BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 50, Number 2, April 2013, Pages 229–266
S 0273-0979(2013)01401-0
Article electronically published on February 14, 2013

COUNTING PROBLEMS IN APOLLONIAN PACKINGS

ELENA FUCHS

Abstract. An Apollonian circle packing is a classical construction which is made by repeatedly inscribing circles into the triangular interstices in a Descartes configuration of four mutually tangent circles. Remarkably, if the original four circles have integer curvature, all of the circles in the packing will have integer curvature, making the packings of interest from a number theoretic point of view. Many of the natural arithmetic problems have required new and sophisticated tools to solve them. The reason for this difficulty is that the study of Apollonian packings reduces to the study of a subgroup of $\mathrm{GL}_4(\mathbb{Z})$ that is thin in a sense that we describe in this article, and arithmetic problems involving thin groups have only recently become approachable in broad generality. In this article, we report on what is currently known about Apollonian packings in which all circles have integer curvature and how these results are obtained. This survey is also meant to illustrate how to treat arithmetic problems related to other thin groups.

1. Introduction

To begin our story about Apollonian circle packings, we consider four mutually tangent circles, one of them internally tangent to the other three as in the first picture in Figure 1. The name *Apollonian packing* as well as the study of these objects stems from the following ancient theorem of Apollonius of Perga, which Apollonius discovered while searching for a straight edge and compass construction of mutually tangent circles and lines.

Theorem 1.1 (Apollonius, circa 200 BCE)**.** *To any three mutually tangent circles or lines there are precisely two other circles or lines that are tangent to all three.*

As far as the first picture in Figure 1 goes, Theorem 1.1 implies that there is a unique circle that can be inscribed into every interstice between the four mutually tangent circles in the picture—these unique circles are shown in the second picture in Figure 1. Inscribing these circles produces 12 new interstices, each of which can again be filled with a unique circle. This process can be continued indefinitely to get a packing of infinitely many circles which is duly called an *Apollonian circle packing* (ACP). Given this procedure of constructing the packing, we say that the original four circles in the first picture of Figure 1 are born in generation 0 of the packing, the new circles in the second picture are born in generation 1, and so on. Note that in Figure 1 we also include a construction of an unbounded Apollonian circle packing, where two of the four circles we start with are parallel lines (these are circles of infinite radius which are tangent at infinity).

Received by the editors August 1, 2012, and, in revised form, September 2, 2012.
2010 *Mathematics Subject Classification.* Primary 11-02.
The author is supported by the Simons Foundation through the Postdoctoral Fellows program.

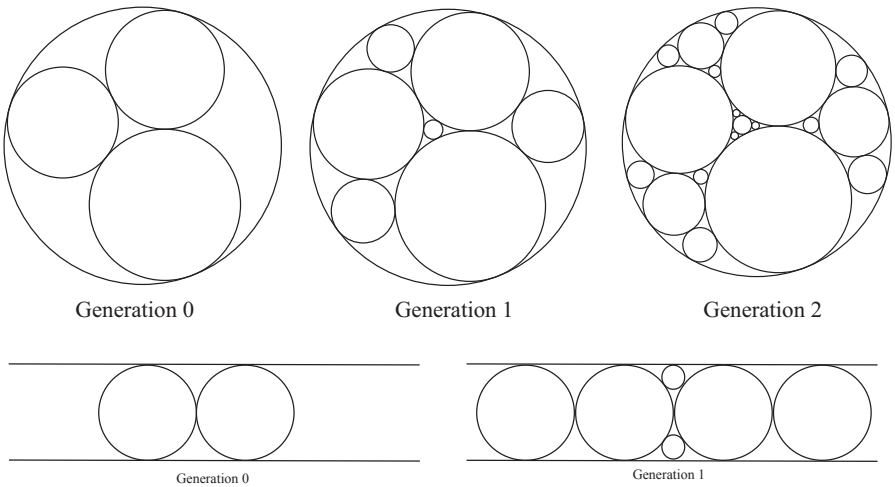


FIGURE 1. Packing circles

One can study Apollonian circle packings from many different angles—various properties of the packings are investigated in [1] and [52], as well as in a beautiful series of articles by Graham, Lagarias, Mallows, Wilks, and Yan (see [24], [25], [26], [27]). A good introduction to number-theoretic questions related to Apollonian packings can be found in [45]: these questions will be the main focus of this article. To understand how such questions arise in the context of this purely geometric construction, consider the *curvatures*, or reciprocals of the radii, of the circles in a given ACP. By the following theorem of Descartes, the curvatures of any four mutually tangent circles (in an ACP in particular) satisfy a certain quadratic equation.

Theorem 1.2 (Descartes, 1643)**.** *Let a, b, c, and d denote the curvatures of four mutually tangent circles, where a circle is taken to have negative curvature iff it is internally tangent to the other three. Then*

$$Q(a,b,c,d) := 2(a^2+b^2+c^2+d^2) - (a+b+c+d)^2 = 0. \tag{1.1}$$

We will refer to the quadratic form Q in (1.1) as the *Descartes quadratic form*, and to the curvatures (a, b, c, d) of any four mutually tangent circles as a *Descartes quadruple*.

In 1936, the Nobel Prize laureate in chemistry, Frederick Soddy, rediscovered Theorem 1.2 and even expressed it in the form of a poem in [49]. He deduced from it that if any one Descartes quadruple (a, b, c, d) in a packing is integral—i.e., $a, b, c, d \in \mathbb{Z}$—all of the circles in the packing must in fact have integer curvature. We call such ACPs in which all circles have integer curvature *integer ACPs*. A few examples of integer Apollonian packings are illustrated in Figure 2: the first packing is generated by starting with circles of curvatures $-1, 2, 2, 3$; the second is generated by starting with circles of curvatures $-11, 21, 24, 28$; and the last packing is an unbounded packing generated by starting with circles of curvature $0, 0, 1, 1$ which is the only unbounded integer ACP up to scaling (see [27] for a proof).

There are many more examples of such packings: in fact, there are infinitely many *primitive*[1] integer ACPs which makes them particularly interesting from a number theoretic point of view.

Indeed, this remarkable integrality feature gives rise to several natural questions about integer ACPs; Graham et al. make some progress towards answering them in [27] and pose striking conjectures, many of which are now theorems or at least better understood (see [7], [8], [9], [13], [19], [20], [21], [22], [32], [46], etc.) In this article we will survey how all these questions are handled and give an overview of what is currently known. We first recall the notion of a *root quadruple* of an ACP from [27] in the following theorem:

Theorem 1.3 (Graham, Lagarias, Mallows, Wilks, and Yan [27])**.** *Define a Descartes quadruple* $\mathbf{v} = (a, b, c, d)^t$ *with* $a + b + c + d > 0$ *to be a* root quadruple *if* $a \leq 0 \leq b \leq c \leq d$ *and* $a + b + c \geq d$*. Then every integer ACP has a unique root quadruple. However, the packing may contain more than one quadruple of mutually tangent circles that yields the root quadruple.*

Essentially, a root quadruple of a packing consists of the curvatures of the four largest circles in the packing and completely defines the ACP in question: for example, the root quadruple of the packing in Figure 2 is $\mathbf{v} = (-1, 2, 2, 3)^t$. The algorithm in [27] for finding the root quadruple of a packing is derived from a convenient representation of the curvatures of circles in an ACP as maximum norms of vectors in an orbit of a group $A \subset \mathrm{GL}_4(\mathbb{Z})$ called the *Apollonian group*, which is a subgroup of the orthogonal group fixing the Descartes form Q and which appears first in work of Hirst in [29]. In fact, an orbit of A containing some Descartes quadruple in a given packing will consist precisely of all of the Descartes quadruples in this packing. This group will be of great importance throughout this article. We introduce it in Section 1.1.

One notable property of the Apollonian group which we discuss in more detail in Section 1.1 is that it is a "thin" group in the following sense.

Definition 1.4. Let Γ be a subgroup of $\mathrm{GL}_n(\mathbb{Z})$, and let $G = \mathrm{Zcl}(\Gamma)$ be its Zariski closure. We say that Γ is *thin* if Γ is of infinite index in $G(\mathbb{Z})$. We say Γ is *arithmetic* if it is not thin.

This thinness property makes the study of integer ACPs quite intricate. To give a flavor of why this is, consider the contrast between thin and arithmetic subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$. One basic tool in problems connected to arithmetic Γ (say, counting primes in orbits of such subgroups) is the theory of modular forms, or more generally for arithmetic subgroups of $\mathrm{GL}_n(\mathbb{Z})$ the theory of automorphic forms and L-functions. Indeed, several long-standing problems in analytic number theory have been reduced to finding good estimates for Fourier coefficients of automorphic forms. An important aspect of studying these forms which also plays a role in the thin case is understanding the spectral theory of the Laplace operator Δ on $L^2(\Gamma\backslash\mathbb{H})$. For example, it is known that the smallest eigenvalue in the spectrum for finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ is $\lambda_0 = 0$, corresponding to the constant eigenfunction. In the special case where Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, Selberg's eigenvalue conjecture states that there are no eigenvalues $0 < \lambda_i < 1/4$.

[1]Primitive integer ACPs are those in which the curvatures in the packing share no common factor greater than 1. It is natural to study only primitive integer packings, as a non-primitive ACP is simply a scaling by an integer factor of a primitive one.

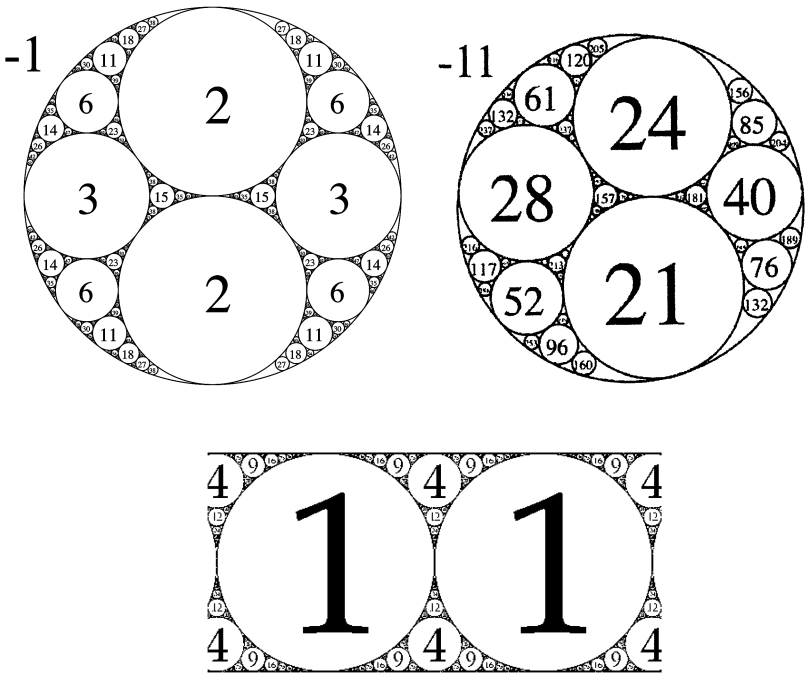


FIGURE 2. Apollonian packings with root quadruples $(-1, 2, 2, 3)^t$, $(-11, 21, 24, 28)^t$, and $(0, 0, 1, 1)^t$.

Selberg himself showed that $\lambda_1 \geq 3/16$, and there have been various subsequent improvements towards $1/4$. There are analogs of this conjecture in the context of more general groups as well.

However, the study of automorphic forms has traditionally focused on forms associated to arithmetic groups. In the case that Γ is an *infinite* index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that is Zariski-dense in SL_2 much less is known: for example, it is no longer true that the smallest eigenvalue is 0—in fact, the constant function is no longer square-integrable in this situation!

Unlike the theory of arithmetic groups, until recently there have been few techniques to handle thin groups; however this has changed. Moreover, thin groups arise naturally whenever the group is given in terms of a finite generating set (see [4]). Furthermore, it is known that all but finitely many discrete groups of motion of hyperbolic n-space generated by reflections in hyperplanes are thin; in fact, all such groups in dimension $n > 300$ are thin. These results, as well as other similar results due to Vinberg and Prokhorov, can be found in Nikulin's ICM article [41].

To come back to integer ACPs, the thin group prevalent in this article is the Apollonian group mentioned above. This example is meant to convince the reader that it is very natural to consider Diophantine problems associated with thin groups as well as to outline the methods one might use to address them. Specifically, our aim in this article is to shed light on the following arithmetic questions.

Question 1. What can be said about the residues modulo an integer d of the curvatures of circles in a given ACP?

We discuss this question in Section 2. Graham et al. were the first to investigate congruence obstructions in Apollonian packings in [27], where they show that

there are always obstructions modulo 12 in any given ACP, and that there are no congruence obstructions modulo d if the greatest common divisor $(d, 30) = 1$. One such result is the following.

Theorem 1.5 (Graham, Lagarias, Mallows, Wilks, and Yan [27]). *Let P be a primitive integer Apollonian packing. For any integer m with $\gcd(m, 30) = 1$, every residue class modulo m occurs as the value of a curvature of some circle in the packing P.*

In Section 2 we review the results in [21] which extend Theorem 1.5 and give a complete answer to Question 1, namely it is shown that the only congruence obstructions for any primitive integer ACP are modulo 24, and that the number 30 in Theorem 1.5 above can be improved to 6. The basic idea is to use the representation of the packing as an orbit of the Apollonian group A and analyze the mod d structure of A. It is worth noting that Graham et al. prove their theorems by considering only unipotent subgroups of A, while in [21] we exploit the full Apollonian group.

Graham et al. also conduct various numerical experiments to better understand the set of curvatures in different integer Apollonian packings. Based on these experiments, they pose a "strong density conjecture" which predicts that given a primitive packing P, any sufficiently large integer satisfying some fixed congruence conditions appears as a curvature in P. This conjecture is posed in a more precise way as a local-to-global conjecture in [22]. As we discuss in Section 4, this precise local-global conjecture has stood up to experimental scrutiny and remains wide open. A much more feasible task is to determine integers which *cannot* occur as curvatures in a given packing by ruling out congruence classes modulo various "bad" primes. We make this notion of badness more precise in Section 2 and explain how such information can suggest local-to-global conjectures both in the Apollonian case and beyond in Section 4.

Question 2. How many circles of curvature with few prime factors are there in a given ACP?

In studying (primitive) integer ACPs, it is interesting to consider which primes appear as curvatures of circles in a given packing. We discuss this question in Section 3. In [46] Sarnak shows that there are infinitely many circles of prime curvature and infinitely many pairs of tangent circles both of prime curvature in any given packing P. We summarize his results in the following theorem.

Theorem 1.6 (Sarnak [46]). *Let $\mathcal{P}$ denote the orbit of Descartes quadruples corresponding to a primitive integer Apollonian circle packing P, and let*

$$C = \{\mathbf{x} \in \mathbb{C}^4 \mid Q(\mathbf{x}) = 0\} \tag{1.2}$$

denote the cone of solutions to the Descartes equation in (1.1). *Fix two integers $1 \leq i, j \leq 4$ and suppose that for every $\mathbf{x} = (x_1, x_2, x_3, x_4)^t \in \mathcal{P}$ we have that x_i and x_j are odd.*

(i) *Let $\tilde{\pi}_P(X)$ denote the number of primes $< X$ that are curvatures of circles in P. Then*

$$\tilde{\pi}_P(X) > \frac{cX}{(\log X)^{3/2}}$$

for large X, where c is a constant depending on P.

(ii) *The set of points* $\{\mathbf{x} \in \mathcal{P} \mid x_i, x_j \text{ are prime}\}$ *is Zariski-dense in* C.
(iii) *There exist arbitrarily long chains of tangent circles in* P *such that every circle in the chain has prime curvature.*

In addition, in [32] Kontorovich and Oh establish upper bounds for the number of circles of prime curvature less than X in a packing P as well as the number of pairs of circles both of prime curvature less than X. These bounds depend on the number of circles of curvature less than T in the packing in question, which was first considered by Boyd in [14]. The notation $y \ll z$ below is taken to mean that there is some constant $c > 0$ such that $y \leq cz$ and the notation $\gg$ is interpreted analogously.

