Arithmetic Properties of Apollonian Circle Packings

Elena Fuchs

ABSTRACT. An Apollonian circle packing (ACP) is an ancient Greek 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 as well, making the packings of great interest from a number theoretic point of view. This point of view has been explored extensively by Graham, Lagarias, Mallows, Wilkes, and Yan as part of a series of papers on ACP's. In this thesis, we use the correspondence between integer ACP's and orbits of a certain Schottky group combined with the recently developed affine linear sieve of Bourgain, Gamburd, and Sarnak to answer many of the questions raised by Graham et.al. in their account.

Acknowledgements

There are many people without whose help and support this thesis would not have been possible. First of all, I would like to thank my adviser, Peter Sarnak, for introducing me to the beautifully simple problem of Apollonian circle packings and the not so simple affine sieve. He has taught me many important lessons not only about mathematics itself, but also about how to do mathematics and will always remain an inspiration and role model to me as I continue my career in mathematics. Besides my adviser, I heartily thank many of the students, faculty, and staff of the Princeton mathematics department for their advice and support, both mathematical and otherwise, during my time as a graduate student.

I would also like to thank Alex Kontorovich, Jeff Lagarias, Alireza Salehi-Golsefidy, and Katherine Sanden for many insightful suggestions and conversations about the work in this thesis. Great thanks to my co-author of the fourth chapter of this thesis, Jean Bourgain.

A warm thank you as always to my wonderful friends and my family Irina, Dmitry, and Katia for their love and support over the last five years.

Contents

The Kiss Precise

For pairs of lips to kiss maybe
Involves no trigonometry.
'Tis not so when four circles kiss
Each one the other three.
To bring this off the four must be
As three in one or one in three.
If one in three, beyond a doubt
Each gets three kisses from without.
If three in one, then is that one
Thrice kissed internally.

Four circles to the kissing come.
The smaller are the benter.
The bend is just the inverse of
The distance from the center.
Though their intrigue left Euclid dumb
There's now no need for rule of thumb.
Since zero bend's a dead straight line
And concave bends have minus sign,
The sum of the squares of all four bends
Is half the square of their sum.

To spy out spherical affairs
An oscular surveyor
Might find the task laborious,
The sphere is much the gayer,
And now besides the pair of pairs
A fifth sphere in the kissing shares.
Yet, signs and zero as before,
For each to kiss the other four
The square of the sum of all five bends
Is thrice the sum of their squares.

– Frederick Soddy, 1936

CHAPTER 1

Introduction

One of the most essential tools in number theory is the theory of automorphic forms and L-functions (see [**45**] and [**31**] for an elegant survey of various applications). For example, several long-standing problems in analytic number theory have been reduced to finding good estimates for Fourier coefficients of automorphic forms, and so, with or without applications in mind, automorphic forms have been studied extensively throughout the past century and are still of great interest today.

One major aspect of these tools is understanding the spectral theory of the Laplace operator Δ on $L^2(\Gamma,\mathbb{H})$, where Γ is classically taken to be a congruence subgroup of $\mathrm{SL}_2(\mathbb{R})$ (more generally one might consider automorphic forms on GL_n over a number field). For example, it is known that the base eigenvalue in the spectrum for such groups is $\lambda_0 = 0$, corresponding to the constant eigenfunction. In the case $\Gamma = \Gamma_0(N)$, the modular group, Selberg's eigenvalue conjecture states that there are no eigenvalues $0 < \lambda < 1/4$, and there are analogs of this conjecture in more general cases as well.

However, in the case that $\Gamma\backslash\mathbb{H}$ has infinite volume (we call Γ *thin* if this is the case) it is unclear how these tools would apply and much less is known. For example, it is no longer true that the base eigenvalue is 0 – in fact, the constant function is no longer square integrable in this situation! Nevertheless, there is a wealth of diophantine problems which can be rephrased precisely in terms of such a group Γ. In this thesis, we approach a particularly beautiful example of this kind of problem and are able to solve several relevant open questions without relying on automorphic forms – rather, certain rich properties of the group in question allow us to make use of the arithmetic analysis recently carried out by Bourgain, Gamburd, and Sarnak in [**7**]. 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.

1. History and setup

Consider four mutually tangent circles, one of them internally tangent to the other three as in the first picture in Fig. 1. One might ask whether there is a unique way to inscribe a circle into each of the curvilinear triangles in this picture. In fact, this uniqueness follows from an ancient theorem of Apollonius of Perga:

THEOREM 1.1. *(Apollonius, circa* 200 BC*): To any three mutually tangent circles or lines there are precisely two other circles or lines which are tangent to all three.*

Apollonius discovered this while attempting the difficult task of constructing mutually tangent circles and straight lines using only a straight edge and compass. Coming back to our picture in Fig. 1, Theorem 1.1 implies that there is a unique circle which can be inscribed into every curvilinear triangle produced by the four mutually tangent circles we have constructed (see the second picture in Fig. 1). We now have 12 new curvilinear triangles, each of which can be filled with a unique inscribed circle again. This process can be continued indefinitely, and the resulting picture is duly called an *Apollonian circle packing* (ACP). Given this process of constructing the packing, we say that the original four circles in the first picture of Fig. 1 are born in the first *generation* of the packing, the new circles in the second picture are born in the second generation, and so on.

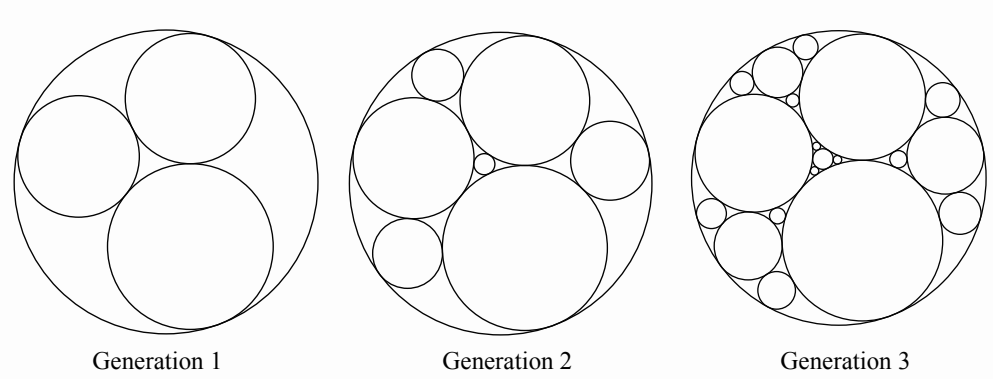

FIGURE 1. Packing Circles

One can study Apollonian circle packings from many different angles – various properties of the packings are investigated in a beautiful series of papers by Graham, Lagarias, Mallows, Wilkes, and Yan (see [**24**], [**21**], [**22**], [**23**]). Such packings are certainly of interest in classical geometry – for example, the process of producing a new circle at generation k is in fact equivalent to reflecting one of the circles born at generation $k-1$ in another circle or straight line (see Section 2.1 for a discussion of this).

We are particularly interested in the number-theoretic questions about ACP's which are addressed extensively by Graham et.al. in [**24**]. To understand how these 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 (equivalently one may consider the radii but these quickly tend to zero, so it is more convenient to work with the curvatures instead). The number theoretic aspect of ACP's traces back to the following theorem due to Descartes, that the curvatures of any four mutually tangent circles in an ACP satisfy a quadratic equation:

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

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

For a proof of this, see [**11**]. 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 Chemistry Nobel Prize Laureate Frederick Soddy rediscovered Theorem 1.2 and expressed it in the form of *The Kiss Precise*, the poem at the beginning of this thesis. He deduced from it that if any Descartes quadruple (a,b,c,d) in an ACP is integral – i.e. $a,b,c,d \in \mathbb{Z}$ – all of the circles in the ACP must in fact have integer curvature. Furthermore, we will see in Section 2.1 that there are infinitely many integer ACP's which makes them particularly interesting from a number-theoretic point of view. One example of an integer ACP is illustrated in Figure 2 – it is the packing generated by starting with circles of curvatures $-1,2,2$, and 3.

This remarkable integrality feature gives rise to several natural questions about integer[1] ACP's – Graham et.al. make some progress towards answering them in [**24**] and make several striking conjectures which we investigate further here. Since each chapter in this thesis addresses a different question from [**24**], we give a brief summary of their content and what is known below. We first recall the notion of a *root quadruple* of an ACP from [**24**] in the following theorem:

THEOREM 1.3. *(Graham, Lagarias, Mallows, Wilkes, Yan, 2003): Define a Descartes quadruple* $\mathbf{v} = (a,b,c,d)$ *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 which yields the root quadruple.*

Essentially, a root quadruple of a packing consists of the four largest circles in the packing and completely defines the ACP in question. For example, the root quadruple of the packing in Fig. 2 is $\mathbf{v} = (-1,2,2,3)$, and it is the only circle packing with this root quadruple. For a detailed discussion of the algorithm for finding the root quadruple of a packing, see [**24**].

With this in mind, our aim is to shed light on the following questions.

1) *What can be said about the residues modulo an integer* $d > 1$ *of the curvatures of circles in a given ACP?*
   Graham et.al. observe by considering subpackings of ACP's that there are always congruence obstructions modulo 12 in any given ACP, and that there are no congruence obstructions modulo $d > 1$ if the greatest common divisor $(d,30) = 1$. Specifically, they show the following regarding possible Descartes quadruples in any integer ACP:

   THEOREM 1.4. *(Graham, Lagarias, Mallows, Wilkes, Yan, 2003): In any primitive integral Apollonian packing, the Descartes quadruples modulo 12 all fall into exactly one of the four possible orbits. The first orbit Y modulo 12 consists of all permutations of*

   $$\{(0,0,1,1),(0,1,1,4),(0,1,4,9),(1,4,4,9),(4,4,9,9)\} \qquad (mod\ 12).$$

   The other three orbits are $(3,3,3,3)-Y$, $(6,6,6,6)+Y$, *and* $(9,9,9,9)-Y$ *modulo 12.*

[1] We consider only *primitive* integer ACP's, or those in which the curvatures share no common factor.

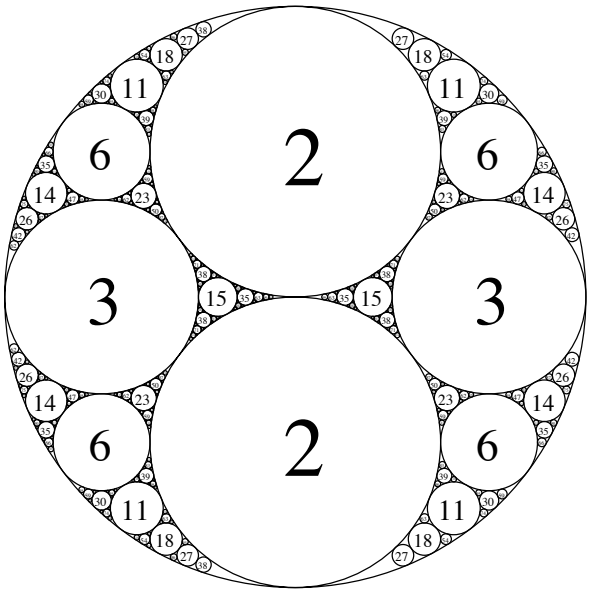

FIGURE 2. The Apollonian circle packing with root quadruple $(-1,2,2,3)$

In their "strong density conjecture," Graham et.al. furthermore predict that any sufficiently large integer satisfying some fixed congruence conditions appears as a curvature in a given ACP. For a detailed discussion of this and convincing data in support of such a local to global conjecture, see [**19**]. While proving this conjecture is seemingly out of reach using what we know today, it is much more feasible to determine which integers *do not* occur as curvatures in an ACP – i.e. what are the congruence obstructions in a given ACP, and how do they depend on the packing in question? Graham et.al. show that there are no congruence obstructions modulo primes $p > 5$ in any integer ACP:

THEOREM 1.5. *(Graham, Lagarias, Mallows, Wilkes, Yan, 2003): Let P be a primitive integral 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 Chapter 2, we further these results and show that the only congruence obstructions for any ACP are modulo 24, and that the 30 in Theorem 1.5 above can be improved to 6. The methods which go into this improvement come from studying ACP's using a convenient representation of the curvatures as maximum-norms of vectors in an orbit of a group A (called the *Apollonian group*), which is a subgroup of the orthogonal group fixing the Descartes form Q. We introduce this group in Section 2.1 and use it throughout. Given this representation of ACP's as orbits of a group, we are able to specify any ACP modulo d by analyzing the mod d structure of the group A. It is worth noting that Graham et.al. prove their theorems by considering only unipotent subgroups of A, while we exploit the full Apollonian group.

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

In studying (primitive) integral ACP's, it is natural to consider which primes appear as curvatures of circles in a given packing. In [**47**] 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, 2007): Let $\mathscr{P}$ denote the orbit of Descartes quadruples corresponding to a primitive integer Apollonian circle packing P, and let*

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

denote the cone of solutions to the Descartes equation in (1.1).

(i) *Let $\pi^P(X)$ denote the number of circles in P of prime curvature less than X. Then*

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

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

(ii) *The set of points $\{\mathbf{x} \in \mathscr{P} \,|\, x_1, x_2$ are prime$\}$ is Zariski dense in C.*

Furthermore, in [**35**] Kontorovich and Oh establish upper bounds for the number $\pi^P(X)$ of circles of curvature less than X in a packing P as well as the number $\pi_2^P(X)$ of pairs of circles both of prime curvature less than X:

THEOREM 1.7. *(Kontorovich, Oh, 2007): Given a primitive integral Apollonian circle packing P,*

(i) $\pi^P(X) \ll \frac{X^\delta}{\log X}$,

(ii) $\pi_2^P(X) \ll \frac{X^\delta}{(\log X)^2}$

where $\delta = 1.3056\ldots$ and the implied constants depend on the packing P.

Note that since Kontorovich and Oh also show that the number of circles in a packing of curvature less than X is asymptotic to $c \cdot X^\delta$ (see Theorem 1.8), the upper bounds above are of the correct order of magnitude. In both of these theorems, the constant δ is in fact the *Hausdorff dimension* of the limit set of the packing P, which is defined to be the smallest positive number so that the series

$$\sum_{C \in P} r(C)^s$$

where C is a circle in the packing P and $r(C)$ is its radius, converges for $s > \delta$. The Hausdorff dimension is the same for every Apollonian circle packing, and has been computed to 5 decimals by McMullen in [**41**].

The proof of Theorem 1.7 relies on the recently developed affine sieve in [**7**]. In [**19**] the results of Chapter 2 are paired with the affine sieve to give a heuristic for precise asymptotics for $\pi^P(X)$ and $\pi_2^P(X)$. In Chapter 3 of this paper, we give a similar heuristic for asymptotics for $\pi_{gen}^P(T)$, the number of circles of prime curvature which are born at generation T.

Another problem we address in Chapter 3 is that of determining the saturation number $r_0(f,\mathscr{P})$, where $\mathscr{P}$ again denotes the set of Descartes quadruples $\mathbf{x} = (x_1,x_2,x_3,x_4)$ in a packing P, and $f(\mathbf{x}) = x_1x_2x_3x_4$ for $\mathbf{x} \in \mathscr{P}$. The *saturation number* in this case is defined to be the smallest positive integer such that the set of points

$$\{\mathbf{x} \in \mathscr{P} \,|\, f(\mathbf{x}) \text{ has at most } r_0 \text{ prime factors}\}$$

is Zariski dense in the cone C in (1.2). Theorem 1.6 states that $r_0 = 2$ if $f(\mathbf{x}) = x_1x_2$. Considering the saturation number in the case of $f(\mathbf{x}) = x_1x_2x_3x_4$ is equivalent to finding Descartes quadruples of circles all of whose curvatures have few prime factors. It is conjectured in [**7**] that the saturation number in this case should be $r_0 = 6$, and the affine sieve guarantees that r_0 is in fact finite. However, we are unable to use it to obtain a good upper bound in the case $f(\mathbf{x}) = x_1x_2x_3x_4$ (we explain this in Chapter 3). Instead, we give a rather crude upper bound of $r_0 \leq 28$ by considering subpackings of ACP's.

3) *Do the integers which come up as curvatures in a given ACP make up a positive fraction of* $\mathbb{N}$*?*

With regard to counting the number of integers represented in a given ACP, Graham et.al. appeal to the existence of unipotent elements in A in [**24**] to establish the lower bound below for the number $\kappa(P,X)$ of distinct curvatures less than X of circles in an integer packing P:

$$\kappa(P,X) \gg \sqrt{X} \tag{1.3}$$

where the notation

$$y \gg_\beta z \text{ or } y \ll_\beta z$$

is taken to mean that there exists a constant $c > 0$ depending only on β such that

$$y \geq cz \text{ or, respectively } y \leq cz.$$

Graham et.al. suggest in [**24**] that the lower bound in (0.29) can be improved. In fact, they conjecture that the integers represented as curvatures in a given ACP actually make up a positive fraction of the positive integers $\mathbb{N}$, and jointly with Jean Bourgain we prove this conjecture in Chapter 4.

It is important to note that this question is different from the one addressed in [**35**] by Kontorovich and Oh about the number $N_P(X)$ of circles in a given packing P of curvature less than X. This involves counting curvatures appearing in a packing with multiplicity, rather than counting every integer which comes up exactly once as we do in Chapter 4 of this thesis. In fact, the results in [**35**] suggest that the integers occurring as curvatures in a given ACP arise with significant multiplicity. Specifically, Kontorovich and Oh prove the following:

THEOREM 1.8. *(Kontorovich, Oh, 2007): Let $N_P(X)$ be the number of circles of curvature less than X in an Apollonian packing P. Then*

$$N_P(X) \sim c_P \cdot X^\delta,$$

where $\delta = 1.3056\ldots$ is the Hausdorff dimension of the limit set of the packing and c_P is a constant depending on P.

Kontorovich and Oh's techniques, however, do not extend in any obvious way to proving that the integers represented by curvatures in an ACP make up a positive fraction in $\mathbb{N}$.

A more fruitful method for this problem is to consider arithmetic Fuchsian subgroups of A. In [**47**] Sarnak uses these subgroups to get a bound of

$$\kappa(P,X) \gg_P \frac{X}{\sqrt{\log X}} \tag{1.4}$$

towards Graham et.al.'s positive density conjecture. This method, which we summarize in Section 1, was further improved to yield a bound of

$$\kappa(P,X) \gg_P \frac{X}{(\log X)^{\varepsilon}}$$

where $\varepsilon = 0.150\ldots$ in a preprint [**18**].

Jointly with J. Bourgain, we refine this Fuchsian subgroup method in a number of ways to settle the positive density question of Graham et.al. and show

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

where the implied constant depends on the packing P.

In order to address any of these questions, we rely on the expression of ACP's as orbits of a subgroup of the orthogonal group $\mathrm{O}_Q(\mathbb{Z})$ fixing the Descartes form Q. We introduce this group in the following section.

2. The Apollonian group

Recall from Theorem 1.2 that if a,b,c, and d are curvatures of four mutually tangent circles,

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

and that in the context of ACP's the outside circle in a bounded packing (which is internally tangent to the other circles) must have negative curvature to satisfy the equation. Note that fixing three of the curvatures (say b,c,d) above yields a quadratic equation which has two solutions $a = a_+, a_-$ such that

$$a_+ + a_- = 2(b+c+d).$$

In fact, the circles C_{a_+} and C_{a_-} of curvatures a_+ and a_-, respectively, are precisely the two circles tangent to all three of the mutually tangent circles of curvature b,c, and d in Theorem 1.1. Thus if $\mathbf{v} = (a,b,c,d)^{\mathrm{T}}$ is a vector of curvatures of mutually tangent circles in a packing P, all of the curvatures of circles in P are given by the coordinates of vectors in the orbit $A\mathbf{v}$, where A is a group given by the

four generators

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{2.1}$$

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

Since its orbits are in one-to-one correspondence with Apollonian circle packings, A is known as the Apollonian group. Note that $S_i^2 = I$ for $1 \leq i \leq 4$, and one can deduce that there are no other relations among the generators of A by considering their geometric representation below.

Specifically, the generators of A can be realized as reflections in dual circles of the packing P. Four such dual circles are drawn in dotted lines for the first generation of a circle packing in Fig. 3. The shaded circle on the inside is the image of the outside circle under reflection through the smallest of the dual circles. Throughout this thesis, the Apollonian group will be our main tool in analyzing ACP's,

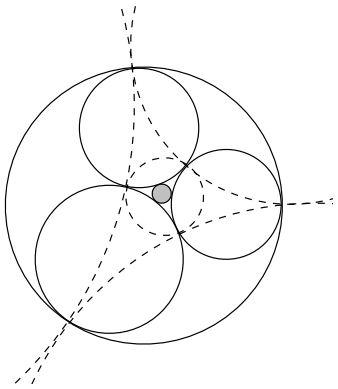

FIGURE 3. Dual circles in an Apollonian circle packing

and we list some of its properties in the following lemma:

LEMMA 2.1. *Let A be the Apollonian group and let Q be the Descartes quadratic form. Then*

(i) *A is an infinite-index subgroup of the orthogonal group $\mathrm{O}_Q(\mathbb{Z})$ fixing Q,*
(ii) *A is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$.*

Since the Descartes form Q has signature $(3,1)$ over $\mathbb{R}$, the group A is a subgroup of $\mathrm{O}_{\mathbb{R}}(3,1) \cong \mathrm{SL}_2(\mathbb{C})$, the isometry group of hyperbolic space $\mathbb{H}^3$. The generators S_i in this context are reflections through the hemispheres above the dual circles in Fig. 3, and the fundamental domain of the action of A on $\mathbb{H}^3$ is the complement of three mutually tangent hemispheres inside an infinite cylinder. This fundamental domain has infinite volume, and so A is an infinite-index subgroup of the orthogonal group

$O_Q(\mathbb{Z})$ as stated in part (i) of Lemma 2.1. In this sense, the Apollonian group is a thin group, and this makes integral ACP's virtually unapproachable via classical methods such as the theory of automorphic forms. However, the richness of the group implied by part (ii) of the lemma is precisely the necessary condition for the analysis in [**7**] and [**52**] to apply in this case. We prove part (ii) below.

PROOF. The Zariski closure G of the Apollonian group A is an algebraic group defined over $\mathbb{R}$, where $G(\mathbb{R})$ is a Lie subgroup of $\mathrm{SL}_2(\mathbb{C})$. Therefore G could be either the full orthogonal group or one of the following:

- A finite group: since A itself is not finite (for example, the unipotent element S_1S_2 has infinite order), its closure cannot be finite.
- The group SO_Q : since the generators of A all have determinant -1, this cannot be the closure of A.
- A torus or parabolic subgroup: Let A' be the Zariski closure of A consider an orbit $\mathscr{P}' = A'\mathbf{v}$ of A'. By Theorem 1.8 we have

$$\#\{\mathbf{x} \in \mathscr{P} \mid ||\mathbf{x}||_{max} \leq X\} \gg c \cdot X^{1.3056\ldots}.$$

  However, this count for a parabolic or a torus subgroup is bounded above by $c \cdot X$. Therefore A' cannot be parabolic or toral.
- The orthogonal group fixing the ternary quadratic form Q' of signature $(2,1)$ over $\mathbb{R}$ obtained by fixing one of the x_i in (1.1). As before, Theorem 1.8 implies that

$$\#\{\mathbf{x} \in \mathscr{P} \mid ||\mathbf{x}||_{max} \leq X\} \gg c \cdot X^{1.3056\ldots},$$

  but for an orthogonal group fixing a form in three variables this count is again bounded above by $c \cdot X$.

Since the Zariski closure of A is none of the above groups, it must be the full orthogonal group, and so A is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$. □

It is precisely the fact that A is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$ that makes its orbits suitable for the affine sieve described in [**7**]. In Chapter 2, we use this to deduce the mod d structure of the orbits of A which is crucial to the sieve on the orbits of A in Chapter 3.

