gamma\backslash\mathbb{R}^3)} + O(\mathrm{Vol}(B_T)^{1-\eta})$$

provided

- $\mathrm{Vol}(\Gamma\backslash\mathbb{R}^3) < \infty$;
- $\mathrm{Vol}(\text{unit neighborhood of } \partial(B_T)) = O(\mathrm{Vol}(B_T)^{1-\eta})$ for some $\eta > 0$.

We have used here that the volume in $\mathbb{R}^3$ is computed with respect to the Lebesgue measure which is clearly left Γ-invariant so that it makes sense to write $\mathrm{Vol}(\Gamma\backslash\mathbb{R}^3)$, and that the ratio $\frac{\mathrm{Vol}(\text{unit neighborhood of } \partial(B_T))}{\mathrm{Vol}(B_T)}$ tends to 0 as $T\to\infty$.

Hyperbolic lattice point counting We now consider the hyperbolic lattice counting problem for $\mathbb{H}^3$. Let $G = \mathrm{PSL}_2(\mathbb{C})$ and Γ be a torsion-free, co-compact, discrete subgroup of G. The group G possess a Haar measure μ_G which is both left and right invariant under G, in particular, it is left-invariant under Γ. By abuse of notation, we use the same notation μ_G for the induced measure on $\Gamma\backslash G$. Fix $o = (0,0,1)$ so that $g \mapsto g(o)$ induces an isomorphism of $\mathbb{H}^3$ with $G/\mathrm{PSU}(2)$ and hence μ_G also induces a left G-invariant measure on $\mathbb{H}^3$, which will again be denoted by μ_G. Consider the hyperbolic ball $B_T = \{x \in \mathbb{H}^3 : d(o,x) \le T\}$ where d is the hyperbolic distance in $\mathbb{H}^3$. Then, for a fixed fundamental domain $\mathcal{F}$ for Γ in $\mathbb{H}^3$ which contains o in its interior, we have inequalities similar to (3.1):

$$\begin{aligned}\frac{\mathrm{Vol}(B_{T-d})}{\mathrm{Vol}(\Gamma\backslash G)} &\le \#\{\gamma(\mathcal{F}) \subset B_{T-d} : \gamma\in\Gamma\}\\ &\le \#\Gamma(o)\cap B_T \le \#\{\gamma(\mathcal{F})\subset B_{T+d}:\gamma\in\Gamma\} \le \frac{\mathrm{Vol}(B_{T+d})}{\mathrm{Vol}(\Gamma\backslash G)} \quad (3.2)\end{aligned}$$

where d is the diameter of $\mathcal{F}$ and the volumes $\mathrm{Vol}(B_{T\pm d})$ and $\mathrm{Vol}(\Gamma\backslash G)$ are computed with respect to μ_G on $\mathbb{H}^3$ and $\Gamma\backslash G$ respectively.

If we had $\mathrm{Vol}(B_{T-d}) \sim \mathrm{Vol}(B_{T+d})$ as $T\to\infty$ as in the Euclidean case, we would be able to conclude from here that $\#\Gamma(o)\cap B_T \sim \frac{\mathrm{Vol}(B_T)}{\mathrm{Vol}(\Gamma\backslash G)}$ from (3.2). However, one can compute that $\mathrm{Vol}(B_T) \sim c\cdot e^{2T}$ for some $c > 0$ and hence the asymptotic formula $\mathrm{Vol}(B_{T-d}) \sim \mathrm{Vol}(B_{T+d})$ is not true. This suggests that the above inequality (3.2) gives too crude estimation of the edge effect arising from the intersections of $\gamma(\mathcal{F})$'s with B_T near the boundary of B_T. It turns out that the mixing phenomenon of the geodesic flow on the unit tangent bundle $\mathrm{T}^1(\Gamma\backslash\mathbb{H}^3)$ with respect to μ_G precisely clears out the fuzziness of the edge effect. The mixing of the geodesic flow follows

from the following mixing of the frame flow, or equivalently, the decay of matrix coefficients due to Howe and Moore [28]: Let $a_t := \begin{pmatrix} e^{t/2} & 0 \\ 0 & e^{-t/2} \end{pmatrix}$.

Theorem 3.3 (Howe-Moore). *Let $\Gamma < G$ be a lattice. For any $\psi_1, \psi_2 \in C_c(\Gamma\backslash G)$,*

$$\lim_{t\to\infty} \int_{\Gamma\backslash G} \psi_1(ga_t)\psi_2(g)d\mu_G(g) = \frac{1}{\mu_G(\Gamma\backslash G)} \int_{\Gamma\backslash G} \psi_1 d\mu_G \cdot \int_{\Gamma\backslash G} \psi_2 d\mu_G.$$

Indeed, using this mixing property of the Haar measure, there are now very well established counting result due to Duke-Rudnick-Sarnak [15], and Eskin-McMullen[17]): we note that any symmetric subgroup of G is locally isomorphic to $\mathrm{SL}_2(\mathbb{R})$ or $\mathrm{SU}(2)$.

Theorem 3.4 (Duke-Rudnick-Sarnak, Eskin-McMullen). *Let H be a symmetric subgroup of G and $\Gamma < G$ a lattice such that $\mu_H(\Gamma \cap H\backslash H) < \infty$, i.e., $H \cap \Gamma$ is a lattice in H. Then for any well-rounded sequence B_T of compact subsets in $H\backslash G$ and a discrete Γ-orbit $[e]\Gamma$, we have*

$$\#[e]\Gamma \cap B_T \sim \frac{\mu_H((H\cap\Gamma)\backslash H)}{\mu_G(\Gamma\backslash G)} \cdot \mathrm{Vol}(B_T) \quad \text{as } T \to \infty.$$

Here the volume of B_T is computed with respect to the invariant measure $\mu_{H\backslash G}$ on $H\backslash G$ which satisfies $\mu_G = \mu_H \otimes \mu_{H\backslash G}$ locally.

A sequence $\{B_T \subset H\backslash G\}$ is called *well-rounded* with respect to a measure μ on $H\backslash G$ if the boundaries of B_T are μ-negligible, more precisely, if for all small $\epsilon > 0$, the μ-measure of the ϵ-neighborhood of the boundary of B_T is $O(\epsilon \cdot \mu(B_T))$ as $T \to \infty$.

The idea of using the mixing of the geodesic flow in the counting problem goes back to Margulis' 1970 thesis (translated in [34]).

We now consider the case when $\Gamma < G = \mathrm{PSL}_2(\mathbb{C})$ is not a lattice, that is, $\mu_G(\Gamma\backslash G) = \infty$. It turns out that as long as we have a left Γ-invariant measure, say, μ on G, satisfying

- $\mu(\Gamma\backslash G) < \infty$;
- μ is the mixing measure for the frame flow on $\Gamma\backslash G$,

then the above heuristics of comparing the counting function for $\#\Gamma(o)\cap B_T$ to the volume $\mu(B_T)$ can be made into a proof.