Theorem 1.7 (Kontorovich and Oh [32])**.** *Given a primitive integer Apollonian circle packing* P*, let* $N_P(X)$ *denote the number of circles of curvature less than* X *in* P*, let* $\pi_P(X)$ *denote the number of circles of prime curvature less than* X *in* P*, and let* $\pi_P^2(X)$ *denote the number of pairs of tangent circles both of prime curvature less than* X *in* P*. Then there is a constant* c *depending on* P *such that*

(i) $N_P(X) \sim c \cdot X^\delta$,
(ii) $\pi_P(X) \ll \frac{N_P(X)}{\log X}$,
(iii) $\pi_P^2(X) \ll \frac{N_P(X)}{(\log X)^2}$,

where $\delta = 1.30568\cdots$ *and the implied constants depend on the packing* P.

The constant δ above is in fact the Hausdorff dimension of the residual set of a packing P (see [27] for a discussion of this), which is the same for every Apollonian circle packing (see [39] where this was first noted) and has been computed to five decimals by McMullen in [38]. We should mention that part (i) of the theorem above applies to non-integer Apollonian packings as well as integer packings, and that Oh and Shah specify the constant c in [42], while recent work of Lee and Oh in [34] and independently of Vinogradov in [50] gives a formula for $N_P(X)$ together with an error term. The proof of parts (ii) and (iii) of Theorem 1.7 relies on the recently developed affine sieve in [10], which we elaborate on in Section 3. Note that the upper bounds for $\pi_P(x)$ and $\pi_P^2(X)$ above are of the correct order of magnitude.

In [22] the results of [21] are paired with the affine sieve to give a heuristic for precise asymptotics for $\pi_P(X)$ and $\pi_P^2(X)$. In [20] there is a similar heuristic for asymptotics for $\pi_{\text{gen}}^P(T)$, the number of circles of prime curvature that are born at generation T, and we discuss both of these heuristics in Section 3. The rather different question of counting primes that come up as curvatures of circles in a given ACP (that is, counting circles of prime curvature *without* multiplicity) has also been considered in [9] and [7]. In fact, we should mention that an immediate consequence of results in [7] and [13] is that, given a packing P, the primes that do not come up as curvatures in P make up a zero-density subset of all primes.

Another problem we address in Section 3 is that of determining the saturation number $r_0(f, \mathcal{P})$, where $\mathcal{P}$ denotes the set of Descartes quadruples $\mathbf{x} = (x_1, x_2, x_3, x_4)^t$ in a packing P and $f(\mathbf{x})$ is an integer valued polynomial on $\mathcal{P}$. In this notation the *saturation number* is defined to be the smallest positive integer r_0 such that the set of points

$$\{\mathbf{x} \in \mathcal{P} \mid f(\mathbf{x}) \text{ has at most } r_0 \text{ prime factors}\}$$

is Zariski-dense in the cone C in (1.2). Part (ii) of Theorem 1.6 states that $r_0 = 2$ if $f(\mathbf{x}) = x_i x_j$. In Section 3 we consider the saturation number in the case of

$$f(\mathbf{x}) = x_1 x_2 x_3 x_4/12,$$

which is equivalent to finding Descartes quadruples all of whose curvatures have few prime factors and show that $r_0 \leq 28$ in this case (the 12 above has to do with the fact that $12|x_1x_2x_3x_4$ for all $\mathbf{x} \in \mathcal{P}$ for any packing $\mathcal{P}$). As we discuss in Section 3, it is conjectured that $r_0 = 4$ in this case.

Question 3. Do the integers that come up as curvatures in a given ACP make up a positive fraction of $\mathbb{N}$?

In counting the number of integers represented in a given ACP, Graham et al. appeal to the existence of unipotent elements in A in [27] to establish the following bounds.

Theorem 1.8 (Graham, Lagarias, Mallows, Wilks, and Yan [27])**.** *Let P be an integer Apollonian packing, and let $\kappa(P, X) := |\{a \in \mathbb{N} \mid a < X,\ a$ is a curvature of a circle in $P\}|$. Then*

$$\kappa(P, X) \gg \sqrt{X}.$$

Graham et.al. suggest in [27] that the lower bound above can be improved. In fact, they conjecture that the answer to Question 3 is "yes" and that much more is true.

We note here that this question is different from the one addressed in part (i) of Theorem 1.7. The latter involves counting curvatures appearing in a packing with multiplicity, rather than counting every integer that comes up exactly once, as is done in [8] and summarized in Section 4 of this article.

A more fruitful method for this problem is to consider arithmetic Fuchsian subgroups of the Apollonian group A. In [46] Sarnak uses these subgroups to prove the following bound towards Graham et al.'s positive density conjecture.

Theorem 1.9 (Sarnak [46])**.** *Let $\kappa(P, X)$ be as above. Then*

$$\kappa(P, X) \gg \frac{X}{\sqrt{\log X}}.$$

Sarnak's method was further improved to yield a bound of

$$\kappa(P, X) \gg \frac{X}{(\log X)^{\epsilon}},$$

where $\epsilon = 0.153\cdots$ in a preprint [19]. In [8], this Fuchsian subgroup method was enhanced in a number of ways to settle Question 3 and to prove Theorem 4.2 below, that

$$\kappa(P, X) \gg X,$$

where the implied constant depends on the packing P. Recently, a further refinement of this analysis coupled with new techniques, introducing the circle method for thin orbits ([12], [13]) as well as the congruence analysis in [21], has given asymptotics for $\kappa(P, X)$ as $X \to \infty$ (see Theorem 4.3 and the discussion in Section 4).

All of these questions can be asked in the context of integer orbits of more general subgroups of $\mathrm{GL}_n(\mathbb{Z})$, and in many cases these questions can be handled precisely as they are for the Apollonian group. However, the Apollonian group is particularly attractive as it is so far the only one we have seen to arise as naturally as it does. In

this sense it is often regarded as the quintessential thin group. On the other hand, it also appears that the Apollonian group is not a typical thin group in many ways (for example, it has many unipotent and arithmetic subgroups, it is geometrically finite, its Hausdorff dimension is > 1, etc.), and this is one reason that so much progress has been made in understanding its arithmetic.

1.1. **The Apollonian group.** We mentioned above that the arithmetic of the set of curvatures of circles in a given integer ACP is best studied with the help of the Apollonian group, since any ACP can be realized as some orbit of this group acting on the root quadruple of the packing. In this section we explain how this group is derived and what role it plays in our study of Apollonian packings. Recall from Theorem 1.2 that if a, b, c, and d are curvatures of four mutually tangent circles, then

$$Q(a,b,c,d) = 2(a^2+b^2+c^2+d^2) - (a+b+c+d)^2 = 0.$$

If we fix three of the curvatures (say b, c, d) above, we may solve the above equation for two solutions $a = a_+, a_-$ with

$$a_+ + a_- = 2(b+c+d). \tag{1.3}$$

Geometrically, this amounts to finding the two circles (see Theorem 1.1) C_{a_+} and C_{a_-} of curvatures a_+ and a_-, respectively, which are tangent to all three circles of curvature b, c, and d. Thus if there is a Descartes quadruple a_+, b, c, d in a given ACP, then another Descartes quadruple in the packing is $-a_+ + 2b + 2c + 2d, b, c, d$.

Evidently, it is very natural to consider the curvatures of quadruples of mutually tangent circles (Descartes quadruples) rather than curvatures of individual circles. In fact, we lose no information about the set of curvatures of circles in a given packing by studying instead the set of Descartes quadruples in the packing, since every circle in the packing is a member of a Descartes quadruple. Moreover, the set of Descartes quadruples encodes geometric information (the tangencies in the packing) that is not detectable in the set of curvatures of circles alone. Therefore, given an Apollonian packing, we associate to it a set of Descartes quadruples and study this set.

Returning to the process giving (1.3) above, we note that we could just as well have fixed any other triple from (a, b, c, d) and solved for the fourth. Geometrically, this corresponds to choosing a triangular interstice and filling it with a circle as in our original construction in Figure 1. Similarly, inscribing a circle in any triangular interstice corresponds to solving such a quadratic equation. We summarize this as follows: if $\mathbf{v}_P = (a, b, c, d)^t$ is a Descartes quadruple in a packing P, the collection of Descartes quadruples in P is precisely the orbit $A\mathbf{v}_P$, where A is the group generated by the four matrices

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{1.4}$$

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

This group A encodes everything about Apollonian packings and is therefore known as the *Apollonian group*. In the literature, the vector $\mathbf{v}_P$ is usually taken to be the

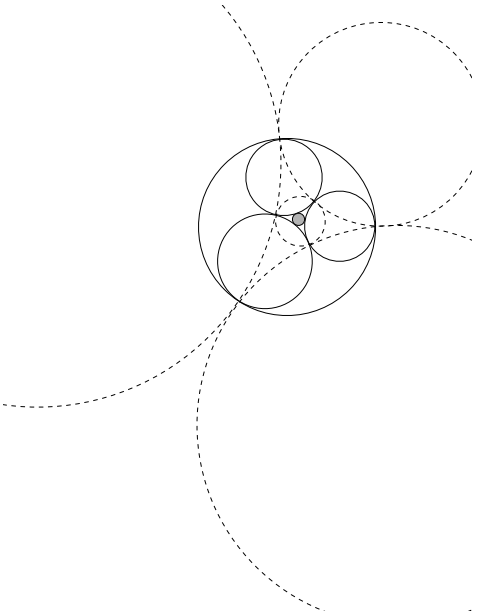


FIGURE 3. Dual circles in an Apollonian circle packing

root quadruple of the packing P, but this is not necessary. Note that $S_i^2 = I$ for $1 \leq i \leq 4$, and in fact there are no other relations among the generators of A. Perhaps the best way to see this is by considering the geometric representation of these generators, which we describe next.

Note that to any triple of mutually tangent circles (C_1, C_2, C_3) there is a unique *dual circle* or *dual line* $\mathcal{D}_{123}$ which passes through the tangency points of the three. Four such dual circles are drawn in dotted lines for the circle packing in Figure 3. Now, if (C_1, C_2, C_3, C_4) are mutually tangent circles in a packing, the generators S_1, S_2, S_3, S_4 of A then transform (C_1, C_2, C_3, C_4) via inversions in $\mathcal{D}_{234}, \mathcal{D}_{134}, \mathcal{D}_{124}, \mathcal{D}_{123}$, respectively. In Figure 3, the shaded circle on the inside is the image of the outside circle under inversion in the smallest of the dual circles, while the other three circles in the quadruple are fixed by this inversion. In fact, any generator S_i acting in this way on a quadruple of mutually tangent circles in the packing fixes three of the circles and maps the ith circle to the one other circle tangent to the fixed three.

Furthermore, since the Descartes form Q is of signature $(3, 1)$, the group A is a subgroup of $\mathrm{O}_{\mathbb{R}}(3, 1)$, the isometry group of hyperbolic 3-space

$$\mathbb{H}^3 = \{(x, y, z) \in \mathbb{R}^3 \mid z > 0\},$$

where the metric is given by $\frac{dx^2+dy^2+dz^2}{z^2}$ and the boundary of the space is $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$. Thus the Apollonian group A acts on this space in a natural way, and in fact it is a subgroup of the *Vinberg group* W_Q, the subgroup of $\mathrm{O}_Q(\mathbb{Z})$ generated by reflections in hyperplanes in $\mathbb{H}^3$. To see this, we first embed an Apollonian packing into $\mathbb{C}$ and note that the geometric action of A on the circles of the packing as described above extends to an action on $\mathbb{C}$. This action on the plane is then easily extended to an action on $\mathbb{H}^3$: the generators of A act on $\mathbb{H}^3$ as reflections

through the hemispheres lying above the dual circles of the packing. A fundamental domain for this action is the intersection of the exteriors of the hemispheres lying above $\mathcal{D}_{234}, \mathcal{D}_{134}, \mathcal{D}_{124}, \mathcal{D}_{123}$, the dual circles corresponding to the root quadruple of the packing. This fundamental domain has infinite volume with respect to the hyperbolic volume form which, as we mentioned before, renders the theory of automorphic forms inapplicable to counting in the orbit of A.

Now that we have introduced the Apollonian group, we list some notable properties of A and the bigger group W_Q:

1) A is an infinite-index subgroup of the orthogonal group $O_Q(\mathbb{Z})$ fixing Q;
2) A is Zariski-dense in $\mathrm{O}_Q(\mathbb{C})$;
3) W_Q is of finite index in $\mathrm{O}_Q(\mathbb{Z})$.

Property 1 was first proven in [27]. Properties 1 and 2 together imply that the Apollonian group is thin (for a proof of Property 2, see [20], Lemma 2.1). Property 3 is essentially a theorem in [17] after one passes to the spin double cover of $\mathrm{SO}_Q(\mathbb{R})$ (we discuss this passage in the following section). The fact that A is Zariski-dense in $\mathrm{O}_Q(\mathbb{C})$ can be interpreted as saying that A is large in an algebro-geometric sense: it simply means that any polynomial with complex coefficients in variables x_{ij}, $1 \leq i, j \leq 4$, that vanishes on A vanishes on $\mathrm{O}_Q(\mathbb{C})$ as well.

The fact that A is Zariski-dense in $\mathrm{O}_Q(\mathbb{C})$ is precisely what makes its integer orbits suitable for the affine sieve described in [10]. It is also for this reason that, as we will see, its orbits are quite rich in some sense, even though A is thin in the sense of Definition 1.4. The ability to sieve in ACPs allows us to tackle quite a few of the questions outlined above. To illustrate how one does this, we begin the next section with a short summary of how sieving works in a more classical situation. The ingredients that go into this classical sieve have natural analogs in the higher dimensional group-orbit setting: the basic requirements are

(i) a "Chinese Remainder Theorem" for the orbits of the group;
(ii) an expansion property for the Cayley graphs associated to finite quotients of the group.

We discuss requirement (i) and how to show it is satisfied in the next section. In Section 3 we explain the role of requirement (ii) in the sieve and discuss how it can be applied together with (i) in two different sieves in the ACP example: one application is to count points all of whose coordinates have few prime factors in various orbits of the Apollonian group; and the other is to count circles of prime curvature. We note that Section 4, concerning the density of integers that appear as curvatures in a given ACP, is of a somewhat different flavor and does not appeal to the affine sieve at all. One reason for this is that this problem concerns the number of integers $< X$ that occur as curvatures in an ACP *without* multiplicity while the affine sieve is a counting tool in the *orbit* of A and counts with multiplicity. The results in all of these sections, however, all point to one general rule that the curvatures in an integer ACP are structured much like all of $\mathbb{N}$ even though they come from an orbit of a thin group. Finally, we say a few words on future directions in the study of general thin groups in Section 5.

2. Congruence obstructions in Apollonian packings

In this section we consider Question 1 of the Introduction regarding congruence obstructions for integers appearing as curvatures in a given ACP. Studying these

congruence obstructions has many benefits: one concrete benefit is the ability to count primes in Apollonian packings as discussed in Question 2 of the Introduction. A natural way to do this is by sieving in orbits of the Apollonian group A. To give an idea of what this entails and how congruence obstructions come in, we next review the setup of a more classical Brun sieve (which was introduced by Viggo Brun in 1915). For a good brief overview of sieves both in the classical and in the group orbit setting, see [33].

The Brun sieve. The Brun sieve is a tool that can be used to tackle various classical questions in number theory: it can give meaningful upper and lower bounds, depending on $N \in \mathbb{N}$, on the number of values less than N of a given integer polynomial that have at most k prime factors, for k fixed and sufficiently large. For example, Chen used this in [15] to show that there are infinitely many values of the polynomial $x(x+2)$ that have at most three prime factors: if one could replace the 3 with 2, the twin prime conjecture would be proven.