CHAPTER 2

Congruence Obstructions

In this chapter we determine the reduction of any integer orbit $A\mathbf{v}$ of the Apollonian group modulo integers $d > 1$. This analysis is central to understanding the arithmetic of ACP's. For example, many diophantine problems over orbits of Zariski dense subgroups of the orthogonal group can be handled using the affine sieve as described in [**7**] (see [**19**] for a concrete application of the sieve to integer ACP's). To execute such a sieve one needs to know the structure of the orbit modulo d – in particular it is important that the orbit possesses a strong approximation property, or the analog of the Chinese Remainder Theorem over the integers. A theorem of Weisfeiler (see Theorem 0.2) implies that such a strong approximation principle can be specified given Lemma 2.1, and we do this in the following sections.

We first consider the reduction of the Apollonian group modulo square free d. For this it is convenient to work with the preimage of A in the spin double cover of SO_Q rather than the Apollonian group itself. The main reason for this is that A is a subgroup of the orthogonal group $\mathrm{O}_{\mathbb{R}}(3,1)$ where strong approximation does not hold, and it is difficult to say anything about the projection of A into $\mathrm{O}_Q(\mathbb{Z}/p\mathbb{Z})$ by working in the orthogonal group alone. However, the preimage Γ of A under the *spin homomorphism* in (1.1) is a Zariski dense subgroup of $\mathrm{SL}_2(\mathbb{C})$ where general results regarding strong approximation are known. Specifically, Weisfeiler proves the following in [**52**]:

THEOREM 0.2. *(Weisfeiler, 1984): Let $\mathscr{O}$ be the ring of integers of a number field k, let V be the set of non-archimedean non-equivalent valuations of k, and let k_v denote the completion of k at a valuation $v \in V$. Let Γ be a Zariski dense subgroup of an absolutely almost simple, simply connected algebraic group G over k so that the subfield of k generated by 1 and the traces of $Ad\,\Gamma$ is k itself. Then there exists a finite subset $S \subset V$ such that the closure of Γ in $G(\prod_{v\notin S} k_v)$ is open.*

In the context of integer ACP's, the field k in Theorem 0.2 is $\mathbb{Q}(\sqrt{-1})$, the ring of integers $\mathscr{O} = \mathbb{Z}(\sqrt{-1})$, and Γ is a Zariski dense subgroup of $G = \mathrm{SL}_2(k')$ where $k' = \mathbb{C}$ is the algebraic closure of k. For this case Weisfeiler's theorem implies that there is a finite set of primes $\mathfrak{P}$ in $\mathscr{O}$, so that Γ projects onto $\mathrm{SL}_2(\mathbb{Z}(\sqrt{-1})/\mathfrak{p})$ for $\mathfrak{p} \notin \mathfrak{P}$. This is precisely what we need to specify the structure of the Apollonian group modulo p. In the following sections we will make this statement more precise for our case and apply it in the context of orbits of A.

1. The preimage Γ of A in $\mathbf{SL}_2(\mathbb{C})$

Since strong approximation does not hold in $\mathrm{O}_Q(\mathbb{Z})$, we consider the mod $\mathfrak{p}$ reduction of the preimage Γ of $A \cap \mathrm{SO}_Q(\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{C})$ under the spin homomorphism ρ. Since strong approximation does hold in SL_2, it is the natural setting in which to ask this question – we then map back to A via the spin homomorphism in order to complete the analysis of the orbits.

We recall from [**15**] that there is a 2-to-1 homomorphism ρ defined over $\mathbb{Q}$ from $\mathrm{SL}_2(\mathbb{C})$ into the special orthogonal group SO fixing a quadratic form $\tilde{Q}$:

$$\mathrm{SL}_2 \xrightarrow{\rho} \mathrm{SO}_{\tilde{Q}}, \tag{1.1}$$

The homomorphism ρ is defined explicitly in [**15**] for M in $\mathrm{SL}_2(\mathbb{C})$[2]:

$$\text{For } M = \begin{pmatrix} a_0 + a_1\sqrt{\text{-}1} & b_0 + b_1\sqrt{\text{-}1} \\ c_0 + c_1\sqrt{\text{-}1} & d_0 + d_1\sqrt{\text{-}1} \end{pmatrix}, \tag{1.2}$$

we have that $\rho(M)$ is

$$\begin{pmatrix} \frac{a_0^2+b_0^2+c_0^2+d_0^2+a_1^2+b_1^2+c_1^2+d_1^2}{2} & \frac{-a_0^2+b_0^2-c_0^2+d_0^2-a_1^2+b_1^2-c_1^2+d_1^2}{2} & -a_0b_0-d_0c_0-a_1b_1-c_1d_1 & -a_0b_1+d_0c_1+a_1b_0-d_1c_0 \\ \frac{-a_0^2-b_0^2+c_0^2+d_0^2-a_1^2-b_1^2+c_1^2+d_1^2}{2} & \frac{a_0^2-b_0^2-c_0^2+d_0^2+a_1^2-b_1^2-c_1^2+d_1^2}{2} & a_0b_0-d_0c_0+a_1b_1-c_1d_1 & a_0b_1+d_0c_1-a_1b_0-d_1c_0 \\ -a_0c_0-d_0b_0-a_1c_1-b_1d_1 & a_0c_0-d_0b_0+a_1c_1-b_1d_1 & a_0d_0+c_0b_0+b_1c_1+a_1d_1 & a_0d_1-d_0a_1-c_1b_0+b_1c_0 \\ a_0c_1-d_0b_1-a_1c_0+b_0d_1 & -a_0c_1-d_0b_1+a_1c_0+b_0d_1 & -a_0d_1+a_1d_0-b_0c_1+b_1c_0 & a_0d_0-b_0c_0+a_1d_1-b_1c_1 \end{pmatrix}.$$

In order to determine the preimage of $A \cap \mathrm{SO}_Q$, we rewrite the Descartes form in a suitable way as follows.

LEMMA 1.1. *Let Q be the Descartes quadratic form as before, and let*

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

Then the orthogonal group $O_Q(\mathbb{Z}[\frac{1}{2}])$ preserving Q is isomorphic to $O_{\tilde{Q}}(\mathbb{Z}[\frac{1}{2}])$ preserving $\tilde{Q}$. Under this isomorphism, the Apollonian group $A \subset O_Q(\mathbb{Z})$ is mapped to a group $A' \subset O_{\tilde{Q}}(\mathbb{Z})$.

PROOF. Let Q' be the form $Q'(x_1,x_2,x_3,x_4) = -4x_1^2 + 4x_2^2 + 4x_3^2 + 4x_4^2$, with determinant $d = -16$. It is equivalent to the Descartes form Q, since $Q' = C^T Q C$, where

$$C = \begin{pmatrix} 1 & 0 & \text{-}1 & 1 \\ 1 & 0 & \text{-}1 & \text{-}1 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & \text{-}1 & 0 \end{pmatrix}. \tag{1.3}$$

The group $O_{Q'}(\mathbb{Z}[\frac{1}{2}])$ fixing Q' is isomorphic to the group $O_{\tilde{Q}}(\mathbb{Z}[\frac{1}{2}])$, where

$$\tilde{Q}(x_1,x_2,x_3,x_4) = x_1^2 - x_2^2 - x_3^2 - x_4^2. \tag{1.4}$$

[2]There is a small typo in the formula printed in [**15**]. It is corrected here.

Since every element in A is congruent to the identity modulo 2, we have that $A \subset \mathrm{O}_Q(\mathbb{Z})$ is mapped to a group $A' \subset \mathrm{O}_{\tilde{Q}}(\mathbb{Z})$ as desired. □

The Apollonian group A is thus isomorphic to a subgroup of $\mathrm{O}_{\tilde{Q}}(\mathbb{Z})$ which we denote by A'. We denote the isomorphism by s:

$$A' \xrightarrow{s} A \tag{1.5}$$

and relate A' to $\mathrm{SL}_2(\mathbb{Z}(i))$ via the homomorphism ρ in 1.1. Specifically, we get

$$\rho(\mathrm{SL}_2(\mathbb{Z}(i))) = A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$$

where the intersection $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ consists of elements of A' with positive determinant. It is known (see [**15**]) that ρ is in fact a surjection from $\mathrm{SL}_2(\mathbb{Z}(i))$ onto $\mathrm{SO}^+_{\tilde{Q}}(\mathbb{Z})$, a subgroup of index 2 in $\mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ consisting precisely of matrices of $\mathrm{SO}_{\tilde{Q}}$ with a positive entry in the upper left corner. It is easy to check that every element of $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$ is in $\mathrm{SO}^+_{\tilde{Q}}$, so we think of ρ as a homomorphism from Γ onto $A' \cap \mathrm{SO}_{\tilde{Q}}(\mathbb{Z})$. Similarly, we have an onto homomorphism from Γ to $A \cap \mathrm{SO}_Q(\mathbb{Z})$ via the isomorphism s:

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

so by considering Γ we simultaneously consider the Apollonian group A as well. The explicit formula for ρ in 1.1 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 and their inverses, where S_i are the generators of A defined in (4.9) allows us to determine exactly the generators and relations of Γ. We describe this in the following lemma.

LEMMA 1.2. *Let Γ be as before. It is a free group generated by $\pm\gamma_1, \pm\gamma_2, \pm\gamma_3$ and their inverses, where γ_i are as below.*

$$\gamma_1 = \begin{pmatrix} 2 & -i \\ -i & 0 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} -2-2i & -4-3i \\ i & 2i \end{pmatrix}, \quad \gamma_3 = \begin{pmatrix} 1 & -4i \\ 0 & 1 \end{pmatrix}. \tag{1.6}$$

This follows from applying the homomorphism ρ together with the map s to the generators. Note that this group is a free subgroup of SL_2 – since the elements S_1S_2, S_2S_3, and S_2S_4 have no relations in A, the same holds for the elements $\gamma_i \in \Gamma$. In the next section we use Lemma 1.2 to determine the reduction of Γ modulo ideals (d) where d is square free. 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 (1.5) is defined over $\mathbb{Z}(1/2)$. We deal with this separately in Section 4.

2. The reduction of Γ modulo square free (d)

Recall from Lemma 2.1 that A is Zariski dense in O_Q, we have $A \cap \mathrm{SO}_Q$ is Zariski dense in SO_Q, and so the group Γ is also Zariski dense in SL_2. We can also check that the subfield of $k = \mathbb{Q}(\sqrt{-1})$

generated by 1 and the traces of the group Γ is in fact the whole field k. For example, the trace of

$$\gamma_1\gamma_2\gamma_3 = \begin{pmatrix} \text{-3-4}i & \text{-22}+6i \\ 2i\text{-2} & 12i+5 \end{pmatrix} \tag{2.1}$$

is $2+8i$, and the field generated by this trace and 1 is indeed all of k. Thus by Theorem 0.2 we have that outside a finite set of prime ideals $\mathfrak{P} \subset \mathbb{Z}(\sqrt{\text{-1}})$ the projection of Γ into $\mathrm{SL}_2/\mathfrak{p}$ is surjective for $\mathfrak{p} \notin \mathfrak{P}$. Our goal is to specify this set $\mathfrak{P}$ and thus determine what the reduction of Γ is modulo arbitrary square free d. Given the generators of Γ as well as Theorem 0.2, this is a question of elementary group theory. We use a classification due to L.E. Dickson (Theorem 8.27 in [**29**]) of subgroups of PSL_2 over finite fields:

LEMMA 2.1. *(Dickson, 1901): Let q be a power of a prime $p \geq 5$. Then the following are the only possible proper subgroups of* $\mathrm{PSL}_2(\mathbb{F}_q)$.

(1) *Elementary abelian p-groups;*
(2) *Cyclic groups of order z where* $z|\frac{q\pm1}{2}$*;*
(3) *Dihedral groups of order* $q\pm1$ *and their subgroups;*
(4) *Semidirect products of elementary abelian groups of order* p^r *and cyclic groups of order t where* $t|p^r-1$ *and* $t|q-1$*;*
(5) A_4*,* S_4*, or* A_5*;*
(6) $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ *where* $p^r|q$.

For q prime, the proper subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ given by Lemma 2.1 are metabelian except for the groups of small order in (5) (see [**12**] for a proof). This is also true for proper subgroups of $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ which properly contain $PSL_2(\mathbb{F}_p)$ for p prime. We use this classification to prove the following proposition regarding the reduction of Γ modulo square free d.

PROPOSITION 2.2. *Let Γ and $\mathcal{O}$ be as before, let $\mathfrak{p}$ denote a prime ideal in $\mathcal{O}$, and let (d) denote an ideal generated by $d \in \mathcal{O}$. Denote by $\mathfrak{P}$ the set of prime ideals in $\mathcal{O}$ containing (6). Let $d>1$ be a square free integer such that $d = d_1c$, where $c|6$ and $gcd(d_1,6)=1$, we have*

$$\Gamma \hookrightarrow \Gamma_c \times \mathrm{SL}_2(\mathcal{O}/(d_1)) \tag{2.2}$$

where Γ_c is the image of Γ in $\mathrm{SL}_2(\mathcal{O}/(c))$, and Γ maps as a product group onto the second factor. Thus the reduction of Γ modulo any prime $\mathfrak{p} \notin \mathfrak{P}$ is onto $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$.

PROOF. We first consider the reduction of Γ modulo prime ideals $\mathfrak{p} \in \mathcal{O}$ and then show that Γ maps as a product group onto the second factor in (2.2). We split this up into three cases:

(1) $\mathfrak{p}^2 = (2)$;
(2) $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ where $p \equiv 1 \ (\mathrm{m}od\ 4)$; here p splits in $\mathcal{O}$, and -1 is a square mod p, so the reduction of Γ modulo (p) is mapped to $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$;

(3) $\mathfrak{p} = (p)$ where $p \equiv 3 \pmod 4$; here p does not split in $\mathscr{O}$, and -1 is not a square mod p, so the reduction of Γ modulo (p) is mapped to $\mathrm{SL}_2(\mathbb{F}_{p^2})$.

Case 1:

Reducing Γ modulo (2) yields a group of order 2, which is clearly not all of $\mathrm{SL}_2(\mathscr{O}/(2))$. Another unpleasant feature of 2 in this context is that it is the only prime which ramifies in $\mathbb{Q}(i)$, since $(2) = (1+i)^2$. We handle the other two cases separately, and note that we will not need to worry about ramification in $\mathbb{Q}(i)$ there.

Case 2:

Let $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\overline{\mathfrak{p}}$ is the conjugate of the prime ideal $\mathfrak{p}$ in $\mathscr{O}$. We want to show that Γ reduces onto each factor of $\mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\overline{\mathfrak{p}})$ by first noting that both of these factors are isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ (we immediately note that the image of Γ in each factor is not trivial – for example, none of the generators of Γ reduce to the identity I modulo $\mathfrak{p} \not\supset (2)$). We prove this for $\Gamma_{\mathfrak{p}}$, the reduction of Γ modulo $\mathfrak{p}$. The proof in the case of reduction modulo $\overline{\mathfrak{p}}$ is then the same argument applied to the conjugate of Γ.

Note that $\Gamma \supset Z(\mathrm{SL}_2)$ contains the center of SL_2 and consider $\Gamma' = \Gamma/Z \subseteq \mathrm{PSL}_2(\mathbb{C})$. If the reduction $\Gamma'_{\mathfrak{p}}$ of Γ' modulo $\mathfrak{p}$ 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. We follow [**20**] to show that this would violate a girth bound for $\Gamma'_{\mathfrak{p}}$ for large enough primes $p = \mathfrak{p}\overline{\mathfrak{p}}$.

Let $S = \{\gamma_1, \gamma_1^{-1}, \gamma_2, \gamma_2^{-1}, \gamma_3, \gamma_3^{-1}\}_{\mathfrak{p}}$ be the set of generators of $\Gamma'_{\mathfrak{p}}$. For example, the generators of $\Gamma'_{(2+i)}$ are

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

Consider the Cayley graph $C(\Gamma_{\mathfrak{p}}, S)$, where the vertices correspond to elements of $\Gamma_{\mathfrak{p}}$, and two vertices v, w are connected by an edge iff $v = \gamma w$ for some $\gamma \in S$. Define the *girth* $c(\Gamma_{\mathfrak{p}})$ of $C(\Gamma_{\mathfrak{p}}, S)$ to be the length of the shortest cycle in $C(\Gamma_{\mathfrak{p}}, S)$. From [**40**] we have that

$$c(\Gamma_{\mathfrak{p}}) \geq 2\log_{\alpha}(p/2) - 1 \tag{2.3}$$

where

$$\alpha := \max_i(||\gamma_i||).$$

Here we define the norm of a matrix γ as follows:

$$||\gamma|| := \sup_{\mathbf{x} \neq \mathbf{0}} \frac{||\gamma \mathbf{x}||}{||\mathbf{x}||}$$

and recall that

$$||\gamma||^2 = ||\gamma^* \gamma||$$

where γ^* is the conjugate transpose of γ, and the norm of $\gamma^*\gamma$ is its largest eigenvalue. Using this we compute that in our case

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

Thus for $\mathfrak{p}\overline{\mathfrak{p}} = p$ large enough, $\Gamma'_{\mathfrak{p}}$ cannot be A_4, S_4, or A_5 since these groups contain elements of small order which violate the girth bound in (2.3). So if $\Gamma'_{\mathfrak{p}}$ is a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$, it must be metabelian – i.e., for any $A,B,C,D \in \Gamma_{\mathfrak{p}}$ we have

$$[[A,B],[C,D]] := (ABA^{-1}B^{-1})(CDC^{-1}D^{-1})(BAB^{-1}A^{-1})(DCD^{-1}C^{-1}) = I \tag{2.4}$$

However, this yields a cycle of length 16 which also violates the girth bound for primes $p > 2.57 \cdot 10^7$, and so $\Gamma'_{\mathfrak{p}} = \mathrm{PSL}_2(\mathbb{F}_p)$ for large enough primes p.

We are left with a finite number of cases which we handle using a program in Matlab. We check that taking $A = \gamma_1, B = \gamma_2, C = \gamma_3$, and $D = \gamma_1\gamma_2\gamma_3$ where γ_i are as in (1.6) we have

$$[[A,B],[C,D]] \neq I \tag{2.5}$$

in $\mathrm{PSL}_2(\mathbb{F}_p)$ for $2 < p < 2.57 \cdot 10^7$, and thus Γ'_p is not metabelian in these cases. Similarly we check that for $p > 3$ we have $\left|\Gamma'_{\mathfrak{p}}\right| > 60$, and so $\Gamma_{\mathfrak{p}} \neq A_4, A_5$, or S_4. Thus $\Gamma'_{\mathfrak{p}} = \mathrm{PSL}_2(\mathbb{F}_p)$ for all primes in this case. Since no proper subgroup of SL_2 maps onto PSL_2 (see [**49**] for a proof), we have that Γ maps onto $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ and $\mathrm{SL}_2(\mathcal{O}/\overline{\mathfrak{p}})$ as desired.

Case 3:

In this case $\mathfrak{p} = (p)$ where $p \equiv 3 \pmod 4$ and we want to show that the reduction $\Gamma_p = \Gamma_{\mathfrak{p}}$ of Γ modulo $\mathfrak{p}$ is onto $\mathrm{SL}_2(\mathbb{F}_{p^2})$. Note $\Gamma_p \not\subset \mathrm{SL}_2(\mathbb{F}_p)$ – for example if γ_1/p is the generator γ_1 in Γ_p, we have $\gamma_1/p \notin \mathrm{SL}_2(\mathbb{F}_p)$ for any prime $p \equiv 3 \pmod 4$.

Again, consider $\Gamma' = \Gamma/Z$ as in Case 2. Since Γ'_p properly contains $\mathrm{PSL}_2(\mathbb{F}_p)$, it is a proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ iff it is one of the groups in parts (1) - (5) of Lemma 2.1 and is thus either metabelian or one of the groups A_4, A_5, or S_4.

The girth bounds calculated in Case 2 again imply that Γ'_p cannot be metabelian for

$$p > 2.57 \cdot 10^7$$

Similarly, $\Gamma'_p \neq A_4, A_5$,or S_5 for p in this range, and so $\Gamma'_p = \mathrm{PSL}_2(\mathbb{F}_{p^2})$ for large enough p. As in Case 2, we check that if $A = \gamma_1, B = \gamma_2, C = \gamma_3$, and $D = \gamma_1\gamma_2\gamma_3$,

$$[[A,B],[C,D]] \neq I$$

in Γ_p for $p \geq 3$, and that $|\Gamma_p| > 120$ for $p > 3$. We also check that for $p > 3$ we have $|\Gamma_p| > 120$ and so $|\Gamma'_p| > 60$. Thus Γ maps onto $\mathrm{SL}_2(\mathbb{F}_{p^2})$ for $p > 3$.

If $p = 3$, however, $\Gamma'_p = \mathrm{A}_5$ and so Γ_p is not the full $\mathrm{SL}_2(\mathbb{F}_9)$.

It remains to show that Γ maps as a product group onto the second factor in $\Gamma_c \times \mathrm{SL}_2(\mathcal{O}/(d_1))$. For this we need the following lemma.

LEMMA 2.3. *(Goursat): Let G, G' be groups, and let H be a subgroup of $G \times G'$ such that the two projections $\pi_1 : H \to G$ and $\pi_2 : H \to G'$ are surjective. Let N be the kernel of π_1, and let N' be the kernel of π_2. Then the image of H in $G/N \times G'/N'$ is the graph of an isomorphism $G/N \cong G'/N'$.*

We have shown above that Γ maps onto $\mathrm{SL}_2(\mathbb{F}_{q^2})$ where $q > 3$ is a prime congruent to 3 mod 4, and onto $\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$ where p is a prime congruent to 1 mod 4. To verify the product structure of $\Gamma/(d_1)$ in Proposition 2.2, we prove the following two lemmas.

LEMMA 2.4. *Let Γ, d, c, and d_1 be as in Proposition 2.2, let p denote a prime such that $p \equiv 1\,(4)$, and let $q > 3$ denote a prime such that $q \equiv 3\,(4)$. Write $d_1 = \prod_{p|d_1} p \prod_{q|d_1} q$, and let*

$$H_q = \mathrm{SL}_2(\mathbb{F}_{q^2}), \quad G_q = \mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p).$$

Then the projection

$$\Gamma_{(d)} \longrightarrow \Gamma_{(c)} \times \Gamma_{(d_1)}$$

is surjective onto each factor, and the diagonal projection

$$\Gamma_{(d_1)} \longrightarrow \prod_{q|d_1} H_q \times \prod_{p|d_1} G_p \tag{2.6}$$

is surjective onto each factor.

The centers $Z(H_q)$ and $Z(G_p)$ are finite, and the factor groups $H_q/Z(H_q)$ and $G_p/Z(G_p)$ are of the form $\mathrm{PSL}_2(\mathbb{F}_p)$ which is simple for $p > 4$, so its composition factors consist of itself and the trivial group. Therefore H_q and G_p have no composition factors in common for large enough primes p and q, so Lemma 2.3 immediately implies Lemma 2.4. However, since every prime ideal (p) in the product in 2.6 splits, we have that $p = \mathfrak{p}\bar{\mathfrak{p}}$ and we must still show that every G_p maps as a product onto its two factors as in the next lemma.

LEMMA 2.5. *Let $\mathscr{O}$ and G_p be as before, where $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p}$ is a prime ideal in $\mathscr{O}$. Then the diagonal projection*

$$G_p \longrightarrow \mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}}) \tag{2.7}$$

is surjective onto each factor.

