Thin groups and superstrong approximation
MSRI Publications
Volume **61**, 2013

Some Diophantine applications of the theory of group expansion

JEAN BOURGAIN

1. Introduction

The recent years have seen considerable progress in the theory of expansion and spectral gaps for so-called thin groups (as opposed to the classical theory of arithmetic groups.) These developments rely in part on methods and results from the rather novel research area of "arithmetic combinatorics" and underlying are general principles such as the "sum-product theorem" in finite fields and "product theorems" in linear groups. These advances turned out to be of interest well beyond group theory and have applications to geometry, number theory, theoretical computer science and even mathematical physics. At this point, many aspects of the extensive story were already accounted for in several survey papers, such as [Bourgain 2010], the Bourbaki exposé of E. Kowalski [2012] and those of B. Green [2009] and A. Lubotzky [2012] based on AMS lectures. A discussion of the "ubiquity" of thin groups from a broader perspective appears in [Sarnak 2014] in the present volume.

We will focus here on two specific number-theoretic applications. The first relates to integral Apollonian circle packings (ACP for short) and the problem of a local/global principle for the curvatures, as proposed in [Graham et al. 2003] and [Sarnak 2011]. The other concerns progress towards Zaremba's conjecture [1972] on continued fraction expansions of rationals and we will briefly review the paper [Bourgain and Kontorovich 2011]. Another exciting application of the theory of group expansion to finiteness in arithmetic geometry may be found in the work of J. Ellenberg, C. Hall and E. Kowalski [Ellenberg et al. 2012] but will not be discussed here. Neither will we get into the role of expansion to sieving theory (originating from [Bourgain et al. 2010a]) which triggered many of the later developments.

Our reference list is far from complete and strictly serves this exposé.

2. Background on expansion in Cayley graphs induced by thin groups

We start by recalling the notion of graph expansion and expander families. The reader is referred to the excellent survey paper [Hoory et al. 2006] for a detailed

discussion of this theory. Let $\mathcal{G}$ be a k-regular graph on a finite vertex set V, with $|V| = n$. Here one should see k as fixed whereas $n \to \infty$. The Busemann–Cheeger constant is then defined as

$$h(\mathcal{G}) = \min_{|S| \le n/2} \frac{|\partial S|}{|S|}, \tag{2-1}$$

where the minimum is taken over all subsets S of V and ∂S refers to the set of edges from S to $V \setminus S$. Having fixed k, a collection of k-regular graphs $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \ldots$ on vertex sets $V_1, V_2, V_3, \ldots$ with $|V_i| \to \infty$ is called an expander family provided

$$h(\mathcal{G}_i) > c \quad \text{for all } i, \tag{2-2}$$

for some $c > 0$.

Expansion has a well-known spectral interpretation on the level of the adjacency matrix $A(\mathcal{G})$ of $\mathcal{G}$, defined by

$$A_{i,j} = \begin{cases} 1 \text{ if } (i,j) \in \mathcal{G}, \\ 0 \text{ otherwise.} \end{cases} \tag{2-3}$$

Since $\mathcal{G}$ is undirected, A is symmetric and $k = \lambda_0 \ge \lambda_1 \ge \cdots \ge \lambda_{n-1}$ since we assumed $\mathcal{G}$ k-regular. The following inequalities relate then the Cheeger constant to the "spectral gap" $\lambda_0 - \lambda_1$

$$\tfrac{1}{2}(k - \lambda_1) \le h(\mathcal{G}) \le \sqrt{2k(k - \lambda_1)}. \tag{2-4}$$

Do expander families exist? It was proven by Pinsker [1973] that given $k \ge 3$, a random (= typical) k-regular graph on n vertices ($n \to \infty$) is an expander graph. Around the same time, Margulis [1973] came up with explicit constructions based on Cayley graphs of groups. Recall that if $V = \langle S \rangle$ is a group generated by a finite set S of elements, the Cayley graphs $\mathcal{G}(V, S)$ consists of the edges $(x, y), x, y \in V$, for which $xy^{-1} \in S \cup S^{-1}$. Of particular importance to our discussion is Selberg's theorem on the congruence graphs induced by $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 1. *Assume $\langle S \rangle$ a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and denote by $\pi_q : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(q)$ the $(\mathrm{mod}\, q)$ reduction. There is an integer q_0 such that the family of Cayley graphs*

$$\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big), \quad \text{where } q \in \mathbb{Z}_+,\ (q, q_0) = 1, \tag{2-5}$$

is an expander family.