To introduce this sieve, we focus on the following general problem. Let $f(x)$ be a polynomial with integer coefficients such that the gcd of the coefficients is 1, and suppose we wish to count the number of primes (with multiplicity) that can be written as $f(b)$ for some positive integer $b < N$ where $N \in \mathbb{N}$ is fixed. Brun's sieve can give a good estimate of this count in terms of N and the number of solutions to the equation $f(x) \equiv 0 \pmod{d}$ for various square-free integers d; see (2.3) for a more precise statement of this. To derive this answer, consider the sequence $\{a_n\}_{n\geq 1}$, where

$$a_n = |\{b \in \mathbb{N} \mid b < N, f(b) = n\}|,$$

and let

$$X = \sum_{n\geq 1} a_n.$$

The basic idea now is reminiscent of the sieve of Eratosthenes: We consider all values of $f(b)$ where $b < N$ and strike out all multiples of 2 that are greater than 2. We then strike out all multiples of 3 in a similar way, but in doing so we have now crossed out multiples of 6 twice. Thus to count how many integers have survived the sieve so far, we subtract from X the number of values of f that are multiples of 2 or 3, and then add back in the number of values of f that are multiples of 6. We keep subtracting off multiples of primes and adding back in what we subtract more than once. One can express this count in a neat formula in terms of the number of values of f that are multiples of d for various square-free positive integers d (see (2.3)). To this end we introduce a bit of notation. For some parameter z depending on N, usually a small power of N, let

$$P_z = \prod_{\substack{p \text{ prime} \\ p<z}} p \quad \text{and} \quad S(z) = \sum_{\substack{n>0 \\ (n,P_z)=1}} a_n.$$

Note that $S(z)$ counts precisely those integers that survive the process above when one strikes out multiples of primes less than z. Furthermore, if z is large enough, $S(z)$ is a fairly good estimate of how many primes there are among $f(b)$ where $b < N$, since it is essentially the number of values of f that have all prime factors $> z$. We note here that usually a sieve cannot be used to pick out primes only: outside of very few examples, the best one can do is to pick up integers with at most two prime factors, but this tends to be a good estimate for the number of primes

alone. So our mission to count prime values of f can be translated into evaluating the sum $S(z)$ above. Let

$$S_d = \sum_{\substack{n>0 \\ d|n}} a_n.$$

Then we may express $S(z)$ in terms of S_d as

$$S(z) = \sum_{d|P_z} S_d \cdot \mu(d), \tag{2.1}$$

where the Möbius function $\mu(d) = 1$ if d is square-free and has an even number of prime factors, $\mu(d) = -1$ if d is square-free and has an odd number of prime factors, and $\mu(d) = 0$ otherwise. Indeed, (2.1) is just a concise way of describing the inclusion/exclusion strategy above. Our aim is now to compute the values S_d appearing in the second sum in (2.1). Note that

$$S_d = \sum_{\substack{0<b<N \\ f(b)\equiv 0 \ (d)}} 1,$$

and that the condition $f(b) \equiv 0 \bmod d$ above depends only on the value of b mod d. Therefore, we may write

$$S_d = \sum_{\substack{m\in\mathbb{Z}/d\mathbb{Z} \\ f(m)\equiv 0 \ (d)}} \sum_{\substack{b<N \\ b\equiv m \ (d)}} 1.$$

Finally, this boils down to evaluating

$$\omega(d) = |\{m \in \mathbb{Z}/d\mathbb{Z} \mid f(m) \equiv 0 \ (\mathrm{mod}\ d)\}|.$$

Specifically, we get that

$$S_d = \frac{\omega(d)}{d} X + O(1). \tag{2.2}$$

Here $\omega(d)$ is multiplicative by the Chinese Remainder Theorem (this is crucial in evaluating $\omega(d)$ for arbitrary square-free integers d), and the remainder term is small in the sense that even when one sums $S_d \cdot \mu(d)$ over all d as we do in (2.1), we get

$$S(z) = \sum_{d|P_z} S_d \cdot \mu(d) = X \cdot \sum_{d|P_z} \frac{\omega(d)}{d} + R, \tag{2.3}$$

where R is small compared to the main term. This gives us an upper bound on the number of primes we were interested in counting above. The main moral of this story is that we need a Chinese Remainder Theorem to sieve, and we need to control the remainder term R when we proceed as above with z large.

Sieving in orbits. Passing from this classical example to a more general setting, suppose we would like to sieve for vectors with prime first coordinate in an orbit of a subgroup of $\mathrm{GL}_n(\mathbb{Z})$. The affine sieve which is developed in [10] and [43] is a machine that allows us to count such vectors in fairly general situations. While there are various subtleties in this group orbit counting that are not present in the classical situation above, the general idea of this affine sieve is very similar. For example, in order to be able to sieve in an integer orbit $\Gamma\mathbf{v} \subset \mathbb{Z}^n$, where $\Gamma \leq \mathrm{GL}_n(\mathbb{Z})$, one needs to know the exact structure of the orbit modulo square-free

integers d, just as one needs to understand the values of the polynomial f mod d in the classical example above. To this end, let $\Gamma_d\mathbf{v}$ denote the projection of $\Gamma\mathbf{v}$ in $(\mathbb{Z}/d\mathbb{Z})^n$. If one sieves for points $\mathbf{w}$ with prime first coordinate w_1 in $\Gamma\mathbf{v}$, one needs to evaluate the ratio

$$\beta(d) = \frac{|\{\mathbf{w} \in \Gamma_d\mathbf{v} \mid w_1 \equiv 0 \pmod{d}\}|}{|\{\mathbf{w} \in \Gamma_d\mathbf{v}\}|} \tag{2.4}$$

for every square-free integer $d > 1$. This ratio is the analog of $\omega(d)/d$ in (2.2) and it plays an identical role in counting prime points in the group-orbit setting as $\omega(d)/d$ plays above. The rest of this section will be concerned with understanding the analog of the Chinese Remainder Theorem in this general setting to guarantee that the ratios in (2.4) are multiplicative in d. Along the way, we will pave the road to evaluating these $\beta(d)$ in the Apollonian case.

A very general result that is a starting point to such Chinese Remainder Theorems is the strong approximation Theorem 10.1 of Weisfeiler in [51]. In the simple case of subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$, this theorem says that if Γ is Zariski-dense in SL_2, then the reduction of Γ modulo primes p is onto $\mathrm{SL}_2(\mathbb{F}_p)$ for all but finitely many bad primes p.

In the context of integer ACPs, the relevant version of Weisfeiler's theorem says that if Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}])$ that is Zariski-dense in $\mathrm{SL}_2(\mathbb{C})$ and such that traces of elements of Γ generate the field $\mathbb{Q}(\sqrt{-1})$, then there is a finite set of prime ideals $\mathcal{B}$ in $\mathbb{Z}[\sqrt{-1}]$ such that Γ projects onto $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}]/\mathfrak{p})$ for $\mathfrak{p} \notin \mathcal{B}$. We will see how the Apollonian group relates to $\mathrm{SL}_2(\mathbb{C})$ via the *spin homomorphism* later in this section. In order to execute the sieve, however, we need to explicitly determine $\mathcal{B}$. Once we do this, we will be able to evaluate $\beta(p)$ for p prime fairly easily. We then want to show that for arbitrary square-free d the ratio $\beta(d)$ is the product over $p|d$ of $\beta(p)$'s where p is prime. All this is done by specifying the orbits of A mod d. To this end we introduce the following notation where Q denotes the Descartes quadratic form from before. For any prime p, let

$$C_p = \{\mathbf{v} \in (\mathbb{Z}/p\mathbb{Z})^4 \mid \mathbf{v} \not\equiv \mathbf{0} \pmod{p}, Q(\mathbf{v}) \equiv 0 \pmod{p}\}.$$

If $p > 2$, for any integer $r > 1$, let

$$C_{p^r} = \{\mathbf{v} \in (\mathbb{Z}/p^r\mathbb{Z})^4 \mid \mathbf{v} \not\equiv \mathbf{0} \pmod{p^{r-1}}, Q(\mathbf{v}) \equiv 0 \pmod{p^r}\}.$$

Finally, for any integer $r > 1$, let

$$C_{2^r} = \{\mathbf{v} \in (\mathbb{Z}/2^r\mathbb{Z})^4 \mid \mathbf{v} \not\equiv \mathbf{0} \ (2^{r-1}), Q(\mathbf{v}) \equiv 0 \ (2^r), \\ \exists \mathbf{w} \equiv \mathbf{v} \ (2^r) \text{ s.t. } Q(\mathbf{w}) \equiv 0 \ (2^{r+1})\}.$$

The reason that we define C_{2^r} separately is that it is not true in this case that every solution to $Q(\mathbf{v}) \equiv \mathbf{0} \pmod{2^r}$ lifts to some solution of the equation modulo 2^{r+1}—only half of the solutions modulo 2^r lift to solutions modulo 2^{r+1}. With this notation, we have the following description of orbits of A mod d.

Theorem 2.1 (Fuchs [21])**.** *Let $\mathcal{P}$ be an orbit of A acting on the root quadruple $\mathbf{v}_P$ of a primitive packing P, and let $\mathcal{P}_d$ be the reduction of this orbit modulo an integer $d > 1$. Let C_{p^r} be defined as above. Write $d = d_1d_2$ with $(d_2, 6) = 1$ and $d_1 = 2^n3^m$ where $n, m \geq 0$.*

(i) *The canonical projection $\mathcal{P}_d \longrightarrow \mathcal{P}_{d_1} \times \mathcal{P}_{d_2}$ is surjective.*
(ii) *The canonical projection $\mathcal{P}_{d_2} \longrightarrow \prod_{p^r||d_2} \mathcal{P}_{p^r}$ is surjective and $\mathcal{P}_{p^r} = C_{p^r}$.*

(iii) *The canonical projection* $\mathcal{P}_{d_1} \longrightarrow \mathcal{P}_{2^n} \times \mathcal{P}_{3^m}$ *is surjective.*
(iv) *If* $n \geq 4$, *let* $\pi : C_{2^n} \to C_8$ *be the canonical projection. Then* $\mathcal{P}_{2^n} = \pi^{-1}(\mathcal{P}_8)$.
(v) *If* $m \geq 2$, *let* $\phi : C_{3^m} \to C_3$ *be the canonical projection. Then* $\mathcal{P}_{3^m} = \phi^{-1}(\mathcal{P}_3)$.

To paraphrase Theorem 2.1, in order to determine the reduction of any given primitive orbit of A modulo any positive integer $d > 1$, one needs only to determine the reduction modulo 24. Once this is done, the rest of the information about this reduction comes from knowing the solutions to $Q(x) \equiv 0$ modulo various primes p. The fact that the only local obstructions for integers occurring as curvatures in an integer Apollonian packing are modulo 24 was first conjectured in [27], where the authors conducted various numerical experiments to analyze these obstructions.

We note here that Theorem 2.1 is more than one needs for sieving, as it specifies the reductions of orbits $\mathcal{P}$ of A modulo *any* integer d as opposed to just square-free integers, which is all that the sieve requires. However, including integers that are not square-free is natural in specifying the arithmetic structure of integer ACPs and is key to the local to global conjecture discussed in Section 4.

We now give a sketch of the proof of Theorem 2.1 in the case that d above is square-free, before returning to the issue of counting circles whose curvature have few prime factors in the next section. The generalization to the case where d is an arbitrary integer requires some extra work, which we outline briefly at the end of this section. In both cases the idea is to specify the structure of the Apollonian group mod d in order to derive the corresponding structure of the group's orbits. We note that the strategy of this proof applies identically to any Zariski-dense subgroup of $\mathrm{O}_f(\mathbb{Z})$ where f is a signature $(3,1)$ quadratic form in four variables.

Detailed aspects of the proof are included to illustrate methods to obtain results similar to Theorem 2.1 for various groups beyond the Apollonian group. If desired, however, it is possible to proceed immediately to the application of this theorem to counting primes in Section 3, since the exposition in the remainder of the article is independent of the proof.

A first observation is that it is difficult to arrive at Theorem 2.1 by working with the Apollonian group A directly since it is a subgroup of the orthogonal group $\mathrm{O}_Q(\mathbb{Z})$ where strong approximation does not hold: the reduction even of $\mathrm{O}_Q(\mathbb{Z})$ itself (let alone A) modulo p is not onto $\mathrm{O}_Q(\mathbb{Z}/p\mathbb{Z})$ if $p \equiv 3 \bmod 4$. It is therefore difficult to say anything about the projection of A in $\mathrm{O}_Q(\mathbb{Z}/p\mathbb{Z})$ by working in the orthogonal group itself, and consequently it is difficult to quantify the ratios in (2.4) in this way. One can get around this difficulty by working in the spin double cover of the arithmetic group SO_Q where strong approximation does hold. To pass to the spin double cover, let

$$\tilde{Q}(x_1, x_2, x_3, x_4) := x_1^2 - x_2^2 - x_3^2 - x_4^2.$$

In [21] it is shown that $\mathrm{O}_Q(\mathbb{Z}[\frac{1}{2}]) \cong \mathrm{O}_{\tilde{Q}}(\mathbb{Z}[\frac{1}{2}])$ and that there is an isomorphism

$$A' \xrightarrow{s} A \tag{2.5}$$

between A and a subgroup A' of $\mathrm{O}_{\tilde{Q}}(\mathbb{Z})$. With this notation, we consider the preimage Γ of $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ under the 2 to 1 *spin homomorphism* (see [17])

$$\rho : \mathrm{SL}_2(\mathbb{C}) \to \mathrm{SO}_{\tilde{Q}}(\mathbb{R}). \tag{2.6}$$

One can show that $\Gamma \subset \mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}])$, the traces of elements of Γ generate $\mathbb{Q}(\sqrt{-1})$, and Γ is a Zariski-dense subgroup of $\mathrm{SL}_2(\mathbb{C})$ where strong approximation holds in the sense of Weisfeiler's theorem outlined above. Furthermore, since

$$s(\rho(\Gamma)) = A \cap \mathrm{SO}_Q(\mathbb{Z}),$$

and since we have explicit formulas for s and ρ, by considering Γ we simultaneously consider the Apollonian group A. Note that this method of pulling back to the spin double cover is a standard technique for sieving in orbits of subgroups of $\mathrm{O}_f(\mathbb{Z})$ where f is some quadratic form, as explained in [10].

With this in mind, the first step towards proving Theorem 2.1 is to consider the reduction of Γ modulo ideals (d) in $\mathbb{Z}[\sqrt{-1}]$ in order to gain information about reductions of A' and A. We note, however, that to analyze A modulo even integers it is not enough to consider the reduction of Γ modulo ideals (d) where d is even, since the isomorphism in (2.5) is defined over $\mathbb{Z}[1/2]$. This is a technicality that can easily be dealt with separately, and we will suppress its details here for the sake of exposition (for the details, see [21]).

To analyze the reductions of Γ, the explicit formula for ρ given in [17] is combined with the fact that $A \cap \mathrm{SO}_Q(\mathbb{Z})$ is generated by S_1S_2, S_2S_3, and S_2S_4 to produce exactly the generators and relations of Γ. Here the S_i's denote the generators of A as before. We describe this presentation of Γ in the following lemma.