PROOF. In this case, Lemma 2.3 is not immediately applicable as it was in the proof of Lemma 2.4 since it is not the case that the groups in 2.7 have no composition factors in common. Suppose G_p does not map as a product group onto $\mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$. Then by Lemma 2.3 the projection of G_p onto each factor is an isomorphism. In this case, we can write

$$G_p = \{(x, f(x)) \mid x \in \mathrm{SL}_2(\mathscr{O}/\mathfrak{p})\},$$

where f is an isomorphism from $\mathrm{PSL}_2(\mathscr{O}/\mathfrak{p})$ to $\mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$. So identifying each of the factors of G_p with the group $H = \mathrm{SL}_2(\mathbb{F}_p)$, every element of G_p is of the form $(x, \phi(x))$, where $x \in H$, and ϕ is an

automorphism of H. Since all automorphisms of H are inner, ϕ preserves the trace for every $x \in H$:

$$\mathrm{Tr}(\phi(x)) = \mathrm{Tr}(x) \text{ for all } x \in H.$$

However, we find an element in G_p whose trace is not in $\mathbb{Q}$, and so the element's trace in the first factor is not the same as its trace in the second factor for any $\mathfrak{p}$:

$$\begin{pmatrix} -3-4i & -22+6i \\ 2i-2 & 12i+5 \end{pmatrix}, \tag{2.8}$$

so we have a contradiction, and thus G_p maps as a product onto $\mathrm{SL}_2(\mathscr{O}/\mathfrak{p}) \times \mathrm{SL}_2(\mathscr{O}/\bar{\mathfrak{p}})$ as desired. □

Proposition 2.2 follows from Lemma 2.4, Lemma 2.5, and our case analysis above. □

Proposition 2.2 gives us a concrete description the reduction modulo square free d of the Apollonian group itself via the spin-homomorphism ρ. It is desirable, however, to understand the structure of A and its orbit under reduction modulo any d. To this end we specify the reduction of Γ modulo powers of prime ideals $\mathfrak{p}^i$ in the next section and prove a concrete strong approximation theorem for the Apollonian group.

3. The reduction of Γ modulo any ideal (d)

In Section 2 we proved that Γ has a multiplicative structure under reduction modulo square free ideals (d) outside a finite set of primes. In this section, we extend this multiplicativity to reduction modulo *any* (d) by considering the image of Γ modulo powers of primes $\mathfrak{p}$. An essential tool in this consideration is a generalization of the following we recall a lemma of J.P. Serre (see [**49**] for a proof).

LEMMA 3.1. *(Serre, 1968): Let p be a prime greater than 3. If X is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ whose image in $\mathrm{SL}_2(\mathbb{F}_p)$ is $\mathrm{SL}_2(\mathbb{F}_p)$, we have $X = \mathrm{SL}_2(\mathbb{Z}_p)$.*

We extend this lemma to apply in the situation of $\Gamma \subset \mathrm{SL}_2(\mathbb{C})$ below.

LEMMA 3.2. *Let $\mathscr{O}$ be the ring of integers in $\mathbb{Q}(i)$ as before. Let $\mathfrak{q} \neq (1+i)$ or (3) be a prime ideal in $\mathscr{O}$ and let $\mathscr{O}_\mathfrak{q}$ denote the completion of $\mathscr{O}$ at $\mathfrak{q}$. Let G be a closed subgroup of $\mathrm{SL}_2(\mathscr{O}_\mathfrak{q})$. If the projection of G into $\mathrm{SL}_2(\mathscr{O}_\mathfrak{q}/\mathfrak{q})$ is surjective, then $G = \mathrm{SL}_2(\mathscr{O}_\mathfrak{q})$.*

The proof of this follows the same argument as the proof of Lemma 3.1 in [**49**] – we outline a modification of it in the special case of reduction modulo powers of (2) below. Since the projection of Γ into $\mathrm{SL}_2(\mathscr{O}_\mathfrak{q}/\mathfrak{q})$ is surjective for all but finitely many primes $\mathfrak{q}$ by Proposition 2.2 we may use the result in Lemma 3.2 to determine the reduction of Γ modulo powers of $\mathfrak{q}$. We first handle the reduction modulo powers of prime ideals $\mathfrak{q}$ contained in the ideals (2) and (3) in the following lemma and obtain the complete picture in Theorem 3.5.

LEMMA 3.3. *Let Γ and $\mathscr{O}$ be as before. Let $K_n(2)$ denote the kernel of the projection of $SL_2(\mathscr{O}/(2^n))$ onto $\mathrm{SL}_2(\mathscr{O}/(2^{n-1}))$, and let $K_n(3)$ denote the kernel of the projection of $\mathrm{SL}_2(\mathscr{O}/(3^n))$ onto $\mathrm{SL}_2(\mathscr{O}/(3^{n-1}))$. Denoting the reduction of Γ modulo (d) by Γ_d, we have*

(i) $\Gamma_2 = D_1$, *the dihedral group containing 2 elements.*
(ii) Γ_4 *is an abelian group of 8 elements.*
(iii) *Let τ_n denote the projection of Γ_{2^n} onto $\Gamma_{2^{n-1}}$. The kernel of this projection is $K_n(2)$ for $n \geq 4$.*
(iv) $\Gamma_3/Z(\Gamma_3) = A_5$.
(v) *Let σ_n denote the projection of Γ_{3^n} onto $\Gamma_{3^{n-1}}$. The kernel of this projection is $K_n(3)$ for $n \geq 2$.*

PROOF. The images of Γ modulo (2) and (4) are seen trivially from the generators of Γ, while the image under reduction modulo (3) can be deduced from Lemma 2.1.

The number of elements in the kernels of τ_3 and τ_4 can be computed using a simple program in Matlab, and we obtain

$$|\{\gamma \in \Gamma_{16} \,|\, \tau_4(\gamma) = I\}| = 520 = |K_4(2)|, \tag{3.1}$$
$$|\{\gamma \in \Gamma_9 \,|\, \sigma_2(\gamma) = I\}| = 738 = |K_2(3)|.$$

Thus the kernel of τ_4, respectively σ_2, is the full kernel $K_4(2)$, respectively $K_2(3)$. We proceed as in [**49**] to prove part (iii) of the Lemma for $n \geq 4$. The proof of part (v) regarding the kernel of σ_n for $n \geq 2$ is identical.

Let π_n be the canonical homomorphism from $\mathrm{SL}_2(\mathscr{O}/(2^n))$ onto $\mathrm{SL}_2(\mathscr{O}/(2^{n-1}))$, and let ϕ_n be the projection from $\mathrm{SL}_2(\mathscr{O}/(2^n))$ onto Γ_{2^n}. The the following diagram commutes for $n \geq 4$:

$$\begin{array}{ccc} \Gamma_{2^{n-1}} & \xleftarrow{\quad\tau_n\quad} & \Gamma_{2^n} \\ {\scriptstyle\phi_n}\uparrow & & \uparrow{\scriptstyle\phi_n} \\ \mathrm{SL}_2(\mathscr{O}/(2^{n-1})) & \xleftarrow{\quad\pi_n\quad} & \mathrm{SL}_2(\mathscr{O}/(2^n)) \end{array} \tag{3.2}$$

We want to show that $\ker(\tau_n) = \ker(\pi_n)$ for $n \geq 4$. We prove this by induction on n.

From (3.1), this is true in the base case, $n = 4$. We suppose it is true for n, and show that it must also be true for $n+1$. Let X denote the inverse limit of the groups Γ_{2^i} for $i \geq 4$:

$$X := \varprojlim \Gamma_{2^i} \text{ where } i \geq 4$$

and denote by

$$\mathrm{SL}_2(\mathscr{O}_2) := \varprojlim \mathrm{SL}_2(\mathscr{O}/(2^i))$$

the inverse limit of the groups $\mathrm{SL}_2(\mathscr{O}/(2^i))$. We would like to show that for any $\gamma \in \mathrm{SL}_2(\mathscr{O}_2)$ congruent to the identity $\mathscr{I}$ modulo 2^n, there is an element $x \in X$ such that

$$x \equiv \gamma \,(\mathrm{mod}\, 2^{n+1}).$$

As in [**49**], we write

$$\gamma = \mathscr{I} + 2^n \mu.$$

Since $\det(\gamma) = 1$, we must have that $\mathrm{Tr}(\mu) \equiv 0 \pmod 2$. Thus μ can be written mod 2 as a sum of some matrices μ_i such that $\mu_i^2 = 0$, and so $\mu^2 \equiv 0 \pmod 2$.

By the induction hypothesis, we have that there is an element $\beta \in X$ such that

$$\beta = \mathscr{I} + 2^{n-1}\mu + 2^n \delta,$$

where δ has entries in $\mathbb{Z}_2(i)$. Let $x = \beta^2$. That is, we have

$$x = \mathscr{I} + 2^n \mu + 2^{n+1}\delta + 2^{2n-2}\mu^2 + 2^{2n-1}\mu\delta + 2^{2n-1}\delta\mu + 2^{2n}\delta^2.$$

Since $n \geq 5$ and $\mu^2 \equiv 0 \bmod 2$, we have produced an element $x \in X$ such that

$$x \equiv \mathscr{I} + 2^n \mu \pmod{2^{n+1}}$$

as desired. The proof of part (v) regarding reduction mod 3 is identical. □

It remains to determine the image of Γ under reduction mod (c), where $c = 2^n 3^m$. It turns out that powers of (2) do not interact with powers of (3) at all in this context – namely, Γ_c is simply the product of Γ_{2^n} and Γ_{3^n}.

LEMMA 3.4. *Let Γ and c be as above. Then*

$$\Gamma_c = \Gamma_{2^n} \times \Gamma_{3^m}.$$

PROOF. It is easy to check that the groups Γ_{2^n} and Γ_{3^m} have no composition factors in common for any n and m. The order of Γ_{2^n} is a power of 2, and the same is true of its composition factors. The orders of the composition factors of Γ_{3^n}, however, are all divisible by a power of 3. Thus our claim follows from Lemma 2.3. □

THEOREM 3.5. *Let $d = cd'$, where $c = 2^n 3^m$, and $gcd(d', c) = 1$. Let*

$$d' = \prod_{1 \leq i \leq r} p_i^{a_i} \prod_{1 \leq j \leq s} q_j^{b_j}$$

be the prime factorization of d', where $p_i \equiv 1$ mod 4 for all $1 \leq i \leq r$, and $q_j \equiv 3$ mod 4 for all $1 \leq j \leq s$. Then Γ maps as a product group onto

$$\Gamma_c \times \prod_{1 \leq i \leq r} (\mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}) \times \mathrm{SL}_2(\mathbb{Z}/p_i^{a_i})) \times \prod_{1 \leq j \leq s} \mathrm{SL}_2(\mathscr{O}_{\mathbb{Z}}/q_j^{b_j}), \tag{3.3}$$

where Γ_c is the image of Γ under reduction modulo c, as described in Lemma 3.4.

This theorem follows from Proposition 2.2, Lemma 3.3, and Lemma 3.4, as well as the discussion in [**49**]. It describes completely the structure of $A \bigcap \mathrm{SO}_Q(\mathbb{Z})$ modulo any integer d via the homomorphism ρ together with s. In the next section, we use Theorem 3.5 to describe the orbit of A modulo square free integers d.

4. Congruence obstructions for the orbit

Since we are ultimately interested in the local structure of the orbit of A, we extend Theorem 3.5 to the setting of the orbit $\mathscr{P} = \mathscr{P}(P) = A\mathbf{v}$ where $\mathbf{v} = \mathbf{v}_P$ is the root quadruple of a packing P. Throughout this section, we consider the cone

$$C = \{\mathbf{v} = (v_1, v_2, v_3, v_4) \,|\, \mathbf{v} \neq \mathbf{0}, Q(\mathbf{v}) = 0\} \tag{4.1}$$

where Q is the Descartes quadratic form. Note that the Apollonian group A acts on C by mapping any quadruple of mutually tangent circles represented by a point of C to another quadruple of mutually tangent circles in the same packing. In other words, for $\alpha \in A$ we have

$$(a,b,c,d) \xrightarrow{\alpha} (a',b',c',d')$$

where (a,b,c,d) and (a',b',c',d') are Descartes quadruples in a packing P. We would like to elaborate on how this action behaves under reduction modulo integers $d > 1$. Given the multiplicative property of the group Γ in Section 0.28, this amounts to specifying how orbits of A modulo powers of primes sit inside C_{p^r}, defined recursively as follows:

- For $p > 2$,

$$\begin{aligned} C_p &= \{\mathbf{v} \in \mathbb{Z}/p\mathbb{Z} \,|\, \mathbf{v} \not\equiv \mathbf{0}\ (p), Q(\mathbf{v}) \equiv 0\ (p)\}, \\ C_{p^r} &= \{\mathbf{v} \in \mathbb{Z}/p^r\mathbb{Z} \,|\, \mathbf{v} \in C_{p^{r-1}}\ (p^{r-1}), Q(\mathbf{v}) \equiv 0\ (p^r)\} \end{aligned} \tag{4.2}$$

  for $r > 1$.
- For $p = 2$,

$$\begin{aligned} C_2 &= \{\mathbf{v} \in \mathbb{Z}/2\mathbb{Z} \,|\, \mathbf{v} \not\equiv \mathbf{0}\ (2), Q(\mathbf{v}) \equiv 0\ (2)\}, \\ C_{2^r} &= \{\mathbf{v} \in \mathbb{Z}/2^r\mathbb{Z} \,|\, \mathbf{v} \in C_{2^{r-1}}\ (2^{r-1}), Q(\mathbf{v}) \equiv 0\ (2^r), \exists \mathbf{w} \equiv \mathbf{v}\ (2^r) \text{ s.t. } Q(\mathbf{w}) \equiv 0\ (2^{r+1})\} \end{aligned} \tag{4.3}$$

  for $r > 1$.

Note that we need to define C_{2^r} separately because it is not true in this case that every solution to $Q(\mathbf{v}) \equiv \mathbf{0}\ (2^r)$ lifts to some solution of the equation modulo 2^{r+1} – only half of the solutions modulo 2^r lift to solutions modulo higher powers, and every element of C_{2^r} as defined above has 8 elements lying above it in $C_{2^{r+1}}$. Furthermore, since the isomorphism in (1.5) is over $\mathbb{Z}[1/2]$, we cannot apply results about Γ to reduction of the orbit modulo powers of 2 or modulo even integers. We thus consider the reduction of A modulo odd integers first, and complete the picture with an analysis of reduction modulo powers of 2 in Lemmas 4.3 and 4.4.

Recall that A acts on C by mapping any quadruple of mutually tangent circles represented by a point of C to another quadruple of mutually tangent circles in the same packing. Similarly, the group Γ acts on the cone C via the spin homomorphism ρ and the change of variables map s in (1.5). Namely, for

any $\gamma \in \Gamma$, we have the action

$$(a,b,c,d) \xrightarrow{s(\rho(\gamma))} (a',b',c',d') \tag{4.4}$$

of γ on a quadruple (a,b,c,d) in the packing P. Since $s(\rho(\gamma)) \in A \cap \mathrm{SO}_Q(\mathbb{Z})$, this action does not depict the whole action of the Apollonian group, but rather only the action of elements of even word length in the four generators of A. However, we can easily relate it to the action of all of A by multiplying on the left by the generator S_1.

LEMMA 4.1. *Let $\tilde{A} = A \cap \mathrm{SO}_Q(\mathbb{Z})$, and let $S_1 \in A$ be as before. Then*

$$A = \tilde{A} \cup S_1 \tilde{A}.$$

In general, we have

$$\mathrm{O}_Q(\mathbb{Z}) = \mathrm{SO}_Q(\mathbb{Z}) \cup S_1 \,\mathrm{SO}_Q(\mathbb{Z}).$$

Since we can view the action of the Apollonian group on the cone as the action of Γ in this way, we apply Theorem 3.5 to obtain the desired structure of the orbit of A modulo odd integers d in the following lemma.

LEMMA 4.2. *Let C and C_{p^r} be as above, let $\mathscr{P}$ be an orbit of A acting on a root quadruple $\mathbf{v} = \mathbf{v}_P$ of a packing P and let $\mathscr{P}_d$ be the reduction of this orbit modulo an odd integer $d > 1$. Write $d = d_1 d_2$ with $(d_2, 3) = 1$ and $d_1 = 3^m$ where $m \geq 0$ is an integer. Then*

(i) *If $m \geq 1$, the natural projection $\mathscr{P}_d \longrightarrow \mathscr{P}_{d_1} \times \mathscr{P}_{d_2}$ is surjective.*
(ii) *If $m \geq 1$, let $\pi : C_{d_1} \to C_3$ be the natural projection. Then $\mathscr{P}_{d_1} = \pi^{-1}(\mathscr{P}_3)$.*
(iii) *The natural projection $\mathscr{P}_{d_2} \longrightarrow \prod_{p^r || d_2} \mathscr{P}_{p^r}$ is surjective and $\mathscr{P}_{p^r} = C_{p^r}$.*

Proof: We derive (i) directly from Lemma 4.4 and the product group structure of Γ in Theorem 3.5. This structure translates to the orbit setting via the action in (4.4) of Γ_d on the cone. For simplicity, we refer to this action as $\rho(\gamma)$ as opposed to $s(\rho(\gamma))$ above. Using the notation of (3.3) and assuming $d_1 > 1$, for $\mathbf{v} = \mathbf{v}_P$ we have

$$\begin{aligned} \rho(\Gamma_d)(\mathbf{v}) = \rho\left(\Gamma_{d_1} \times \prod_{1\leq i\leq r} \mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}) \times \mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}) \times \prod_{1\leq j\leq s} \mathrm{SL}_2(\mathscr{O}/q_j^{b_j})\right)(\mathbf{v}) = \\ \rho(\Gamma_{d_1})(\mathbf{v}) \times \prod_{1\leq i\leq r} \rho(\mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}))(v) \times \prod_{1\leq j\leq s} \rho(\mathrm{SL}_2(\mathscr{O}/q_j^{b_j}))(\mathbf{v}) = \\ \rho(\Gamma_{d_1})(\mathbf{v}) \times \prod_{p^r | d_2} \mathrm{SO}_Q(\mathbb{Z}/(p^r\mathbb{Z}))(\mathbf{v}) \end{aligned} \tag{4.5}$$

Combining this with the multiplication of S_1 by $\rho(\Gamma_d)(\mathbf{v})$ in Lemma 4.1 we get

$$\mathscr{P}_d = S_1 \cdot \rho(\Gamma_d)(\mathbf{v}) \cup \rho(\Gamma_d)(\mathbf{v}) = \Big(S_1 \cdot \rho(\Gamma_{d_1})(\mathbf{v}) \cup \rho(\Gamma_{d_1})(\mathbf{v})\Big) \times \prod_{p^r | d_2} C_{p^r} = \mathscr{P}_{d_1} \times \prod_{p^r | d_2} C_{p^r}$$

as desired.

We prove (ii) in a similar way, using the characterization of Γ_c in Lemma 3.4. To realize the structure of $\rho(\Gamma_{3^m})(\mathbf{v})$, note that the following diagram, where τ_m and τ'_m are the natural projections obtained by reduction mod 3^m, is commutative:

$$\begin{array}{ccc} \tilde{A}_{3^m} & \xleftarrow{\tau'_m} & \tilde{A}_{3^{m+1}} \\ \rho \uparrow & & \rho \uparrow \\ \Gamma_{3^m} & \xleftarrow{\tau_m} & \Gamma_{3^{m+1}} \end{array} \tag{4.6}$$

We recall from Lemma 3.4 that $ker(\tau_m) = K_m(3)$ for $m \geq 2$, where $K_m(3)$ is the kernel of the projection

$$\mathrm{SL}_2(\mathscr{O}/3^{m+1}) \xrightarrow{\pi_n} \mathrm{SL}_2(\mathscr{O}/3^m).$$

We would like to relate this to $ker(\tau'(m))$. For this we note that the elements in Γ lying above the identity in $\tilde{A}$ are $\pm I$, where I is the identity in Γ. However, it is easy to check that none of the groups Γ_{3^m} will contain $-I$, so the only element of Γ_{3^m} lying over the identity in $\tilde{A}_{3^m}$ is in fact I. Thus

$$ker(\tau'_m) = \rho(ker(\tau(m))) = \rho(K_m(3)).$$

Let π'_m be the projection from $\mathrm{SO}_Q(\mathbb{Z}/3^m\mathbb{Z})$ onto $\mathrm{SO}_Q(\mathbb{Z}/3^{m-1}\mathbb{Z})$, and let $K'_m(3)$ be the kernel of π'_m. Since the diagram

$$\begin{array}{ccc} \mathrm{SO}_Q(\mathbb{Z}/3^m\mathbb{Z}) & \xleftarrow{\pi'_m} & \mathrm{SO}_Q(\mathbb{Z}/3^{m-1}\mathbb{Z}) \\ \rho \uparrow & & \rho \uparrow \\ \mathrm{SL}_2(\mathscr{O}/3^m) & \xleftarrow{\pi_m} & \mathrm{SL}_2(\mathscr{O}/3^{m-1}) \end{array} \tag{4.7}$$

also commutes, we have that $\rho(K_m(3)) = K'_m(3)$ for $m \geq 2$. Finally, we note that the diagram

$$\begin{array}{ccc} C_{3^m} & \longleftarrow & C_{3^{m+1}} \\ \uparrow & & \uparrow \\ \mathscr{P}_{3^m} & \longleftarrow & \mathscr{P}_{3^{m+1}} \end{array} \tag{4.8}$$

commutes for $m \geq 2$. Combined with our analysis of the kernel of τ'_m above, we have that every $\mathbf{v} \in C_{3^{m+1}}$ lying above a vector $\mathbf{v} \in \mathscr{P}_{3^m}$ is also in $\mathscr{P}_{3^{m+1}}$. Thus $\mathscr{P}_{3^m} = \pi^{-1}(\mathscr{P}_3)$ as desired. □

It remains to extend Lemma 4.2 to all integers d. We first prove an analog of part (ii) of Lemma 4.2 for powers of 2.

LEMMA 4.3. *Let $\mathscr{P}$ be a primitive integer orbit of the Apollonian group, and let $\mathscr{P}_{2^n}$ denote the reduction of $\mathscr{P}$ mod 2^n. Let C_{2^n} be as in (4.3) and let π_n be the natural projection*

$$\pi_n : C_{2^n} \longrightarrow C_{2^{n-1}}.$$

With this notation, we have

$$\mathscr{P}_{2^n} = \pi_n^{-1}(\mathscr{P}_{2^{n-1}})$$

for $n \geq 4$. In particular, if $\pi : C_{2^n} \longrightarrow C_8$ is the natural projection where $n \geq 4$, then $\mathscr{P}_{2^n} = \pi^{-1}(\mathscr{P}_8)$.