For what kind of discrete groups Γ, do we have a left-Γ-nvariant measure on G satisfying these two conditions? Indeed when Γ is geometrically finite, the Bowen-Margulis-Sullivan measure m^{BMS} on $\Gamma\backslash G$ satisfies these properties. Moreover when Γ is convex cocompact (that is, geometrically finite with no parabolic elements), the Bowen-Margulis-Sullivan measure is supported on a compact subset of $\Gamma\backslash G$. Therefore Γ acts co-compactly in the convex hull $CH(\Lambda(\Gamma))$ of the limit set $\Lambda(\Gamma)$; recall that $\Lambda(\Gamma)$ is the set of all accumulation points of Γ-orbits on the boundary $\partial(\mathbb{H}^3)$. Hence if we denote by $\mathcal{F}_0$ a compact fundamental domain for Γ in $CH(\Lambda(\Gamma))$, the inequality

(3.2) continues to hold if we replace the fundamental domain $\mathcal{F}$ of Γ in $\mathbb{H}^3$ by $\mathcal{F}_0$ and compute the volumes with respect to m^{BMS}:

$$\frac{\tilde{m}^{\mathrm{BMS}}(B_{T-d_0})}{m^{\mathrm{BMS}}(\Gamma\backslash G)} \le \#\{\gamma(\mathcal{F}_0) \subset B_{T-d_0} : \gamma \in \Gamma\}$$
$$\le \#\Gamma(o) \cap B_T \le \#\{\gamma(\mathcal{F}_0) \subset B_{T+d_0} : \gamma \in \Gamma\} \le \frac{\tilde{m}^{\mathrm{BMS}}(B_{T+d_0})}{m^{\mathrm{BMS}}(\Gamma\backslash G)} \quad (3.5)$$

where $\tilde{m}^{\mathrm{BMS}}$ is the projection to $\mathbb{H}^3$ of the lift of m^{BMS} to G and d_0 is the diameter of $\mathcal{F}_0$. This suggests a heuristic expectation:

$$\#\Gamma(o) \cap B_T \sim \frac{\tilde{m}^{\mathrm{BMS}}(B_T)}{m^{\mathrm{BMS}}(\Gamma\backslash G)}$$

which turns out to be true.

We denote by δ the Hausdorff dimension of $\Lambda(\Gamma)$ which is known to be equal to the critical exponent of Γ. Patterson [46] and Sullivan[56] constructed a unique geometric probability measure ν_o on $\partial(\mathbb{H}^3)$ satisfying that for any $\gamma \in \Gamma$, $\gamma_*\nu_o$ is absolutely continuous with respect to ν_o and for any Borel subset E,

$$\nu_o(\gamma(E)) = \int_E \left(\frac{d(\gamma_*\nu_o)}{d\nu_o}\right)^{\delta} d\nu_o.$$

This measure ν_o is called the Patterson-Sullivan measure viewed from $o \in \mathbb{H}^3$. Then the Bowen-Margulis-Sullivan measure m^{BMS} on $\mathrm{T}^1(\mathbb{H}^3)$ is given by

$$dm^{\mathrm{BMS}}(v) = f(v)\, d\nu_o(v^+) d\nu_o(v^-) dt$$

where $v^{\pm} \in \partial(\mathbb{H}^3)$ are the forward and the backward endpoints of the geodesic determined by v and $t = \beta_{v^-}(o, v)$ measures the signed distance of the horospheres based at v^- passing through o and v. The density function f is given by $f(v) = e^{\delta(\beta_{v^+}(o,v)+\beta_{v^-}(o,v))}$ so that m^{BMS} is left Γ-invariant Clearly, the support of m^{BMS} is given by the set of v with $v^{\pm} \subset \Lambda(\Gamma)$. Noting that $\mathrm{T}^1(\mathbb{H}^3)$ is isomorphic to G/M where $M = \{\mathrm{diag}(e^{i\theta}, e^{-i\theta})\}$, we will extend m^{BMS} to an M-invariant measure on G. We use the same notation m^{BMS} to denote the measure induced on $\Gamma\backslash G$.

Theorem 3.6. *For Γ geometrically finite and Zariski dense,*

(1) Finiteness: $m^{\mathrm{BMS}}(\Gamma\backslash G) < \infty$

(2) Mixing: *For any $\psi_1, \psi_2 \in C_c(\Gamma\backslash G)$, as $t \to \infty$,*

$$\int_{\Gamma\backslash G} \psi_1(ga_t)\psi_2(g) dm^{\mathrm{BMS}}(g) \to \tfrac{1}{m^{\mathrm{BMS}}(\Gamma\backslash G)} \int_{\Gamma\backslash G} \psi_1 dm^{\mathrm{BMS}} \int_{\Gamma\backslash G} \psi_2 dm^{\mathrm{BMS}}.$$

The finiteness result (1) is due to Sullivan [56] and the mixing result (2) for frame flow is due to Flaminio-Spatzier [21] and Winter [59] based on the work of Rudolph [50] and Babillot [8].

In order to state an analogue of Theorem 3.4 for a general geometrically finite group, we need to impose a condition on $(H \cap \Gamma)\backslash H$ analogous to

the finiteness of the volume $\mu_H(\Gamma \cap H\backslash H)$. In [44], we define the so called skinning measure μ_H^{PS} on $(\Gamma \cap H)\backslash H$, which is intuitively the slice measure on H of m^{BMS}. We note that μ_H^{PS} depends on Γ, not only on $H \cap \Gamma$. A finiteness criterion for μ_H^{PS} is given in [44]. The following is obtained in [44] non-effectively and [38] effectively.

Theorem 3.7 (O.-Shah, Mohammadi-O.)**.** *Let H be a symmetric subgroup of G and $\Gamma < G$ a geometrically finite and Zariski dense subgroup. Suppose that the skinning measure of $H \cap \Gamma\backslash H$ is finite, i.e., $\mu_H^{\mathrm{PS}}(\Gamma \cap H\backslash H) < \infty$. Then there exists an explicit locally finite Borel measure $\mathcal{M}_{H\backslash G}$ on $H\backslash G$ such that for any well-rounded sequence B_T of compact subsets in $H\backslash G$ with respect to $\mathcal{M}_{H\backslash G}$ and a discrete Γ-orbit $[e]\Gamma$, we have*

$$\#[e]\Gamma \cap B_T \sim \frac{\mu_H^{\mathrm{PS}}((H \cap \Gamma)\backslash H)}{m^{\mathrm{BMS}}(\Gamma\backslash G)} \cdot \mathcal{M}_{H\backslash G}(B_T) \quad \text{as } T \to \infty.$$

A special case of this theorem implies Theorem 1.8, modulo the computation of the measure $\mathcal{M}_{H\backslash G}(E_T)$ where E_T is given in (2.2). We mention that in the case when the critical exponent δ of Γ is strictly bigger than 1, both Theorem 3.7 and Theorem 1.8 can be effectivized by [38].

The reason that we have the α-dimensional Hausdorff measure in the statement of Theorem 1.8 is because the slice measure of m^{BMS} on each horizontal plane is the Patterson-Sullivan measure multiplied with a correct density function needed for the Γ-invariance, which turns out to coincide with the δ-dimensional Hausdorff measure on the limit set of $\Lambda(\Gamma)$ when all cusps of Γ are of rank at most 1, which is the case for the Apollonian group.

Counting problems for Γ-orbits in $H\backslash G$ are technically much more involved when H is non-compact than when H is compact, and relies on understanding the asymptotic distribution of $\Gamma\backslash\Gamma H a_t$ in $\Gamma\backslash G$ as $t \to \infty$. When $H = \mathrm{PSL}_2(\mathbb{R})$, the translate $\Gamma\backslash\Gamma H a_t$ corresponds to the orthogonal translate of a totally geodesic surface for time t, and we showed that, after the correct scaling of $e^{(2-\delta)t}$, $\Gamma\backslash\Gamma H a_t$ becomes equidistributed in $\Gamma\backslash G$ with respect to the Burger-Roblin measure m^{BR}, which is the unique non-trivial ergodic horospherical invariant measure on $\Gamma\backslash G$. We refer to [42], [43], [45] for more details.