Lemma 2.2 (Fuchs [21])**.** *Let Γ be as before. It is generated by $\pm\gamma_1, \pm\gamma_2, \pm\gamma_3$, where γ_i are as below and there are no relations between γ_1, γ_2, and γ_3 :*

$$\gamma_1 = \begin{pmatrix} 2 & -i \\ -i & 0 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} -2-2i & -4-3i \\ i & 2i \end{pmatrix}, \quad \gamma_3 = \begin{pmatrix} 1 & -4i \\ 0 & 1 \end{pmatrix}. \tag{2.7}$$

Given this presentation of Γ, finding the set $\mathcal{B}$ of bad primes turns out to be a problem in elementary group theory: the main tool in accomplishing this is a classification due to L. E. Dickson (Theorem 8.27 in [31]) of subgroups of PSL_2 over finite fields. In the case that the finite field is $\mathbb{F}_p$ for p prime, it is shown in [16] that most of the groups in this classification are *metabelian*, meaning their commutator subgroups are Abelian. In light of this, we state the following version of Dickson's classification:

Theorem 2.3 (Dickson, 1901)**.** *Let $p \geq 5$ be prime. A proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$ is either metabelian or one of A_4, S_4, or A_5.*

Using Dickson's classification, one can show that the reduction mod $\mathfrak{p}$ of our group Γ must be $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}]/\mathfrak{p})$ for all but finitely many $\mathfrak{p}$ as well as specify these finitely many $\mathfrak{p}$. The strategy for this is to determine a *girth bound* for every $\Gamma/\mathfrak{p}$ and then to show that for all but finitely many $\mathfrak{p} \in \mathbb{Z}[\sqrt{-1}]$ the proper subgroups in Dickson's theorem would violate this bound, meaning that $\Gamma/\mathfrak{p}$ cannot be a proper subgroup of SL_2. We note here that one reason that it is feasible to carry this out for Γ is that the classification of subgroups of SL_2 over finite fields is particularly simple. In the case of a higher rank group, the relevant classification would be much more complex, and consequently the corresponding result on reductions of the group modulo d would be much harder to prove. In the case of Γ, one has the following.

Proposition 2.4 (Fuchs [21])**.** *Let Γ be as before, let $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$, let $\mathfrak{p}$ denote a prime ideal in $\mathcal{O}$, and let (d) denote an ideal generated by $d \in \mathcal{O}$. Denote by $\mathcal{B}$*

the set of prime ideals in $\mathcal{O}$ containing (6). *Let $d > 1$ be a square-free integer such that $d = d_1 c$, where $c|6$ and $\gcd(d_1, 6) = 1$. We have that the product of canonical projections*

$$\pi : \Gamma \longrightarrow \Gamma_c \times \prod_{\mathfrak{p} \supset (d_1)} \mathrm{SL}_2(\mathcal{O}/\mathfrak{p}), \tag{2.8}$$

where Γ_c is the image of Γ in $\mathrm{SL}_2(\mathcal{O}/(c))$, is surjective. In particular the reduction of Γ modulo any prime $\mathfrak{p} \notin \mathcal{B}$ is onto $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$.

Theorem 2.1 in the case of d square-free follows quickly from this proposition. The main ingredient in the proof is Theorem 2.3 combined with the girth bound mentioned above, as well as an application of Goursat's lemma for the multiplicative aspect. Our method of proving Proposition 2.4 is quite general and gives an effective version of Weisfeiler's theorem for subgroups of $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}])$ given in terms of generators. In this particular case, one can also give a shorter argument using results of Hall in [28] since one of Γ's generators (γ_3) is a pseudo-reflection. Specifically, Theorem 3.1 in [28] implies that the only potentially bad primes in this case are 2 and 3. Next we outline the more general proof which does not require any extra conditions on the generators.

We first show that $\Gamma/\mathfrak{p}$ surjects onto $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ for prime ideals $\mathfrak{p} \not\supset (6)$. There are three cases to consider:

(1) $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ where $p \equiv 1 \pmod 4$—here p splits in $\mathcal{O}$, and the reduction of Γ modulo (p) is mapped to $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$;
(2) $\mathfrak{p} = (p)$ where $p \equiv 3 \pmod 4$—here p does not split in $\mathcal{O}$, and the reduction of Γ modulo (p) is mapped to $\mathrm{SL}_2(\mathbb{F}_{p^2})$;
(3) $\mathfrak{p}^2 = (2)$.

We sketch the proof that for $\mathfrak{p}$ as in case (1) we have $\Gamma/\mathfrak{p} = \mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ for all $\mathfrak{p}$. The proof that $\Gamma/\mathfrak{p} = \mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ for all $\mathfrak{p} \neq (3)$ as in case (2) is essentially identical, and case (3) is quickly taken care of by hand (it is not hard to see that $\Gamma/(2)$ is not all of $\mathrm{SL}_2(\mathcal{O}/(2))$ for example).

Let $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ where p denotes a prime congruent to 1 mod 4 as in case (1). One can check that the center Z of $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}])$ is contained in Γ. Denoting $\Gamma' = \Gamma/Z \subseteq \mathrm{PSL}_2(\mathbb{C})$, our strategy is now to determine when the reduction $\Gamma'_{\mathfrak{p}}$ of Γ' modulo $\mathfrak{p}$ is all of $\mathrm{PSL}_2(\mathbb{F}_p) \times \mathrm{PSL}_2(\mathbb{F}_p)$ as this can be shown to imply that the reduction of Γ mod $\mathfrak{p}$ is all of $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$. In fact, it is enough in this case to check that the projection of Γ' in the first factor $\mathrm{PSL}_2(\mathbb{F}_p)$ is surjective, as we do next.

By Theorem 2.3, if the image of $\Gamma'_{\mathfrak{p}}$ in the first factor is a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$, it is either metabelian or is one of the groups A_4, S_4, or A_5. To rule out these proper subgroups, we appeal to a result of Margulis in [37] on girth bounds, which we define next. The method of using this bound to rule out proper subgroups as candidates for $\Gamma'_{\mathfrak{p}}$ is a useful tool that has previously been featured in [16] and [23], for example. From now on we denote the image of $\Gamma'_{\mathfrak{p}}$ in the first factor $\mathrm{PSL}_2(\mathbb{F}_p)$ by $\Gamma'_{\mathfrak{p},1}$.

For $\gamma \in \Gamma'$ let $\overline{\gamma}$ denote the image of γ in $\Gamma'_{\mathfrak{p},1}$, and let

$$S_{\mathfrak{p}} = \{\overline{\gamma}_1, \overline{\gamma}_1^{-1}, \overline{\gamma}_2, \overline{\gamma}_2^{-1}, \overline{\gamma}_3, \overline{\gamma}_3^{-1}\},$$

where γ_i are, as in (2.7), a set of generators of $\Gamma'_{\mathfrak{p},1}$. Consider the Cayley graph $C(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}})$, where the vertices correspond to elements of $\Gamma'_{\mathfrak{p},1}$ and two vertices v, w are connected by an edge if and only if $vw^{-1} \in S_{\mathfrak{p}}$. The *girth* $c(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}})$ of

$C(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}})$ is defined to be the length of the shortest cycle $(v_1, v_2, \ldots, v_k)$ with $v_k = v_1$ in $C(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}})$ where $v_{i-1} \neq v_{i+1}$ for any $1 < i < k$. From [37] we have that

$$c(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}}) \geq 2\log_\alpha(p/2) - 1, \tag{2.9}$$

where

$$\alpha := \max_{1 \leq i \leq 3}(||\gamma_i||),$$

where $||\gamma||$ is positive and

$$||\gamma||^2 = \lambda_{\max}(\gamma^*\gamma).$$

Here γ^* is the conjugate transpose of γ, and $\lambda_{\max}(\gamma^*\gamma)$ is the largest eigenvalue of $\gamma^*\gamma$. Using this, we compute that in our case

$$\alpha = \sqrt{19 + 6\sqrt{10}} = 6.1623\cdots.$$

Note that an upper bound for the girth of any Cayley graph corresponding to A_4, S_4, or A_5 is 6, since an element in any of these groups has order ≤ 6. On the other hand, the bound in (2.9) implies that

$$c(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}}) > 6 \quad \text{for } p > 1161,$$

and so $\Gamma'_{\mathfrak{p},1}$ cannot be A_4, S_4, or A_5 if $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ where $p > 1161$. We then check with the help of a computer that for $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ where $5 \leq p < 1161$ we have $\left|\Gamma'_{\mathfrak{p},1}\right| > 60$, and so $\Gamma'_{\mathfrak{p},1} \neq A_4, A_5$, or S_4.

It remains to show that $\Gamma'_{\mathfrak{p},1}$ cannot be metabelian. If it were metabelian, we would have that for any $A, B, C, D \in \Gamma'_{\mathfrak{p},1}$,

$$[[A,B],[C,D]] := (ABA^{-1}B^{-1})(CDC^{-1}D^{-1})(BAB^{-1}A^{-1})(DCD^{-1}C^{-1}) = I. \tag{2.10}$$

This would give an upper bound of 16 for $c(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}})$. However, the bound in (2.9) implies that

$$c(\Gamma'_{\mathfrak{p},1}, S_{\mathfrak{p}}) > 16 \quad \text{for } p > 2.57 \cdot 10^7,$$

and so $\Gamma'_{\mathfrak{p},1}$ cannot be metabelian in this case. We are left with a finite number of cases, which are handled with the help of a computer in [21]. Namely, one can check that taking $A = \overline{\gamma}_1, B = \overline{\gamma}_2, C = \overline{\gamma}_3$, and $D = \overline{\gamma}_1\overline{\gamma}_2\overline{\gamma}_3$ where γ_i are as in (2.7), one has

$$[[A,B],[C,D]] \neq I \tag{2.11}$$

in $\mathrm{PSL}_2(\mathbb{F}_p)$ for $5 \leq p < 2.57 \cdot 10^7$, and thus $\Gamma'_{\mathfrak{p},1}$ is not metabelian in these cases. Combined with the fact that $\Gamma'_{\mathfrak{p},1}$ is not A_4, S_4, or A_5, we have that $\Gamma'_{\mathfrak{p},1} = \mathrm{PSL}_2(\mathbb{F}_p)$ for all $\mathfrak{p}$ as in case (1). Since no proper subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ maps onto $\mathrm{PSL}_2(\mathbb{F}_p)$ (see [48] for a proof), this implies that the projection of $\Gamma_{\mathfrak{p}}$ is surjective in the first factor of $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$ as well. Again, in this case this implies that $\Gamma_{\mathfrak{p}}$ is indeed the full $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$.

After handling case (2) using very similar arguments as in case (1) for $p > 3$, we can identify $p = 2, 3$ as the bad primes as far as reduction of Γ mod (p) goes. It remains to show the surjectivity of the map π in Proposition 2.4, and this is done in [21] using Goursat's lemma together with an analysis of the composition factors of $\Gamma/(d)$.

It is then not difficult to derive the part of Theorem 2.1 concerning square-free integers $d > 1$ which is the necessary ingredient for sieving in orbits of the Apollonian group A as we do in Section 3.

Theorem 2.1, however, gives much more than the bare minimum required for sieving: it specifies in particular the structure of A modulo any integer which paints a clearer picture of which integers appear in any given ACP, as we discuss in Section 4. Thus in order to finish the proof of Theorem 2.1, one needs to determine the reduction of Γ modulo an arbitrary ideal (d). The ingredients in doing this are similar to the ingredients in determining the reduction modulo square-free ideals. First, just as we determined the reductions $\Gamma/(p)$ above, we must determine the reductions $\Gamma/(p^k)$ for arbitrary integers $k > 1$. The basic idea is to look at the sequence of canonical projections

$$\Gamma/(p) \longleftarrow \Gamma/(p^2) \longleftarrow \Gamma/(p^3) \cdots \tag{2.12}$$

for every prime p and to determine at which level in the sequence the kernels of the projections above begin to coincide with those in the sequence

$$\mathrm{SL}_2(\mathcal{O}/(p)) \xleftarrow{\pi_1} \mathrm{SL}_2(\mathcal{O}/(p^2)) \xleftarrow{\pi_2} \mathrm{SL}_2(\mathcal{O}/(p^3)) \cdots . \tag{2.13}$$

It is known that the kernels must coincide from some finite power of p onwards by Weisfeiler's theorem. The crucial observation is that as soon as the kernels do coincide (say, starting at $\Gamma/(p^k)$) and given $m \geq k$, one can simply lift from $\Gamma/(p^m)$ to $\Gamma/(p^{m+1})$ in the natural way that one lifts in the second sequence above. In other words, an element $\gamma \in \Gamma/(p^m)$ has precisely the elements

$$\{\gamma' \in \mathrm{SL}_2(\mathcal{O}/(p^{m+1})) \,|\, \pi_m(\gamma') = \gamma\}$$

lying above it.

If p is "good", meaning $p \nmid 6$, the reduction of Γ modulo (p) is onto $\mathrm{SL}_2(\mathcal{O}/(p))$, and the two sequences in (2.12) and (2.13) are identical by a slight generalization of Serre's Lemma 3 on page IV-23 in [48]. Namely, it can be shown that if $\mathfrak{q} \neq (1+i), (3)$ is a prime ideal in $\mathcal{O}$ and $\mathcal{O}_\mathfrak{q}$ denotes the completion of $\mathcal{O}$ at $\mathfrak{q}$, then a closed subgroup G of $\mathrm{SL}_2(\mathcal{O}_\mathfrak{q})$ whose projection into $\mathrm{SL}_2(\mathcal{O}_\mathfrak{q}/\mathfrak{q})$ is surjective is precisely $\mathrm{SL}_2(\mathcal{O}_\mathfrak{q})$.

On the other hand, in the case where $p = 2$ or 3, we have seen that $\Gamma/(p)$ is not all of $\mathrm{SL}_2(\mathcal{O}/(p))$ and so the sequences above are not identical for such primes. However, the kernels of the maps do begin to coincide quite quickly—starting at π_3 for $p = 2$ and at π_1 for $p = 3$—and combining this with an analog of Serre's lemma gives a complete description of Γ modulo powers of "bad" ideals. Combining this with Goursat's lemma to show that the reduction mod (d) is in some sense multiplicative gives the desired description of $\Gamma/(d)$ for arbitrary ideals (d). For more details of this proof, see [21]. Again, this strategy applies similarly to Zariski-dense subgroups of $\mathrm{O}_f(\mathbb{Z})$ where f is of signature $(3, 1)$.

3. Prime number theorems and sieving

In this section we survey how a sieve can be used to count circles of prime curvature as well as Descartes quadruples of circles all of whose curvatures have few prime factors in Apollonian packings. As we mentioned in the Introduction, there are two main ingredients in such a sieve, the first of which is a Chinese Remainder Theorem that we discussed in Section 2 (see Theorem 2.1). To elaborate on the second ingredient regarding the expansion property in the context of Apollonian packings, consider the following problem. Let P be a bounded Apollonian circle packing, and suppose we want to count the number of circles of prime curvature in P that are born at a fixed generation T. With this in mind, let a_n be the number

of circles of curvature n in P born at generation T, and denote the sequence of such a_n's by $\mathcal{A} := \{a_n\}_{n>0}$. Note that there is a finite number of circles of curvature n in any bounded packing P since all circles in the packing are contained in a circle of fixed radius r and thus $a_n \leq r^2 n^2$. Let

$$X := \sum_{n>0} a_n.$$

Analogously to the classical sieve described at the beginning of Section 2, let

$$P_z := \prod_{\substack{p \text{ prime} \\ p \leq z}} p \quad \text{and} \quad S(\mathcal{A}, P_z) := \sum_{(n, P_z)=1} a_n,$$

where z depends on T. Our goal is to estimate $S(\mathcal{A}, P_z)$ which can be viewed as an approximation to the total number of circles of prime curvature at generation T if the dependence of z on T is chosen carefully. As in the classical example at the beginning of Section 2 we will compute $S(\mathcal{A}, P_z)$ by estimating the sum in (3.1) for square-free integers $d > 1$. To evaluate these sums, we note that there is a multiplicative density function $0 \leq \beta(d) \leq 1$ such that

$$\sum_{n \equiv 0 \ (d)} a_n = \beta(d) X + R(\mathcal{A}, d), \tag{3.1}$$

where the remainder term $R(\mathcal{A}, d)$ is on average small comparing to X. Theorem 2.1 gives us a good understanding of $\beta(d)$. However to control the size of the remainders $R(\mathcal{A}, d)$ one needs to check whether the Apollonian group A satisfies certain combinatorial properties (essentially, that the Cayley graph associated to A with respect to the generators S_1, S_2, S_3, S_4 is an expander), which we discuss next.