The assumption that $\langle S \rangle$ is of finite index is quite restrictive. What happens with "thin" subgroups? Recall that if G is an algebraic group, a subgroup $\Gamma \subset G(\mathbb{Z})$ is called "thin" provided $[G(\mathbb{Z}) : \Gamma] = \infty$. Assuming $\langle S \rangle \subset \mathrm{SL}_2(\mathbb{Z})$ contains the free group F_2 on 2 generators (equivalently, $\langle S \rangle$ is nonelementary

meaning that $\langle S\rangle$ does not contain a solvable subgroup of finite index), the Zariski closure of $\langle S\rangle$ equals SL_2. Citing the strong approximation property due to Matthews, Vaserstein, and Weisfeiler [1984], recall that if Γ is a subgroup of $\mathrm{SL}_d(\mathbb{Z})$ which is Zariski dense in SL_d, there is some $q_0 \in \mathbb{Z}_+$ such that $\pi_q(\Gamma) = \mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$ for $(q, q_0) = 1$. Thus, if $\langle S\rangle \subset \mathrm{SL}_2(\mathbb{Z})$ is nonelementary, the Cayley graphs $\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big)$ for $q \in \mathbb{Z}_+$, $(q, q_0) = 1$ are connected. Moreover Theorem 1 generalizes.

Theorem 2. *Assume $\langle S\rangle$ a nonelementary subgroup of $\mathrm{SL}_2(\mathbb{Z})$. There is $q_0 \in \mathbb{Z}$ such that $\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big)$, $(q, q_0) = 1$, forms an expander family.*

Under the assumption that the limit set of $\Gamma = \langle S\rangle$ has dimension $\delta_\Gamma > \frac{5}{6}$, Theorem 2 is due to A. Gamburd [2002]. His result left unanswered Lubotzky's 1-2-3 problem [1994] (a folklore question in the subject), noting that Selberg's theorem applies to

$$S_1 = \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\} \quad \text{and} \quad S_2 = \left\{\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\right\},$$

but not to

$$S_3 = \left\{\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}\right\}.$$

The latter case was settled in [Bourgain and Gamburd 2008], which implies Theorem 2 for q prime. A crucial ingredient is Helfgott's product theorem in $\mathrm{SL}_2(p)$ [Helfgott 2008]. Theorem 2 for q square free was proven in [Bourgain et al. 2010a], motivated by applications to prime number sieving, and the case of unrestricted modulus follows from [Bourgain and Varjú 2012]. Meanwhile, based on deep work due to Helfgott [2011], Green, Breuillard, and Tao [2011] and Pyber and Szabó [2010] on the combinatorial side, Theorem 2 has been vastly generalized, at least for prime and square-free moduli (see [Varjú 2012; Salehi Golsefidy and Varjú 2012]). Although the work described later in this exposé is SL_2-based ($\mathrm{SL}_2(\mathbb{Z})$ and the Gauss-integer extension $\mathrm{SL}_2(\mathbb{Z} + i\mathbb{Z})$), we record one of the most general results obtained in this context.

Theorem 3 [Salehi Golsefidy and Varjú 2012]. *Let k be a number field and $\Gamma \subset \mathrm{SL}_d(k)$, $\Gamma = \langle S\rangle$ with S a finite symmetric set. Assume the Zariski-closure of Γ is semisimple. Then the Cayley graphs $\mathcal{G}(\pi_q(\Gamma), \pi_q(S))$ form a family of expanders when q ranges over square-free ideals of the integers $\mathcal{O}$ of k with large prime factors.*

Returning to Lubotzky's problem, let us also mention the Lubotzky–Weiss conjecture, stating that expansion in $\mathrm{SL}_2(p)$ or, more generally, $\mathrm{SL}_n(p)$-Cayley graphs, is in fact a group property:

Conjecture 4. *There is an absolute constant $c = c_k > 0$ such that*

$$h\big(\mathcal{G}(\mathrm{SL}_2(p), S)\big) > c, \tag{2-6}$$

whenever $S \subset \mathrm{SL}_2(p)$, $|S| = k$, is generating and p prime.