PROOF. To prove this, we produce elements of A which effectively lift points in $\mathscr{P}_{2^{n-1}}$ to all possible points in C_{2^n}. Let S_1, S_2, S_3, and S_4 be the generators of the Apollonian group as before, and let $X_0 = S_2S_1S_3$, $Y_0 = S_1S_2S_4$, $Z_0 = S_1S_3$. For integers $n \geq 4$, let $X(n) = X_0^{2^{n-3}}, Y(n) = Y_0^{2^{n-3}}$, and $Z(n) = Z_0^{2^{n-3}}$. We have

$$X(n) \equiv \begin{pmatrix} 1 & 2^{n-1} & 2^{n-1} & 0 \\ 2^{n-1} & 1 & 2^{n-1} & 0 \\ 2^{n-1} & 2^{n-1} & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \pmod{2^n}, \quad Y(n) \equiv \begin{pmatrix} 1 & 2^{n-1} & 0 & 2^{n-1} \\ 2^{n-1} & 1 & 0 & 2^{n-1} \\ 0 & 0 & 1 & 0 \\ 2^{n-1} & 2^{n-1} & 0 & 1 \end{pmatrix} \pmod{2^n}, \tag{4.9}$$

$$Z(n) \equiv \begin{pmatrix} 2^{n-2}+1 & 2^{n-2} & -2^{n-2} & 2^{n-2} \\ 0 & 1 & 0 & 0 \\ 2^{n-2} & -2^{n-2} & 1-2^{n-2} & -2^{n-2} \\ 0 & 0 & 0 & 1 \end{pmatrix} \pmod{2^n}.$$

Let H_n be the abelian group of order 16 generated by $X(n), Y(n)$, and $Z(n)$ modulo 2^n. Note that any primitive orbit $\mathscr{P}$ of A modulo 2 consists of one vector, where two coordinates are 1's, and two coordinates are 0's (this follows from the unique nontrivial solution to the Descartes equation mod 2), and that we can arrange the vector to be $(1,0,0,1)$ and re-order coordinates of all the vectors in the orbit accordingly. With this in mind, let $n \geq 4$, and let $\mathbf{r} \in \mathscr{P}$ be the vector

$$\mathbf{r} = (a + 2^{n-1}k_1, b + 2^{n-1}k_2, c + 2^{n-1}k_3, d + 2^{n-1}k_4)^T$$

which is $(a,b,c,d)^T$ mod 2^{n-1}. Here $0 \leq a,b,c,d < 2^{n-1}$ are integers such that a and d are odd and b and c are even. Since H_n is a subgroup of A, we have that the orbit $H_n\mathbf{r}$ mod 2^n sits inside $\mathscr{P}_{2^n}$. In particular, given that

- $\mathbf{v} \equiv (1,0,0,1)^T \pmod 2$,
- $v_1 + v_2 + v_3 + v_4 \equiv 0 \pmod 2$,
- $v_1 + v_2 + v_3 + v_4 \equiv 0 \pmod 4$

for every $\mathbf{v} = (v_1, v_2, v_3, v_4)^T \in \mathscr{P}$, we have

$$\begin{aligned}
\mathscr{I} \cdot \mathbf{r} &\equiv \mathbf{r} \\
Y(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (2^{n-1}, 0, 0, 2^{n-1})^T \\
Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (2^{n-1}, 0, 0, 0)^T \\
X(n)Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (2^{n-1}, 2^{n-1}, 2^{n-1}, 0)^T \\
Y(n)Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (0, 0, 0, 2^{n-1})^T \\
X(n)Y(n)Z(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (0, 2^{n-1}, 2^{n-1}, 2^{n-1})^T \\
X(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (0, 2^{n-1}, 2^{n-1}, 0)^T \\
X(n)Y(n) \cdot \mathbf{r} &\equiv \mathbf{r} + (2^{n-1}, 2^{n-1}, 2^{n-1}, 2^{n-1})^T
\end{aligned}$$

mod 2^n. This is in fact the full list of points in C_{2^n} lying above $\mathbf{r}$, as desired. □

Finally, we show a multiplicative structure for orbits of the Apollonian group modulo even integers in the following lemma:

LEMMA 4.4. *Let $\delta = 2^n$ be any positive power of 2 and let $\mathscr{P}$ be as before. Let c be an odd integer, and let $d = \delta c$. Then the projection*

$$\mathscr{P}_d \longrightarrow \mathscr{P}_\delta \times \mathscr{P}_c$$

is surjective.

PROOF. Let $c = 3^m c'$, where $gcd(c', 3) = 1$ and $m \geq 0$. For $\tilde{A} = A \cap \mathrm{SO}_Q$, let $\tilde{A}_d$ denote the reduction of $\tilde{A}$ mod d. From the proof of Lemma 4.2, we have that $\tilde{A}_c$ maps as a product group onto

$$\tilde{A}_{3^m} \times \prod_{p^r || c'} \mathrm{SO}_Q(\mathbb{Z}/p^r\mathbb{Z}) \tag{4.10}$$

if $m \geq 1$, or as a product group onto the second factor in (4.10). Assume $m \geq 1$, and note that the projection $\tilde{A}_d$ to

$$\tilde{A}_\delta \times \tilde{A}_{3^m} \times \prod_{p^r || c'} \mathrm{SO}_Q(\mathbb{Z}/p^r\mathbb{Z}) \tag{4.11}$$

is onto each factor by the proof of Lemma 4.2. By Goursat's Lemma 2.3, note that the groups in (4.10) have no composition factors in common. Furthermore, the order of $\tilde{A}_\delta$ is a power of 2, and so all of its composition factors also have order a power of 2. However, this is not true of any of the composition factors of $\tilde{A}_{3^m}$ or $\mathrm{SO}_Q(\mathbb{Z}/p^r\mathbb{Z})$, so by Goursat's lemma we have that $\tilde{A}_d$ does indeed map as a product group onto the expression in (4.11). As in Lemma 4.2, we consider the orbit

$$\tilde{A}_d \mathbf{v} = (\tilde{A}_\delta \times \tilde{A}_{3^m} \times \prod_{p^r | c'} \mathrm{SO}_Q(\mathbb{Z}/(p^r\mathbb{Z}))(\mathbf{v}) \tag{4.12}$$

and combine this with the multiplication of S_1 as described in Lemma 4.1 to get

$$\mathscr{P}_d = (S_1 \cdot \tilde{A}_d)(\mathbf{v}) \cup \tilde{A}_d \mathbf{v} = A_\delta \mathbf{v} \times \mathscr{P}_{3^m} \times \prod_{p^r | c'} C_{p^r} =$$

$$\mathscr{P}_\delta \times \mathscr{P}_c$$

as desired. The proof in the case of $m = 0$ is identical (the factor of $\mathscr{P}_{3^m}$ is simply ommited). □

With this description of the orbits of A modulo even integers, we are now able to give a complete description of orbits of the Apollonian group modulo integers $d > 1$ below.

THEOREM 4.5. *Let $\mathscr{P}$ be an orbit of A acting on a root quadruple $\mathbf{v}_P$ of a packing P and let $\mathscr{P}_d$ be the reduction of this orbit modulo an integer $d > 1$. Let $C = \{\mathbf{v} \neq \mathbf{0} \,|\, Q(\mathbf{v}) = 0\}$ denote the cone without the origin, and let C_{p^r} be as before. Write $d = d_1 d_2$ with $(d_2, 6) = 1$ and $d_1 = 2^n 3^m$ where $n, m \geq 0$.*

(i) *If $d_1 \neq 1$, the natural projection $\mathscr{P}_d \longrightarrow \mathscr{P}_{d_1} \times \mathscr{P}_{d_2}$ is surjective.*
(ii) *The natural projection $\mathscr{P}_{d_2} \longrightarrow \prod_{p^r || d_2} \mathscr{P}_{p^r}$ is surjective and $\mathscr{P}_{p^r} = C_{p^r}$.*
(iii) *If $m, n \geq 1$, the natural projection $\mathscr{P}_{d_1} \longrightarrow \mathscr{P}_{2^n} \times \mathscr{P}_{3^m}$ is surjective.*
(iv) *If $n \geq 4$, let $\pi : C_{2^n} \to C_8$ be the natural projection. Then $\mathscr{P}_{2^n} = \pi^{-1}(\mathscr{P}_8)$.*
(v) *If $m \geq 2$, let $\phi : C_{3^m} \to C_3$ be the natural projection. Then $\mathscr{P}_{3^m} = \phi^{-1}(\mathscr{P}_3)$.*

Theorem 4.5 follows directly from Lemmas 4.2, 4.3, and 4.4. It implies the following improvement of Graham et.al.'s Theorem 1.5.

COROLLARY 4.6. *Let P be a primitive integral Apollonian circle packing, and let $d > 1$ be a square free integer such that $gcd(d, 6) = 1$. The curvatures of circles in P cover all possible congruence classes modulo d.*

PROOF. We wish to show that for any residue class k modulo d, k is a coordinate of some vector $\mathbf{v} \in \mathscr{P}$. Suppose $k \neq 0$. Note that $Q(0,0,k,k) = 0$ for any $k \neq 0$ where Q is the Descartes form, and so $(0,0,k,k) \in C_d$ for all $d \in \mathbb{N}$. Since $\mathscr{P}_d = C_d$ for d relatively prime to 6 by Theorem 3, we have that $(0,0,k,k) \in \mathscr{P}_d$ as well, and so we have what we want. If $k = 0$, then we easily produce a vector with coordinate 0 in $\mathscr{P}_d$ – again, $(0,0,a,a) \in \mathscr{P}_d$ for any $a \neq 0$. □

The description in Theorem 4.5 of the arithmetic structure of $\mathscr{P}$ is crucial to applying the affine linear sieve as described in [**7**] to diophantine problems on the orbit of A. In [**19**] the analysis in this paper is used to verify the sieve conditions and determine the density function for the sieve in order to count prime and almost prime points in $\mathscr{P}$. Furthermore, Theorem 4.5 is one of the ingredient in the conjectured local to global principle for ACP's which is described and motivated in [**19**]:

CONJECTURE 4.7. *(Fuchs, Sanden): Let P be an integral 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.*

This conjecture would suggest that the orbit in this case mimics the full cone C outside of a congruence obstruction modulo 24. Proving this, however, appears rather difficult at this time.

CHAPTER 3

Sieving

1. The affine sieve and the importance of expanders

The analysis of the orbit of A modulo d in Chapter 2 provides an analog of the Chinese remainder theorem in the context of ACP's which allows us to sieve over the curvatures in a packing. The setup of such a sieve in general can be found in [7] and we specify its construction in relation to ACP's here.

Let P be a bounded Apollonian circle packing, and let a_n be the number of circles at generation T of curvature n in P. We denote the sequence of such a_n's by $\mathscr{A} := \{a_n\}$. 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 (thus $a_n \leq r^2 n^2$). With this in mind, denote

$$X := \sum_n a_n.$$

Since we consider the problem of counting circles of prime curvature in P in Section 4, we summarize the setup of the sieve we use there. Let z be a small power of X and denote by P_z the product

$$P_z := \prod_{p \leq z} p,$$

for p prime. Our goal is then to estimate the sum

$$S(\mathscr{A}, P_z) = \sum_{(n, P_z)=1} a_n$$

which essentially approximates the total number of circles of prime curvature at generation T. Let d be a square free integer such that $1 < d < X^\alpha$ for some small power α. In order to compute $S(\mathscr{A}, P_z)$, we estimate the sums of a_n for which $n \equiv 0 \bmod d$. To this end we note that there is a multiplicative density function $0 \leq \beta(d) \leq 1$ such that

$$\sum_{n \equiv 0\,(d)} a_n = \beta(d)X + R(\mathscr{A}, d) \tag{1.1}$$

where the remainder term $R(\mathscr{A}, d)$ is small comparing to X (See (4.11) for a concrete definition of $\beta(d)$). The requirement that $R(\mathscr{A}, d)$ be small turns out to be quite subtle when sieving over an orbit of a group G (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 which occur in some arithmetic progression with difference d. Over the integers, the size of the boundary of such an interval, as well as the arithmetic progression is trivially small compared to the size of the whole interval. In the setting of groups, however, this is generally not true. Consider all those points in an orbit of an arbitrary group

acting on $\mathbb{R}^n$ which 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' 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 $R(\mathscr{A},d)$ is small), it is necessary for G to satisfy some combinatorial properties. Namely, let $\{\alpha_1,...,\alpha_k\}$ be the generators of G. We can then think of G in terms of its associated Cayley graph $(\mathscr{G},S)$ where $S=\{\alpha_1,\alpha_1^{-1},...,\alpha_k,\alpha_k^{-1}\}$, the vertices correspond to elements of G, and two vertices x and y are connected by an edge iff $\alpha x = y$ for some $\alpha \in S$. In this way, we associate with G a $2k$-regular tree. This association is crucial in controlling the remainder term in (1.1) in the orbit setting – namely, if one imposes some conditions (see [**7**]) on the Cayley graphs $\mathscr{G}_p$ which arise from the reduction of G modulo primes p, it is possible to carry out the sieve.

Specifically, for any graph $\mathscr{G}$ with a finite number of vertices $|\mathscr{G}|$ we can define a $|\mathscr{G}|\times|\mathscr{G}|$ *adjacency matrix* $A(\mathscr{G})$ whose rows and columns are indexed by vertices v_i of $\mathscr{G}$, such that

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

In the context of the Apollonian group and in other cases one might consider, the graphs which come up are $2k$-regular graphs on n vertices (once we reduce G modulo p its Cayley graph is of course finite). For such a graph, the adjacency matrix $A(\mathscr{G}_{n,2k})$ is an $n\times n$ symmetric matrix with n eigenvalues between $-2k$ and $2k$ which we arrange in decreasing order:

$$2k=\lambda_0\geq\lambda_1\geq...\geq\lambda_{n-1}\geq -2k,$$

where $\lambda_0>\lambda_1$ if the graph is connected, which we assume for our applications. With this in mind, we would like the graphs arising from the groups G_p to satisfy the following expander property (see [**7**] for a detailed discussion).

DEFINITION 1.1. Let $\mathscr{G}_{n,2k}$ be a connected, $2k$-regular graph on n vertices as before, and let $A(\mathscr{G}_{n,2k})$ be its adjacency matrix. Let λ_i be the eigenvalues of A, and denote by $\lambda(A(\mathscr{G}))$ an eigenvalue of A such that

$$|\lambda(A(\mathscr{G}))|=\max(\{|\lambda_i| \text{ where } -2k<\lambda_i<2k\}.$$

Then the graphs $\mathscr{G}_{n,2k}$ form a family of absolute expanders if we have that

$$\limsup_{n\to\infty}|\lambda(A(\mathscr{G}_{n,2k}))|<2k.$$

It is precisely this expander property which guarantees that the remainder $R(\mathscr{A},d)$ in the sieve is small, and it turns out that the sieve can be carried out for orbits of groups which satisfy this property. The following theorem from [**7**] implies that the Apollonian group A is in fact such a group.

THEOREM 1.2. *(Bourgain, Gamburd, Sarnak): Let G be a non-elementary subgroup of $\tilde{G}=SL_2(\mathbb{Z}(\sqrt{-1}))$ such that G is Zariski dense in $\tilde{G}$, 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 $(SL_2(\mathbb{Z}(\sqrt{-1}))/(d), S)$, where S is a fixed symmetric generating set of generators of G, is a family of absolute expanders.

This theorem applies to the analysis of curvatures of circles in ACP's since we have seen in Chapter 2 that the preimage of A in the spin-double cover of the orthogonal group SO_Q is precisely a Zariski dense subgroup of $\mathrm{SL}_2(\mathbb{Z}(\sqrt{-1}))$ with the set of generators S as in 1.6, and that the traces of the matrices in Γ do in fact generate $\mathbb{Q}(\sqrt{-1})$. Thus the Cayley graphs arising from reduction mod d in the case of ACP's satisfy the expander property by Theorem 1.2, and so we can construct a combinatorial sieve to count curvatures in a packing P. In [**7**], the authors discuss how such a sieve can give upper bounds towards the analog of a prime number theorem in the orbit of an algebraic group – we explore this question in the context of curvatures of circles born at generation T in a packing P in Section 4.2.

Another question which has many variants over the integers that one can also extend to a group orbit setting such as ACP's concerns the infinitude of points in the orbit whose coordinates have few prime factors. For example, given an integer-valued polynomial $f(x)$ over $\mathbb{Z}$, are there infinitely many primes which can be expressed as $f(a)$ for some $a \in \mathbb{Z}$? To phrase this question for affine space it is convenient to consider *r-almost primes*, or integers $s > 0$ with at most r distinct prime factors, rather than primes alone, as the problem of counting primes is much more difficult in this case.

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

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

which we refer to as the set of r-almost prime points. 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 is Zariski dense in the Zariski closure $\mathrm{Zcl}(O)$ of O. Note that if O_r is dense in $\mathrm{Zcl}(O)$ for some $r \in \mathbb{Z}$, then $O_{r'}$ is dense in $\mathrm{Zcl}(O)$ for $r' \geq r$ as well. If such an r exists and is finite, we call the minimum r for which O_r is dense in O the *saturation number*, denoted by $r_0(O, f)$, and say that the pair (O, f) saturates.

Note that this question is best considered in the case that there are no local obstructions for the pair (O, f). For example, for an integer $q \geq 2$, if there is no point $\mathbf{x} \in O$ for which $(f(\mathbf{x}), q) = 1$, 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) to 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 could also allow a finite set B of primes q for which $q | f(\mathbf{x})$ for every $\mathbf{x} \in O$. In this case, the number of primes in B is absorbed into r_0. We state the result for saturation of the orbit in the primitive case here:

THEOREM 1.3. *(Bourgain, Gamburd, Sarnak): Let G be as in Theorem 1.2, 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.

So, in particular, Theorem 1.2 implies that the saturation number r_0 exists and is finite in the setting of orbits $\mathscr{P}$ of A. In the next two sections, we give an upper bound for the saturation number $r_0(\mathscr{P},f)$ where $f(x_1,x_2,x_3,x_4)=x_1x_2x_3x_4$.

Note that since the Apollonian group A is Zariski dense in the orthogonal group O_Q fixing the Descartes form Q, the Zariski closure $\mathrm{Zcl}(\mathscr{P})$ of $\mathscr{P}$ is the affine cone

$$C=\{\mathbf{x}=(x_1,x_2,x_3,x_4)\neq\mathbf{0}\,|\,Q(\mathbf{x})=0\}$$

where Q is the Descartes form. Therefore r_0 is the smallest integer for which $\mathscr{P}_{r_0}$ is Zariski dense in the cone C. In the next section we elaborate on which primes are considered *bad* in the sense of primitivity for the Apollonian orbit and compute an explicit upper bound for r_0 in Section 3.2. We cannot, however, use the full strength of the methods developed in [**7**] in determining r_0. For this one would need to explicitly determine the discrete spectrum of the Laplacian of $A\backslash\mathbb{H}^3$ and since the fundamental domain of this quotient has infinite volume usual integration techniques 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 any ACP. Beyond this, it is shown in [**7**] that there is a spectral gap for the Apollonian case. However, this gap is currently difficult to verify even by using approximate calculations on a computer, and until one can say something explicit about the discrete spectra of infinite volume quotients of $\mathbb{H}^3$ one cannot use the affine linear sieve in order to determine r. On the other hand, A has many subgroups generated by unipotent elements which allow us to obtain a bound on r_0 using only a classical sieve over $\mathbb{Z}$ which does not require the spectral theory discussed here.

2. Bad primes

In Chapter 2 we proved that the mod p reduction of the Apollonian group A for $p>3$ can be extracted from the group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. In particular, the orbit $\mathscr{P}$ of A acting on a root quadruple $\mathbf{v}$ can be realized as follows:

$$\mathscr{P}(\mathbb{Z}/p\mathbb{Z})=s\circ\rho(\Gamma_p)\mathbf{v}=s\circ\rho(\mathrm{SL}_2(\mathbb{F}_p))\mathbf{v}, \tag{2.1}$$

where Γ is the preimage of A under the spin homomorphism ρ, and s is the change of variables defined in (1.5). Let

$$f(\mathbf{x}):=x_1x_2x_3x_4. \tag{2.2}$$

In order to specify the saturation number $r_0(\mathscr{P},f)$ in Theorem 1.3 in this context, we first determine the finite set of primes B for which the primitivity condition is not satisfied. Namely, we check when the reduction modulo p in (2.1) reduces the orbit to a set of points (x_1,x_2,x_3,x_4) in which at least one coordinate of every point is 0 mod p – in other words, $f(\mathbf{x})\equiv 0\,(\mathrm{mod}\ p)$ for all $\mathbf{x}\in\mathscr{P}$. We will call the

primes p in such cases *bad*, since the question of saturation is not interesting if they are included. To make this notion of badness precise, denote

$$\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z}) := \{\mathbf{y} \in \mathscr{P} | f(\mathbf{y}) = y_1y_2y_3y_4 \equiv 0\ (p)\} \tag{2.3}$$

We say a prime p is *bad* if

$$\mathscr{P}(\mathbb{Z}/p\mathbb{Z}) = \mathscr{P}_0(\mathbb{Z}/p\mathbb{Z}). \tag{2.4}$$

With this in mind, we show the following:

THEOREM 2.1. *Let $\mathscr{P}(\mathbb{Z}/p\mathbb{Z})$ and $\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})$ be as before. We have*

$$\mathscr{P}(\mathbb{Z}/p\mathbb{Z}) \neq \mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})$$

for all primes $p > 3$.

Proof:

To prove Theorem 2.1 we again consider the preimage Γ of A under the spin homomorphism and also check for bad primes via computations in the orthogonal group itself. Liu and Sarnak do this for ternary quadratic forms in [**38**], and we develop their argument to fit our situation below. Recall that the Descartes quadratic form is equivalent to $\tilde{Q}(\mathbf{x}) = x_1^2 - x_2^2 + x_3^2 + x_4^2$. Let

$$V_p := V(\mathbb{Z}/p\mathbb{Z}) = \{\mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^4 \,|\, \mathbf{x} \neq 0, x_1^2 - x_2^2 + x_3^2 + x_4^2 \equiv 0\ (p)\} \tag{2.5}$$

and

$$V_p^0 := V^0(\mathbb{Z}/p\mathbb{Z}) = \{\mathbf{x} \in V_p \,|\, x_1x_2x_3x_4 \equiv 0\ (p)\}. \tag{2.6}$$

In this notation, a prime is considered bad if $|V_p| = |V_p^0|$. The following lemma specifies which primes are bad in this sense.

LEMMA 2.2. *Let V_p and V_p^0 be as before. We have*

$$|V_p| > |V_p^0|$$

for all primes $p > 3$.

PROOF. We note that the discriminant of $\tilde{Q}$ is -1, which has no prime factors and thus will not contribute to any local obstructions. We count points in V_p and V_p^0 using the Gauss sum

$$S(m,p) = \sum_{x=0}^{p-1} e_p(mx^2),$$

where $e_p(z) = e^{\frac{2\pi iz}{p}}$. It is known that

$$S(1,p) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e_p(x^2) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1\ (4) \\ i\sqrt{p} & \text{if } p \equiv 3\ (4) \end{cases} \tag{2.7}$$

where $\left(\frac{x}{p}\right)$ above denotes the Legendre symbol. Also, if p is odd and $p \not| m$, we can express $S(m,p)$ in terms of $S(1,p)$:

$$S(m,p) = \left(\frac{m}{p}\right) S(1,p)$$

We write $|V_p|$ and $|V_P^0|$ in terms of these Gauss sums and evaluate them below using (2.7).

$$\begin{aligned} |V_p| &= \frac{1}{p}\sum_{m=0}^{p-1} S(m,p)^3 S(-m,p) \\ &= p^3 + \left(\frac{-1}{p}\right)\frac{S(1,p)^4}{p}\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)^4 \\ &= \begin{cases} p^3 + p(p-1) & \text{if } p \equiv 1\ (4) \\ p^3 - p(p-1) & \text{if } p \equiv 3\ (4) \end{cases} \end{aligned} \tag{2.8}$$

where the second equality is obtained by isolating the $m = 0$ term. To calculate $|V_p^0|$, let $S_a := S(am,p)$ and define the function

$$\begin{aligned} \sigma(m,p) &:= S_1 S_{\text{-}1} S_1 S_1 - (S_1 - 1)^3 (S_{\text{-}1} - 1) \\ &= 3S_1^2 S_{\text{-}1} - 3S_1 S_{\text{-}1} + S_{\text{-}1} + S_1^3 - 3S_1^2 + 3S_1 - 1. \end{aligned}$$

In terms of $\sigma(m,p)$ we have

$$\begin{aligned} |V_p^0| &= \frac{1}{p}\sum_{m=0}^{p-1}\sigma(m,p) \\ &= \frac{1}{p}\left(\sum_{m=0}^{p-1} 3S_1^2 S_{\text{-}1} + \sum_{m=0}^{p-1} S_1^3 - \sum_{m=0}^{p-1} 3S_1 S_{\text{-}1} - \sum_{m=0}^{p-1} 3S_1^2 + \sum_{m=0}^{p-1} 3S_1 + \sum_{m=0}^{p-1} S_{\text{-}1} - \sum_{m=0}^{p-1} 1\right) \\ &= \begin{cases} 3p^2 + p^2 - 3(2p-1) - 3(2p-1) + 3 + 1 - 1 & \text{if } p \equiv 1\ (4) \\ 3p^2 + p^2 - 3(2p-1) - 3 + 3 + 1 - 1 & \text{if } p \equiv 3\ (4) \end{cases} \\ &= \begin{cases} 4p^2 - 12p + 9 & \text{if } p \equiv 1\ (4) \\ 4p^2 - 6p + 3 & \text{if } p \equiv 3\ (4) \end{cases} \end{aligned} \tag{2.9}$$

Therefore we have

$$|V_p| - |V_p^0| = \begin{cases} p^3 - 3p^2 + 11p - 9 & \text{if } p \equiv 1\ (4) \\ p^3 - 5p^2 + 7p - 3 & \text{if } p \equiv 3\ (4) \end{cases}$$

The expression above is positive whenever $p \geq 5$ as desired. □

To complete the proof of Theorem 2.1, we consider mod p orbits of A for $p > 3$ using the fact that $\Gamma_p = \mathrm{SL}_2$ as shown in Chapter 2. This analysis yields the following lemma.