3.1. **The affine sieve and the importance of expanders.** The requirement that $R(\mathcal{A}, d)$ be small on average turns out to be quite subtle when sieving over an orbit of a group $G \subset \mathrm{GL}_n(\mathbb{Z})$ (the Apollonian group in our case) rather than over the integers. Specifically, to carry out a sieve over $\mathbb{Z}$ one considers integers belonging to a large interval that occurs in some arithmetic progression with difference d. Over the integers, the size of the boundary of such an interval is trivially small compared to the size of the whole interval, and the same holds for arithmetic progressions within this interval. In the setting of groups, however, this is generally not true. Namely, consider all points in an orbit of an arbitrary discrete group acting on $\mathbb{Z}^n$ that lie in a large ball $B(x, r)$ of radius r centered at x which is the analog of an interval in $\mathbb{Z}$. Naively, one might propose sifting out all points on the boundaries of balls $B(x, r')$ centered at x, whose radii $r' \leq r$ are in an arithmetic progression of difference d. However, in this setting the points on the boundary may in fact be most of the points in B. In order to ensure this does not happen (equivalently, to make sure that the remainder $R(\mathcal{A}, d)$ is small), it is necessary for G to satisfy some combinatorial properties. To this end for p prime, let G_p denote the reduction of G modulo p and let $S_p = \{\alpha_1, \alpha_1^{-1}, \ldots, \alpha_k, \alpha_k^{-1}\}$ be the generators of G mod p. We associate to every such reduction G_p the Cayley graph

$$\mathcal{G}_p := \mathrm{Cay}(G_p, S_p),$$

where the vertices correspond to elements of G_p, and two vertices x and y are connected by an edge if and only if $xy^{-1} \in S_p$. If G is free on $2k$ generators

(one can always replace G with a suitable free subgroup of G as far as the affine sieve goes) we associate with G_p a $2k$-regular graph. If G is the Apollonian group, the corresponding graph is 4-regular. This association is crucial in controlling the remainder term in (3.1) in the orbit setting—namely, under certain conditions on the Cayley graphs $\mathcal{G}_p$ one can show that the remainders are small as desired.

Specifically, for any finite graph $\mathcal{G}$ with n vertices, let $V = V(\mathcal{G})$ denote the set of vertices of $\mathcal{G}$. For any subset $S \subset V$, let ∂S denote the set of edges that connect some vertex in S with a vertex in the complement of S. We define the *Cheeger constant* of the graph $\mathcal{G}$ to be

$$h(\mathcal{G}) = \min_{S \subset V, |S| \leq \frac{n}{2}} \frac{|\partial S|}{|S|}. \tag{3.2}$$

Perhaps the most intuitive definition of expanders is that an infinite family of finite, connected, d-regular graphs $\{\mathcal{G}_i\}_{i \geq 1}$, where $d \in \mathbb{N}$ is fixed, is called a family of expanders if there is an $\epsilon > 0$ such that

$$h(\mathcal{G}_i) \geq \epsilon \quad \text{for all } i \geq 1.$$

There are several other equivalent definitions of expander families, and the most useful one for our purposes is the algebraic Definition 3.1. Specifically, if $|\mathcal{G}| = n$, we can define an $n \times n$ *adjacency matrix* $M = M(\mathcal{G})$ whose rows and columns are indexed by vertices v_i of $\mathcal{G}$, such that

$$M_{ij} = \begin{cases} 1 & \text{iff } v_i \text{ and } v_j \text{ are adjacent,} \\ 0 & \text{otherwise.} \end{cases}$$

In the case that $\mathcal{G}$ is d-regular, we have that

$$d = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1} \geq -d,$$

where $\lambda_0 > \lambda_1$ if the graph is connected, which we assume for our applications. Thus in the context of a Cayley graph $\mathcal{G}$ associated to a free group of order n on $2k$ generators, the adjacency matrix $M(\mathcal{G})$ is an $n \times n$ symmetric matrix with n eigenvalues between $-2k$ and $2k$. With this in mind, we would like the set of Cayley graphs $\{\mathcal{G}_p \,|\, p \text{ prime}\}$ defined earlier to satisfy the following expander property (see [30] for a beautiful introduction to expander graphs).

Definition 3.1. Let $\{\mathcal{G}_i\}_{i \geq 1}$ be an infinite family of connected, d-regular finite graphs with $n_i = |\mathcal{G}_i| \to \infty$ as $i \to \infty$, and let $M(\mathcal{G}_i)$ be the adjacency matrix of $\mathcal{G}_i$. Let $\{\lambda_0(i), \lambda_2(i), \ldots, \lambda_{n_i-1}(i)\}$ be the set of eigenvalues of $M(\mathcal{G}_i)$ and denote by $\lambda(M(\mathcal{G}_i))$ an eigenvalue of $M(\mathcal{G}_i)$ such that

$$|\lambda(M(\mathcal{G}_i))| = \max(\{|\lambda_j(i)|, \text{ where } |\lambda_j(i)| \neq d\}).$$

We say that the graphs $\mathcal{G}_i$ form a family of expanders if and only if

$$\limsup_{j \to \infty} |\lambda(M(\mathcal{G}_j))| < d. \tag{3.3}$$

This definition is equivalent to the previous one by theorems of Alon in [2] and Alon and Milman in [3] relating the eigenvalue λ_2 to the Cheeger constant in (3.2). The spectral gap implied in (3.3) is a measure of the "expansion" in an expander family $\{\mathcal{G}_i\}$. It is precisely this expander property that guarantees that the remainder $R(\mathcal{A}, d)$ in the sieve is small, and it turns out that the affine sieve can be carried out precisely for orbits of groups that satisfy this property. The following theorem implies that the Apollonian group A is in fact such a group. We

should mention that the spectral gap has proven to be useful beyond the sieve as well: for example, it is a key ingredient in the work of Bourgain and Kontorovich in [13] that we discuss in Section 4.

Theorem 3.2 (Bourgain, Gamburd, and Sarnak [10]). *Let G be a subgroup of $\tilde{G} = \mathrm{SL}_2(\mathbb{Z}[\sqrt{-1}])$ such that G is Zariski-dense in $\mathrm{Zcl}(\tilde{G})$, and such that the traces of elements of G generate the field $\mathbb{Q}(\sqrt{-1})$. Then as (d) varies over square-free ideals in $\mathbb{Z}[\sqrt{-1}]$, the Cayley graphs $(G/(d), S)$, where S is a fixed symmetric generating set of G, is a family of expanders.*

This theorem applies to the analysis of curvatures of circles in Apollonian packings since the preimage of A in the spin-double cover of the orthogonal group SO_Q satisfies the conditions on G above. Thus the Cayley graphs arising from reduction mod d in the case of ACPs satisfy the expander property, and we can use the affine sieve to count prime curvatures in a packing P. In [10], the authors discuss how such a sieve can be applied to "prime point" counting in the orbit of a subgroup of $\mathrm{SL}_2(\mathbb{Z})$; we explore this question in the context of curvatures of circles in Apollonian packings in Section 3.2.

A similar question that has many variants over the integers concerns the infinitude of points in the orbit whose coordinates have few prime factors. For example, given an integer-valued polynomial $f(x)$ over $\mathbb{Z}$, one might ask whether there are infinitely many primes that can be expressed as $f(a)$ for some $a \in \mathbb{Z}$. This question extends to the affine setting as follows.

Consider a discrete group G generated by linear transformations that take $\mathbb{Z}^n$ to $\mathbb{Z}^n$, and let O be the orbit of G acting on $\mathbf{b} \in \mathbb{Z}^n$. Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a polynomial that takes integer values on O. Let

$$O_{r,f} := \{\mathbf{x} \in O |\ f(\mathbf{x}) \text{ has at most } r \text{ prime factors}\},$$

which we refer to as the set of r-almost prime points in O. We ask whether there is an $r \in \mathbb{Z}$ such that there are "many" points $\mathbf{x} \in O$ for which $f(\mathbf{x})$ has at most r prime factors. In particular, we are interested in finding an r such that the set $O_{r,f}$ is Zariski-dense in the Zariski closure $\mathrm{Zcl}(O)$ of O. Note that if $O_{r,f}$ is dense in $\mathrm{Zcl}(O)$ for some $r \in \mathbb{Z}$, then $O_{r',f}$ is dense in $\mathrm{Zcl}(O)$ for $r' \geq r$ as well. If such an r exists and is finite, we call the minimal r for which $O_{r,f}$ is dense in O the *saturation number* of $(\mathcal{O}, f)$, denoted by $r_0(O, f)$, and say that the pair (O, f) *saturates*.

This question is most interesting if there are no local obstructions for the pair (O, f). For example, if there is an integer $q \geq 2$ such that $(f(\mathbf{x}), q) > 1$ for all $\mathbf{x} \in O$ we have that $f(\mathbf{x})$ is divisible by some factor of q for every $\mathbf{x} \in O$. Thus r_0 will be larger than what one might expect from the arithmetic properties of O alone, which is ultimately what interests us. For this reason, we demand that the pair (O, f) be *primitive*, meaning that for every $q \geq 2$ we have at least one point $\mathbf{x} \in O$ for which $(f(\mathbf{x}), q) = 1$. We state the result for saturation of the orbit in the primitive case here:

Theorem 3.3 (Bourgain, Gamburd, and Sarnak [10]). *Let G be as in Theorem 3.2, and let O be an orbit of G acting on a vector $\mathbf{b} \in \mathbb{Z}^n$ as before. Let f be as above, and suppose (O, f) is primitive. Then the pair (O, f) saturates, and the saturation number $r_0(O, f)$ can be explicitly given in terms of the spectral gap in the expander family.*

In particular, Theorem 3.3 combined with Theorem 3.2 implies that the saturation number r_0 exists and is finite in the setting of orbits $\mathcal{P}$ of A, and in [20] we show that $r_0(\mathcal{P}, f) \leq 28$ if f is defined as

$$f(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4/12.$$

In this case if $\mathcal{P}$ is an orbit associated to a primitive packing, the pair $(\mathcal{P}, f)$ is indeed primitive; this can be derived from Theorem 2.1. However, the methods to obtain this upper bound do not rely on the affine sieve, since there is not enough information about the Apollonian group to obtain good bounds in this way. To see why this is, note that the affine sieve gives an upper bound for r_0 in terms of a lower bound for the spectral gap in (3.3) associated to the Cayley graphs of finite quotients of A: the larger the spectral gap, the smaller r_0. Lower bounds for this spectral gap can be extracted from the analysis in [44], where the authors give necessary and sufficient conditions for a family of such graphs associated to more general groups to be an expander family—in fact, the authors show that their methods are technically effective. However, the lower bounds for the spectral gap that one can extract from their proof would yield upper bounds for r_0 that are several orders of magnitude larger than what one can obtain using simpler methods such as those outlined below. It is conceivable that in the near future a good lower bound for the spectral gap in the Apollonian case will become available, in which case the above bound could probably be significantly improved.

One other possible method to get a lower bound for the spectral gap in (3.3) is to relate the combinatorial spectral gap coming from the adjacency matrices described above to the spectral gap of the Laplacians of $A_d\backslash\mathbb{H}^3$ where A_d are "congruence subgroups" of A: a lower bound for the gaps between the first and second eigenvalues of these Laplacians would imply a lower bound for the combinatorial spectral gap and vice versa. However, since the fundamental domains of these quotients have infinite volume, usual integration techniques to determine the spectra of the Laplacians do not apply. In fact, the only eigenvalue known in this case is the first eigenvalue $\lambda_0 = \delta(2 - \delta)$, where δ is the Hausdorff dimension of the limit set of a packing. Beyond this, the existence of a combinatorial spectral gap guarantees some spectral gap in this setting but says nothing about how large it is. In fact, it is currently difficult to approximate this spectral gap even numerically, so one is perhaps better off approaching the problem from the combinatorial side.

On the other hand, A has many subgroups generated by unipotent elements that can be exploited to obtain a bound on r_0 using a classical sieve over $\mathbb{Z}$ rather than the affine sieve, and this does not require the spectral theory discussed here. We state the theorem for the orbit $\mathcal{P} = A(-1, 2, 2, 3)^t$ and give a brief overview of its proof next.

Theorem 3.4 (Fuchs [20])**.** *Let A be the Apollonian group, and let $\mathcal{P} = A(-1, 2, 2, 3)^t$. For $\mathbf{x} = (x_1, x_2, x_3, x_4)^t \in \mathcal{P}$, let $f(\mathbf{x}) = x_1x_2x_3x_4/12$, and let $\mathcal{P}_{28}$ denote those points $\mathbf{x} \in \mathcal{P}$ for which $f(\mathbf{x})$ has at most 28 prime factors. Then $\mathcal{P}_{28}$ is Zariski-dense in* $\mathrm{Zcl}(\mathcal{P})$.

The number 28 in Theorem 3.4 has no particular significance; it is the best one can do with the method outlined below. In fact, one expects that, given a primitive Apollonian orbit $\mathcal{P}$, the set of points $\mathbf{x} \in \mathcal{P}$ for which $f(\mathbf{x})$ is 4-almost prime should already be Zariski-dense in $\mathrm{Zcl}(\mathcal{P})$. Since 4 is the smallest number of prime factors possible (see [20]), one basically expects the best case scenario to be true.

The theorem above is proven by considering the groups U_{ij} generated by S_iS_j, where $i \neq j$ and S_i denotes a generator of A, noting that the product of any two of the group generators is a unipotent element. For example,

$$(S_1S_2)^k = \begin{pmatrix} 2k+1 & -2k & 2k(2k+1) & 2k(2k+1) \\ 2k & 1-2k & 2k(2k-1) & 2k(2k-1) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where the top two rows are switched if k is even (note that since we are ultimately interested in taking the products of coordinates of vectors in the orbit, this switch is of no consequence to us). Let $\mathcal{P}(i,j)$ denote the orbit of U_{ij} acting on $(-1,2,2,3)^t$. It can be shown that the union of these $\mathcal{P}(i,j)$ is Zariski-dense in $\mathrm{Zcl}(\mathcal{P})$, and so to prove Theorem 3.4 it is enough to prove its analog for the orbits $\mathcal{P}(i,j)$. This is done by counting for various r the number of r-almost prime points in a ball in $\mathcal{P}(i,j)$ where $1 \leq i \neq j \leq 4$. Such a counting problem is reminiscent of the Brun sieve example at the beginning of Section 2. For example, we have that

$$\mathcal{P}(1,2) = (20s^2 + 4s - 1, 20s^2 - 16s + 2, 2, 3),$$

where the parameter s ranges over non-negative integers. Thus the values of $f(\mathbf{x})$ on this orbit are precisely the values of the polynomial

$$p(s) = 200s^4 - 120s^3 - 22s^2 + 12s - 1$$

for non-negative $s \in \mathbb{Z}$. Counting the number of r-almost prime points for the orbit $\mathcal{P}(1,2)$ thus reduces to counting the number of r-almost prime values of $p(s)$. The number of r-almost prime points in other orbits $\mathcal{P}(i,j)$ similarly reduces to counting r-almost prime values of polynomials over $\mathbb{Z}$. This is done via a classical sieve, and the lower bound in all cases is large enough to show Zariski-density if $r \geq 28$.

3.2. **Prime number theorems.** As we pointed out before, the above method of counting r_0-almost prime points is not actually an application of the affine sieve: the affine sieve tells us that the saturation number r_0 exists but we need extra information to determine what it is with any accuracy. We now demonstrate how one *can* use the affine sieve in order to produce prime number conjectures of two different flavors in the context of ACPs. The one main assumption made in arriving at these conjectures is that the Möbius function μ is random in a suitable sense. If this assumption were true, then these conjectures would in fact be theorems.

One such conjecture concerns counting circles of prime curvature less than X in a given primitive packing. Specifically, combining the sieve constructed in [10] with the analysis in [21] that we summarized in Section 2, one obtains precise heuristics for $\pi_P(X)$. These heuristics are computed and checked in [22]: according to the data presented there, they are most likely correct. The strategy is to consider

$$\psi_P(X) = \sum_{\substack{a(C) \leq X \\ a(C) \text{ prime}}} \log\big(a(C)\big), \tag{3.4}$$

where C denotes a circle in the packing P and $a(C)$ denotes its curvature. See [22] for an explanation of how $\pi_P(X)$ can be derived from $\psi_P(X)$. The heuristic obtained in [22] for $\psi_P(X)$ is as follows.