More circle packings. This viewpoint of approaching Apollonian circle packings via the study of Kleinian groups allows us to deal with more general circle packings, provided they are invariant under a non-elementary geometrically finite Kleinian group.

One way to construct such circle packings is as follows:

Example 3.8. Let X be a finite volume hyperbolic 3-manifold with non-empty totally geodesic boundary. Then

- $\Gamma := \pi_1(X)$ is a geometrically finite Kleinian group;
- By developing X in the upper half space $\mathbb{H}^3$, the domain of discontinuity $\Omega(\Gamma) := \hat{\mathbb{C}} - \Lambda(\Gamma)$ consists of the disjoint union of open disks

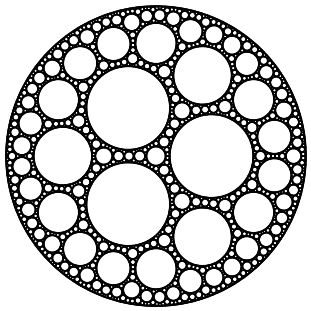


FIGURE 7. Sierpinski curve

(corresponding to the boundary components of the universal cover $\tilde{X}$).

Set $\mathcal{P}$ to be the union of circles which are boundaries of the disks in $\Omega(\Gamma)$. In this case, $\mathrm{Res}(\mathcal{P})$ defined as the closure of all circles in $\mathcal{P}$ is equal to the limit set $\Lambda(\Gamma)$.

In section 2, we explained how Apollonian circle packings can be described in this way.

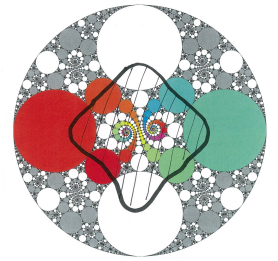
Figure 7, due to McMullen, is also an example of a circle packing obtained in this way, here the symmetry group Γ is the fundamental group of a compact hyperbolic 3-manifold with totally geodesic boundary being a compact surface of genus two. This limit set is called a Sierpinski curve, being homeomorphic to the well-known Sierpinski Carpet.

Many more pictures of circle packings constructed in this way can be found in the book "Indra's pearls" by Mumford, Series and Wright (Cambridge Univ. Press 2002).

For $\mathcal{P}$ constructed in Example 3.8, we define as before $N_{\mathcal{P}}(T, E) := \#\{C \in \mathcal{P} : C \cap E \neq \emptyset, \mathrm{curv}(C) \leq T\}$ for any bounded Borel subset E in $\mathbb{C}$.

Theorem 3.9 (O.-Shah, [44]). *There exist a constant $c_\Gamma > 0$ and a locally finite Borel measure $\omega_{\mathcal{P}}$ on $\mathrm{Res}(\mathcal{P})$ such that for any bounded Borel subset $E \subset \mathbb{C}$ with $\omega_{\mathcal{P}}(\partial(E)) = 0$,*

$$N_{\mathcal{P}}(T, E) \sim c_\Gamma \cdot \omega_{\mathcal{P}}(E) \cdot T^\delta \quad \text{as } T \to \infty$$



where $\delta = \dim_{\mathcal{H}}(\mathrm{Res}(\mathcal{P}))$. *Moreover, if* Γ *is convex cocompact or if the cusps of* Γ *have rank at most* 1, *then* $\omega_{\mathcal{P}}$ *coincides with the* δ*-dimensional Hausdorff measure on* $\mathrm{Res}(\mathcal{P})$.

We refer to [44] for the statement for more general circle packings.

4. Integral Apollonian circle packings

We call an Apollonian circle packing $\mathcal{P}$ *integral* if every circle in $\mathcal{P}$ has integral curvature. Does there exist *any* integral $\mathcal{P}$? The answer is positive thanks to the following beautiful theorem of Descartes:

Theorem 4.1 (Descartes 1643, [13])**.** *A quadruple* (a, b, c, d) *is the curvatures of four mutually tangent circles if and only if it satisfies the quadratic equation:*

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2.$$

In the above theorem, we ask circles to be oriented so that their interiors are disjoint with each other. For instance, according to this rule, the quadruple of curvatures of four largest four circles in Figure 3 is $(-1, 2, 2, 3)$ or $(1, -2, -2, -3)$, for which we can easily check the validity of the Descartes theorem: $2((-1)^2 + 2^2 + 2^2 + 3^2) = 36 = (-1 + 2 + 2 + 3)^2$

In what follows, we will always assign the negative curvature to the largest bounding circle in a bounded Apollonian packing, so that all other circles will then have positive curvatures.

Given three mutually tangent circles of curvatures a, b, c, the curvatures, say, d and d', of the two circles tangent to all three must satisfy $2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2$ and $2(a^2 + b^2 + c^2 + (d')^2) = (a + b + c + d')^2$ by the Descartes theorem. By subtracting the first equation from the second,

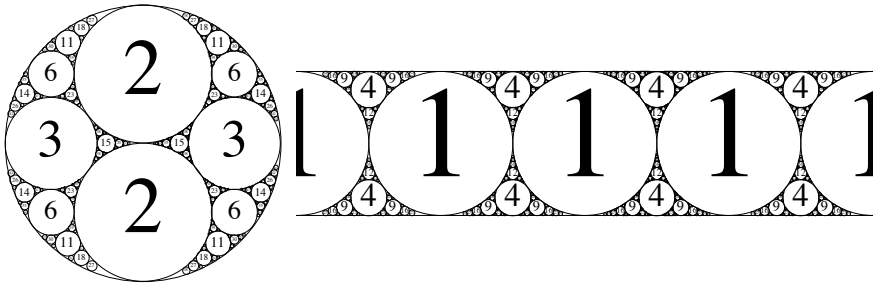


FIGURE 8. Integral Apollonian packings

we obtain the linear equation:

$$d + d' = 2(a + b + c).$$

So, if a, b, c, d are integers, so is d'. Since the curvature of every circle from the second generation or later is d' for some 4 mutually tangent circles of curvatures a, b, c, d from the previous generation, we deduce:

Theorem 4.2 (Soddy 1937)**.** *If the initial 4 circles in an Apollonian packing $\mathcal{P}$ have integral curvatures, $\mathcal{P}$ is integral.*

Combined with Descartes' theorem, for any integral solution of $2(a^2+b^2+c^2+d^2) = (a+b+c+d)^2$, there exists an integral Apollonian packing! Because the smallest positive curvature must be at least 1, an integral Apollonian packing cannot have arbitrarily large circles. In fact, any integral Apollonian packing is either bounded or lies between two parallel lines.

For a given integral Apollonian packing $\mathcal{P}$, it is natural to inquire about its Diophantine properties such as

Question 4.3.
- *Are there infinitely many circles with prime curvatures?*
- *Which integers appear as curvatures?*

We call $\mathcal{P}$ primitive, if $\mathrm{g.c.d}_{C\in\mathcal{P}}(\mathrm{curv}(C)) = 1$. We call a circle is prime if its curvature is a prime number, and a pair of tangent prime circles will be called twin prime circles. There are no triplet primes of three mutually tangent circles, all having odd prime curvatures.