A positive answer would be conceptually very pleasing.

Evidence of its truth is the result of Breuillard and Gamburd [2010] establishing the conjecture for p outside a small exceptional set of the primes. Lubotzky–Weiss' problem will not be essential in our subsequent discussion as the Cayley graphs will be induced by a fixed set of elements in $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{SL}_2(\mathbb{Z}+i\mathbb{Z})$. On the other hand, what is essential for us is to have unrestricted modulus q.

3. Hyperbolic lattice point counting

The spectral gap in congruence Cayley graphs described above in conjunction with Brun's combinatorial sieve, have been used to carry out prime and pseudo-prime sieving in the orbits of thin groups (see [Bourgain et al. 2010a; Sarnak 2008; Salehi Golsefidy and Sarnak 2011] for the ultimate generalization of this theory.) The "balls" involved in the sieving process are defined in terms of the word metric on the generators.

Other number-theoretic applications as presented in the next sections are based on different analytical tools (more specifically, the Hardy–Littlewood circle method) and require precise counting in Archimedean balls in the congruence subgroups. Such information may be obtained by hyperbolic lattice point counting and we briefly review the results for thin groups obtained in [Bourgain et al. 2011]. See the same paper also for related references.

Denote by $\mathbb{H} = \mathbb{H}^2 = \{x + iy \in \mathbb{C} : y > 0\}$ the hyperbolic plane on which $\mathrm{SL}_2(\mathbb{R})$ acts by Moebius transformation

$$gz = \frac{az+b}{cz+d}, \quad \text{where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}). \tag{3-1}$$

Note that the theory discussed below has a counterpart for $\mathbb{H}^3$ and the action of $\mathrm{SL}_2(\mathbb{C})$, which is relevant for the application to the Apollonian group discussed in the next section. With g as in (3-1), we have

$$\|g\|^2 = a^2 + b^2 + c^2 + d^2 = 4u(gi, i) + 2, \tag{3-2}$$

where

$$u(z, w) = \frac{|z-w|^2}{4 \operatorname{Im} z \operatorname{Im} w} \quad \text{and} \quad \cosh d_{\mathbb{H}}(z, w) = 1 + 2u(z, w).$$

This clarifies the significance of hyperbolic space to the Archimedean counting problem.

Next, let Γ be a finitely generated subgroup of $\mathrm{SL}_2(\mathbb{Z})$, $L = L(\Gamma) \subset \mathbb{R}$ its limit set and $\delta = \delta_\Gamma$ the Hausdorff dimension of L. The assumption that Γ is nonelementary is equivalent to $0 < \delta \leq 1$. Thus our goal is Archimedean counting in the orbits of Γ and its congruence subgroups. We distinguish two cases.

• $\delta > \frac{1}{2}$: In this case, the hyperbolic surface $\mathbb{H}/\Gamma$ (which has infinite volume if $\delta < 1$) has an L^2-spectral theory and we rely on Lax–Phillips' theory based on automorphic methods and the wave equation.

• $\delta > 0$: If $0 < \delta \leq \frac{1}{2}$, there is no L^2-spectral theory and instead we use the thermodynamical approach based on symbolic dynamics and Ruelle's transfer operator, as developed by Lalley, Dolgopyat, Naud and others. This method is quite flexible and applies also in the semigroup setting (relevant in the application to Zaremba's problem in Section 5.)