Conjecture 3.5 (Fuchs and Sanden [22])**.** *Recall that $N_P(X)$ is the number of circles in a packing P of curvature less than X, and let $\psi_P(X)$ be as in* (3.4)*. Then as $X \to \infty$,*

$$\psi_P(X) \sim L(2, \chi_4) \cdot N_P(X),$$

where $L(2, \chi_4) = 0.9159\cdots$ is the value of the Dirichlet L-series at 2 with character $\chi_4(p) = 1$ for $p \equiv 1$ (4) and $\chi_4(p) = -1$ for $p \equiv 3$ (4).

This implies, in particular, that

$$\pi_P(X) \sim \frac{L(2, \chi_4) \cdot N_P(X)}{\log X}.$$

These asymptotics are reminiscent of the classical prime number theorem, which states that the weighted count $\psi(x) \sim x$ and that $\pi(x) \sim x/\log x$.

We now outline how one obtains the heuristics in Conjecture 3.5. To count circles of prime curvature, we observe that to every circle C in a given packing one can associate a unique vector $\mathbf{x}$ in the corresponding orbit in the following manner. Suppose P has root quadruple $\mathbf{v}$ of curvatures of circles C_1, C_2, C_3, and C_4. We will associate $\mathbf{v}$ with each of these circles C_i. For any other circle C in the packing there is exactly one element γ of the Apollonian group which transforms the circles C_1, C_2, C_3, and C_4 to a quadruple of circles containing C, of which C has the largest curvature. In terms of the orbit, this means that C corresponds to one vector $\mathbf{x} = \gamma\mathbf{v} \in A\mathbf{v}$ in which the maximal coordinate is the curvature of C. Denote by $||\mathbf{x}||$ the maximal coordinate of $\mathbf{x}$. Given the observation above, counting circles of prime curvature amounts to counting $\mathbf{x} \in A\mathbf{v}$ for which $||\mathbf{x}||$ is prime. Here we define $A\mathbf{v}$ to be the *multiset* of vectors $\{\gamma\mathbf{v} \,|\gamma \in A\}$. As we mentioned above, it is convenient to count primes in the orbit of A with a logarithmic weight. To this end, let

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^l \text{ for some } l > 0, \\ 0 & \text{otherwise.} \end{cases}$$

Equivalently,

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d, \tag{3.5}$$

where $\mu(d)$ is the Möbius function. Note that if d is not square-free, we have $\mu(d) = 0$, so in the following we assume d is square-free. It is shown in [22] that

$$\psi_P(X) = \sum_{\substack{\mathbf{x} \in A\mathbf{v} \\ ||\mathbf{x}|| \le X}} \Lambda(||\mathbf{x}||) + \mathrm{O}(X) = -\sum_{d>1} \sum_{\substack{\mathbf{x} \in A\mathbf{v} \\ ||\mathbf{x}|| \le X \\ ||\mathbf{x}|| \equiv 0 \ (d)}} \mu(d) \log d + \mathrm{O}(X). \tag{3.6}$$

Now, sieve theory can only help us to evaluate the right-hand side of (3.6) if we sum over $d < D$ where D is a small power of $N_P(X)$, the number of circles of curvature less than X in the packing. We therefore split the sum in (3.6) as follows:

$$\psi_P(x) = -\left(\sum_{d \le D} \mu(d) \log d \sum_{\substack{\mathbf{x} \in A\mathbf{v} \\ ||\mathbf{x}|| \le X \\ ||\mathbf{x}|| \equiv 0 \ (d)}} 1 \right) - \left(\sum_{d > D} \mu(d) \log d \sum_{\substack{\mathbf{x} \in A\mathbf{v} \\ ||\mathbf{x}|| \le X \\ ||\mathbf{x}|| \equiv 0 \ (d)}} 1 \right) + \mathrm{O}(X). \tag{3.7}$$

Assuming that $\mu(d)$ above becomes random as d grows, the sum over $d > D$ in (3.7) is negligible, and so we ignore it (if we could prove the validity of this step, the conjecture above would be a theorem). The task is now to evaluate the first sum,

and it is here that we rely heavily on the affine sieve developed in [10]. Specifically, the analysis in [10] guarantees that there is a function $\beta : \mathbb{Z}^{>0} \to [0,1]$ such that $\beta(pq) = \beta(p)\beta(q)$ for primes $p \neq q$, and such that for every square-free $d < D$, we have

$$\sum_{\substack{\mathbf{x} \in A\mathbf{v} \\ ||\mathbf{x}|| \leq X \\ ||\mathbf{x}|| \equiv 0 \ (d)}} 1 = \beta(d) \cdot N_P(X) + r(d),$$

where the remainder $r(d)$ is small on average in the sense that

$$\sum_{d \leq D} r(d) = \mathrm{O}(N_P(X)^{1-\epsilon_0})$$

for some $\epsilon_0 > 0$. Thus, since we have assumed that we can ignore the second sum in (3.7), this evaluation of the remainder term allows us to rewrite (3.7) as

$$-\left(\sum_{d \leq D} \beta(d)\mu(d)\log d\right) N_P(X) + \mathrm{O}(N_P(X)^{1-\epsilon}) \tag{3.8}$$

for some $0 < \epsilon < 1$. To compute this expression, note that

$$\sum_{d \leq D} \beta(d)\mu(d)\log d = \sum_{d>0} \beta(d)\mu(d)\log d - \sum_{d>D} \beta(d)\mu(d)\log d. \tag{3.9}$$

Assuming once again that the sum over $d > D$ is insignificant due to the conjectured randomness of the Möbius function, we have that the sum over $d \leq D$ in (3.9) can be approximated by the sum over all d. To evaluate this sum, we must have a precise formula for $\beta(d)$ in the Apollonian situation, which is obtained in [22] using the results outlined in Section 2 of this article. First of all, letting $\mathcal{O}_d$ denote the orbit $A\mathbf{v}$ reduced modulo d (this is finite), we define β_i for $1 \leq i \leq 4$ as

$$\beta_i(d) = \frac{\#\{\mathbf{x} = (x_1, x_2, x_3, x_4)^t \in \mathcal{O}_d \,|\, x_i = 0\}}{\#\{\mathbf{x} \in \mathcal{O}_d\}}. \tag{3.10}$$

We have that $\beta_i(pq) = \beta_i(p)\beta_i(q)$ for primes $p \neq q$ from the analysis in Section 2, and so to determine $\beta_i(d)$ for square-free d we must simply determine it for primes p. It turns out that $\beta_i(p)$ is independent of i for all primes $p > 2$, and indeed our function $\beta(d)$ will simply be $\beta_i(d)$ for any $1 \leq i \leq 4$ if d is odd. For d even, β is only a bit more complicated, but we suppress this technical detail here (essentially, the issue is that the orbit $A\mathbf{v}$ is even at two coordinates and odd at the other two). More specifically, if $p \neq 2$, we have $\beta(p) = \beta_i(p)$ for $1 \leq i \leq 4$ and

$$\beta(p) = \begin{cases} \frac{1}{p+1} & \text{for } p \equiv 1 \bmod 4, \\ \\ \frac{p+1}{p^2+1} & \text{for } p \equiv 3 \bmod 4. \end{cases} \tag{3.11}$$

With this precise form of β, computing the sum over positive integers d from (3.9) is a problem in elementary number theory as soon as one understands β for even d, and we refer the reader to [22] for this computation which yields

$$-\sum_{d>0} \beta(d)\mu(d)\log d = L(2, \chi_4).$$

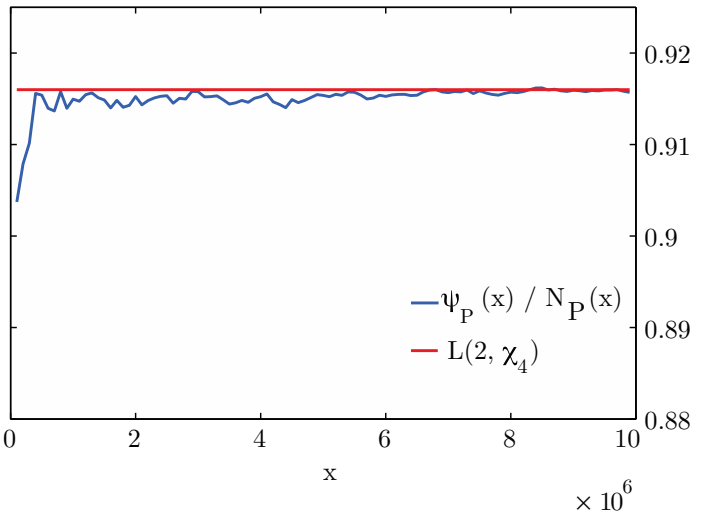


FIGURE 4. Prime number heuristic for the packing P generated by $(-1, 2, 2, 3)$

Combined with (3.6) and the discussion above, this yields the heuristic in Conjecture 3.5 as desired. Figure 4 indicates that the heuristic in Conjecture 3.5 is quite accurate. It depicts the straight line $y = L(2, \chi_4)$, as well as the graph of $\psi_P(X)/N_P(X)$ for $0 \leq X \leq 10^7$ where P is the packing generated by $(-1, 2, 2, 3)$, which clearly tends towards the straight line as X grows. Similar numerical tests have been carried out in [22] for other packings, and the heuristic appears accurate in all such tests.

The argument above can also be carried out for counting circles of prime curvature that are created at generation T, rather than according to their size. Although this seems to be a different proposition at first glance, in some sense it is quite similar, since the curvatures of circles produced at generation T do tend to be larger than those produced at previous generations. This idea can be made rigorous by considering the *Lyapunov exponent* in the case of a random walk on the generators S_i of the Apollonian group, which gives a relationship between the curvatures of most circles born at generation T to the generation T itself: basically, it is known that for most circles C born at a large generation T in an Apollonian packing, the curvature $a(C)$ is of size $e^{\gamma T}$ for some exponent γ. This exponent is approximated experimentally as $\gamma \approx 0.9149$ in [20], where prime number conjectures in the case of counting circles of prime curvature born at generation T are then derived using sieve methods similar to those outlined above.

To summarize, the inputs into these prime number conjectures are

(i) the existence of a spectral gap;
(ii) an explicit formula for the function $\beta(d)$;
(iii) the determination of the Lyapunov exponent for random walks on the generators of the group.

In many Diophantine problems concerning integer orbits of a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ where these three inputs are attainable, one can proceed as above to determine a heuristic prime number conjecture.

4. Density of curvatures and the local-to-global conjecture

So far we have seen that the integers that occur as curvatures in any given ACP behave very similarly to all of $\mathbb{N}$ in general: there are very few local obstructions that we have defined completely in Section 2, there are infinitely many prime numbers in any packing, and the conjectured prime number theorem in the case of ACPs described in Section 3 mimics the classical prime number theorem over the integers. In fact, it is predicted that the integers that come up as curvatures in a given primitive Apollonian packing are precisely all those that are not ruled out by the congruence obstructions specified in Section 2 outside finitely many exceptions. This very strong local-to-global conjecture which we state below holds up under experimental scrutiny but remains open.

Conjecture 4.1 (Fuchs and Sanden [22], Graham, Lagarias, Mallows, Wilks, and Yan [27])**.** *Let P be an integer ACP, and let P_{24} be the set of residue classes* mod 24 *of curvatures in P. Then there exists $X_P \in \mathbb{Z}$ such that any integer $x > X_P$ whose residue* mod 24 *lies in P_{24} is in fact a curvature of a circle in P.*

Note that the "24" in this conjecture comes precisely from the statement of Theorem 2.1, which roughly states that to determine the reduction of an ACP mod d it is essentially enough to know its reduction modulo 24. The conjecture is saying that for any packing P, all large enough integers that satisfy some easily computable congruence conditions mod 24 are in fact curvatures in P. Furthermore, these integers are precisely the set of curvatures larger than X_P in P. At least at first glance, it is remarkable that an infinite index subgroup of $\mathrm{O}_Q(\mathbb{Z})$ should possess such a rich property. However, several experiments outlined in [22] indicate that the conjecture is true. For example, if P is taken to be the packing generated by $(-1, 2, 2, 3)$, it is shown that $P_{24} = \{2, 3, 6, 11, 14, 15, 18, 23\}$ and that all integers $10^6 < x < 5 \cdot 10^8$ such that $x \in P_{24}$ modulo 24 appear as curvatures in P.

An immediate consequence of Conjecture 4.1 is the positive density conjecture of Graham et al. in [27] that the curvatures in a given packing have positive density in $\mathbb{N}$ which was first proven in [8]. In this section we outline the proof of this positive density conjecture and survey what is currently known about this density and about the local-to-global conjecture above.

The natural way to approach Graham et al.'s positive density statement is to count integers that come up as curvatures in an ACP. This is no longer a problem suitable for the affine sieve (sieves do not count points in a ball, rather they sift out points in a ball that in some sense have many prime factors). In fact, the problem of counting how many integers less than X (without multiplicity) one picks up in the curvatures of an ACP is a very different question from counting circles of curvature less than X in an ACP, which is what we have done so far. It is unclear how to derive the former from the latter.

However, although the problem we now discuss is of a different flavor from what we have seen earlier, the methods do resemble somewhat the strategy used to bound the saturation number r_0 in Section 3: the basic idea will be to exploit the fact that while the Apollonian group A is thin, it does have various nice subgroups that are easier to work with.

To set up notation, for any primitive packing P we let

$$\kappa(P, X) := \#\{a \in \mathbb{N} \,|\, a \leq X,\ a \text{ is a curvature of a circle in } P\}.$$

Conjecture 4.1 would imply that the limit below exists and is positive:

$$\lim_{X\to\infty} \frac{\kappa(P,X)}{X} > 0.$$

In fact, Conjecture 4.1 combined with the analysis in [21] predicts (see [22]) the exact limit

$$\lim_{X\to\infty} \frac{\kappa(P,X)}{X} = \frac{1}{4} \text{ or } \frac{1}{3}, \tag{4.1}$$

depending on the packing P. Both the positive density conjecture and the existence of the limit (with correct constants) is now known. We state the former below and review its proof next.

Theorem 4.2 (Bourgain and Fuchs [8])**.** *For an integer Apollonian circle packing P, let $\kappa(P,X)$ denote the number of distinct integers up to X occurring as curvatures in the packing. Then for X large we have*

$$\kappa(P,X) \gg X,$$

where the implied constant depends on the packing P.

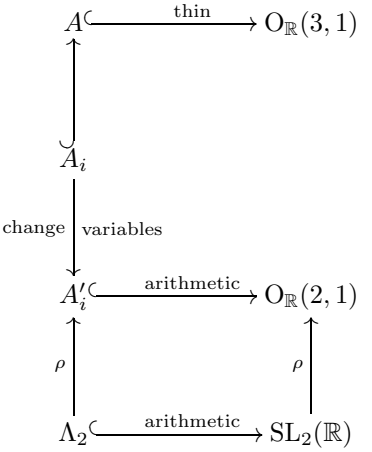
This theorem is proven by counting curvatures in different "subpackings" of an ACP which we sketch next. Since counting integers in the full Apollonian group's orbit is quite difficult given the thinness of the group, we consider instead of the full group A some special subgroups of A. In doing so we are confronted with a much easier counting problem. Namely, let A_i be the group generated by all but the ith generators of A:

$$A_i := \langle \{S_1, S_2, S_3, S_4\} - \{S_i\} \rangle . \tag{4.2}$$

Geometrically, such a group fixes one circle in the packing (the ith circle in the root quadruple) and produces circles that are tangent to the fixed one. This is readily seen by observing that the generator S_i is the only generator which acts on the ith coordinate of a vector in $\mathbb{R}^4$. In [46], Sarnak showed that one can realize these subgroups as subgroups of $\mathrm{SO}(2,1)$ acting on $\mathbb{H}$, and that the fundamental domain of this new action is in fact finite. Furthermore, he showed that the integers occurring in the orbits of these groups acting on Descartes quadruples contain the set of integers represented by a certain binary quadratic form whose coefficients are expressed in terms of the root quadruple of the packing (and this is a set in which we know how to count).