Theorem 4.4 (Sarnak 07)**.** *There are infinitely many prime circles as well as twin prime circles in any primitive integral Apollonian packing.*

In the rest of this section, we let $\mathcal{P}$ be a bounded primitive integral Apollonian packing. Theorem 4.4 can be viewed as an analogue of the infinitude of prime numbers. In order to formulate what can be considered as an analogue of the prime number theorem, we set

$$\Pi_T(\mathcal{P}) := \#\{\text{prime } C \in \mathcal{P} : \mathrm{curv}(C) \le T\}$$

and

$$\Pi_T^{(2)}(\mathcal{P}) := \#\{\text{twin primes } C_1, C_2 \in \mathcal{P} : \text{curv}(C_i) \leq T\}.$$

Using the sieve method based on heuristics on the randomness of Möbius function, Fuchs and Sanden [21] conjectured:

Conjecture 4.5 (Fuchs-Sanden)**.**

$$\Pi_T(\mathcal{P}) \sim c_1 \frac{N_{\mathcal{P}}(T)}{\log T}; \quad \Pi_T^{(2)}(\mathcal{P}) \sim c_2 \frac{N_{\mathcal{P}}(T)}{(\log T)^2}$$

where $c_1 > 0$ and $c_2 > 0$ can be given explicitly.

Based on the breakthrough of Bourgain, Gamburd, Sarnak [3] proving that the Cayley graphs of congruence quotients of the integral Apollonian group form an expander family, together with Selberg's upper bound sieve, we obtain upper bounds of true order of magnitude:

Theorem 4.6 (Kontorovich-O. [30])**.** *For $T \gg 1$,*

- $\Pi_T(\mathcal{P}) \ll \frac{T^\alpha}{\log T}$*;*
- $\Pi_T^{(2)}(\mathcal{P}) \ll \frac{T^\alpha}{(\log T)^2}$ *.*

The lower bounds for Conjecture 4.5 are still open and very challenging. However a problem which is more amenable to current technology is to count curvatures without multiplicity. Our counting Theorem 1.5 for circles says that the number of integers at most T arising as curvatures of circles in integral $\mathcal{P}$ counted with multiplicity, is of order $T^{1.3\ldots}$. So one may hope that a positive density (=proportion) of integers arises as curvatures, as conjectured by Graham, Lagarias, Mallows, Wilkes, Yan (Positive density conjecture) [24].

Theorem 4.7 (Bourgain-Fuchs [2])**.** *For a primitive integral Apollonian packing $\mathcal{P}$,*

$$\#\{\text{curv}(C) \leq T : C \in \mathcal{P}\} \gg T.$$

A stronger conjecture, called the Strong Density conjecture, of Graham et al. says that every integer occurs as the value of a curvature of a circle in $\mathcal{P}$, unless there are congruence obstructions. Fuchs [19] showed that the only congruence obstructions are modulo 24, and hence the strong positive density conjecture (or the local-global principle conjecture) says that every sufficiently large integer which is congruent to a curvature of a circle in $\mathcal{P}$ modulo 24 must occur as the value of a curvature of some circle in $\mathcal{P}$. This conjecture is still open, but there is now a stronger version of the positive density theorem:

Theorem 4.8 (Bourgain-Kontorovich [5])**.** *For a primitive integral Apollonian packing $\mathcal{P}$,*

$$\#\{\text{curv}(C) \leq T : C \in \mathcal{P}\} \sim \frac{\kappa(\mathcal{P})}{24} \cdot T$$

where $\kappa(\mathcal{P}) > 0$ is the number of residue classes mod 24 of curvatures of $\mathcal{P}$.

Improving Sarnak's result on the infinitude of prime circles, Bourgain showed that a positive fraction of prime numbers appear as curvatures in $\mathcal{P}$.

Theorem 4.9 (Bourgain [6])**.**

$$\#\{\text{prime curv}(C) \le T : C \in \mathcal{P}\} \gg \frac{T}{\log T}.$$

Integral Apollonian group. In studying the Diophantine properties of integral Apollonian packings, we work with the integral Apollonian group, rather than the geometric Apollonian group which was defined in section 2.

We call a quadruple (a, b, c, d) a Descartes quadruple if it represents curvatures of four mutually tangent circles (oriented so that their interiors are disjoint) in the plane. By Descartes' theorem, any Descartes quadruple (a, b, c, d) lies on the cone $Q(x) = 0$, where Q denotes the so-called Descartes quadratic form

$$Q(a, b, c, d) = 2(a^2 + b^2 + c^2 + d^2) - (a + b + c + d)^2.$$

The quadratic form Q has signature $(3, 1)$ and hence over the reals, the orthogonal group O_Q is isomorphic to $\mathrm{O}(3, 1)$, which is the isometry group of the hyperbolic 3-space $\mathbb{H}^3$.

We observe that if (a, b, c, d) and (a, b, c, d') are Descartes quadruples, then $d' = -d + 2(a + b + c)$ and hence $(a, b, c, d') = (a, b, c, d)S_4$ where

$$S_1 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix},$$

$$S_3 = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix}, \quad S_4 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Now the integral Apollonian group $\mathcal{A}$ is generated by those four reflections S_1, S_2, S_3, S_4 in $\mathrm{GL}_4(\mathbb{Z})$ and one can check that $\mathcal{A} < \mathrm{O}_Q(\mathbb{Z})$.

Fixing an integral Apollonian circle packing $\mathcal{P}$, all Descartes quadruples associated to $\mathcal{P}$ is a single $\mathcal{A}$-orbit in the cone $Q = 0$. Moreover if we choose a root quadruple $v_{\mathcal{P}}$ from $\mathcal{P}$, which consists of curvatures of four largest mutually tangent circles, any reduced word $w_n = v_{\mathcal{P}} S_{i_1} \cdots S_{i_n}$ with $S_{i_j} \in \{S_1, S_2, S_3, S_4\}$ is obtained from $w_{n-1} = v_{\mathcal{P}} S_{i_1} \cdots S_{i_{n-1}}$ by changing precisely one entry and this new entry is the maximum entry of w_n, which is the curvature of a precisely one new circle added at the n-th generation [24]. This gives us the translation of the circle counting problem for a *bounded* Apollonian packings as the orbital counting problem of an $\mathcal{A}$-orbit in a cone $Q = 0$:

$$N_T(\mathcal{P}) = \#\{v \in v_{\mathcal{P}}\mathcal{A} : \|v\|_{\max} \le T\} + 3.$$

The integral Apollonian group $\mathcal{A}$ is isomorphic to the geometric Apollonian group $\mathcal{A}_{\mathcal{P}}$ (the subgroup generated by four inversions with respect to the dual circles of four mutually tangent circles in $\mathcal{P}$): there exists an explicit isomorphism between the orthogonal group O_Q and $\mathrm{M\ddot{o}b}(\hat{\mathbb{C}})$ which maps the integral Apollonian group $\mathcal{A}$ to the geometric Apollonian group $\mathcal{A}_{\mathcal{P}}$. In particular, $\mathcal{A}$ is a subgroup $\mathrm{O}_Q(\mathbb{Z})$ which is of infinite index and Zariski dense in O_Q. Such a subgroup is called a thin group. Diophantine properties of an integral Apollonian packing is now reduced to the study of Diophantine properties of an orbit of the thin group $\mathcal{A}$. Unlike orbits under an arithmetic subgroup (subgroups of $\mathrm{O}_Q(\mathbb{Z})$ of finite index) which has a rich theory of automorphic forms and ergodic theory, the study of thin groups has begun very recently, but with a great success. In particular, the recent developments in expanders is one of key ingredients in studying primes or almost primes in thin orbits (see [6]).