We first discuss the spectral approach, assuming $\delta(L) > \frac{1}{2}$. The spectrum

$$0 \leq \lambda_0 < \lambda_1 \leq \cdots \leq \lambda_{\max} < \tfrac{1}{4} \quad \xrightarrow{\text{continuous spectrum}} \tag{3-3}$$

of the Laplace operator on $\mathbb{H}/\Gamma$ has lowest eigenvalue $\lambda_0 = \delta(1-\delta)$ and $\lambda_1 > \lambda_0$. Defining δ_j by $\lambda_j = \delta_j(1-\delta_j)$ and denoting by $\{\varphi_j\}$ the corresponding eigenfunctions, we state the theorem of Lax and Phillips [1982].

Theorem 5. *With the above notation, one has for* $w_0, w \in \mathbb{H}$

$$\big|\{\gamma \in \Gamma : d_{\mathbb{H}}(w, \gamma w_0) \leq s\}\big| = \sum_{j \geq 0} C_j \varphi_j(w)\varphi_j(w_0) e^{\delta_j s} + O\big(e^{\frac{1}{3}(1+\delta_0)s}\big). \tag{3-4}$$

What happens in congruence subgroups $\Gamma(q) = \big\{\gamma \in \Gamma : \gamma = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) (\mathrm{mod}\, q)\big\}$?

Considering the spectrum of $\mathbb{H}/\Gamma(q)$, it is an elementary fact that $\lambda_0(\Gamma(q)) = \lambda_0(\Gamma)$ and the issue is a uniform gap $\lambda_1(\Gamma(q)) - \lambda_0$ when q varies. When $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Selberg proved that $\lambda_1(\Gamma(q)) \geq \frac{3}{16}$ and conjectured $\lambda_1(\Gamma(q)) \geq \frac{1}{4}$ (no exceptional eigenvalues). The current record seems to be

$$\lambda_1(\Gamma(q)) > \tfrac{1}{4} - \big(\tfrac{7}{64}\big)^2,$$

due to Kim and Sarnak [1995].

Returning to thin groups $\Gamma = \langle S \rangle$ with $\delta_\Gamma > \frac{1}{2}$, one has the following extension of Selberg's result.

Theorem 6. *There is* $\varepsilon = \varepsilon(\Gamma) > 0$ *such that* $\lambda_1(\Gamma(q)) > \lambda_0 + \varepsilon$ *for all* $q \in \mathbb{Z}_+$.

The proof relies essentially on the expander family $\mathcal{G}\big(\mathrm{SL}_2(q), \pi_q(S)\big)$ and the conversion of the combinatorial spectral gap to a geometric one follows arguments due to Burger and Brooks in the finite volume case.

Combining Theorem 5 and Theorem 6 leads to the following Archimedean-modular distributional property.

Corollary 7. *Let* $\Gamma = \langle S \rangle \subset \mathrm{SL}_2(\mathbb{Z})$, *and* $\delta_\Gamma > \frac{1}{2}$. *There is some* $q_0 = q_0(\Gamma) \in \mathbb{Z}$ *such that, if* $(q, q_0) = 1$ *and* $g \in \mathrm{SL}_2(q)$,

$$\left|\{\gamma \in \Gamma : \|\gamma\| \le N \text{ and } \pi_q(\gamma) = g\}\right| = \frac{cN^{2\delta}}{|\mathrm{SL}_2(q)|} + O(q^C N^{2\delta-\varepsilon}), \qquad (3\text{-}5)$$

where ε, c *and* C *only depend on* Γ.

This type of result plays a key role in the diophantine applications discussed in the next sections of this exposé. A similar (though slightly weaker) statement may be obtained in the general case $\delta_\Gamma > 0$ following the thermodynamical approach which we review next.

Assuming $\Gamma = \langle T_1, \dots, T_k \rangle \subset \mathrm{SL}_2(\mathbb{Z})$ has no parabolic elements, one identifies Γ with the set Σ_* of finite sequences on the alphabet $\{\pm 1, \dots, \pm k\}$ compatible with a transition matrix and the limit set $L(\Gamma)$ with the corresponding set Σ of infinite sequences. The Nielsen map $F : L \to L$ corresponds to a finite type shift $\sigma : \Sigma \to \Sigma$ under the symbolic conversion and the distortion function $f = \log |F'|$ is expressed by $\tau(x) = d_{\mathbb{H}}(i, xi) - d_{\mathbb{H}}(i, x_2 x_3 \dots i)$ for $x = (x_1, x_2, \dots) \in \Sigma$. Taking $0 < \rho < 1$, we define a metric on Σ by

$$d(x, y) = \rho^m, \quad \text{with } m = \max\{j : x_j = y_j\}, \qquad (3\text{-}6)$$

and denote by $\mathcal{F}$ the corresponding space of Hölder functions f, i.e., those satisfying

$$|f(x) - f(y)| \le K d(x, y) \quad \text{for some } K > 0. \qquad (3\text{-}7)$$