LEMMA 2.3. *Let $\mathscr{P}(\mathbb{Z}/p\mathbb{Z})$ and $\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})$ be as before. For $p \geq 11$ we have*

$$|\mathscr{P}(\mathbb{Z}/p\mathbb{Z})| > |\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})|.$$

PROOF. Let V_p be as in (2.8), and let $\tilde{Q}$ be the quadratic form in (1.4) equivalent to the Descartes form Q. Suppose $p \neq 2,3$, and let $p \equiv 1 \pmod 4$ – i.e. -1 is a square mod p. The proof in case where -1 is not a square mod p is identical. Since the discriminant of $\tilde{Q}$ is $d(Q) = -1$, we have that $p \not| d$, and the action over $\mathbb{F}_p$ of $\Gamma_p = \mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)$ on $V_p(\tilde{Q})$ is defined via the morphism

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \xrightarrow{\tau} \begin{pmatrix} \frac{\alpha^2+\beta^2+\gamma^2+\delta^2}{2} & \frac{-\alpha^2+\beta^2-\gamma^2+\delta^2}{2} & -\alpha\beta-\gamma\delta & 0 \\ \frac{-\alpha^2-\beta^2+\gamma^2+\delta^2}{2} & \frac{\alpha^2-\beta^2-\gamma^2+\delta^2}{2} & \alpha\beta-\gamma\delta & 0 \\ -\alpha\gamma-\beta\delta & \alpha\gamma-\beta\delta & \alpha\delta+\beta\gamma & 0 \\ 0 & 0 & 0 & \alpha\delta-\beta\gamma \end{pmatrix} \tag{2.10}$$

The orbits of $\tau(G(\mathbb{Z}/p\mathbb{Z}))$ on $V_p(Q')$ can be described as follows:

$$(0,0,0,0), \quad (1,1,0,0)\tau(G(\mathbb{Z}/p\mathbb{Z})), \quad (r,r,0,0)\tau(G(\mathbb{Z}/p\mathbb{Z})), \tag{2.11}$$

where r is a quadratic non-residue mod p. It is clear that $(1,1,0,0)$ and $(r,r,0,0)$ are in distinct orbits. To see that these are in fact all of the orbits, note that the stabilizer of $(1,1,0,0)$ and $(r,r,0,0)$ in $G(\mathbb{Z}/p\mathbb{Z}))$ is

$$\overset{+}{-}\left\{ \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \middle| \xi \in \mathbb{F}_p \right\},$$

of order $2p$. It is now elementary to compute the cardinality of each of these orbits:

$$|\mathscr{P}_{(1,1,0,0)}| = |\mathscr{P}_{(r,r,0,0)}| = \frac{p(p-1)(p+1)}{2p} = \frac{p^2-1}{2}$$

Since $|V_p(\tilde{Q})| = p^2$, the set of orbits in (2.11 is complete. To see which of these points belong to $\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})$, let L_1, L_2, L_3, L_4 be linearly independent linear forms over $\mathbb{F}_p$, with

$$\left(\bigcup_{j=1}^{4} ker(L_j) \right) \cap \mathscr{P}(\mathbb{Z}/p\mathbb{Z}) = \mathscr{P}_0(\mathbb{Z}/p\mathbb{Z}).$$

For every j, we have from above that

$$\left| ker(L_j) \cap V_p(\tilde{Q}) \right| \leq 2p.$$

In fact, since $\mathscr{P}_{(r,r,0,0)}(\mathbb{Z}/p\mathbb{Z}) = r\mathscr{P}_{(1,1,0,0)}(\mathbb{Z}/p\mathbb{Z})$, and $ker(L_j) \cap V_p(\tilde{Q})$ is invariant under multiplication by a nonzero scalar, we have that

$$\left| ker(L_j) \cap \mathscr{P}(\mathbb{Z}/p\mathbb{Z}) \right| \leq p.$$

Thus we get

$$|\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})| = \left| \left(\bigcup_{j=1}^{4} ker(L_j) \right) \cap \mathscr{P}(\mathbb{Z}/p\mathbb{Z}) \right| \leq 4p.$$

For $p \geq 11$, we have

$$|\mathscr{P}(\mathbb{Z}/p\mathbb{Z})| = \frac{p^2-1}{2} > 4p = |\mathscr{P}_0(\mathbb{Z}/p\mathbb{Z})|.$$

This completes the proof of Lemma 2.3. □

We check experimentally that the primes 5 and 7 are not bad in the sense that one can always find a point $\mathbf{x}$ in the orbit of A for which $f(\mathbf{x}) \not\equiv 0 \bmod 5$ or 7. Thus the only bad primes are 2 and 3 as desired.

We have shown that the pair $(\mathscr{P}, f)$ where f is as in (2.2) is primitive for all primes $p \geq 5$. In the next section, we use this to prove that the saturation number $r_0(\mathscr{P}, f) \leq 28$.

3. 28-almost prime points

Recall that for $\mathbf{x} \in \mathbb{R}^4$ we defined $f(\mathbf{x}) = x_1x_2x_3x_4$, and that $\mathscr{P}$ denotes an integer orbit of the Apollonian group A. Theorem 1.3 states that there is a positive integer r_0 such that the set points $\mathbf{x} \in \mathscr{P}$ for which $f(\mathbf{x})$ has at most r_0 prime factors is Zariski dense in $\mathrm{Zcl}(\mathscr{P}) = C$. To specify this r_0, one would need to apply the affine sieve developed in [**7**] – in particular, one would need to input the spectral gap which comes from the expander property of the group as described in Theorem 1.2. One way to realize this expander property is by analyzing the discrete spectrum of the Laplacian of $A\backslash\mathbb{H}^3$, which is difficult as we mentioned before.

Luckily for us, the Apollonian group has some nice properties which are characteristic of most Schottky groups that allow us to compute an upper bound for $r_0(\mathscr{P}, f)$ by studying the question for orbits of subgroups generated by a unipotent element. This problem reduces to sieving for polynomials in $\mathbb{Z}[x]$ and does not require the sophisticated tools developed in [**7**].

We are able to prove a stronger statement regarding the saturation number if we consider $f(\mathbf{x})/12$ as opposed to just $f(\mathbf{x})$. Specifically, it is known (see [**19**]) that every point in any primitive orbit of A contains two even coordinates and two odd coordinates. Also, we can see from the diagrams of possible Apollonian orbits mod 3 in Figures 3 and 4 that $f(\mathbf{x}) \equiv 0 \bmod 3$ for any x in a primitive orbit of A (this is not true mod 9). With this in mind, we have the following.

THEOREM 3.1. *For $\mathbf{x} = (x_1, x_2, x_3, x_4) \in \mathscr{P}$ let $f(\mathbf{x}) = x_1x_2x_3x_4$, and let $\mathscr{P}_{28}$ denote those points $\mathbf{x} \in \mathscr{P}$ for which $f(\mathbf{x})/12$ has at most 28 prime factors. Then $\mathscr{P}_{28}$ is Zariski dense in* $\mathrm{Zcl}(\mathscr{P})$.

Proof: Note that the product of any two of the group generators S_1, S_2, S_3, and S_4 is a unipotent element – for example,

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

Taking kth powers of these unipotent elements associates every ordered pair (i, j) where $1 \leq i, j \leq 4$ and $i \neq j$ with a map ϕ_{ij} from $\mathbb{Z}$ into the Apollonian group A:

$$\mathbb{Z} \xrightarrow{\phi_{ij}} A$$

$$k \longmapsto (S_iS_j)^k.$$

Denote by U_{ij} the group generated by S_iS_j and its inverse. Recall that the orbits of A and thus the orbits of U_{ij} lie on the affine cone C defined in (1.2). In particular, for $\mathbf{v} \in C$ the Zariski closure $\mathrm{Zcl}(U_{ij}\mathbf{v})$ of the orbit $U_{ij}\mathbf{v}$ is a curve on C, and the collection of all such curves associated with the orbits of U_{ij} make up a Zariski dense subset of C.

We first prove that the set of integer points $\mathbf{x}$ on a curve associated with a group U_{ij} for which $f(\mathbf{x})/12$ has at most 28 prime factors is Zariski dense in the curve. The fact that $r_0(\mathscr{P}, f) = 28$ then follows from the fact that the curves associated with the subgroups U_{ij} are dense on the cone.

We write

$$n = P_r^{12}$$

if $n/12$ has at most r prime factors. With this notation we have the following lemma.

LEMMA 3.2. *Let U_{ij} be the group generated by S_iS_j and its inverse, and let $v = (-1,2,2,3)$. Denote the orbit of U_{ij} acting on v by $O(i,j)$, and define $O_{28}(i,j)$ as follows:*

$$O_{28}(i,j) = \{(x_1,x_2,x_3,x_4) \in O(i,j) | x_1x_2x_3x_4 = P_{28}^{12}\}.$$

Then the Zariski closure of O_{28} is $\mathrm{Zcl}(O(i,j))$.

We use a standard setup of a 4-dimensional sieve (see [**25**], for example) to prove Lemma 3.2. Let $\mathbf{x} = (x_1,x_2,x_3,x_4)$ be a point in the orbit $O(i,j)$ of one of our subgroups U_{ij}. For $T > 10$, let $F_T : \mathbb{R}^4 \to \mathbb{R}$ be a family of smooth functions depending only on the Euclidean norm $|\mathbf{x}|$ of $\mathbf{x}$, such that

$$\begin{cases} (i) & 0 \le F_T(\mathbf{x}) \le 1; \\ (ii) & F_T(\mathbf{x}) = 1 \qquad \text{if } |\mathbf{x}| \le T/c_0; \\ (iii) & F_T(\mathbf{x}) = 0 \qquad \text{if } |\mathbf{x}| \ge c_0T. \end{cases}$$

where c_0 is a positive constant that depends on i and j. With F_T as above, for $n \ge 0$ we define

$$a_n(T) := \sum_{\substack{\mathbf{x}\in O(i,j) \\ x_1x_2x_3x_4=n}} F_T(\mathbf{x}), \tag{3.1}$$

and denote the sequence by $\mathscr{A} := \{a_n\}$. Let

$$X = \sum_{n\ge1} a_n(T). \tag{3.2}$$

Note that X counts the number of points of the orbit in a ball of radius T. Our aim is to compute the following sum over r-almost prime n:

$$\sum_{n=P_r^{12}} a_n(T).$$

To estimate this sum, we restrict the sum in (3.2) to $n \equiv 0 \bmod d$ for a square free integer $1 < d < D$ where D is taken to be a small power of T. We write

$$\mathscr{A}_d = \{a_n \in \mathscr{A} | n \equiv 0 (\bmod d)\}$$

for $d \in \mathbb{Z} - \{0\}$ and define

$$\omega(d) := \#\{\mathbf{x} \in O(i,j) \,|\, x_1x_2x_3x_4 \equiv 0 \,(\mathrm{mod}\, d)\}. \tag{3.3}$$

Note that $\omega(d)$ is a nonnegative multiplicative function and that if $B = \{2,3\}$ is the finite set of bad primes in Theorem 2.1 and p denotes a prime, we have

$$\begin{cases} \omega(1) = 1; \\ 0 \leq \omega(p) < p, & \text{if } p \notin B; \\ \omega(p) = p, & \text{if } p \in B; \end{cases} \tag{3.4}$$

We prove the following condition on $\omega(d)$ which is necessary to carry out the sieve in this context (see [**25**] for further explanation of this condition).

LEMMA 3.3. *Let $\omega(d)$, X, and $\mathscr{A}_d$ be as above, and let p denote a prime.*

(i) *There are fixed constants $\kappa > 1$ and $A \geq 2$ such that for any z_1 and z with $2 \leq z_1 < z$ we have*

$$\prod_{z_1 \leq p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \leq \left(\frac{\log z}{\log z_1}\right)^{\kappa} \left(1 + \frac{A}{\log z_1}\right). \tag{3.5}$$

(ii) *If R_d denotes the error term*

$$R_d := |\mathscr{A}_d| - \frac{\omega(d)}{d} X,$$

then there exist some constants τ with $0 < \tau < 1$, $A_1 \geq 1$, and $A_2 \geq 2$ such that

$$\sum_{\substack{d < X^{\tau} \log^{-A_1} X \\ (d, \mathscr{P}) = 1}} \mu^2(d) 4^{\nu(d)} |R_d| \leq A_2 \frac{X}{(\log X)^{\kappa+1}}, \tag{3.6}$$

where $\nu(d)$ denotes the number of prime factors of d.

PROOF. Since the groups U_{ij} are generated by two of generators of the Apollonian group which fix two of the coordinates of the root quadruple $\mathbf{v}$, we have that two of the x_i in (3.4) remain constant throughout the orbit $O(i,j)$. Therefore $n \geq c_1 T^2$ for some constant c_1.

The elements of the orbits $O(i,j)$ can be summarized as follows:

$$\begin{aligned} O(1,2) &= (20s^2 + 4s - 1, 20s^2 - 16s + 2, 2, 3), \\ O(1,3) &= (20s^2 + 4s - 1, 2, 20s^2 - 16s + 2, 3), \\ O(1,4) &= (16s^2 - 1, 2, 2, 16s^2 - 16s + 3), \\ O(2,3) &= (-1, 8s^2 + 4s + 2, 8s^2 - 4s + 2, 3), \\ O(2,4) &= (-1, 4s^2 + 2, 2, 4s^2 - 4s + 3), \\ O(3,4) &= (-1, 2, 4s^2 + 2, 4s^2 - 4s + 3). \end{aligned}$$

for nonnegative $s \in \mathbb{Z}$. Also, for our purposes the orbits $(S_iS_j)^k\mathbf{v}$ and $(S_jS_i)^k\mathbf{v}$ are equivalent, since the two differ by a permutation of coordinates and changing the sign of s above.

As in the statement of Lemma 3.2, we consider products of the coordinates of points in the $O(i,j)$ above, which yields four different possible polynomials:

$$\begin{aligned} p_1(s) &= 2400s^4 - 1440s^3 - 264s^2 + 144s - 12, \\ p_2(s) &= 1024s^4 - 1024s^3 + 128s^2 + 64s - 12, \\ p_3(s) &= -192s^4 - 48s^2 - 12, \text{ and} \\ p_4(s) &= -32s^4 + 32s^3 - 40s^2 + 16s - 12. \end{aligned} \tag{3.7}$$

for nonnegative $s \in \mathbb{Z}$. Each of these polynomials gives rise to a different $\omega(d)$. Namely, let

$$V_{d_i} := \{s \in \mathbb{Z}/d\mathbb{Z} \,|\, p_i(s) \equiv 0 \,(\mathrm{mod}\, d)\}$$

denote the set of values of s modulo d for which $p_i(s) \equiv 0 \bmod d$ and let

$$\omega_i(d) := |V_{d_i}|$$

denote the cardinality of this set. Clearly, $\omega(d)$ is multiplicative, and for all but a finite set of primes we have

$$\begin{aligned} \frac{\omega_1(p)}{p} = \frac{|V_{p_1}|}{p} &= \begin{cases} \frac{4}{p} & \text{if 6 is a square mod } p \\ 0 & \text{otherwise} \end{cases} \\ \frac{\omega_2(p)}{p} = \frac{|V_{p_2}|}{p} &= \frac{3}{p} \\ \frac{\omega_3(p)}{p} = \frac{|V_{p_3}|}{p} &= \begin{cases} \frac{4}{p} & \text{if } -3 \text{ is a square mod } p \\ 0 & \text{otherwise} \end{cases} \\ \frac{\omega_4(p)}{p} = \frac{|V_{p_4}|}{p} &= \begin{cases} \frac{4}{p} & \text{if } -2 \text{ is a square mod } p \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

Note that for every $1 \le i \le 4$ we have that

$$\prod_{z_1 \le p < z} \left(1 - \frac{\omega_i(p)}{p}\right)^{-1} \le \prod_{z_1 \le p < z} \left(1 - \frac{4}{p}\right)^{-1}$$

So, by Merten's theorem, there is a constant $A \ge 2$ such that

$$\prod_{z_1 \le p < z} \left(1 - \frac{\omega_i(p)}{p}\right)^{-1} \le \left(\frac{\log z}{\log z_1}\right)^4 \left(1 + \frac{A}{\log z_1}\right) \text{ for } 2 \le z_1 < z, \tag{3.8}$$

establishing (3.5) with

$$\kappa = 4.$$

We also have that for every $1 \le i \le 4$

$$|\mathscr{A}_d| = \sum_{n \equiv 0 \,(\mathrm{mod}\, d)} a_n(T) = \frac{\omega_i(d)}{d} X + R_d(T) \tag{3.9}$$

where the error term is

$$R_d(T) \ll cT^{1/2}$$

for some constant c, as desired. □

Denote by μ a constant for which

$$\max_{a_n \in \mathscr{A}} n \leq X^{\tau\mu}. \tag{3.10}$$

Since $1 \leq n \ll T^2$ for $a_n \in \mathscr{A}$, we have that (3.10) holds with

$$\tau\mu = 2. \tag{3.11}$$

To prove Lemma 3.2, we recall the following lemmas from [**25**], using the same notation as above.

LEMMA 3.4. *Let $\kappa > 1$ be given, and let $\sigma_\kappa(u)$ be the continuous solution of the differential difference problem*

$$\begin{cases} u^{-\kappa}\sigma(u) = A_\kappa^{-1}, & \text{for } 0 < u < 2, A_\kappa = (2e^\gamma)^\kappa \Gamma(\kappa+1), \\ (u^{-\kappa}\sigma(u))' = -\kappa u^{-\kappa-1}\sigma(u-2), & \text{for } 2 < u; \end{cases}$$

where γ denotes the Euler contant. Then there exist numbers α_κ and β_κ, satisfying

$$\alpha_\kappa \geq \beta_\kappa \geq 2$$

such that the simultaneous differential-difference system

$$\begin{cases} F(u) = 1/\sigma_\kappa(u), & \text{for } 0 < u \leq \alpha_\kappa, \\ f(u) = 0, & \text{for } 0 < u \leq \beta_\kappa, \\ (u^\kappa F(u))' = \kappa u^{\kappa-1} f(u-1), & \text{for } u > \alpha_\kappa, \\ (u^\kappa f(u))' = \kappa u^{\kappa-1} F(u-1), & \text{for } u > \beta_\kappa, \end{cases} \tag{3.12}$$

has continuous solutions $F_\kappa(u)$ and $f_\kappa(u)$ such that

$$F_\kappa(u) = 1 + O(e^{-u}),\ f_\kappa(u) = 1 + O(e^{-u}), \tag{3.13}$$

and that $F_\kappa(u)$ and $f_\kappa(u)$, respectively, decreases and increases monotonically towards 1 as u approaches infinity.

LEMMA 3.5. *Let $\mathscr{A}$, B, ω, F_κ, f_κ, τ, and ν be as above. Then, for any two real numbers u and v satisfying*

$$\frac{1}{\tau} < u \leq v,\ \beta_\kappa < \tau\nu,$$

we have

$$\sum_{n \in P_r^{12}} a_n \gg X \prod_{p < X^{1/v}} \left(1 - \frac{\omega(p)}{p}\right) \tag{3.14}$$

only when

$$r > \tau\mu u - 1 + \frac{\kappa}{f_\kappa(\tau\nu)} \int_1^{\nu/u} F_\kappa(\tau\nu - s)\left(1 - \frac{u}{\nu}s\right)\frac{ds}{s}. \tag{3.15}$$

Using this setup, we proceed to prove Lemma 3.2.

PROOF OF LEMMA 3.2: According to Lemma 3.5, we have

$$\sum_{n=P_r^{12}} a_n(T) \gg X \prod_{p<X^{1/v}} \left(1-\frac{\omega(p)}{p}\right) \tag{3.16}$$

provided that

$$r > 4u-1+\frac{4}{f_4(\tau v)}\int_1^{v/u} F_3(\tau v-s)\left(1-\frac{u}{v}s\right)\frac{ds}{s}. \tag{3.17}$$

While we do not compute $F_4(u)$ and $f_4(u)$ explicitly, we can use estimates for τu and τv:

$$\tau u = 1+\xi-\frac{\xi}{\beta_\kappa},\ \ \tau v = \frac{\beta_\kappa}{\xi}+\beta_\kappa-1,$$

where $0<\tau\leq 1$ and $\kappa>1$, with $0<\xi<\beta_\kappa$. In our case, $\kappa=4$ and $\tau=\frac{1}{4}-\frac{7}{128}$ is the closest value to the Selberg conjecture.

So, our estimate for possible r is

$$\begin{aligned} r &> \mu+\xi\mu-\frac{\xi\mu}{\beta_4}-1+(4+\xi)\log\frac{\beta_4}{\xi}-4-\frac{4\xi}{\beta_4} \\ &= (1+\xi\mu)-1+(4+\xi)\log\frac{\beta_4}{\xi}-4-\xi\frac{\mu-4}{\beta_4}. \end{aligned} \tag{3.18}$$

From the table of β's in [**25**], we have that

$$\beta_4 = 9.0722,$$

and it remains to find the minimum of the function in (3.18). A simple program in Matlab yields that the minimum is just under 28. We combine 3.8 and 3.16 to get

$$\sum_{n=P_{28}^{12}} a_n(T) \gg \sum_{\substack{p<X^{1/v}\\ p\notin\mathscr{B}}} \left(1-\frac{4}{p}+O\left(\frac{1}{p^2}\right)\right) \gg \frac{X}{(\log X)^4}.$$

Therefore O_{28} is Zariski dense in $\mathrm{Zcl}(O(i,j))$, as desired (see [**38**] for a discussion). □

The proof of Theorem 3.1 is now straightforward:

PROOF. Since each of the curves $\mathrm{Zcl}(O(i,j))$ we analyzed are Zariski dense in the cone C, and since the corresponding subgroups span all of A, Lemma 3.2 extends to the points on the whole cone. □

It is worthwhile to note that, while we avoid dealing with the spectral analysis of A in this case by utilizing the unipotent elements in the group, it is still an important problem to determine the spectrum of the Laplacian on its fundamental domain both in this case and in the general case of groups acting on hyperbolic space with infinite volume fundamental domain. However, even in computing this spectrum, we would likely make use of the nice structure and the presence of unipotent elements in the group in question.

4. A prime number theorem

Another natural application of the affine sieve is counting points with prime coordinates in an orbit of the group. In [**35**], the authors use the sieve to give an upper bound on the number $\pi_P(X)$ of circles of prime curvature less than X in a given packing P (see Theorem 1.7). Combining this with the analysis in Chapter 2 of this thesis, one obtains heuristic asymptotics for $\pi_P(X)$ which are computed and checked in [**19**]. The same can be done in the case of counting circles of prime curvature at generation T, rather than according to their size. In this section, we give a heuristic for a prime number theorem for ACP's in the generation case (an upper bound has been computed in [**7**]). Our heuristic argument suggests the following conjecture.

CONJECTURE 4.1. *Let $\pi^P_{gen}(T)$ denote the number of circles of prime curvature in a primitive packing P which are born at generation T. Then*

$$\pi^P_{gen}(T) \sim \frac{N(T)\cdot L(2,\chi_4)}{\gamma T},$$

where $\gamma = 0.9149\ldots$, $N(T) = 4\cdot 3^{T-1}$ is the number of circles born at generation T in the packing P, and $L(2,\chi_4) = 0.91597\ldots$ is the value of the Dirichlet L-function at 2 with character

$$\chi_4(p) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ (mod 4)} \\ -1 & \text{if } p \equiv 3 \text{ (mod 4)} \end{cases}$$

The value γ in the conjecture above is the Lyapunov exponent in the case of a random walk on the generators S_i of A (see Lemma 4.3). Since γT is meant to be a good estimate for most values $\log(a(C_T))$, where C_T is a circle at generation T and $a(C)$ is its curvature, Conjecture 4.1 has the same flavor as the classical prime number theorem over the integers.