5. Expanders and Sieve

All graphs will be assumed to be simple (no multiple edges and no loops) and connected in this section. For a finite k-regular graph $X = X(V, E)$ with $V = \{v_1, \cdots, v_n\}$ the set of vertices and E the set of edges, the adjacency matrix $A = (a_{ij})$ is defined by $a_{ij} = 1$ if $\{v_i, v_j\} \in E$ and $a_{ij} = 0$ otherwise. Since A is a symmetric real matrix, it has n real eigenvalues: $\lambda_0(X) \geq \lambda_1(X) \geq \cdots \geq \lambda_{n-1}(X)$. As X is simple and connected, the largest eigenvalue $\lambda_0(X)$ is given by k and has multiplicity one.

Definition 5.1. *A family of k-regular graphs $\{X_i\}$ with ($\#X_i \to \infty$) is called an expander family if there exists an $\epsilon_0 > 0$ such that*

$$\sup_i \lambda_1(X_i) \leq k - \epsilon_0.$$

Equivalently, $\{X_i\}$ is an expander family if there exists a uniform positive lower bound for the Cheeger constant (or isoperimetric constant)

$$h(X_i) := \min_{0<\#W\leq \#X_i/2} \frac{\#\partial(W)}{\#W}$$

where $\partial(W)$ means the set of edges with exactly one vertex in W. Note that the bigger the Cheeger constant is, the harder it is to break the graph into two pieces. Intuitively speaking, an expander family is a family of sparse graphs (as the regularity k is fixed) with high connectivity properties (uniform lower bound for the Cheeger constants).

Although it was known that there has to be many expander families using probabilistic arguments due to Pinsker, the first explicit construction of an expander family is due to Margulis in 1973 [35] using the representation theory of a simple algebraic group and automorphic form theory. We explain his construction below; strictly speaking, what we describe below is not exactly same as his original construction but the idea of using the

representation theory of an ambient algebraic group is the main point of his construction as well as in the examples below.

Let G be a connected simple non-compact real algebraic group defined over $\mathbb{Q}$, with a fixed $\mathbb{Q}$-embedding into SL_N. Let $G(\mathbb{Z}) := G \cap \mathrm{SL}_N(\mathbb{Z})$ and $\Gamma < G(\mathbb{Z})$ be a finitely generated subgroup. For each positive integer q, the principal congruence subgroup $\Gamma(q)$ of level q is defined to be $\{\gamma \in \Gamma : \gamma = e \mod q\}$.

Fix a finite symmetric generating subset S for Γ. Then S generates the group $\Gamma(q)\backslash\Gamma$ via the canonical projection. We denote by $X_q := \mathcal{C}(\Gamma(q)\backslash\Gamma, S)$ the Cayley graph of the group $\Gamma(q)\backslash\Gamma$ with respect to S, that is, vertices of X_q are elements of $\Gamma(q)\backslash\Gamma$ and two elements g_1, g_2 form an edge if $g_1 = g_2 s$ for some $s \in S$. Then X_q is a connected k-regular graph for $k = \#S$. Now a key observation due to Margulis is that if Γ is *of finite index* in $G(\mathbb{Z})$, or equivalently if Γ is a lattice in G, then the following two properties are equivalent: for any $I \subset \mathbb{N}$,

(1) The family $\{X_q : q \in I\}$ is an expander;
(2) The trivial representation 1_G is isolated in the sum $\oplus_{q\in I} L^2(\Gamma(q)\backslash G)$ in the Fell topology of the set of unitary representations of G.

We won't give a precise definition of the Fell topology, but just say that the second property is equivalent to the following: for a fixed compact generating subset Q of G, there exists $\epsilon > 0$ (independent of $q \in I$) such that any unit vector $f \in L^2(\Gamma(q)\backslash G)$ satisfying $\max_{q\in Q} \|q.f - f\| < \epsilon$ is G-invariant, i.e., a constant. Briefly speaking, it follows almost immediately from the definition of an expander family that the family $\{X_q\}$ is an expander if and only if the trivial representation 1_Γ of Γ is isolated in the sum $\oplus_q L^2(\Gamma(q)\backslash\Gamma)$. On the other hand,the induced representation of 1_Γ from Γ to G is $L^2(\Gamma\backslash G)$, which contains the trivial representation 1_G, if Γ is a lattice in G. Therefore, by the continuity of the induction process, the weak containment of 1_Γ in $\oplus_q L^2(\Gamma(q)\backslash\Gamma)$ implies the weak-containment of 1_G in $\oplus_q L^2(\Gamma(q)\backslash G)$, which explains why (2) implies (1).

The isolation property of 1_G as in (2) holds for G; if the real rank of G is at least 2 or G is a rank one group of type $Sp(m,1)$ or F_4^{-20}, G has the so-called Kazhdan's property (T) [29], which says that the trivial representation of G is isolated in the whole unitary dual of G. When G is isomorphic to $\mathrm{SO}(m,1)$ or $\mathrm{SU}(m,1)$ which do not have Kazhdan's property (T), the isolation of the trivial representation is still true in the subset of all automorphic representations $L^2(\Gamma(q)\backslash G)$'s, due to the work of Selberg, Burger-Sarnak [11] and Clozel [14]. This latter property is referred as the phenomenon that G has property τ with respect to the congruence family $\{\Gamma(q)\}$.

Therefore, we have:

Theorem 5.2. *If Γ is of finite index in $G(\mathbb{Z})$, then the family $\{X_q = \mathcal{C}(\Gamma(q)\backslash\Gamma, S) : q \in \mathbb{N}\}$ is an expander family.*

In the case when Γ is of infinite index, the trivial representation is not contained in $L^2(\Gamma(q)\backslash G)$, as the constant function is not square-integrable, and the above correspondence cannot be used, and deciding whether X_q forms an expander or not for a thin group was a longstanding open problem. For instance, if S_k consists of four matrices $\begin{pmatrix} 1 & \pm k \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ \pm k & 1 \end{pmatrix}$, then the group Γ_k generated by S_k has finite index only for $k = 1, 2$ and hence we know the family $\{X_q(k) = \mathcal{C}(\Gamma_k(q)\backslash\Gamma_k, S_k)\}$ forms an expander for $k = 1, 2$ by Theorem 5.2 but the subgroup Γ_3 generated by S_3 has infinite index in $\mathrm{SL}_2(\mathbb{Z})$ and it was not known whether $\{X_q(3)\}$ is an expander family until the work of Bourgain, Gamburd and Sarnak [3].

Theorem 5.3 (Bourgain-Gamburd-Sarnak [3], Salehi-Golsefidy-Varju [51])**.** *Let $\Gamma < G(\mathbb{Z})$ be a thin subgroup, i.e., Γ is Zariski dense in G. Let S be a finite symmetric generating subset of Γ. Then $\{\mathcal{C}(\Gamma(q)\backslash\Gamma, S) : q$: square-free$\}$ forms an expander family.*

If G is simply connected in addition, the strong approximation theorem of Matthews, Vaserstein and Weisfeiler [33] says that there is a finite set $\mathcal{B}$ of primes such that for all q with no prime factors from $\mathcal{B}$, $\Gamma(q)\backslash\Gamma$ is isomorphic to the finite group $G(\mathbb{Z}/q\mathbb{Z})$ via the canonical projection $\Gamma \to G(\mathbb{Z}/q\mathbb{Z})$; hence the corresponding Cayley graph $\mathcal{C}(G(\mathbb{Z}/q\mathbb{Z}), S)$ is connected. Similarly, Theorem 5.3 says that the Cayley graphs $\mathcal{C}(G(\mathbb{Z}/q\mathbb{Z}), S)$ with q square-free and with no factors from $\mathcal{B}$ are highly connected, forming an expander family; called the *super-strong approximation Theorem*.