Given a function $f \in \mathcal{F}$, define the transfer operator $\mathcal{L}_f : \mathcal{F} \to \mathcal{F}$ by

$$(\mathcal{L}_f g)(x) = \sum_{\sigma(y) = x} e^{f(y)} g(y). \qquad (3\text{-}8)$$

Recall Ruelle's theorem to the effect that for $f \in \mathcal{F}$ real, there is a simple largest eigenvalue $\lambda_f > 0$ of $\mathcal{L}_f$ with strictly positive eigenfunction h_f and a Borel probability measure ν_f on Σ satisfying

$$\mathcal{L}^* \nu = \lambda \nu \quad \text{and} \quad \int h \, d\nu = 1.$$

Denote by $P(f) = \log \lambda_f$ the pressure function. Taking $f = -s\tau$ with τ as above, $P(-s\tau)$ is strictly increasing in $s \in \mathbb{R}$ and, according to a result due to Patterson and Sullivan, vanishes at $s = \delta = \dim L(\Gamma)$.

The renewal approach to the counting problem consists in introducing a counting function

$$N_\phi(T, x) = \sum_{n=0}^{\infty} \sum_{\sigma^n y = x} \phi(y) 1_{\{S_n \tau(y) \le T\}}, \qquad (3\text{-}9)$$

where

$$S_n f = f + (f \circ \sigma) + \cdots + (f \circ \sigma^{n-1}). \tag{3-10}$$

Thus in particular, for x the identity and $\phi = 1$, we obtain the number of elements of Γ for which $d_{\mathbb{H}}(\gamma i, i) \le T$.

The counting function satisfies the renewal equation

$$N_\phi(T, x) = \phi(x) 1_{\{T \ge 0\}} + \sum_{\sigma(y)=x} N_\phi(T - \tau(y), y). \tag{3-11}$$

Introducing its Laplace transform

$$F(s, x) = \int_{-\infty}^{\infty} e^{-sT} N(T, x)\, dT \quad (\mathrm{Re}\, s \gg 1), \tag{3-12}$$

(3-11) is converted to

$$F(s, x) = -\mathcal{R}_s \frac{\phi(x)}{s}, \tag{3-13}$$

where $\mathcal{R}_s = (I - \mathcal{L}_{-s\tau})^{-1}$ is the resolvent and is analytic for $\mathrm{Re}\ s > \delta$. The following statement results from the work of Lalley and Naud (based on work of Dolgopyat).

Theorem 8. (i) *$\mathcal{R}_s$ has a meromorphic extension to a strip* $\mathrm{Res} > \delta - \varepsilon$ *with a simple pole at* $s = \delta$.

(ii) $\|\mathcal{R}_s\| < C(1 + |\mathrm{Im}\, s|^2)$ *for* $|s| \to \infty$.

(iii) $|\{\gamma \in \Gamma : d_{\mathbb{H}}(i, \gamma i) \le s\}| = Ce^{\delta s} + O(e^{(\delta-\varepsilon)s})$.

Statement (iii) follows from (i) and (ii) by standard Tauberian arguments (see [Bourgain et al. 2011] for details) and a widening of the analyticity region leads to improved error terms in the counting.

The next step consists in extending this theory in order to capture congruence subgroups $\Gamma(q)$ of Γ with uniformity in q.