This can be seen by first noting that A_i is isomorphic to a subgroup of $\mathrm{GL}_3(\mathbb{Z})$ (in particular A_i acts only on three of the four coordinates of the root quadruple $\mathbf{v}_P$). Specifically, a variable change sends the group A_i to a subgroup A_i' of $\mathrm{O}_{\mathbb{R}}(2,1)$. Next, one notes that the preimage of $A_i' \cap \mathrm{SO}(2,1)$ under the spin homomorphism $\rho : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{SO}(2,1)$ is the principal congruence 2-subgroup Λ_2 of $\mathrm{SL}_2(\mathbb{Z})$. Combined with the map ρ, this gives a very nice expression for the orbits of A_i'. From this expression it is not hard to derive the relationship between the integers appearing in the orbit $A_i\mathbf{v}_P$ and integers represented by a binary quadratic form as described

above. We illustrate this process in the following diagram.



We refer the reader to [46] and section 2 of [8] for the details of this manipulation which leads to the following result if $i = 1$ (there are analogous results for every $1 \le i \le 4$). Let $\mathbf{v}_P = (a_0, b, c, d)^t$ is the root quadruple of a bounded packing P, and let C_{a_0} be a circle of curvature a_0 in the root quadruple. For $X \in \mathbb{N}$, let

$$\mathcal{P}_1 = \{n \in \mathbb{N} \mid n \le X,\ n = |x_j| \text{ for some } 1 \le j \le 4, \text{ for some } \mathbf{x} = (x_1, x_2, x_3, x_4)^t \in A_1\mathbf{v}_P\},$$

and let

$$f_{a_0}(x, y) = Ax^2 + 2Bxy + Cy^2,$$

where

$$A = b + a_0, \qquad B = \frac{a_0 + b + d - c}{2}, \qquad C = d + a_0.$$

The process described in the diagram above then yields that $\mathcal{P}_1$ contains the set

$$\mathcal{A}(a_0) = \{a \in \mathbb{N} \mid a \le X,\ a = f_{a_0}(x, y) - a_0 \text{ for some } x, y \in \mathbb{Z},\ \gcd(x, y) = 1\}. \tag{4.3}$$

So, since the orbit $A_1\mathbf{v}_P$ above is contained in the full orbit $A\mathbf{v}_P$, a lower bound on the number of integers less than X represented by the shifted quadratic form $f_{a_0} - a_0$ will also serve as a lower bound for $\kappa(P, X)$. Getting a lower bound on the number of integers represented by a binary quadratic form is quite classical. For example, in his 1912 thesis [5] Bernays showed that for a positive definite binary quadratic form f over $\mathbb{Z}$ of discriminant $-D$, the number $B(X)$ of integers less than X represented by f is

$$B(X) = \frac{c \cdot X}{\sqrt{\log X}} + O\left(\frac{X}{\log X}\right), \tag{4.4}$$

where c is a positive constant such that

$$\pi c^2 = \prod_{\substack{q \equiv 3 \ (4) \\ q \nmid D}} \left(1 - \frac{1}{q^2}\right)^{-1} \prod_{p \mid D} \left(1 - \frac{1}{p}\right) \sum_{n=1}^{\infty} \left(\frac{-D}{n}\right) n^{-1}.$$

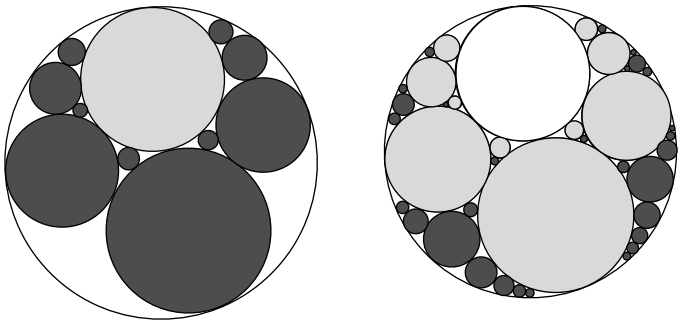


FIGURE 5. A pictorial representation of the proof of Theorem 4.2.

It is not hard to see that the form f_{a_0} is indeed positive definite, so the expression in (4.4) combined with the fact that $\mathcal{A}(a_0) \subset \mathcal{P}_1$ implies that

$$\kappa(P, X) \gg \frac{X}{\sqrt{\log X}}. \tag{4.5}$$

This lower bound was first proven by Sarnak in [46]. Shortly thereafter, the idea of counting in suborbits of $A\mathbf{v}_P$ was refined to yield a slightly better bound in [19] and subsequently to prove Theorem 4.2 in [8]. Recently, this idea was taken a step further to get a precise formula for $\kappa(P, X)$ in [13].

The idea in both of these refinements is as follows: counting in the orbit of one group A_i reflects only those circles that are tangent to a fixed circle in P, and one wants to count some of the missed circles to improve the bound in (4.5). This is done as follows. To obtain the lower bound in (4.5), we fixed a circle of curvature a_0 and associated curvatures of circles tangent to it with the set of integers represented by $f_{a_0}(x, y) - a_0$. We denoted the set of these integers that are less than X by $\mathcal{A}(a_0)$ in (4.3).

Now, to every integer $a \in \mathcal{A}(a_0)$ one can associate a circle C_a of curvature a tangent to C_{a_0} in the packing P. One can again relate the integers less than X occurring as curvatures of circles tangent to C_a to integers represented by a shifted binary form and thus get a lower bound on the number of such integers. Specifically, for every $a \in \mathcal{A}(a_0)$ there is a binary quadratic form f_a such that the set

$$\{\alpha \in \mathbb{N} \mid \alpha \leq X, \alpha \text{ is the curvature of a circle tangent to } C_a \text{ in } P\}$$

contains the set

$$\{\alpha \in \mathbb{N} \mid \alpha \leq X,\ \alpha = f_a(x, y) - a \text{ for some } x, y \in \mathbb{Z},\ \gcd(x, y) = 1\}.$$

We now wish to count the integers represented by the new shifted forms $f_a(x, y) - a$ for $a \in \mathcal{A}(a_0)$. This strategy is depicted in Figure 5: in the picture on the left we fix the lightly shaded circle, and count some of the darkly shaded circles as in the argument leading to (4.5). On the right in Figure 5, we fix one by one some of the circles we counted in the left picture, and count the dark circles tangent to those, taking care not to count any of the shaded circles more than once. This is the natural next step to improving the bound in (4.5).

One might worry that perhaps the sets of integers coming from circles tangent to each of the ones we fix (the clusters of dark circles in the second picture above) are not significantly different, in which case we are wasting our time trying to

meticulously count the cardinality of the union of these sets. However, this is not the case. To see why, we introduce a bit of notation. For each $a \in \mathcal{A}(a_0)$, let

$$\tilde{S}_a = \{n \in \mathbb{N} \,|\, n \leq X, n = f_a(x,y) \text{ for some relatively prime integers } x, y\}.$$

One can show that the discriminant of each f_a is simply $-4a^2$, which in fact implies that $\tilde{S}_a$ is a subset of the integers that can be written as a sum of two squares. Thus the union

$$\bigcup_{a \in \mathcal{A}(a_0)} \tilde{S}_a$$

is not very big, and the sets $\tilde{S}_a$ do not differ much from one another. However, if one considers instead (as we do) the union of sets S_a of integers less than X represented by the *shifted* form $f_a - a$,

$$S_a = \{n \in \mathbb{N} \,|\, n \leq X, n = f_a(x,y) - a \text{ for some relatively prime integers } x, y\},$$

one gains a substantial amount of new integers, since this shift by a makes the sets S_a quite different from one another. In fact, Theorem 4.2 is proven in [8] by showing that

$$\Big| \bigcup_{a \in \mathcal{A}(a_0)} S_a \Big| \gg X.$$

We now mention some of the obstacles in showing this and give an idea of how to overcome them.

One important consideration in evaluating the size of these sets S_a, i.e., in counting integers represented by the forms f_a, is that the discriminants and thus the coefficients of f_a can be very large with respect to X. In this case many of the represented integers may be $> X$. In particular, the count in (4.4) is not uniform in D, so one cannot rely on this bound alone to determine $|S_a|$ if a is large. Therefore one must understand how exactly $|S_a|$ depends on the size of a. This question has been addressed by Blomer and Granville in [6], where the authors give lower and/or upper bounds for the number of integers $\leq X$ represented by a positive definite binary quadratic form which depends almost solely on the size of the form's discriminant as compared to X. In their notation, let $U_f(X)$ be the number of integers less than X represented by f, and let $D < 0$ denote the discriminant of f. Blomer and Granville show

- if $-D \in [0, (\log X)^{\log 2}]$, then $U_f(X) \gg_\epsilon \frac{X}{(\log X)^{1/2+\epsilon}}$;
- if $-D \in [(\log X)^{\log 2}, (\log X)^{2\log 2}]$, there are no good known *lower* bounds on $U_f(X)$;
- if $-D \in [(\log X)^{2\log 2}, X]$, then $U_f(X) \gg \frac{X}{\sqrt{-D}}$.

For our purposes, this translates into the following information about the sets S_a, since f_a has discriminant $-4a^2$:

- if $2a \in [0, (\log X)^{(\log 2)/2}]$, then $|S_a| \gg_\epsilon \frac{X}{(\log X)^{1/2+\epsilon}}$;
- if $2a \in [(\log X)^{(\log 2)/2}, (\log X)^{\log 2}]$, there are no good known *lower* bounds on $|S_a|$;
- if $2a \in [(\log X)^{\log 2}, \sqrt{X}]$, then $|S_a| \gg \frac{X}{2a}$.

Since we are interested in lower bounds, only the first and third range above are useful to us in proving Theorem 4.2. In [19], we consider only the first range and

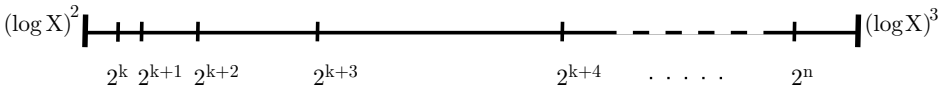


FIGURE 6. Constructing a subset $\mathbf{S} \subset \mathcal{A}(a_0) \cap I$.

show that

$$\kappa(P, X) > \Big| \bigcup_{\substack{a \in \mathcal{A}(a_0) \\ a < (\log X)^{(\log 2)/2}}} S_a \Big| \gg \frac{X}{(\log X)^{0.153}}. \tag{4.6}$$

This is the best bound that can be obtained by working in the first range and of course it does not give a positive fraction of all integers.

On the other hand, one can apply the method used to obtain the bound in (4.6) in the *third* range above to get a better bound and to prove Theorem 4.2. However, in the third range one encounters a new obstacle that has to be handled by considering only a very small subset of all possible S_a where a is in the third range $I = [(\log X)^{\log 2}/2, \sqrt{X}/2]$. To see why this is necessary, note that the most intuitive way to obtain a lower bound on

$$\Omega := \Big| \bigcup_{a \in \mathcal{A}(a_0) \cap I} S_a \Big| \tag{4.7}$$

is as follows:

$$\Omega \geq \sum_{a \in \mathcal{A}(a_0) \cap I} |S_a| \; - \sum_{a \neq a' \in \mathcal{A}(a_0) \cap I} |S_a \cap S_{a'}|. \tag{4.8}$$

Specifically, one needs to obtain a lower bound on the first sum above, and an upper bound on the second sum. However, the upper bound that we can hope to obtain on the second sum will be larger than the lower bound we can hope to obtain for the first sum, and so we do not learn anything of interest about Ω by doing just this. Instead, we consider a small subset $\mathbf{S}(X)$ of $\mathcal{A}_0 \cap I$ and compute the relevant bounds on the two sums in (4.8) taken over $\mathbf{S}(X)$. This subset needs to be chosen carefully: On the one hand, it needs to be large enough so that the lower bound on $\sum |S_a|$ is a positive fraction of X. At the same time it needs to be small enough so that the upper bound on $\sum |S_a \cap S_{a'}|$ is small. Additionally, for the purpose of determining these bounds, one wants that as X grows the integers in $\mathbf{S}(X)$ are equidistributed modulo any prime q.

Since the construction of such a subset is crucial to the proof of Theorem 4.2, we recall it below (for details, see [8]). We first consider the subinterval $[(\log X)^2, (\log X)^3]$ of the third range I and break it into dyadic ranges, as in Figure 6.

For k satisfying $(\log X)^2 < 2^k < (\log X)^3/2$, denote by $\mathbf{S}^{(k)}$ the following subset of $[2^k, 2^{k+1}]$,

$$\mathbf{S}^{(k)} = \mathcal{A}(a_0) \cap [2^k, 2^k + \eta \frac{2^k}{\sqrt{k}}], \tag{4.9}$$

where $0 < \eta < 1$ is a parameter independent of k that we are free to choose and which will play an important role momentarily: we will see that the bounds on the two sums in (4.8) will depend in a crucial way on η, and it is this parameter

that will allow us to ensure that the difference between the two sums is a positive fraction of X. We explain in what sense $\mathbf{S}^{(k)}$ is chosen "optimally" to produce a positive fraction of integers shortly. Namely, we take $\mathbf{S}$ to be the union of all of these sets $\mathbf{S}^{(k)}$:

$$\mathbf{S} = \bigcup \mathbf{S}^{(k)}, \tag{4.10}$$

where k ranges over all positive integers satisfying $(\log X)^2 < 2^k < (\log X)^3/2$ as before. This subset of $\mathcal{A}(a_0) \cap I$ is optimal in the sense that if it were any smaller, we would not get the desired lower bound in (4.11) below. Furthermore, the set $\mathbf{S}$ does satisfy the equidistribution modulo primes property mentioned above (see [8]). We now return to bounding Ω as in (4.8). Using the results of Blomer and Granville in [6], we are able to show that

$$\sum_{a \in \mathbf{S}} |S_a| \gg \eta X, \tag{4.11}$$

where the implied constant depends only on a_0. It remains to obtain a good upper bound on the second sum in (4.8). To do this, we must first get an upper bound for $S_a \cap S_{a'}$ where $a \neq a' \in \mathbf{S}$. In [8] this is done rather crudely by counting points $(x, y, x'y')$ in a closed region[2] on the quadric

$$f_a(x, y) - f_{a'}(x', y') = a - a' \tag{4.12}$$

for each $a \neq a' \in \mathbf{S}$. This is crude because it counts every integer in the intersection $S_a \cap S_{a'}$ with multiplicity (the more representations of the integer by f_a and $f_{a'}$ there are, the higher the multiplicity), while in fact every integer in $S_a \cap S_{a'}$ comes up only once. Nevertheless, the upper bound we obtain with this method is good enough to prove Theorem 4.2. Specifically, this crude count produces the upper bound

$$\sum_{a \neq a' \in \mathbf{S}} |S_a \cap S_{a'}| \leq c\eta^2 X, \tag{4.13}$$

where $c > 0$ is a constant depending only on a_0. This bound is obtained by using the circle method as refined in [40] to compute the representation numbers of $a - a'$ by the quaternary quadratic forms $f_a(x, y) - f_{a'}(x', y')$.

Combining (4.11) and (4.13), we have that

$$\kappa(P, X) \geq \sum_{a \in \mathcal{A}(a_0) \cap I} |S_a| - \sum_{a \neq a' \in \mathcal{A}(a_0) \cap I} |S_a \cap S_{a'}| \gg (\eta - c\eta^2)X.$$

Since we are free to choose $0 < \eta < 1$, we can in particular choose η such that $c\eta^2 < \eta$, and so we have that

$$\kappa(P, X) \gg X$$

as desired. So by repeating Sarnak's method in the third range of Blomer and Granville and by introducing this parameter η, we are able to control the sums in (4.8) and prove that the positive integers appearing as curvatures in any integer ACP make up a positive fraction of $\mathbb{N}$.