In support of this, we give a heuristic argument based on the assumption that the Moebius function μ is random which yields Conjecture 4.2 below, in which we consider the problem of counting circles of prime curvature p with a weight of $\log p$. At the end of this section we show that Conjecture 4.2 implies Conjecture 4.1 and test the conjectures in the cases $T \leq 14$ using a program in Matlab.

CONJECTURE 4.2. *Let p denote a prime, let C_T denote a circle born at generation T, and let $a(C_T)$ denote its curvature. Given a primitive packing P, let*

$$\psi^P_{gen}(T) = \sum_{\substack{C_T \\ a(C_T)=p}} \log p$$

Then we have

$$\psi^P_{gen}(T) \sim N(T)\cdot L(2,\chi_4) \tag{4.1}$$

where $N(T)$ and $L(2,\chi_4)$ are as before.

Remarkably, the heuristic obtained in [**19**] for $\psi_P(X)$, the weighted count of circles with prime curvature less than X, is nearly identical to our Conjecture 4.2.

The main difficulty in counting primes using a combinatorial norm (generation) as we do here is that one doesn't immediately know how large the curvatures of circles born at generation T are with respect to T. Graham et.al. conjecture in [**24**] that this depends only on the generation and on the Hausdorff dimension $\delta = 1.3056\ldots$ of the residual set of the packing. Specifically, they predict

$$\lim_{T\to\infty} \frac{1}{T} \log M_T = \frac{\log 3}{\delta} = 0.8415\ldots \tag{4.2}$$

where M_T denotes the median of the curvatures of circles born at generation T. However, this prediction appears to be slightly inaccurate for most packings. It is more natural to consider the expectation of $(\log a(C_T))/T$ over curvatures $a(C_T)$ of all circles C_T born at generation T instead of the value $(\log M_T)/T$. In this case it is known that there exists a constant γ known as the Lyapunov exponent so that

$$\lim_{T\to\infty} \mathbb{E}\left(\frac{1}{T}\log a(C_T)\right) = \gamma \tag{4.3}$$

It is possible that γ does in fact depend on the Hausdorff dimension δ. However, since it is very difficult to determine γ explicitly, we can only approximate it experimentally and its dependence on δ is unclear.

The existence of a Lyapunov exponent for ACP's comes from a version of the Furstenburg-Kesten theorem regarding random walks on Markovian sequences of matrices. The original Furstenburg-Kesten theorem concerns sequences of independent, identically distributed matrices; since we are interested in chains of matrices of length T comprised of the four generators $\{S_1, S_2, S_3, S_4\}$ of A which cannot be reduced via the relation

$$S_i^2 = I \text{ for } 1 \leq i \leq 4 \tag{4.4}$$

the original theorem does not quite apply, and we refer to [**1**] and [**50**] for generalizations. We first introduce the notion of word length of a vector in an orbit of A. For $\mathbf{x} \in \mathscr{P}$, write

$$\mathbf{x} = \prod_{j=1}^{k} S(j)\mathbf{v} \tag{4.5}$$

where $S(j) \in \{S_1, S_2, S_3, S_4\}$, the set of generators of the Apollonian group. Denote by $w(\mathbf{x})$ the smallest possible k in (4.5) and call $w(\mathbf{x})$ the *word length* of $\mathbf{x}$. A word of length T in these matrices is *reduced* if it is of the shortest length in the class of words equivalent up to (4.4). With this in mind, we have the following lemma which has been proven in various degrees of generality by Furstenburg, Kesten, Oseledec, and others.

LEMMA 4.3. *Let* $\mathbf{S} = \{S_1, S_2, S_3, S_4\}$ *be the set of generators of the Apollonian group as before and let* $\mathbf{v}$ *be the root quadruple of a packing. For* $S(i) \in \mathbf{S}$*, let* $\mathbf{v}_T = \prod_{i=1}^{T} S(i)\mathbf{v}$ *denote a vector of reduced word length* T.

(i) *There exists a constant γ, called the Lyapunov exponent, such that*

$$\lim_{T\to\infty} \frac{\log||\mathbf{v}_T||}{T} = \gamma, \tag{4.6}$$

where $||\mathbf{x}|| = \max_i(x_i)$ for a 4-dimensional vector $\mathbf{x} = (x_1, x_2, x_3, x_4)$.

(ii) *Let $\mathbb{E}(X)$ denote the expectation of X. There is a constant α such that*

$$\lim_{T\to\infty} \mathbb{E}\left(\frac{(\log||v_T|| - \gamma T)^2}{T}\right) \sim \alpha T + o(T) \tag{4.7}$$

(iii) *Let $\mathbb{P}(X)$ denote the probability of X. We have $\mathbb{P}\left(\frac{(\log||v_T||-\gamma T)^2}{T} \geq T^{1-\varepsilon}\right) \leq \alpha/T^{1-\varepsilon}$*

(iv) $\mathbb{P}\left(\frac{(\log||v_T||-\gamma T)^4}{T^2} \geq T^{2-\varepsilon}\right) \leq 720 \cdot \alpha^2/T^{2-\varepsilon}$

For our purposes, Lemma 4.3 implies that if $a(C_T)$ denotes the curvature of a circle C_T born at generation T, then $(\log a(C_T))/T$ is close to a constant γ for large T. Moreover, part (ii) of Lemma 4.3 implies that the distribution of $(\log a(C_T))/T$ is Gaussian for T large, and that the variance of this distribution is very small (meaning that the curvatures of circles born at generation T are mostly of the same size if T is large). Parts (iii) and (iv) are essentially Chebyshev inequalities for the second and fourth moments of $(\log||v_T|| - \gamma T)/\sqrt{T}$. We rely on this in estimating the magnitude of $a(C_T)$ in order to predict the number of primes born at generation T.

In practice one can prove that the Lyapunov exponent γ exists, but there is currently no algorithm to determine what γ should be, given a set of generators $\{S_i\}$. We approximate γ as well as the constant α in Lemma 4.3 by running a computer program to evaluate $\log(a(C_T))/T$ for various ACP's and $10 \leq T \leq 100$. The data suggests that

$$\gamma \approx 0.9149,\ \alpha \approx 0.065. \tag{4.8}$$

Lemma 4.3 then predicts that for circles C_T born at a large generation T, we expect 95 percent of the values of $\log(a(C_T))/T$ to be within the interval $[0.8325, 0.9875]$. In Figures 1 and 2, we show histograms of the values of $\log(a(C))/100$, where C denotes a circle born at generation 100 in two different packings. The curves depicted in these figures are the Gaussian curves of mean γ and variation $6.4 \cdot 10^{-4}$.

With this relationship between the generation of circles and the magnitude of their curvatures, we are able to give a heuristic for the number of circles with prime curvature at generation T.

We first count circles of prime curvature p with a weight of $\log p$ using Selberg's upper bound sieve in the affine setting – we calculate this by assuming that the Moebius μ function is random, and Lemma 4.3 does not play a significant role in this calculation. It is crucial, however, when we proceed to remove the weights of $\log p$ at the end, as well as in checking that the number of circles of curvature p^i for $i > 1$ is small compared to the number of prime circles.

Unlike our approach to proving Theorem 3.2, where we used unipotent elements in the Apollonian group A to reduce the problem to a sieve simply over the integers, the sieve here is over the *orbit* of A, and we rely heavily on Theorem 1.2 to control the remainder term in the sieve.

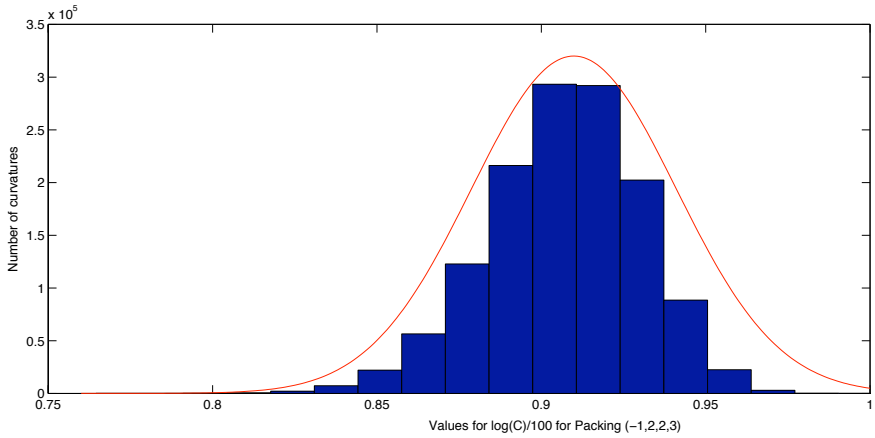

FIGURE 1. Histogram for the packing $(-1,2,2,3)$ at generation 100

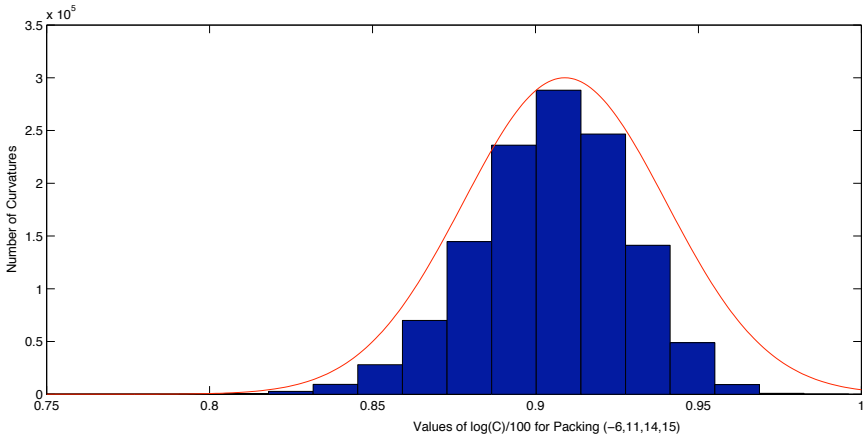

FIGURE 2. Histogram for packing $(-6,11,14,15)$ at generation 100

As before we have a finite sequence $\mathscr{A} := \{a_n\}$ where

$$a_n = (\log n) \cdot \#\{\text{circles of curvature } n \text{ born at generation } T\}$$

for $n \geq 1$. Let X denote the sum

$$\sum_n a_n = X,$$

and let z be a small power of X (note that both X and z are very large if we consider a large enough generation T). Let $B' := \{2,3\}$ and define $P(z)$ to be the product of all primes $p \notin B'$ that are less than z:

$$P(z) = \prod_{\substack{p \leq z \\ p \notin B'}} p.$$

With this notation, the expression we need for the heuristic in Conjecture 4.2 is the sum

$$S(\mathscr{A}, P(z)) = \sum_{(n,P(z))=1} a_n. \tag{4.9}$$

We evaluate this sum by considering sums over congruence classes $n \equiv 0 \pmod{d}$. We first check that the following sieve conditions hold.

(1) For square free $1 < d < X$, let

$$X_d := \sum_{d|n} a_n.$$

Then there is a multiplicative function $\beta(d)$ so that

$$\beta(p) \leq 1 - \frac{1}{c_1} \text{ for a fixed } c_1 \tag{4.10}$$

where p is prime, and

$$X_d = \beta(d)X + R(\mathscr{A}, d).$$

We assume as before that the main term $\beta(d)X$ is a good approximation to X_d, so that the error term $R(\mathscr{A}, d)$ is very small in comparison.

(2) $\mathscr{A}$ has level distribution $D(X) < X-$ that is,

$$\sum_{d \leq D} |r(d,A)| \ll X^{1-\alpha_0} \text{ for some } \alpha_0 > 0.$$

(3) $\mathscr{A}$ has sieve dimension $t > 0$, so that for a fixed C we have that

$$\left| \sum_{\substack{w \leq p \leq z \\ p \notin B'}} \rho(p) \log p - t \log \frac{z}{w} \right| \leq C$$

for $2 \leq w \leq z$.

To check (1), define $\beta(d) := \beta_T(d)$ as follows:

$$\beta_T(d) = \frac{\#\{\mathbf{v}_T \in \mathscr{P}(\mathbf{v})/d \mid ||\mathbf{v}_T|| \equiv 0 \,(\mathrm{mod}\, d)\}}{\#\{\mathbf{v}_T \in \mathscr{P}(\mathbf{v})/d\}}, \tag{4.11}$$

where $\mathbf{v}$ denotes a root quadruple, $\mathscr{P}_{\mathbf{v}}$ is the orbit of A acting on $\mathbf{v}$, and $\mathbf{v}_T$ is a vector of word length T. We also define

$$\beta_T^i(d) = \frac{\#\{\mathbf{v}_T \in \mathscr{P}(\mathbf{v})/d \mid ||\mathbf{v}_T|| = \mathbf{v}_T(i) \equiv 0 \,(\mathrm{mod}\, d)\}}{\#\{\mathbf{v}_T \in \mathscr{P}(\mathbf{v})/d \mid ||\mathbf{v}_T|| = \mathbf{v}_T(i)\}},$$

where $\mathbf{v}_T(i)$ denotes the ith coordinate of $\mathbf{v}_T$. From the multiplicativity of the orbit $\mathscr{P}$ modulo d in Theorem 3.5 we have the following lemma:

LEMMA 4.4. *Let $d = \prod p_i$ be the prime factorization of a square free integer $d > 1$ and let $\beta_T(d)$ be as above. Then*

(i) $\beta_T^j(d) = \prod \beta_T^j(p_i)$ *for* $T \geq 1$ *and* $1 \leq j \leq 4$.

(ii) $\beta_T^i(d) = \beta_T^j(d)$ *for* $1 \leq i, j \leq 4$.

(iii) *For any orbit $\mathscr{P}$ of A there exist two coordinates, i and j, such that*

$$\beta_T^i(2) = \beta_T^j(2) = 1,$$

$$\beta_T^k(2) = 0 \text{ for } k \neq i, j.$$

for any generation $T > 1$. We say that the ith and jth coordinates are even throughout the orbit, while the other two coordinates are odd throughout the orbit.

(iv) *For $p \neq 2$, let $\beta_T(p) = \beta_T^i(p)$ for $1 \leq i \leq 4$. Then*

$$\beta_T(p) = \begin{cases} \frac{1}{p+1} & \text{for } p \equiv 1 \ (4) \\ \frac{p+1}{p^2+1} & \text{for } p \equiv 3 \ (4) \end{cases} \tag{4.12}$$

for large enough T.

PROOF. The statements in (i) and (ii) follow from Theorem 4.5. Let $\mathbf{v}$ be the root quadruple (the quadruple of the smallest curvatures) of the packing P. To show (iii), note that any quadruple in a primitive integral ACP consists of two even and two odd curvatures (see [**19**] for a discussion). Without loss of generality, assume $\mathbf{v} = (1,1,0,0)$ mod 2, so $i = 1$ and $j = 2$ in this case. Since the Apollonian group is trivial modulo 2, we have that every vector in the orbit is of the form $(1,1,0,0)$ mod 2, so we have what we want.

To prove (iv), we recall from Theorem 4.5 that the reduction $\mathscr{P}_p$ of $\mathscr{P}$ mod p is the cone C_p for $p > 3$. Thus the numerator of $\beta_T^j(p)$ for T large is

$$\#\{\mathbf{v_T} \in \mathscr{P}_p \,|\, \mathbf{v}_T(j) = 0\} = \#\{(v_1, v_2, v_3) \in \mathbb{F}_p^3 - \{\mathbf{0}\} \,|\, Q(v_1, v_2, v_3, 0) = 0\}$$

where Q is the Descartes quadratic form and $p > 3$. So the numerator counts the number of nontrivial solutions to the ternary quadratic form obtained by setting one of the v_i in the Descartes form $Q(\mathbf{v})$ to 0. Similarly we have that the denominator of $\beta_T^j(p)$ is

$$\#\{\mathbf{v}_T \in \mathscr{P}_p\} = \#\{\mathbf{v} = (v_1, v_2, v_3, v_4) \in \mathbb{F}_p^4 - \{\mathbf{0}\} \,|\, Q(\mathbf{v}) = 0\}$$

where $p > 3$. So the denominator counts the number of nontrivial solutions to the Descartes form. The number of nontrivial solutions to ternary and quaternary quadratic forms over finite fields is well known (see [**9**], for example). Namely,

$$\#\{\mathbf{v} = (v_1, v_2, v_3, v_4) \in \mathbb{F}_p^4 - \{\mathbf{0}\} \,|\, Q(\mathbf{v}) = 0\} = \begin{cases} p^3 + p^2 - p - 1 & \text{for } p \equiv 1 \ (4) \\ p^3 - p^2 + p - 1 & \text{for } p \equiv 3 \ (4) \end{cases} \tag{4.13}$$

for $p > 3$, and

$$\#\{(v_1, v_2, v_3) \in \mathbb{F}_p^3 - \{\mathbf{0}\} \,|\, Q(v_1, v_2, v_3, 0) = 0\} = p^2 - 1 \text{ for all odd primes } p. \tag{4.14}$$

Combining (4.13) and (4.14), we obtain the expression in (4.12) for $p > 3$. For $p = 3$, we compute $\mathscr{P}_p$ explicitly and find that there are two possible orbits of A modulo 3 which are illustrated via finite graphs in Fig. 3 and Fig. 4. Both of these orbits consist of 10 vectors $\mathbf{v} \in \mathbb{Z}^4$. In both orbits, 4 of the vectors $\mathbf{v}_T$ have $\mathbf{v}_T(i) = 0$ for any $1 \leq i \leq 4$. Thus $\beta(3) = \frac{2}{5}$ as desired. □

Condition (2) is checked in [7] – it is proven using Theorem 1.2 and we have

$$D = X^{(1-\tau)/\dim G}, \tag{4.15}$$

where G in our case is $SO(3,1)$ of dimension 6, and

$$\tau = \frac{\log\left(\frac{\kappa+\sqrt{\kappa^2-4r}}{2}\right)}{\log r} < 1.$$

This can be seen from the fact that $\kappa < 4$ since the Cayley graph associated with A/d is a 4-regular graph, and $r = 3$.

Recall that

$$X = \sum_{\substack{a(C)\\ w(C)=T}} \log(a(C)),$$

where $a(C)$ denotes the curvature of a circle C in the packing, and $w(C)$ is the generation of C. We can evaluate this using the Lyapunov exponent in Lemma 4.3:

$$X = N(T)\gamma T + O(\sqrt{T}),$$

where $N(T) = 4 \cdot 3^{T-1}$ is the number of circles born at generation T. Therefore we have

$$D \leq (3^T \gamma T)^{\frac{1-\tau}{6}} \ll 3^{\alpha_0 T} \tag{4.16}$$

where α_0 is a small positive constant. Condition 3 follows quickly from the level distribution.

With the conditions of the sieve satisfied, we may now use it to obtain a heuristic for the number of circles of prime curvature born at generation T. In the notation above, we wish to compute

$$\sum_{\substack{a(C) \text{ prime}\\ w(C)=T}} \log(a(C)), \tag{4.17}$$

where C is a circle in the packing, $a(C)$ is the curvature of the circle, and $w(C)$ is the generation in which it is born. With this in mind, let

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

for which it is well known that $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.

In this notation, we compute $\psi^P_{gen}(T)$ as follows.

LEMMA 4.5. *Let v_T, $\psi^P_{gen}(T)$, and $\mathscr{P}$ be as before. Denote by $\psi^i_P(T)$ denote the sum of $\log(p)$ over circles born at generation T which have curvature p^i for p prime and $i > 1$:*

$$\psi^i_P(T) = \sum_{i>1} \sum_{\substack{w(x)=T\\ ||\mathbf{v}_T||=p^i}} \log p.$$

Then we have

$$\psi^P_{gen}(T) = -\sum_{\substack{\mathbf{v}_T \in \mathscr{P} \\ v_i^* \leq x}} \Lambda(||\mathbf{v}_T||) - \psi^i_P(T) \tag{4.18}$$

We first compute the sum in (4.18) and then show that $\psi^i_P(T)$ is of a smaller order of magnitude. Let D be the level distribution from Condition (2) of the sieve. To compute (4.18) we use the expression for $\Lambda(n)$ in terms of $d|n$ for moduli $1 < d \leq D$. Note that the number of vectors $\mathbf{v}_T$ whose maximal coordinate is the ith coordinate $\mathbf{v}_T(i)$ is the same as the number of vectors $\mathbf{v}_T$ whose maximal coordinate is in the jth coordinate $\mathbf{v}_T(j)$ for any $1 \leq i, j \leq 4$:

$$\#\{\mathbf{v}_T \in \mathscr{P} \,|\, ||\mathbf{v}_T|| = \mathbf{v}_T(i)\} = \#\{\mathbf{v}_T \in \mathscr{P} \,|\, ||\mathbf{v}_T|| = \mathbf{v}_T(j)\}$$

Combined with Lemma 4.5, this gives us

$$\begin{aligned} & -\sum_{1\leq i\leq 4} \sum_{\substack{\mathbf{v}_T\in\mathscr{P} \\ ||\mathbf{v}_T||=\mathbf{v}_T(i)}} \sum_{d|\mathbf{v}_T(i)} \mu(d)\log d \\ = \; & -\sum_{1\leq i\leq 4} \sum_{\substack{\mathbf{v}_T\in\mathscr{P} \\ ||\mathbf{v}_T||=\mathbf{v}_T(i)}} \sum_{d\leq D} \mu(d)\log d \sum_{\mathbf{v}_T(i)\equiv 0\,(d)} 1 \\ & -\sum_{1\leq i\leq 4} \sum_{\substack{\mathbf{v}_T\in\mathscr{P} \\ ||\mathbf{v}_T||=\mathbf{v}_T(i)}} \sum_{d> D} \mu(d)\log d \sum_{\mathbf{v}_T(i)\equiv 0\,(d)} 1 \end{aligned} \tag{4.19}$$

Assuming that the Moebius function $\mu(d)$ above becomes random as d grows, the sum over $d > D$ in (4.19) is negligible, and we omit it below. We proceed by rewriting the sum over $d \leq D$ in (4.19) using the density function $\beta_T(d)$ in (4.11). Recall that the analysis in [**7**] gives us that

$$\sum_{n\equiv 0\,(d)} a_n = \beta_T(d)\cdot N(T) + r(A,d)$$

where $r(A,d)$ is small on average. In particular,

$$\sum_{d\leq D} r(A,d) = \mathrm{O}(X^{1-\alpha_0})$$

for some $\alpha_0 > 0$. Paired with the assumption that μ is random, this evaluation of the remainder term allows us to rewrite (4.19) as follows:

$$\begin{aligned} & -\sum_{1\leq i\leq 4} \frac{N(T)}{4} \sum_{d\leq D} \beta^i_T(d)\mu(d)\log d + \mathrm{O}(X^{1-\alpha_0}) \\ = \; & -\frac{N(T)}{4} \sum_{1\leq i\leq 4} \sum_{d\leq D} \beta^i_T(d)\mu(d)\log d + \mathrm{O}(X^{1-\alpha_0}) \end{aligned} \tag{4.20}$$

To compute the innermost sum in the final expression above, note that

$$\sum_{d\leq D} \beta^i_T(d)\mu(d)\log d = \sum_{d>0} \beta^i_T(d)\mu(d)\log d - \sum_{d>D} \beta^i_T(d)\mu(d)\log d. \tag{4.21}$$

Assuming once again that the sum over $d > D$ is insignificant due to the conjectured randomness of the Moebius function, we have that the sum over $d \leq D$ in (4.21) can be approximated by the sum over all d. With this in mind, the following lemma yields the heuristic in Conjecture 4.2.