The proof of Theorem 5.3 is based on additive combinatorics and Helfgott's work on approximate subgroups [27] and generalizations made by Pyber-Szabo [47] and Breuillard-Green-Tao [9] (see also [25]).

The study of expanders has many surprising applications in various areas of mathematics (see [54]). We describe its application in sieves, i.e., in the study of primes. For motivation, we begin by considering an integral polynomial $f \in \mathbb{Z}[x]$. The following is a basic question:

Are there infinitely many integers $n \in \mathbb{Z}$ such that $f(n)$ is prime?

- If $f(x) = x$, the answer is yes; this is the infinitude of primes.
- If $f(x) = ax + b$, the answer is yes if and only if a, b are co-prime. This is Dirichlet's theorem.
- If $f(x) = x(x + 2)$, then there are no primes in $f(\mathbb{Z})$ for an obvious reason. On the other hand, Twin prime conjecture says that there are infinitely many n's such that $f(n)$ is a product of at most 2 primes. Indeed, Brun introduced what is called Brun's combinatorial sieve to attack this type of question, and proved that there are infinitely many n's such that $f(n) = n(n + 2)$ is 20-almost prime, i.e., a product of at most 20 primes. His approach was improved by Chen [12] who was able to show such a tantalizing theorem that there are infinitely many n's such that $f(n) = n(n + 2)$ is 3-almost prime.

In view of the last example, the correct question is formulated as follows:

Is there $R < \infty$ such that the set of $n \in \mathbb{Z}$ such that $f(n)$ is R-almost prime is infinite?

Bourgain, Gamburd and Sarnak [4] made a beautiful observation that Brun's combinatorial sieve can also be implemented for orbits of Γ on an affine space via affine linear transformations and the expander property of the Cayley graphs of the congruence quotients of Γ provides a crucial input needed in executing the sieve machine.

Continuing our setup that $G \subset \mathrm{SL}_N$ and $\Gamma < G(\mathbb{Z})$, we consider the orbit $\mathcal{O} = v_0\Gamma \subset \mathbb{Z}^N$ for a non-zero $v_0 \in \mathbb{Z}^N$ and let $f \in \mathbb{Q}[x_1, \cdots, x_N]$ such that $f(\mathcal{O}) \subset \mathbb{Z}$.

Theorem 5.4 (Bourgain-Gamburd-Sarnak [4], Sarnak-Salehi-Golsefidy [52])**.** *There exists $R = R(\mathcal{O}, f) \geq 1$ such that the set of vectors $v \in \mathcal{O}$ such that $f(v)$ is R-almost prime is Zariski dense in v_0G.*

We ask the following finer question:

Describe the distribution of the set $\{v \in \mathcal{O} : f(v)$ is R-almost prime$\}$ in the variety v_0G.

In other words, is the set in concern focused in certain directions in $\mathcal{O}$ or *equi-distributed* in $\mathcal{O}$? This is a very challenging question at least in the same generality as the above theorem, but when G is the orthogonal group of the Descartes quadratic form Q, $Q(v_0) = 0$, and Γ is the integral Apollonian group, we are able to give more or less a satisfactory answer by [30] and [32]. More generally, we have the following: Let F be an integral quadratic form of signature $(n, 1)$ and let $\Gamma < \mathrm{SO}_F(\mathbb{Z})$ be a geometrically finite Zariski dense subgroup. Suppose that the critical exponent δ of Γ is bigger than $(n-1)/2$ if $n = 2, 3$ and bigger than $n - 2$ if $n \geq 4$. Let $v_0 \in \mathbb{Z}^{n+1}$ be non-zero and $\mathcal{O} := v_0\Gamma$. We also assume that the skinning measure associated to v_0 and Γ is finite.

Theorem 5.5 (Mohammadi-O. [38])**.** *Let $f = f_1 \cdots f_k \in \mathbb{Q}[x_1, \cdots, x_{n+1}]$ be a polynomial with each f_i absolutely irreducible and distinct with rational coefficients and $f_i(\mathcal{O}) \subset \mathbb{Z}$. Then we construct an explicit locally finite measure $\mathcal{M}$ on the variety v_0G, depending on Γ such that for any family $\mathcal{B}_T$ of subsets in v_0G which is effectively well-rounded with respect to $\mathcal{M}$, we have*

(1) Upper bound: $\#\{v \in \mathcal{O} \cap \mathcal{B}_T : \text{each } f_i(v) \text{ is prime}\} \ll \frac{\mathcal{M}(\mathcal{B}_T)}{(\log \mathcal{M}(\mathcal{B}_T))^k}$;

(2) Lower bound: *Assuming further that $\max_{x \in \mathcal{B}_T} \|x\| \ll \mathcal{M}(B_T)^\beta$ for some $\beta > 0$, there exists $R = R(\mathcal{O}, f) > 1$ such that*

$$\#\{v \in \mathcal{O} \cap \mathcal{B}_T : f(v) \text{ is } R\text{-almost prime}\} \gg \frac{\mathcal{M}(\mathcal{B}_T)}{(\log \mathcal{M}(\mathcal{B}_T))^k}.$$

The terminology of $\mathcal{B}_T$ being effectively well-rounded with respect to $\mathcal{M}$ means that there exists $p > 0$ such that for all small $\epsilon > 0$ and for all

$T \gg 1$, the $\mathcal{M}$-measure of the ϵ-neighborhood of the boundary of $\mathcal{B}_T$ is at most of order $O(\epsilon^p \mathcal{M}(\mathcal{B}_T))$ with the implied constant independent of ϵ and T. For instance, the norm balls $\{v \in v_0 G : \|v\| \le T\}$ and many sectors are effectively well-rounded (cf. [38]).

When Γ is of finite index, $\mathcal{M}$ is just a G-invariant measure on $v_0 G$ and this theorem was proved earlier by Nevo-Sarnak [41] and Gorodnik-Nevo [22].

If Q is the Descartes quadratic form, $\mathcal{A}$ is the integral Apollonian group, and $\mathcal{B}_T = \{v \in \mathbb{R}^4 : Q(v) = 0, \|v\|_{\max} \le T\}$ is the max-norm ball, then for any primitive integral Apollonian packing $\mathcal{P}$, the number of prime circles in $\mathcal{P}$ of curvature at most T is bounded by

$$\sum_{i=1}^{4} \#\{v \in v_{\mathcal{P}} \mathcal{A} \cap \mathcal{B}_T, f(v) := v_i \text{ prime}\}$$

which is bounded by $\frac{\mathcal{M}(\mathcal{B}_T)}{\log(\mathcal{M}(\mathcal{B}_T))}$ by Theorem 5.5. Since we have $\mathcal{M}(\mathcal{B}_T) = c \cdot T^\alpha + O(T^{\alpha-\eta})$ where $\alpha = 1.305...$ is the critical exponent of $\mathcal{A}$, this gives an upper bound $T^\alpha / \log T$ for the number of prime circles of curvature at most T, as stated in Theorem 4.6. The upper bound for twin prime circle count can be done similarly with $f(v) = v_i v_j$.