As we mentioned before, there is now a stronger positive density theorem which we state below.

[2]The region in these points are counted is determined by the condition that $f_a(x, y) \leq X$.

Theorem 4.3 (Bourgain and Kontorovich [13])**.** *Let P be an integer ACP, and let $\sigma = \sigma(P)$ be the number of residue classes* mod 24 *of curvatures in P. Then there exists some absolute constant $\epsilon > 0$ such that as $X \to \infty$*

$$\kappa_P(X) = \frac{\sigma}{24} \cdot X + O(X^{1-\epsilon}).$$

The proof of this theorem builds upon the methods of [8] in that the authors consider an infinite family of binary quadratic forms and count integers represented by this family. The family they choose is a larger one than the one used in [8] and their method of counting represented integers is more intricate, utilizing a version of the Hardy–Littlewood circle method similar to the one introduced in [12], where the authors count integers represented in orbits of thin subgroups of $\mathrm{SL}_2(\mathbb{Z})$. This counting method relies heavily on the existence of the combinatorial spectral gap for the Apollonian group as discussed in Section 3 together with methods from [11] to relate the combinatorial spectral gap to the Laplacian spectral gap. It also utilizes results of Vinogradov in [50] on bisector counting in hyperbolic 3-folds as well as on the congruence analysis in [21]. This method is quite general and can be applied to counting integers in orbits of various other thin subgroups of $\mathrm{O}_f(\mathbb{Z})$ where f is signature $(3, 1)$. One should note, however, that it is unlikely that the counting methods outlined here would lead to a proof of the local-to-global conjecture, which would likely require a deeper understanding of the Apollonian group's orbits.

5. The quest to better understand thin groups

Having perhaps convinced the reader that thin groups are interesting objects to study from an arithmetic point of view, we end this article with a few words about the contrast between thin and arithmetic groups as well as what remains to be done to put our knowledge of thin groups on the same footing as our knowledge of arithmetic groups. For more information, see [47] for a beautiful account of thin groups and related problems.

Throughout this article we have dealt at length with various arithmetic problems connected to orbits of the Apollonian group, and the methods we described can be applied to other thin subgroups of $\mathrm{GL}_n(\mathbb{Z})$. As we saw in Section 3, a powerful tool in such problems is the affine sieve, which applies to thin and arithmetic groups alike as long as the connected component of the Zariski closure of the group is perfect. This is proven in [43] and [44]. Since this condition has little to do with whether the group is thin or not, one might ask why we should focus on thin groups in particular. To address this, we note that a key input into the affine sieve is showing that the group involved satisfies the expander property discussed in Section 3.1. It is in the case of thin groups that this input has only recently become available, and it is also in this case that a lot of work remains to be done. Indeed, showing that an arithmetic group satisfies the expander property, and even determining the corresponding spectral gap is much more classical. For example, consider for $n > 2$ a finite index subgroup Γ of $\mathrm{SL}_n(\mathbb{Z})$ that is Zariski-dense in SL_n, and suppose we want to show that the Cayley graphs associated to finite quotients of Γ form an expander family. We can argue as follows: for $n > 2$ the group $\mathrm{SL}_n(\mathbb{Z})$ as well as all of its finite index subgroups have Kazhdan property T (see [35] for a definition). Furthermore, the fact that they have property T implies that they possess the desired expander property; this observation is an old result due to Margulis in [36], and is the idea behind the first explicit construction of expanders, also in [36]. Yet

for the general thin group, property T will not help. Similarly, while one can usually get reasonable bounds on the spectral gap connected to an arithmetic group (e.g., Selberg's 3/16 theorem implies a gap of 3/16 for congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and this in turn gives a combinatorial spectral gap in this context), as we mentioned at the end of Section 3.1 there is not currently a way to give good bounds for the spectral gap in the case of a thin group. Thus a natural next step in understanding the arithmetic of orbits of thin groups is to attempt to improve these bounds. In particular, this would make the affine sieve a much more precise tool for counting in such orbits.

We should also mention that thin groups come up very naturally in arithmetic problems that are quite different from the counting problems we outline in this article. For example, Ellenberg, Hall, and Kowalski have recently obtained results in [18] about rational p-torsion points for Abelian varieties over $\mathbb{Q}$ by considering the monodromy groups (thin monodromy groups in particular) connected to these varieties. Like the fundamental theorem of the affine sieve, their results rely heavily on expander graphs—they need that the Cayley graphs coming from the finite quotients of the monodromy group involved form an expander family.

In both the problem of counting primes in orbits of groups and in the problems considered in [18], it is natural to ask how one can tell whether a group is thin. This question in general is not easy, mostly because there is currently no easily verifiable characteristic of a group that would imply it is thin: as we have seen throughout this article, in some sense thin groups are just as "rich" as arithmetic groups so it is hard to tell the two apart. A different question of a similar flavor is, how generic are thin groups? For example, given a meaningful definition of "generic", is the generic group to which one can apply the affine sieve thin? Is the generic monodromy group in applications in [18] thin? A positive answer to these questions will give all the more reason to study these groups in more detail.

Acknowledgments

We thank P. Sarnak for introducing us to ACPs and for inspiring much of the work presented here. We thank A. Kontorovich, P. Sarnak, Mark Goresky, and the referees for helpful comments on a previous version of this article. Finally, we thank K. Sanden for providing several of the pictures in this article.

About the author

Elena Fuchs is a Simons Visiting Assistant Professor at the University of California, Berkeley. Her research combines techniques from number theory, hyperbolic geometry, and geometric group theory to study arithmetic properties of thin groups.

References

[1] D. Aharonov and K. Stephenson, *Geometric sequences of discs in the Apollonian packing*, Algebra i Analiz **9** (1997), no. 3, 104–140; English transl., St. Petersburg Math. J. **9** (1998), no. 3, 509–542. MR1466797 (98f:52019)

[2] N. Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), no. 2, 83–96, DOI 10.1007/BF02579166. Theory of Computing (Singer Island, Fla., 1984). MR875835 (88e:05077)

[3] N. Alon and V. D. Milman, λ_1, *isoperimetric inequalities for graphs, and superconcentrators*, J. Combin. Theory Ser. B **38** (1985), no. 1, 73–88, DOI 10.1016/0095-8956(85)90092-9. MR782626 (87b:05092)

[4] Richard Aoun, *Random subgroups of linear groups are free*, Duke Math. J. **160** (2011), no. 1, 117–173, DOI 10.1215/00127094-1443493. MR2838353

[5] P. Bernays, *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht quadratischen Diskriminante*, Ph.D. dissertation, Georg-August-Universität, Göttingen, Germany (1912).

[6] Valentin Blomer and Andrew Granville, *Estimates for representation numbers of quadratic forms*, Duke Math. J. **135** (2006), no. 2, 261–302, DOI 10.1215/S0012-7094-06-13522-6. MR2267284 (2007i:11132)

[7] J. Bourgain, *Integral Apollonian circle packings and prime curvatures*, J. Anal. Math. **118** (2012), 221–249, DOI 10.1007/s11854-012-0034-2. MR2993027

[8] Jean Bourgain and Elena Fuchs, *A proof of the positive density conjecture for integer Apollonian circle packings*, J. Amer. Math. Soc. **24** (2011), no. 4, 945–967, DOI 10.1090/S0894-0347-2011-00707-8. MR2813334 (2012d:11072)

[9] J. Bourgain and E. Fuchs, *On representation of integers by binary quadratic forms*, Int. Math. Res. Not., doi: 10.1093/imrn/rnr253 (2012).

[10] Jean Bourgain, Alex Gamburd, and Peter Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** (2010), no. 3, 559–644, DOI 10.1007/s00222-009-0225-3. MR2587341 (2011d:11018)

[11] Jean Bourgain, Alex Gamburd, and Peter Sarnak, *Generalization of Selberg's $\frac{3}{16}$ theorem and affine sieve*, Acta Math. **207** (2011), no. 2, 255–290, DOI 10.1007/s11511-012-0070-x. MR2892611

[12] Jean Bourgain and Alex Kontorovich, *On representations of integers in thin subgroups of* $\mathrm{SL}_2(\mathbb{Z})$, Geom. Funct. Anal. **20** (2010), no. 5, 1144–1174, DOI 10.1007/s00039-010-0093-4. MR2746949 (2012i:11008)

[13] J. Bourgain and A. Kontorovich, *On the strong density conjecture for integral Apollonian circle packings*, arXiv:1205.4416v1 (2012).

[14] David W. Boyd, *The sequence of radii of the Apollonian packing*, Math. Comp. **39** (1982), no. 159, 249–254, DOI 10.2307/2007636. MR658230 (83i:52013)

[15] Jing Run 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. MR0434997 (55 #7959)

[16] Giuliana Davidoff, Peter Sarnak, and Alain Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Mathematical Society Student Texts, vol. 55, Cambridge University Press, Cambridge, 2003. MR1989434 (2004f:11001)

[17] J. Elstrodt, F. Grunewald, and J. Mennicke, *Groups acting on hyperbolic space*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1998. Harmonic Analysis and Number Theory. MR1483315 (98g:11058)

[18] Jordan S. Ellenberg, Chris Hall, and Emmanuel Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math. J. **161** (2012), no. 7, 1233–1275, DOI 10.1215/00127094-1593272. MR2922374

[19] E. Fuchs, *A note on the density of Apollonian curvatures in* $\mathbb{Z}$, http://math.berkeley.edu/~efuchs/posdensapollo.pdf (2009).

[20] Elena Fuchs, *Arithmetic properties of Apollonian circle packings*, ProQuest LLC, Ann Arbor, MI, 2010. Thesis (Ph.D.)–Princeton University. MR2941628

[21] Elena Fuchs, *Strong approximation in the Apollonian group*, J. Number Theory **131** (2011), no. 12, 2282–2302, DOI 10.1016/j.jnt.2011.05.010. MR2832824 (2012g:11123)

[22] Elena Fuchs and Katherine Sanden, *Some experiments with integral Apollonian circle packings*, Exp. Math. **20** (2011), no. 4, 380–399, DOI 10.1080/10586458.2011.565255. MR2859897 (2012j:52039)

[23] Alex Gamburd, *On the spectral gap for infinite index "congruence" subgroups of* $\mathrm{SL}_2(\mathbf{Z})$, Israel J. Math. **127** (2002), 157–200, DOI 10.1007/BF02784530. MR1900698 (2003b:11050)

[24] 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** (2005), no. 4, 547–585, DOI 10.1007/s00454-005-1196-9. MR2173929 (2009a:11090a)

[25] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks, and Catherine H. Yan, *Apollonian circle packings: geometry and group theory. II. Super-Apollonian group and integral packings*, Discrete Comput. Geom. **35** (2006), no. 1, 1–36, DOI 10.1007/s00454-005-1195-x. MR2183489 (2009a:11090b)

[26] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks, and Catherine H. Yan, *Apollonian circle packings: geometry and group theory. III. Higher dimensions*, Discrete Comput. Geom. **35** (2006), no. 1, 37–72, DOI 10.1007/s00454-005-1197-8. MR2183490 (2009a:11090c)

[27] Ronald L. Graham, Jeffrey C. Lagarias, Colin L. Mallows, Allan R. Wilks, and Catherine H. Yan, *Apollonian circle packings: number theory*, J. Number Theory **100** (2003), no. 1, 1–45, DOI 10.1016/S0022-314X(03)00015-5. MR1971245 (2004d:11055)

[28] Chris Hall, *Big symplectic or orthogonal monodromy modulo l*, Duke Math. J. **141** (2008), no. 1, 179–203, DOI 10.1215/S0012-7094-08-14115-8. MR2372151 (2008m:11112)

[29] K. E. Hirst, *The Apollonian packing of circles*, J. London Math. Soc. **42** (1967), 281–291. MR0209981 (35 #876)

[30] Shlomo Hoory, Nathan Linial, and Avi Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561 (electronic), DOI 10.1090/S0273-0979-06-01126-8. MR2247919 (2007h:68055)

[31] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967 (German). MR0224703 (37 #302)

[32] Alex Kontorovich and Hee Oh, *Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds*, J. Amer. Math. Soc. **24** (2011), no. 3, 603–648, DOI 10.1090/S0894-0347-2011-00691-7. With an appendix by Oh and Nimish Shah. MR2784325

[33] E. Kowalski, *Sieve in expansion*, Séminaire Bourbaki No. 1028 (2011).

[34] M. Lee and H. Oh, *Effective circle count for Apollonian packings and closed horospheres*, GAFA, to appear (2012).

[35] Alexander Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics, vol. 125, Birkhäuser Verlag, Basel, 1994. With an appendix by Jonathan D. Rogawski. MR1308046 (96g:22018)

[36] G. A. Margulis, *Explicit constructions of expanders*, Problemy Peredači Informacii **9** (1973), no. 4, 71–80 (Russian). MR0484767 (58 #4643)

[37] G. A. Margulis, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica **2** (1982), no. 1, 71–78, DOI 10.1007/BF02579283. MR671147 (83j:05053)

[38] Curtis T. McMullen, *Hausdorff dimension and conformal dynamics. III. Computation of dimension*, Amer. J. Math. **120** (1998), no. 4, 691–721. MR1637951 (2000d:37055)

[39] Z. A. Melzak, *Infinite packings of disks*, Canad. J. Math. **18** (1966), 838–852. MR0203594 (34 #3443)

[40] N. Niedermowwe, *The circle method with weights for the representation of integers by quadratic forms*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **377** (2010), no. Issledovaniya po Teorii Chisel. 10, 91–110, 243, DOI 10.1007/s10958-010-0180-y (English, with English and Russian summaries); English transl., J. Math. Sci. (N.Y.) **171** (2010), no. 6, 753–764. MR2753652 (2012f:11204)

[41] V. V. Nikulin, *Discrete reflection groups in Lobachevsky spaces and algebraic surfaces*, (Berkeley, Calif., 1986), Amer. Math. Soc., Providence, RI, 1987, pp. 654–671. MR934268 (89d:11032)

[42] Hee Oh and Nimish Shah, *The asymptotic distribution of circles in the orbits of Kleinian groups*, Invent. Math. **187** (2012), no. 1, 1–35, DOI 10.1007/s00222-011-0326-7. MR2874933 (2012k:37011)

[43] A. Salehi-Golsefidy, P. Sarnak, *Affine sieve*, arXiv:1109.6432v1 (2011).

[44] Alireza Salehi Golsefidy and Péter P. Varjú, *Expansion in perfect groups*, Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891, DOI 10.1007/s00039-012-0190-7. MR3000503

[45] Peter Sarnak, *Integral Apollonian packings*, Amer. Math. Monthly **118** (2011), no. 4, 291–306, DOI 10.4169/amer.math.monthly.118.04.291. MR2800340 (2012e:52047)

[46] P. Sarnak, *Letter to Lagarias*, http://www.math.princeton.edu/sarnak (2007).

[47] P. Sarnak, *Notes on thin groups*, MSRI Hot Topics Workshop, http://www.msri.org/attachments/workshops/652_Sarnak-notes.pdf (2012).

[48] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute. MR1043865 (91b:11071)

[49] F. Soddy, *The Kiss Precise*, Nature **137** No. 1021 (1936).

[50] I. Vinogradov, *Effective bisector estimate with application to Apollonian circle packings*, Princeton University Thesis (2012).

[51] Boris Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. of Math. (2) **120** (1984), no. 2, 271–315, DOI 10.2307/2006943. MR763908 (86m:20053)

[52] J. B. Wilker, *Inversive geometry*, The geometric vein, Springer, New York, 1981, pp. 379–442. MR661793 (83j:51009)

Department of Mathematics, University of California, Berkeley, California
E-mail address: efuchs@math.berkeley.edu