LEMMA 4.6. *Let $\beta_T^i(d)$ be as before. We have*

$$\sum_{1\leq i\leq 4}\sum_{d>0}\beta_T^i(d)\mu(d)\log d = 4\cdot L(2,\chi_4)$$

where $L(2,\chi_4) = 0.91597\ldots$ is the value of the Dirichlet L-function at 2 with character

$$\chi_4(p) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ (mod 4)} \\ -1 & \text{if } p \equiv 3 \text{ (mod 4)} \end{cases}$$

PROOF. We introduce a function

$$f(s) = \sum_d \beta_T^i(d)\mu(d)d^{-s},$$

and note that its derivative at 0 is precisely what we want:

$$f'(0) = -\sum_d \beta_T^i(d)\mu(d)\log d.$$

Since the functions β, μ, and d^s are all multiplicative, we may rewrite $f(s)$ as an Euler product and obtain

$$\begin{aligned} f(s) &= \prod_p \left(1-\beta_T^i(p)p^{-s}\right) \\ &= \prod_p (1-p^{-s-1})\cdot\frac{1-\beta_i(p)p^{-s}}{1-p^{-s-1}} \\ &= \zeta^{-1}(s+1)\cdot\prod_p \frac{1-\beta_i(p)p^{-s}}{1-p^{-s-1}} \\ &= \zeta^{-1}(s+1)\cdot H(s), \end{aligned}$$

where $H(s) = \prod_p (1-\beta_i(p)p^{-s})(1-p^{-s-1})^{-1}$ is holomorphic in $\Re(s) > 1/2$. Differentiating, we obtain

$$f'(0) = -\zeta'(1)\zeta^{-2}(1)\cdot H(0) + \zeta^{-1}(1)\cdot H'(0) = H(0)$$

since $-\zeta'(1)\zeta^{-2}(1) = 1$ and $\zeta^{-1}(1) = 0$. Thus it remains to compute

$$H(0) = \prod_p \frac{1-\beta_i(p)}{1-p^{-1}}.$$

Part (iii) of Lemma 4.4 says $\beta_T^i(2) = \beta_T^j(2) = 1$ for two coordinates $1 \le i, j \le 4$. For these two coordinates $1 - \beta_T^i(2) = 0$ and so $H(0) = 0$. Otherwise $\beta_T^i(2) = 0$ and we have

$$\begin{aligned} H(0) &= \frac{1}{1-\frac{1}{2}} \cdot \prod_{p \equiv 1\,(4)} \left(1 - \frac{1}{p+1}\right) \frac{1}{1-p^{-1}} \prod_{p \equiv 3\,(4)} \left(1 - \frac{p+1}{p^2+1}\right) \frac{1}{1-p^{-1}} \\ &= 2 \cdot \prod_{p \equiv 1\,(4)} \frac{p^2}{p^2-1} \prod_{p \equiv 3\,(4)} \frac{p^2}{p^2+1} \\ &= 2 \cdot L(2, \chi_4). \end{aligned}$$

Thus the sum we wish to compute is $4 \cdot L(2, \chi_4)$, as desired. □

Lemma 4.6 implies that the contribution of the two of the coordinates that are even throughout the orbit to the sum in (4.20) is 0, and the contribution for the other two coordinates is

$$\frac{N(T)}{4} \cdot 4 \cdot L(2, \chi_4) = N_P(x) \cdot L(2, \chi_4),$$

yielding the predicted result in Conjecture 4.2.

Determining the contribution from powers of primes:

We now use Selberg's upper bound sieve again to put a crude upper bound on $\psi_P^i(T)$. Define the sequence a_n' to be the sequence of logs of curvatures at level T which are primes or powers of primes:

$$a_n' := \log n' \cdot \#\{\text{circles of curvature } n \text{ at generation } T\}$$

for $n = p^i$ where $i \ge 1$ and p denotes a prime. We say a_n' is 0 otherwise. So we have

$$X' = \sum_n a_n',$$

where X' is approximated by $\psi_{gen}^P(T)$ above. We would like to compute this sum after removing all of the residue classes for which n is not a square mod d (this will count the curvatures which are even powers of primes). To this end, let Ω_d be the set of residue classes modulo d such that $\nu \in \Omega_d$ is a square mod d, and compute an upper bound for

$$S(A, \Omega) = \sum_{p < z'} \sum_{n \in \Omega_p} a_n',$$

where z' is the sieving limit for this sieve. Selberg's method is to bound this by $S^+(A, \Omega)$, where

$$S^+(A, \Omega) = \sum_n a_n' \Big(\sum_{\substack{d \\ n \in \Omega_p \\ \text{for every } p \mid d}} \lambda_d \Big)^2, \tag{4.22}$$

for any real numbers λ_d for $d | P'$, and $\lambda_1 = 1$, where

$$P' = \prod_{p < z'} p.$$

Expanding the expression in 4.22, we have

$$S^+(A,\Omega) = \sum_{d_1}\sum_{d_2} \lambda_{d_1}\lambda_{d_2} A_{\mathrm{lcm}(d_1,d_2)}(\Omega), \tag{4.23}$$

where

$$A_d(\Omega) = \sum_{\nu\in\Omega_d} \sum_{n\equiv\nu\ (d)} a_n.$$

Again, in order to carry out the sieve, we must check that the afore-mentioned sieve conditions hold. This follows once again from [7], and we get that

$$A_d(\Omega) = \rho(d)X' + r(d,\Omega),$$

with level distribution is $\sqrt{D}$, where D is the level of our first sieve in (4.16). One aspect of Selberg's idea is the optimization of the λ_d's chosen in expression (4.23). This is done in [**?**], yielding

$$S^+(A,\Omega) = GX' + R,$$

where $G = J^{-1}$, with

$$J = \sum_{d\le\sqrt{D}, d|P'} h(d),$$

where $h(d)$ is the multiplicative function

$$h(p) = \frac{\rho(p)}{1-\rho(p)},$$

where ρ is the density function for Ω in our orbit. This gives a crude estimate

$$J \approx \sqrt{D},$$

and so

$$\psi_T^{2i}(P) \ll \frac{2N(T)L(2,\chi_4)}{3^{\frac{\alpha_0 T}{2}}} \ll O(3^{\alpha' T})$$

where $\alpha' > 0$ is small. Computing bounds for $\psi_T^{2i+1}(P)$ in the case of odd powers is identical. This gives us

$$\psi_T^{i}(P) \ll O(3^{\alpha' T}),$$

and

$$\psi_{gen}^{P}(T) = N(T)\cdot L(2,\chi_4) + O(3^{\alpha' T}) \tag{4.24}$$

which yields the heuristic in Conjecture 4.2. Now we have only to deduce from this a formula for $\pi_{gen}^{P}(T)$, which counts prime curvatures without a weight of log.

LEMMA 4.7. *Conjecture 4.2 implies Conjecture 4.1.*

PROOF. Note that part (iv) of Lemma 4.3 implies

$$\begin{aligned}\frac{\psi^P_{gen}(T)}{N(T)} &= \sum_{\substack{|a(C_T)-e^{\gamma T}|<T^{1-\varepsilon'}\\ a(C_T)=p}} \frac{\log p}{N(T)} + \sum_{\substack{|a(C_T)-e^{\gamma T}|\geq T^{1-\varepsilon'}\\ a(C_T)=p}} \frac{\log p}{N(T)} \\ &\leq \sum_{a(C_T)=p} \frac{\gamma T}{N(T)} + \frac{720\cdot\alpha^2}{T^{2-\varepsilon}} \\ &\leq \frac{\gamma T\cdot \pi^P_{gen}(T)}{N(T)} + o(T)\end{aligned}$$

Therefore

$$\liminf_{T\to\infty} \pi^P_{gen}(T) \geq \frac{N(T)\cdot L(2,\chi_4)}{\gamma T} - o(T). \tag{4.25}$$

On the other hand, let

$$\psi^P_{gen}(T)^+ := \sum_{\substack{a(C_T)=p\\ a(C_T)\geq e^{\gamma T/2}}} \log p \tag{4.26}$$

$$\pi^P_{gen}(T)^- := \sum_{\substack{a(C_T)=p\\ a(C_T)< e^{\gamma T/2}}} 1.$$

Since each $\log p \geq \gamma T$ for every p in the sum in (4.26), we have

$$\psi^P_{gen}(T)^+ \geq \left(\pi^P_{gen}(T) - \pi^P_{gen}(T)^-\right)\cdot \gamma T \tag{4.27}$$

Note that if V is the area of the outermost circle in the packing (this constant is fixed for any given P), there are at most $V\cdot e^{\gamma T}$ circles of curvature $e^{\gamma T/2}$. Combined with Conjecture 4.2 this implies

$$\limsup_{T\to\infty} \frac{\psi^+_P(T) + \pi^-_P(T)\cdot\gamma T}{N(T)} \leq L(2,\chi_4) + \limsup_{T\to\infty} \frac{V\cdot e^{\gamma T}\cdot \gamma T}{N(T)}$$

Combined with (4.27) this gives us

$$L(2,\chi_4) + \limsup_{T\to\infty} \frac{e^{\gamma T}\cdot\gamma T}{N(T)} \geq \limsup_{T\to\infty} \frac{\pi^P_{gen}(T)\cdot\gamma T}{N(T)}$$

Since $N(T) > 3^T$, the lim sup on the left is 0, and so

$$\limsup_{T\to\infty} \pi^P_{gen}(T) \leq \frac{N(T)\cdot L(2,\chi_4)}{\gamma T}. \tag{4.28}$$

Together with (4.25), this implies that

$$\pi^P_{gen}(T) \sim \frac{N(T)\cdot L(2,\chi_4)}{\gamma T},$$

as desired. □

Conjecture 4.1 is supported by experimental data – Figure 5 depicts a dotted graph of our heuristic for $\frac{\pi^P_{gen}(T)}{N(T)}$ and the graph of the true $\frac{\pi^P_{gen}(T)}{N(T)}$ for the first 14 generations for the packing generated by $(-1,2,2,3)$.

We note that this process of determining a prime number theorem conjecture can be mimicked for any orbit of a group satisfying the conditions of [**7**], for which a Lyapunov exponent can be experimentally determined.

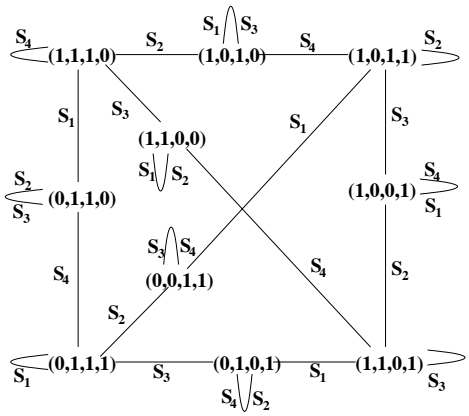

FIGURE 3. Orbit I modulo 3

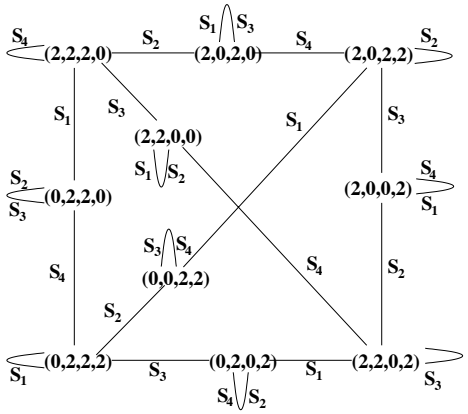

FIGURE 4. Orbit II modulo 3

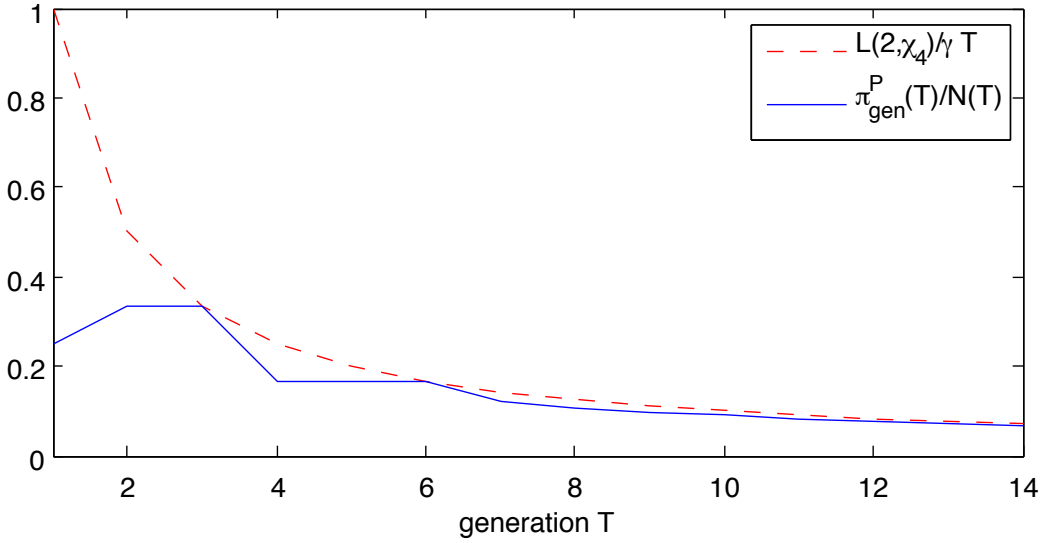

FIGURE 5. Comparison of experimental prime count to heuristic calculation of the number of prime curvatures in the packing generated by $(-1,2,2,3)$ for the first 14 generations.

CHAPTER 4

Density of Curvatures *(joint with Jean Bourgain)*

So far we have seen that the integers that come up in any given ACP behave very similarly to all of $\mathbb{Z}$ in general – there are very few local obstructions which we have defined completely in Chapter 2, there are infinitely many prime numbers in any packing, and the conjectured prime number theorem in the case of ACP's mimics the classical prime number theorem over the integers. This suggests that the curvatures in a given packing have positive density in $\mathbb{N}$, as conjectured by Graham et.al. in [**24**].

Ultimately, one would like to show that if

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

is the number of integers less than X counted without multiplicity which appear as curvatures in a given packing P, the limit below exists and is positive:

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

The local to global conjecture for ACP's as phrased in [**19**] predicts that this limit always exists and that

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

depending on the packing P. In this chapter, we make progress towards Graham et.al. exploit the existence of unipotent elements of A in [**24**] to establish the lower bound below for the number $\kappa(P,X)$ of distinct curvatures less than X of circles in an integer packing P:

$$\kappa(P,X) \gg_P \sqrt{X} \tag{0.29}$$

where we recall the notation

$$y \gg_\beta z \text{ or } y \ll_\beta z$$

is taken to mean that there exists a constant $c > 0$ depending only on β such that

$$y \geq cz \text{ or, respectively } y \leq cz.$$

Graham et.al. conjectured that the integers represented as curvatures in a given ACP actually make up a positive fraction of the positive integers $\mathbb{N}$, and in [**47**] Sarnak uses the existence of arithmetic Fuchsian subgroups of A to get a bound of

$$\kappa(P,X) \gg_P \frac{X}{\sqrt{\log X}} \tag{0.30}$$

towards Graham.et.al.'s positive density conjecture. This method, which we summarize in Section 1, was further improved to yield a bound of

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

where $\alpha = 0.150\ldots$ in [**18**].

In this chapter, written jointly with Jean Bourgain, we settle the positive density question of Graham et.al. in the following theorem:

THEOREM 0.8. *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*

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

where the implied constant depends on the packing P.

We treat this question by counting curvatures in different "subpackings" of an ACP. Namely, we fix a circle C_0 of curvature a_0 and investigate which integers occur as curvatures of circles tangent to C_0. This gives the preliminary lower bound in (0.30) which was first proven by Sarnak in [**47**]. The essential observation which leads to this lower bound is that the set of integers appearing as curvatures of circles tangent to C_0 contain the integers represented by an inhomogeneous binary quadratic form

$$f_{a_0}(x,y) - a_0$$

of discriminant $-4a_0^2$. Our approach in Section 2 is to repeat this method for a subset of the circles which we find are tangent to C_0 in this way. For every circle C of curvature a tangent to C_0, we can produce a shifted binary quadratic form

$$f_a(x,y) - a$$

where f_a has discriminant $-4a^2$ and consider the integers represented by f_a. We consider a in a suitably reduced subset of $[(\log X)^2, (\log X)^3]$ and count the integers represented by $f_a - a$ for a in this subset. It is important to note that the integers represented by f_a and $f_{a'}$ for $a \neq a'$ are a subset of integers which can be written as a sum of two squares since both forms have discriminant of the form $-\delta^2$. In fact, f_a and $f_{a'}$ represent practically the same integers (see the Appendix for a more detailed discussion). It is rather the *shift* of each form f_a by a that makes the integers found in this way vary significantly. Our final step is to give an upper bound on the number of integers in the intersection

$$\{m \text{ represented by } f_a - a\} \cap \{m' \text{ represented by } f_{a'} - a'\}$$

In obtaining this upper bound, we count integers with multiplicity, which is a sacrifice we can afford to make for our purposes. This method leads to a proof of the conjecture of Graham et.al. that the integers appearing as curvatures in a given integer ACP make up a positive fraction of all integers.

Since the Descartes quadratic form in (1.1) is of signature $(3,1)$ over $\mathbb{R}$, we have that A is a subgroup of $\mathrm{O}(3,1)$ and can be thought of as a subgroup of the group of motions of hyperbolic 3-space $\mathbb{H}^3$. In this

way A is a discrete group acting on $\mathbb{H}^3$ where the complement of three mutually tangent hemispheres inside an infinite cylinder is the fundamental domain of the action. This fundamental domain has infinite volume, which makes counting integers in the group's orbit quite difficult. We note, however, that A contains Fuchsian triangle subgroups generated by any three of the S_i above, which are lattices in the corresponding $\mathrm{O}(2,1)$'s. We use this fact extensively throughout this paper.

To this end, denote by A_i the subgroup of A generated by three of the four generators as follows:

$$A_i := (\{S_1, S_2, S_3, S_4\} - \{S_i\}).$$

This group is the Schottky group generated by reflections in the three circles intersecting the ith circle in the root quadruple and perpendicular to the initial circles in the packing; in particular, the ith circle is fixed under this action. The fundamental domain of A_i is then a triangle bounded by the three circles, and has hyperbolic area π.

1. A preliminary lower bound

In this section, we follow [**47**] in order to count integer points in an orbit of a subgroup A_i of the Apollonian group as described in Section 2.1. This produces a preliminary lower bound on the number $\kappa(P,X)$ of integers less than X occurring as curvatures in an Apollonian packing P.

PROPOSITION 1.1. *For an integer Apollonian circle packing P, let $\kappa(P,X)$ denote the number of distinct integers less than X occurring as curvatures in the packing. Then we have*

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

PROOF. We fix a circle C_0 of non-zero curvature a_0 in the packing P, and count the integers which occur as curvatures of circles tangent to C_0 in P. This is identical to considering the orbit of A_1 acting on a quadruple $\mathbf{v}$ of mutually tangent circles (a_0, b, c, d), since A_1 fixes the first coordinate of $\mathbf{v}$ and its orbit represents all of the circles tangent to C_a. Note that A generates all possible Descartes configurations in the packing P, and there can only be finitely many circles of curvature a_0 in the packing since the total area of all the inscribed circles is bounded by the area of the outside circle. Therefore it is reasonable to count the circles represented in the orbit of A_1, since they make up a positive fraction of all of the circles in P tangent to a circle of curvature a_0.

In this orbit, we have that the first coordinate a_0 is fixed, and the other coordinates of points in the orbit of A_1 vary to satisfy

$$Q(a_0, x_2, x_3, x_4) = 2(a_0^2 + x_2^2 + x_3^2 + x_4^2) - (a_0 + x_2 + x_3 + x_4)^2 = 0,$$

where Q is the Descartes form in (1.1). A change of variables $\mathbf{y} = (y_2, y_3, y_4) = (x_2, x_3, x_4) + (a_0, a_0, a_0)$ allows us to rewrite the equation above as

$$g(\mathbf{y}) + 4a_0^2 = 0, \tag{1.1}$$

where $g(\mathbf{y}) = y_2^2 + y_3^2 + y_4^2 - 2y_2y_3 - 2y_2y_4 - 2y_3y_4$ is the resulting ternary quadratic form. We can thus conjugate the action of A_1 on (a_0, x_2, x_3, x_4) to an action independent of a_0 which preserves the form g. This is the action of a group Γ on $\mathbf{y}$, generated by

$$\begin{pmatrix} -1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & -1 \end{pmatrix}.$$

Moreover, the action of Γ on

$$\mathbf{v}' = (b + a_0, c + a_0, d + a_0)$$

is related to the action of A_1 on $\mathbf{v}$ by

$$A_1\mathbf{v} = (a_0, \Gamma[\mathbf{v}' - (a_0, a_0, a_0)]),$$

so we count the same number of curvatures occurring in the packing before and after this change of variables. We change variables once again by letting

$$y_2 = A,\ y_3 = A + C - 2B,\ y_4 = C.$$

We note that $(y_2, y_3, y_4) \in \mathbb{Z}^3$ implies that A, B, and C are integers, and the primitivity of the packing is preserved as well – the gcd of A, B, and C is 1. With this change of variables, Γ is conjugated to an action of a group Γ' on (A, B, C) which is generated by

$$\begin{pmatrix} 1 & -4 & 4 \\ 0 & -1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & 0 \\ 4 & -4 & 1 \end{pmatrix}.$$

Under this change of variables, the expression in (1.1) becomes

$$4(B^2 - AC) = -4a_0^2. \tag{1.2}$$

Letting $\Delta(A, B, C)$ denote the discriminant of the binary quadratic form $Ax^2 + 2Bxy + Cy^2$, (1.2) is simply

$$\Delta(A, B, C) = a_0^2,$$

and thus Γ' is a subgroup of $\mathrm{O}_\Delta(\mathbb{Z})$, the orthogonal group preserving Δ. Let $\tilde{\Gamma}$ denote the intersection $\Gamma' \cap \mathrm{SO}_\Delta(\mathbb{Z})$. The spin double cover of SO_Δ is well known (see [**15**]) to be SL_2, and is obtained via the homomorphism

$$\begin{array}{ccc} \rho : \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SO}_\Delta(\mathbb{Z}) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \overset{\rho}{\longmapsto} & \frac{1}{\alpha\delta - \beta\gamma} \cdot \begin{pmatrix} \alpha^2 & 2\alpha\gamma & \gamma^2 \\ \alpha\beta & \alpha\delta + \beta\gamma & \gamma\delta \\ \beta^2 & 2\beta\delta & \gamma^2 \end{pmatrix} \end{array} \tag{1.3}$$

written here over $\mathbb{Z}$ as this is the situation we work with. It is natural to ask for the preimage of $\tilde{\Gamma}$ under ρ which we determine in the following lemma.