Here are a few words on Brun's combinatorial sieve and its use in Theorem 5.5. Let $\mathsf{A} = \{a_m\}$ be a sequence of non-negative numbers and let B be a finite set of primes. For $z > 1$, let $P_z = \prod_{p \notin B, p<z} p$ and $S(\mathsf{A}, P_z) := \sum_{(m,P_z)=1} a_m$. To estimate $S_z := S(\mathsf{A}, P_z)$, we need to understand how A is distributed along arithmetic progressions. For q square-free, define

$$\mathsf{A}_q := \{a_m \in \mathsf{A} : n \equiv 0(q)\}$$

and set $|\mathsf{A}_q| := \sum_{m \equiv 0(q)} a_m$.

We use the following combinatorial sieve (see [26, Theorem 7.4]):

Theorem 5.6. (A_1) *For q square-free with no factors in B, suppose that*

$$|\mathsf{A}_q| = g(q)\mathcal{X} + r_q(\mathsf{A})$$

where g is a function on square-free integers with $0 \le g(p) < 1$, g is multiplicative outside B, i.e., $g(d_1 d_2) = g(d_1)g(d_2)$ if d_1 and d_2 are square-free integers with $(d_1, d_2) = 1$ and $(d_1 d_2, B) = 1$, and for some $c_1 > 0$, $g(p) < 1 - 1/c_1$ for all prime $p \notin B$.

(A_2) A *has level distribution D, in the sense that for some $\epsilon > 0$ and $C_\epsilon > 0$,*

$$\sum_{q<D} |r_q(\mathsf{A})| \le C_\epsilon \mathcal{X}^{1-\epsilon}.$$

(A_3) A *has sieve dimension k in the sense that there exists $c_2 > 0$ such that for all $2 \le w \le z$,*

$$-c_2 \le \sum_{(p,B)=1, w \le p \le z} g(p) \log p - r \log \frac{z}{w} \le c_2.$$

Then for $s > 9r$, $z = D^{1/s}$ and $\mathcal{X}$ large enough,

$$S(\mathsf{A}, P_z) \asymp \frac{\mathcal{X}}{(\log \mathcal{X})^k}.$$

For our orbit $\mathcal{O} = v_0\Gamma$ and f as in Theorem 5.5, we set

$$a_m(T) := \#\{x \in \mathcal{O} \cap \mathcal{B}_T : f(x) = m\};$$
$$\Gamma_{v_0}(q) := \{\gamma \in \Gamma : v_0\gamma \equiv v_0 \ (q)\},$$
$$|\mathsf{A}(T)| := \sum_m a_m(T) = \#\mathcal{O} \cap \mathcal{B}_T;$$
$$|\mathsf{A}_q(T)| := \sum_{m \equiv 0(q)} a_m(T) = \#\{x \in \mathcal{O} \cap \mathcal{B}_T : f(x) \equiv 0 \ (q)\}.$$

Suppose we can verify the sieve axioms for these sequences $\mathsf{A}_q(T)$ and z of order T^η. Observe that if $(f(v) = m, P_z) = 1$, then all prime factors of m have to be at least of order $z = T^\eta$. It follows that if $f(v) = m$ has R prime factors, then $T^{\eta R} \ll m \ll T^{\text{degree}(f)}$, and hence $R \ll (\text{degree f})/\eta$. Therefore, $S_z := \sum_{(m,P_z)=1} a_m(T)$ gives an estimate of the number of all $v \in \mathcal{O}$ such that $f(v)$ is R-almost prime for $R = (\text{degree f})/\eta$.

In order to verify these sieve axioms for $\mathcal{O} = v_0\Gamma$, we replace Γ by its preimage under the spin cover $\tilde{G}$ of G, so that Γ satisfies the strong approximation property that $\Gamma(q)\backslash\Gamma = \tilde{G}(\mathbb{Z}/q\mathbb{Z})$ outside a fixed finite set of primes. The most crucial condition is to understand the distribution of $a_m(T)$'s along the arithmetic progressions, i.e., $\sum_{m=0 \ (q)} a_m(T)$ for all square-free integers q, more precisely, we need to have a uniform control on the remainder term r_q of $\mathsf{A}_q(T) = \sum_{m=0 \ (q)} a_m = g(q)\mathcal{X} + r_q$ such as $r_q \ll \mathcal{X}^{1-\epsilon}$ for some $\epsilon > 0$ independent of q. By writing

$$\mathsf{A}_q(T) = \sum_{\gamma \in \Gamma_{v_0}(q)\backslash\Gamma, f(v_0\gamma)=0 \ (q)} \#(v_0\Gamma_{v_0}(q)\gamma \cap \mathcal{B}_T)$$

the following uniform counting estimates provide such a control on the remainder term:

Theorem 5.7 (Mohammadi-O. [38])**.** *Let Γ and $\mathcal{B}_T$ be as in Theorem 5.5. For any $\gamma \in \Gamma$ and any square-free integer q,*

$$\#v_0\Gamma(q)\gamma \cap \mathcal{B}_T = \frac{c_0}{[\Gamma : \Gamma(q)]}\mathcal{M}(\mathcal{B}_T) + O(\mathcal{M}(\mathcal{B}_T)^{1-\epsilon})$$

where $c_0 > 0$ and $\epsilon > 0$ are independent over all $\gamma \in \Gamma$ and q.

A basic ingredient of Theorem 5.7 is a uniform spectral gap for the Laplacian acting on $L^2(\Gamma(q)\backslash\mathbb{H}^n)$. Note that zero is no more the base-eigenvalue of the Laplacian when $\Gamma(q)$ is a thin group, but $\delta(n-1-\delta)$ is by Sullivan [57] and Lax-Phillips [31]. However, the expander result (Theorem 5.3) implies a uniform lower bound for the gap between the base eigenvalue $\delta(n-1-\delta)$ and the next one; this transfer property was obtained by Bourgain, Gamburd and Sarnak. As explained in section 3, the mixing of frame flow of the

Bowen-Margulis-Sullivan measure is a crucial ingredient in obtaining the main term in Theorem 5.7, and the (uniform) error term in the counting statement of Theorem 5.7 is again a consequence of a uniform error term in the effective mixing of frame flow, at least under our hypothesis on δ.

References

[1] Jean Bourgain. Integral Apollonian circle packings and prime curvatures. *Preprint.* arXiv:1105:5127, 2011

[2] Jean Bourgain and Elena Fuchs. A proof of the positive density conjecture for integer Apollonian packings *J. Amer. Math. Soc.* 24, 945–967, 2011

[3] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Affine linear sieve, expanders, and sum-product *Inventiones* 179, (2010) 559-644

[4] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Generalization of Selberg's 3/16 theorem and Affine sieve *Acta Math.* 207, (2011) 255–290

[5] Jean Bourgain and Alex Kontorovich. On the Local-Global conjecture for Integral Apollonian gaskets *To appear in Inventiones.* arXiv:1205:4416, 2012

[6] Jean Bourgain. Some Diophantine applications of the theory of group expansion *In Thin groups and superstrong approximation*, edited by Breulliard and Oh, MSRI Publ 61, Cambridge press.

[7] David W. Boyd. The sequence of radii of the Apollonian packing. *Math. Comp.*, 39(159):249–254, 1982.

[8] Martine Babillot. On the mixing property for hyperbolic systems. Israel J. Math., 129:61–76, 2002.

[9] E. Breuillard, B. Green and T. Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.* 21 (2011) 774–819

[10] Marc Burger. Horocycle flow on geometrically finite surfaces. *Duke Math. J.*, 61(3):779–803, 1990.

[11] Marc Burger and Peter Sarnak. Ramanujan duals II. *Inventiones*, 106 (1991), 1–11

[12] J. R. Chen On the representation of a larger even integer as the sum of a prime and the product of at most two primes. *Sci. Sinica* 16 (1973) 157–176.