Replace Σ by $\Sigma \times \mathrm{SL}_2(q)$ and $\mathcal{F}$ by the space $\mathcal{F}_q = \mathcal{F}\big(\Sigma \times \mathrm{SL}_2(q)\big)$ of vector-valued Hölder functions f on Σ with norm

$$\|f\|_\rho = \|f\|_\infty + |f|_\rho,$$

where

$$\|f\|_\infty = \max_x \Big(\sum_{g \in \mathrm{SL}_2(q)} |f(x, g)|^2 \Big)^{\frac{1}{2}} \tag{3-14}$$

and

$$|f|_\rho = \max_m \frac{\mathrm{Var}_m f}{\rho^m}, \tag{3-15}$$

with

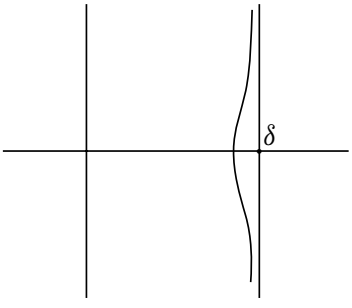
$$\mathrm{Var}_m f = \sup\left\{\left(\sum_{g\in \mathrm{SL}_2(q)} |f(x,g)-f(y,g)|^2\right)^{\frac{1}{2}} : x_j = y_j \text{ for } j\le m\right\} \quad (3\text{-}16)$$

On the extended space $\mathscr{F}_q$, introduce the transfer operator as

$$(\mathscr{L}_{-s\tau} f)(x,g) = \sum_{\sigma(y)=x} e^{s\tau(y)} f(y, yx^{-1}g). \quad (3\text{-}17)$$

The resonance-free region obtained in [Bourgain et al. 2011] is of the form

$$\mathrm{Re}\, s > \delta - \frac{c}{\log(2+|\mathrm{Im}\, s|)}, \quad (3\text{-}18)$$



where (3-18) is uniform in q. The proof makes again essential use of the expansion in $\Gamma/\Gamma(q)$. Using (3-18), following analogue of Corollary 7 is deduced.

Theorem 9. *There is* $q_0 = q_0(\Gamma) \in \mathbb{Z}$ *such that for* $(q, q_0) = 1$ *and* $g \in \mathrm{SL}_2(q)$

$$\left|\{\gamma \in \Gamma : \|\gamma\| \le N \text{ and } \pi_q(\gamma) = g\}\right| = \frac{cN^{2\delta}}{|\mathrm{SL}_2(q)|}\left(1 + O(N^{-1/\log\log N})\right) + O(q^C N^{2\delta-\varepsilon}). \quad (3\text{-}19)$$

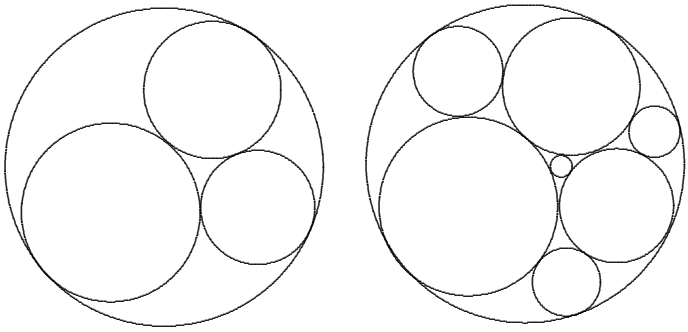
Compared with Corollary 7, the error term is a bit worse, but the term in $O\big(N^{-1/\log\log N}\big)$ may be further reduced (and even removed) if $1_{[\|\gamma\|\le N]}$ is replaced by a suitable weighted average.

In both Corollary 7 and Theorem 9, one may moreover specify the expanding direction v_+ of g to be in a sector I, with the effect of introducing a factor $\mu(I)$ in the main term, where μ is the Sullivan–Patterson measure.

4. Integral Apollonian circle packings

For background, see [Graham et al. 2003; Sarnak 2011]. Recall Apollonius' theorem: Given three mutually tangent circles in the plane, there are exactly two circles tangent to all three. Starting from four mutually tangent circles as

depicted below and filling in repeatedly the lacunae with tangent circles leads to so-called Apollonian circle packings (ACPs):



It was observed by F. Soddy that if the curvatures of the initial four circles — known as the *root quadruple* — are integers, all circles in the packing will have integral curvature, leading to integral ACPs. An example is shown in Figure 1.

This phenomenon may be explained by considering the Descartes quadratic form

$$F(x_1, x_2, x_3, x_4) = 2(x_1^2 + x_2^2 + x_3^2 + x_4^2) - (x_1 + x_2 + x_3 + x_4)^2, \quad (4\text{-}1)$$

since $F(x_1, x_2, x_3, x_4) = 0$ is tantamount to x_1, x_2, x_3, x_4 being curvatures of four mutually tangent circles.

Which integers are produced in a given integral ACP? That is the general question proposed in [Graham et al. 2003] and [Sarnak 2011], where the following conjectures were formulated.

(A) *The positive density conjecture*: the set of curvatures in any integral ACP is of positive density in $\mathbb{Z}$.

(B) *Local to global principle*: all integers are produced, up to a finite congruence condition.

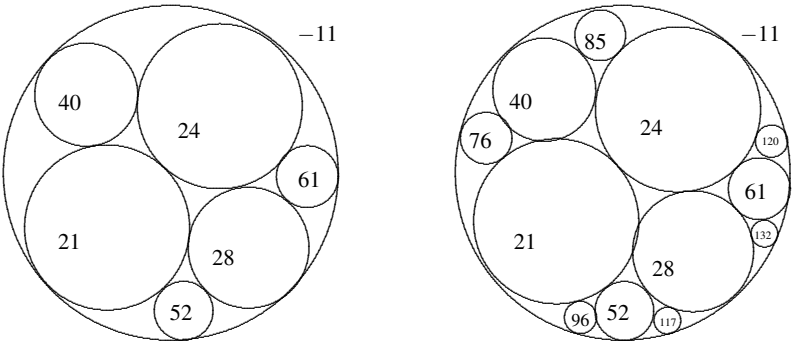


Figure 1. Packing $\mathcal{P}_0$ with root quadruple $(-11, 21, 24, 28)$.

Obviously (B) implies (A).

It turns out that the curvatures in a given integral ACP with root quadruple (a, b, c, d) are obtained as the orbit of a group, the so called Apollonian packing group A, which is the subgroup of the orthogonal group $\mathbb{O}_F$ associated to (4-1), generated by the matrices

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

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

A first important feature of A is that, under the spin double cover, it identifies with a finitely generated subgroup Γ of $\mathrm{SL}_2(\mathbb{Z}+i\mathbb{Z})$ to which the spectral method discussed in the previous section apply. More specifically considering the action on $\mathbb{H}^3$, the limit set L has dimension

$$\delta = \delta_\Gamma = 1.30568\ldots, \tag{4-2}$$

and Lax–Phillips theory is applicable. Denoting $a(C)$ the curvature of the circle C, for any packing $\mathcal{P}$ the Poincaré series

$$\sum_{C\in\mathcal{P}} a(C)^{-s} \tag{4-3}$$

has exponent of convergence equal to δ, which is the dimension of the residual set of the packing $\mathcal{P}$ (and is independent of $\mathcal{P}$).

The other feature of A are its arithmetic subgroups $\langle S_1, S_2, S_3\rangle$, $\langle S_2, S_3, S_4\rangle$, $\langle S_3, S_4, S_1\rangle$, $\langle S_4, S_1, S_2\rangle$, isomorphic to a finite index subgroup of $SO(2,1)(\mathbb{Z})$, and which orbits may be described by binary quadratic forms. Both spectral and arithmetical aspects are important in understanding the properties of the sets of curvatures.

Let

$$N_{\mathcal{P}}(T) = \#\{C \in \mathcal{P} : a(C) \le T\}, \tag{4-4}$$

be the number of curvatures at most T in the packing $\mathcal{P}$, counted with multiplicity. The exact asymptotic is provided by the following result, which is and based on spectral methods.

Theorem 10 [Kontorovich and Oh 2011]. *$N_{\mathcal{P}}(T) \sim bT^\delta$ as $T \to \infty$, where $b = b(\mathcal{P})$.*