[13] H. S. M. Coxeter. The problem of Apollonius. *Amer. Math. Monthly*, 75:5–15, 1968.

[14] L. Clozel. Demonstration de la conjecture . *Invent. Math.* 151 (2003), pp. 297–328.

[15] W. Duke, Z. Rudnick, and P. Sarnak. Density of integer points on affine homogeneous varieties. *Duke Math. J.*, 71(1):143–179, 1993.

[16] Nicholas Eriksson and Jeffrey C. Lagarias. Apollonian circle packings: number theory. II. Spherical and hyperbolic packings. *Ramanujan J.*, 14(3):437–469, 2007.

[17] Alex Eskin and C. T. McMullen. Mixing, counting, and equidistribution in Lie groups. *Duke Math. J.*, 71(1):181–209, 1993.

[18] Elena Fuchs. Counting problems in Apollonian packings. *Bulletin of AMS*, Vol.50 (2013) 229-266

[19] E. Fuchs. Strong Approximation in the Apollonian group. *J. Number Theory*, Vol 131, pp. 2282-2302 (2011)

[20] Elena Fuchs and K. Sanden. Some experiments with integral Apollonian circle packings. *Exp. Math. 20*,380-399, 2011

[21] L. Flaminio and R. Spatzier. Geometrically finite groups, Patterson-Sullivan measures and Ratner's theorem. *Inventiones*, 99, 601-626, 1990.

[22] A. Gorodnik and A. Nevo. Lifting, restricting and sifting integral points on affine homogeneous varieties. *To appear in Compositio Math*, 2012.

[23] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks, and Catherine H. Yan. Apollonian circle packings: geometry and group theory. I. The Apollonian group. *Discrete Comput. Geom.*, 34(4):547–585, 2005.

[24] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan. Apollonian circle packings: number theory. *J. Number Theory 100*, pp. 1-45 (2003)
[25] B. Green. Approximate groups and their applications:work of Bourgain, Gamburd, Helfgott and Sarnak. *Current Events Bulletin of the AMS*, 2010
[26] H. Halberstam and H. Richert. Sieve methods. *Academic Press.,* (1974) 167–242.
[27] Harald Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ *Ann. Math.*, 167. 601–623, 2008.
[28] Roger Howe and Calvin Moore. Asymptotic properties of unitary representations *J. Funct. Anal.*, 72–96, 1979.
[29] David Kazhdan. On a connection between the dual space of a group and the structure of its closed subgroups *Func. Anal. Appl.* 1 (1967), 63–65.
[30] Alex Kontorovich and Hee Oh. Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds. *Journal of AMS*, Vol 24. 603–648, 2011.
[31] Peter D. Lax and Ralph S. Phillips. The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces. *J. Funct. Anal.*, 46(3):280–350, 1982.
[32] Min Lee and Hee Oh. Effective circle count for Apollonian packings and closed horospheres. *GAFA*. Vol 23 (2013), 580–621
[33] C. Matthews, L. Vaserstein and B. Weisfeiler. Congruence properties of Zariski dense subgroups. *Proc. London Math. Soc.* 48, 1984, 514-532.
[34] Gregory Margulis. On some aspects of the theory of Anosov systems. *Springer Monographs in Mathematics. Springer-Verlag,* Berlin, 2004. With a survey by Richard Sharp: Periodic orbits of hyperbolic flows, Translated from the Russian by Valentina Vladimirovna Szulikowska.
[35] Gregory Margulis. Explicit constructions of expanders. *Problems of Information Transmission.* 9 (1973), no. 4, 325-332.
[36] Mattila, Pertti. Geometry of sets and measures in Euclidean spaces. *Cambridge University Press.* ISBN 978-0-521-65595-8.
[37] C. T. McMullen. Hausdorff dimension and conformal dynamics. III. Computation of dimension. *Amer. J. Math.*, 120(4):691–721, 1998.
[38] Amir Mohammadi and Hee Oh. Matrix coefficients, Counting and Primes for geometrically finite groups. *To appear in J. EMS*, arXiv 1208.4139
[39] D. Mauldin and M. Urbanski. Dimension and measures for a curvilinear Sierpinski gasket or Apollonian packings. *Adv. Math.*, 136 (1998), 26-38
[40] David Mumford, Caroline Series, and David Wright. Indra's pearls. *Cambridge University Press*, New York, 2002.
[41] Amos Nevo and Peter Sarnak. Prime and Almost prime integral points on principal homogeneous spaces *Acta Math*, 205 (2010), 361–402
[42] Hee Oh. Dynamics on Geometrically finite hyperbolic manifolds with applications to Apollonian circle packings and beyond. *Proc. of ICM.* (Hyderabad, 2010), Vol III 1308–1331
[43] Hee Oh. Harmonic Analysis, Ergodic theory and Counting for Thin groups. *In Thin groups and superstrong approximation*, edited by Breulliard and Oh, MSRI Publ 61, Cambridge press.
[44] Hee Oh and Nimish Shah. Equidistribution and counting for orbits of geometrically finite hyperbolic groups. *Journal of AMS*. Vol 26 (2013) 511–562
[45] Hee Oh and Nimish Shah. The asymptotic distribution of circles in the orbits of Kleinian groups. *Inventiones*, Vol 187, 1–35, 2012
[46] S.J. Patterson. The limit set of a Fuchsian group. *Acta Mathematica*, 136:241–273, 1976.
[47] L. Pyber, E. Szabo. Growth in finite simple groups of Lie type of bounded rank Preprint (2011) arXiv:1005.1858.
[48] J. G. Ratcliffe. Foundations of hyperbolic manifolds. *Springer-Verlag*, GTM 149

[49] Thomas Roblin. Ergodicité et équidistribution en courbure négative. *Mém. Soc. Math. Fr. (N.S.)*, (95):vi+96, 2003.
[50] Daniel Rudolph. Ergodic behavior of Sullivan's geometric measure on a geometrically finite hyperbolic manifold. *Erg. Th. and Dyn. Syst.*, Vol 2, 1982, 491–512
[51] A. Salehi Golsefidy and P. Sarnak. Affine Sieve *To appear in JAMS.* arXiv:1109.6432
[52] A. Salehi Golsefidy and P. Varju. Expansion in perfect groups *GAFA* Vol 22 (2012), 1832–1891
[53] Peter Sarnak. Integral Apollonian packings. *Amer. Math. Monthly.* 118 (2011), 291-306
[54] Peter Sarnak. Notes on Thin matrix groups *In Thin groups and superstrong approximation*, edited by Breulliard and Oh, MSRI Publ 61, Cambridge press.
[55] B. Stratmann and M. Urbanski. The box-counting dimension for geometrically finite Kleinian groups *Fund. Math.*, (149):83–93, 1996.
[56] Dennis Sullivan. The density at infinity of a discrete group of hyperbolic motions. *Inst. Hautes Études Sci. Publ. Math.*, (50):171–202, 1979.
[57] Dennis Sullivan. Entropy, Hausdorff measures old and new, and limit sets of geometrically finite Kleinian groups. *Acta Math.*, 153(3-4):259–277, 1984.
[58] Ilya Vinogradov. Effective bisector estimate with applications to Apollonian circle packings. *preprint*, 2012, arXiv.1204.5498
[59] Dale Winter. Mixing of frame flow for geometrically finite rank one manifold with application to measure classification. *preprint*, 2013.

Mathematics department, Yale university, New Haven, CT 06520 and Korea Institute for Advanced Study, Seoul, Korea
E-mail address: hee.oh@yale.edu