LEMMA 1.2. *Let $\tilde{\Gamma}$ and ρ be as before. Let $\Lambda(2)$ be the congruence 2-subgroup of $PSL_2(\mathbb{Z})$. Then the preimage of $\tilde{\Gamma}$ in $SL_2(\mathbb{Z})$ under ρ is $\Lambda(2)$.*

PROOF. We can extract from the generators of Γ' as well as the formula in (1.3) that the preimage of $\tilde{\Gamma}$ under ρ contains

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix},$$

and so $\tilde{\Gamma}$ contains the principle congruence subgroup $\Lambda(2)$ of $\mathrm{PSL}_2(\mathbb{Z})$. Recall that the area of $A_1\backslash\mathbb{H}^2$ is π, and note that $\mathrm{SO}_\Delta(\mathbb{Z})\bigcap\Gamma'$ contains exactly those elements of Γ' which have even word length when written via the generators of Γ', making up half of the whole group. Therefore the area of $\tilde{\Gamma}\backslash\mathbb{H}^2$ is 2π, which is equal to the area of $\Lambda(2)\backslash\mathbb{H}^2$, and hence the preimage of $\tilde{\Gamma}$ in $\mathrm{SL}_2(\mathbb{Z})$ is precisely $\Lambda(2)$ as desired. □

Recall that we would like to count the integer values of y_2, y_3, and y_4 – in terms of the action of Γ, we are interested in the set of values A, C, and $A+C-2B$ above. Lemma 1.2 implies that these values contain integers represented by the binary quadratic form

$$f_{a_0}(\zeta,\nu) = A_0\zeta^2 + 2B_0\zeta\nu + C_0\nu^2, \tag{1.4}$$

where $(\zeta,\nu) = 1$, and the coefficients are derived from the change of variables above:

$$A_0 = b + a_0,\ C_0 = d + a_0,\ B_0 = \frac{b+d-c}{2}. \tag{1.5}$$

We note that the discriminant of this form is not a square, since

$$(2B_0)^2 - 4A_0C_0 = -4a_0^2 \tag{1.6}$$

and $a_0 \neq 0$. Since the vectors in the orbit of A_1 are of the form $(a_0, A-a_0, A+C-2B-a_0, C-a_0)$, they correspond to the integer values of

$$f_{a_0}(x,y) - a_0, \tag{1.7}$$

where f_{a_0} is as before. Therefore

$$\kappa(P,X) \gg \#\{m \in \mathbb{Z} \,|\, m > 0,\ f_{a_0}(x,y) - a_0 = m \text{ for some } x,y \in \mathbb{Z}, (x,y) = 1\} \tag{1.8}$$

and we need only to count the integers represented by f_{a_0} in order to get a bound on the number of curvatures in P. This is done both in [**2**] and [**33**], from which we have the following:

LEMMA 1.3. *(James): Let f be a positive definite binary quadratic form over $\mathbb{Z}$ of discriminant $-D$, where D is a positive integer. Denote by $B_D(X)$ the number of integers less than X represented by f. Then*

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

where

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

Lemma 1.3 paired with (1.8) implies that

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

as desired. □

2. Counting in several subpackings at once

In this section we sharpen the bound in Proposition 1.1 in order to answer the question posed by Graham et.al. in [**24**] and prove that the integers appearing as curvatures in any integer ACP make up a positive fraction of all positive integers. Our computation in Section 1 reflects only those circles which are tangent to a fixed circle in P. It is thus natural to count some of the omitted curvatures here. Specifically, we repeat the method from Section 1 several times, fixing a different circle C each time and counting the integers occuring as curvatures of circles tangent to C.

Recall that to prove Proposition 1.1 we fixed a circle of curvature a_0, and associated curvatures of circles tangent to it with the set of integers (without multiplicity) represented by $f_{a_0}(x,y)-a_0$. We denote the set of these integers that are less than X by $\mathscr{A}_0$:

$$\mathscr{A}_0 = \{a \in \mathbb{N} \,|\, a \leq X, f_{a_0}(x,y)-a_0 = a \text{ for some integers } x,y \geq 0\}$$

For every $a \in \mathscr{A}_0$ we use the method in Section 1 to produce another shifted binary quadratic form

$$f_a(x,y)-a$$

of discriminant $-D=-4a^2$. As in Section 1, we wish to count the integers represented by these new forms. For each $a \in \mathscr{A}_0$, let S_a denote the set of integers less than X represented by f_a-a:

$$S_a = \{n \in \mathbb{N} \,|\, n \leq X, n = f_a(x,y)-a \text{ for some relatively prime integers } x,y \geq 0\}$$

Note that the sets S_a depend only on a_0, the curvature of C_0. One important consideration in counting the integers represented by the forms f_a is that their discriminants can be very large with respect to X, and thus many of the represented integers may be $> X$. In particular, the count in Lemma 1.3 is not uniform in D so we use more recent results of Blomer and Granville in [**4**] which specify how the number of integers less than X represented by a binary quadratic form depends on the size of the discriminant of the form[2].

[2]The results of Blomer and Granville concern quadratic forms of square free determinant, but the authors note in section 9.3 of [**4**] that the same can be done for binary quadratic forms of non-fundamental determinant as well.

With this notation, the bounds in [**4**] yield a *lower* bound on $\sum_a |S_a|$ for the a's we consider. We also compute an *upper* bound on $\sum_{a,a'} |S_a \cap S_{a'}|$ for $a \neq a'$ so that

$$\sum_a |S_a| - \sum_{a,a'} |S_a \cap S_{a'}|$$

gives a lower bound for $\kappa(P,X)$. A crucial ingredient to computing this and proving Theorem 0.8 (that the integers appearing as curvatures in a given ACP make up a positive fraction of $\mathbb{N}$) is the balance between these lower and upper bounds – for example, the more sets S_a we choose to include in our count, the bigger the lower bound on $\sum_a |S_a|$. However, choosing too many such sets will also increase the upper bound on the second sum $\sum_{a,a'} |S_a \cap S_{a'}|$. In fact, it is possible to choose so many sets S_a that the upper bound on the intersections outweighs the lower bound on the sizes of S_a. In Section 2.1 we specify how we choose the a's used in our computation, and compute the first sum, $\sum_a |S_a|$. In Section 2.2, we compute an upper bound on $\sum_{a,a'} |S_a \cap S_{a'}|$ for $a \neq a'$ to prove Theorem 0.8.

2.1. Integers represented by multiple binary quadratic forms. In this section, we evaluate the sum $\sum_a |S_a|$, choosing a's in a subset of $\mathscr{A}_0$ in order to ensure that we obtain a positive fraction of X in our final count. Specifically, we consider $a \in \mathscr{A}_0$ such that

$$(\log X)^2 \leq a \leq (\log X)^3$$

This interval is chosen to give us the desired lower bounds in conjunction with results in [**4**] – this will become clear in the computations preceding (2.9). We would like to further reduce the set of a's we consider so that the bounds on the size of the intersections of sets S_a are not too large. To do this, we first partition the interval $[(\log X)^2, (\log X)^3]$ into dyadic ranges $[2^k, 2^{k+1}]$ and select a's within these ranges.

Namely, we consider $\mathscr{A}_0 \cap [2^k, 2^{k+1}]$ where $(\log X)^2 \leq 2^k, 2^{k+1} \leq (\log X)^3$. The size of this set depends only on a_0, the curvature of the original circle we fixed. By Lemma 1.3, we have

$$\left|\mathscr{A}_0 \cap [2^k, 2^{k+1}]\right| \gg \frac{2^k}{\sqrt{k}} \tag{2.1}$$

where the implied constant depends on a_0. We partition each dyadic interval $[2^k, 2^{k+1}]$ into intervals $[2^k + n \cdot \eta \frac{2^k}{\sqrt{k}}, 2^k + (n+1) \cdot \eta \frac{2^k}{\sqrt{k}}]$ of length $\eta \frac{2^k}{\sqrt{k}}$, where $0 < \eta < 1$ is a fixed parameter whose importance will become apparent in Proposition 2.3. We note that the average over $0 \leq n \leq \sqrt{k}\eta^{-1}$ of cardinalities of the corresponding subsets of $\mathscr{A}_0$ is

$$E_n \left(\left| \mathscr{A}_0 \cap [2^k + n \cdot \eta \frac{2^k}{\sqrt{k}}, 2^k + (n+1) \cdot \eta \frac{2^k}{\sqrt{k}}] \right| \right) \gg \eta \frac{2^k}{k} \tag{2.2}$$

by (2.1). Thus for every value of k there exists an $0 \leq n \leq \sqrt{k}\eta^{-1}$ for which the intersection in (2.2) contains $\gg \eta \frac{2^k}{k}$ integers. For simplicity of notation, we assume without loss of generality[1] that $n = 0$,

[1] One can in fact extend Lemma 1.3 to show that this holds for *every* n. Friedlander and Iwaniec do this for $a_0 = 1$ in Theorem 14.4 of [**17**]. However, it is not necessary here.

and define $\mathscr{A}^{(k)}$ to be

$$\mathscr{A}^{(k)} = \mathscr{A}_0 \cap [2^k, 2^k + \eta \frac{2^k}{\sqrt{k}}] \tag{2.3}$$

where we have

$$|\mathscr{A}^{(k)}| \gg \eta \frac{2^k}{k} \tag{2.4}$$

up to a constant which depends only on a_0. Denote the union of these subsets by $\mathscr{A}$:

$$\mathscr{A} = \bigcup \mathscr{A}^{(k)} \tag{2.5}$$

The results in [**4**] imply the following lemma regarding the integers represented by quadratic forms associated with $a \in \mathscr{A}$.

LEMMA 2.1. *Let $\mathscr{A}$ and f_a be as before. Then we have*

$$\sum_{a \in \mathscr{A}} |S_a| \quad \gg \quad \eta X$$

To prove Lemma 2.1, we recall the notation and relevant theorem from [**4**]. Let f be a binary quadratic form of discriminant $-D$, and let $r_f(n)$ be the number of representations of n by f:

$$r_f(n) = \#\{(m_1, m_2) \in \mathbb{Z}^2 - \{\mathbf{0}\} \mid gcd(m_1, m_2) = 1, f(m_1, m_2) = n\} \tag{2.6}$$

Let $U_f^0(X) = \sum_{n \leq X} r_f(n)^0$, the number of integers less than X represented by f, counting without multiplicity. In [**4**], Blomer and Granville compute bounds for $U_f^0(X)$ for D in three ranges between 0 and X. These ranges are defined in terms of the class number h of the binary quadratic form f and by g, the number of genera. Letting $\ell = \ell_{-D} = L(1, \chi_{-D})(\phi(D)/D)$, they create a parameter

$$\kappa = \frac{\log(h/g)}{(\log 2)(\log(\ell_{-D} \log X))}$$

where $h/g = D^{\frac{1}{2}+o(1)}$. Their bounds for $U_f^0(X)$ are then uniform in D for each range below (see Lemma 2.2):

- $0 \leq \kappa \leq \frac{1}{2}$
- $\frac{1}{2} < \kappa < 1$
- $1 \leq \kappa \ll \frac{\log D}{\log \log D}$

In the first and last range, they are able to compute both an upper and lower bound on U. However they prove only an upper bound for $U_f^0(X)$ in the case that D is in the middle range, which is not suitable for our purposes. The lower bound for $U_f^0(X)$ for a form f of discriminant $-D$ where D is in the smallest range is essentially James' result in Lemma 1.3, and is used to show that

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

in [**18**]. Our results and the statement in Lemma 2.1 depend on Blomer and Granville's lower bound for $U_f^0(X)$ where f is of dicriminant $-D$ and D is in the third range above. Specifically, we use Theorem 2 from [**4**], which is summarized in the lemma below.

LEMMA 2.2. *(Blomer, Granville): Let f be a binary quadratic form of discriminant $-D$, and let $U_f^0(X)$ be as before. Let $\mathscr{G}$ be the group of genera of binary quadratic forms of discriminant $-D$. Denote by s the smallest positive integer that is represented by f, and by u the smallest positive integer represented by some form in the coset $f\mathscr{G}$. Then*

$$U_f^0(X) = \pi \cdot \left(1 - \frac{1}{2u}\right) \cdot \frac{X}{\sqrt{D}} + E_0(X,D) \tag{2.7}$$

where

$$E_0(X,D) \ll \sqrt{\frac{X}{s}} + \tau(D) \cdot \left(\frac{X \log X}{D} + \frac{X}{D^{\frac{3}{4}}}\right) \tag{2.8}$$

where $\tau(D)$ is the number of prime divisors of D, and the implied constant does not depend on D.

With this in mind we are ready to prove Lemma 2.1.

Proof of Lemma 2.1:

We use Lemma 2.2 to count the integers less than X represented by forms of discriminant $-D$ where D is a power of $\log X$ in our case. Recall that

$$f_a(x,y) = \alpha x^2 + 2\beta xy + \gamma y^2$$

is of discriminant $-D = -4a^2$. In particular, since $(\log X)^2 \leq a \leq (\log X)^3$, we have that

$$(\log X)^4 \leq D \leq (\log X)^6$$

and the number of prime divisors of D is

$$\tau(D) \ll \log\log X,$$

and so

$$E_0(X,D) \ll \frac{X}{(\log X)^3} + (\log D) \cdot \frac{X}{D^{\frac{3}{4}}}$$

Thus we have that the error $E_0(X,D) \ll \frac{X}{D^{\frac{3}{4}-\varepsilon}}$ for any $\varepsilon > 0$, and thus Lemma 2.2 implies

$$U_f^0(X) \gg \frac{X}{\sqrt{D}} \tag{2.9}$$

where the implied constant does not depend on D. Since $D = -4a^2$, it follows from (2.9) that the number of distinct values less than X represented by f_a is $\gg \frac{X}{a}$ and we have

$$\begin{aligned} \sum_{a\in\mathscr{A}} |S_a| &\gg \sum_{a\in\mathscr{A}} \frac{X}{a} \\ &\gg \eta\cdot X\cdot \sum_{\substack{2^k<(\log X)^3 \\ 2^k>(\log X)^2}} \frac{1}{k} \\ &\gg \eta\cdot X \end{aligned} \tag{2.10}$$

as desired. □

The sum in Lemma 2.1 is the lower bound on the number of integers we count by considering the quadratic forms associated with $a \in \mathscr{A}$. In order to prove Theorem 0.8, we obtain an upper bound on the number of integers we have counted twice in this way in the next section.

2.2. Integers in the intersections. To prove Theorem 0.8 we would like to show

$$\left|\bigcup_{a\in\mathscr{A}} S_a\right| \gg X \tag{2.11}$$

since this union is a subset of all curvatures less than X in the packing P. By Lemma 2.1, we may estimate the size of this union as follows:

$$\begin{aligned} \left|\bigcup_{a\in\mathscr{A}} S_a\right| &\geq \sum_{a\in\mathscr{A}} |S_a| - \sum_{a\neq a'\in\mathscr{A}} |S_a\cap S_{a'}| \\ &\gg \eta X - \sum_{a\neq a'\in\mathscr{A}} |S_a\cap S_{a'}| \end{aligned} \tag{2.12}$$

We need only to determine an upper bound for the last sum above. We do this by counting points $(x,y,x'y')$ in a box on the quadric

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

for each $a \neq a' \in \mathscr{A}$. The region in which we count these points is induced by the condition that $f_a(x,y) < X$. Namely, rewriting the binary form f_a as

$$f_a(x,y) = \frac{(\alpha x+\beta y)^2 + 4a^2y^2}{\alpha} \tag{2.13}$$

we can define a region

$$B_a = \{(x,y)\in\mathbb{R}^2 \text{ s.t. } |\alpha x+\beta y| \ll \sqrt{|\alpha|} \text{ and } |y| \ll \frac{\sqrt{|\alpha|}}{a}\} \tag{2.14}$$

so that $f_a(x,y) \ll 1$ for $(x,y)\in B_a$, and $f_a(x,y) \ll X$ for every $(x,y)\in\sqrt{X}B_a$ as desired. Therefore, the region in $\mathbb{R}^4$ over which we consider the forms $f_a - f_{a'}$ will be

$$\mathscr{B}_{a,a'} = (\sqrt{X}B_a \times \sqrt{X}B_{a'}) \cap \mathbb{Z}^4$$

With this notation, we are ready to prove the following proposition.

PROPOSITION 2.3. *Let $\mathscr{A}$, S_a, $S_{a'}$, η, and X be as before. Then there exists $c > 0$ depending only on a_0 such that*

$$\sum_{a \neq a' \in \mathscr{A}} |S_a \cap S_{a'}| \leq c\eta^2 X \tag{2.15}$$

Note that, since we chose $0 < \eta < 1$, we have $\eta^2 < \eta$, and so this upper bound on the size of the intersection of the sets $S_a - a$ is small compared to the count in Lemma 2.1.

PROOF. We note that the expression inside the sum has an upper bound

$$\begin{aligned} & |S_a \cap S_{a'}| \\ \leq\ & |\{(x,y,x',y') \in \mathscr{B}_{a,a'} \,|\, f_a(x,y) - f_{a'}(x',y') = a - a'\}| \end{aligned} \tag{2.16}$$

Although bounding (2.15) in this way involves counting the integers in $S_a \cap S_{a'}$ with multiplicity, our analysis shows that this sacrifice is in fact not too expensive to our final count. We thus consider the quaternary quadratic form

$$F(x,y,x',y') = f_a(x,y) - f_{a'}(x',y')$$

with discriminant $\Delta = (\beta^2 - \alpha\gamma)(\beta'^2 - \alpha'\gamma') = 16a^2(a')^2$. To obtain an upper bound on the number of points in $\mathbf{x} \in \mathscr{B}_{a,a'}$ for which $F(\mathbf{x}) = a' - a$, one can use the well developed circle method following Kloosterman in [**34**] and Esterman in [**16**] or modular forms (see [**13**]). Both methods would yield what we want – the latter would give the best results but is not as flexible as the former for our purposes since we wish to vary the parameters a and a' which is more straightforward in the circle method. Heath-Brown's Theorem 4 in [**26**] and Niedermowwe's Theorem 5.6 in [**42**] determine representation numbers of a fixed indefinite quadratic form[3]. Since our a, a' are all a small power of $\log X$, the proofs of these theorems can be manipulated slightly to yield the following lemma regarding representation numbers of all the indefinite quaternary quadratic forms we consider:

LEMMA 2.4. *Let F be as before, and let $(\log X)^2 \leq a, a' \leq (\log X)^3$. Let $\chi_{a,a'}$ denote the characteristic function on the region $\mathscr{B}_{a,a'}$, and let*

$$R_{\chi_{a,a'}}(a - a') = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^4 \\ F(\mathbf{x}) = a - a'}} \chi_{a,a'}(\mathbf{x}).$$

Let Δ be as above. Then we have

$$\begin{aligned} & R_{\chi_{a,a'}}(a - a') \\ =\ & |I_{\chi_{a,a'}}(a - a')| \cdot |\mathfrak{S}(a - a')| + O\left(\frac{X \cdot \Delta^{100}}{(\log X)^{\lambda}}\right) \end{aligned} \tag{2.17}$$

[3]Note that in [**26**] one considers representations of an integer m by F where m is asymptotic to the scaling factor P of the unscaled domain B (in our case $B = B_a \times B_{a'}$ and $P = \sqrt{X}$), while in [**42**] m is any nonzero integer.

where the first factor is the singular integral

$$I_{\chi_{a,a'}} = \int_{-\infty}^{\infty} \left[\int_{\mathbb{R}^4} \chi_{a,a'}(x) e(z(F(x) - a + a')) dx \right] dz \tag{2.18}$$

and the second factor is the singular series

$$\mathfrak{S}(a - a') = \prod_p \sigma_p \tag{2.19}$$

where

$$\sigma_p = \lim_{k \to \infty} p^{-3k} \cdot \#\{\mathbf{x} \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^4 \ s.t. \ F(\mathbf{x}) \equiv a - a' \ (p^k)\} \tag{2.20}$$

and $e(z) = e^{2\pi i z}$.

In the error term in (2.17), λ is an arbitrary large fixed constant. With more effort we can in fact get a power saving here by using modular forms – while this would yield the best result, the methods in [**26**] and [**42**] suffice. In particular, the argument in [**42**] lends itself well to our consideration of the quadratic form F, which has a discriminant of size $(\log X)^k$. The error term in Niedermowwe's Theorem 5.6 consists of a power saving in X, and a careful examination of the proof shows that the dependency on the discriminant of the form is absorbed into the error term since it is only logarithmically large – this is reflected in (2.17) via a power of the discriminant Δ of F. It is similarly important here that the distorsion of B_a and $B_{a'}$ with respect to the standard cube discussed in [**26**] and [**42**] is logarithmic in X.

To prove Proposition 2.3 it remains to evaluate the singular integral and singular series in (2.18) and (2.19). For a set $P \subset \mathbb{R}^4$, let $\mathbf{V}(P)$ denote the measure of P. From the definition of f_a and B_a in (2.13) and (2.14), we have

$$\begin{aligned} I_{\chi_{a,a'}} &\ll \lim_{\varepsilon \to 0} \frac{1}{\varepsilon} \cdot \mathbf{V}\left(\{(x,y,x',y') \in \sqrt{X}B_a \times \sqrt{X}B_{a'} \,|\, |f_a(x,y) - f_{a'}(x',y') - a + a'| < \varepsilon\} \right) \\ &\ll \lim_{\varepsilon \to 0} \frac{1}{\varepsilon} \cdot \frac{\varepsilon}{\sqrt{|\alpha| X}} \cdot \frac{\sqrt{|\alpha| X}}{a} \cdot \sqrt{\frac{X}{|\alpha'|}} \cdot \frac{\sqrt{|\alpha'| X}}{a'} \\ &\ll \frac{X}{aa'} \end{aligned} \tag{2.21}$$

To evaluate the singular series $\mathfrak{S}(a - a')$ we prove the following lemma.

LEMMA 2.5. *Let* $\mathfrak{S}(a - a')$ *be the singular series defined in (2.19). We have*

$$\mathfrak{S}(a - a') \ll \prod_{\substack{p | aa'(a - a') \\ p \nmid (a, a')}} \left(1 + \frac{1}{p}\right) \cdot 2^{\omega((a,a'))}$$

PROOF. We compute an upper bound for the expression in the limit in (2.20) by letting $k = 1$ since the expression in the limit decreases with k. Note that if $p | (a, a')$, we have F is not degenerate modulo

p by the primitivity of the packing and the definition of the coefficients of f_a in (1.5). Therefore

$$\sigma_p < p^{-3} \cdot \#\{\mathbf{x} \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^4 \text{ s.t. } F(\mathbf{x}) \equiv 0 \ (p)\},$$

and over $\mathbb{F}_p$, the number of nontrivial representations of 0 by F is bounded above by $2p^3$ (see [**9**], for example), so σ_p is bounded above by 2 in this case. In the other cases, we use exponential sum estimates. Taking $k = 1$ as before, we have

$$\sigma_p = \frac{1}{p} \sum_{r=0}^{p-1} \Big[\sum_{x,y} e_p(r f_a(x,y))\Big] \Big[\sum_{x',y'} e_p(-r f_{a'}(x',y'))\Big] e_p(r(a-a'))$$

where $e_p(z) = \exp(\frac{2\pi i z}{p})$. There are several cases to consider:

Case 1: p does not divide $aa'(a-a')$:

If we diagonalize f_a and $f_{a'}$, we obtain

$$\sigma_p = p^3 + \frac{1}{p} \sum_{r=1}^{p-1} \left(\frac{\tilde{\alpha} r}{p}\right)^2 \left(\frac{\tilde{\alpha}' r}{p}\right)^2 p^2 e_p(r(a-a')) = p^3 + \mathrm{o}(p)$$

since $(a-a', p) = 1$.

Case 2: $p|a-a'$ and does not divide aa':

In this case we have $\sigma_p < p^3 + \mathrm{o}(p^2)$.

Case 3: $p|a$ and $p \not| a'$:

Diagonalizing $f_{a'}$, we obtain

$$\sigma_p = p^3 + \frac{1}{p} \sum_{r=1}^{p-1} \left(\frac{\alpha r}{p}\right) p\sqrt{p} \cdot p \cdot e_p(r(a-a')) < p^3 + \mathrm{o}(p^2)$$

From these bounds and Lemma 2.7, we obtain the desired result in Lemma 2.5. □

Combining our computation of the singular integral in (2.21) and the bound on the singular series in Lemma 2.5, the result of Niedermowwe in Lemma 2.4 yields

$$|S_a \cap S_{a'}| \ll \frac{X}{aa'} \cdot \prod_{\substack{p|aa'(a-a') \\ p \not| (a,a')}} \left(1 + \frac{1}{p}\right) \cdot 2^{\omega((a,a'))} \tag{2.22}$$

where $\omega(n)$ is the number of distinct prime factors of n. Thus to evaluate the last sum in (2.12), we count the number of $a \in \mathscr{A}$ in progressions $a \equiv r \bmod q$. To this end, we recall Theorem 14.5 from [**17**] of Friedlander and Iwaniec regarding sums of squares in progressions in the following lemma[4].

[4]Note that the set of integers in the interval $[2^k, 2^k + \eta \frac{2^k}{\sqrt{k}}]$ which can be written as sums of two squares contains the $a \in \mathscr{A}^{(k)}$ in progressions $a \equiv r\,(q)$, since $\mathscr{A}^{(k)}$ is a set of integers represented by a binary quadratic form of discriminant $-\delta^2$. This count is therefore an upper bound on what we want.

LEMMA 2.6. *(Friedlander, Iwaniec): Let $b(n)$ be a characteristic function defined as*

$$b(n) = \begin{cases} 1 & \text{if } n = s^2 + t^2 \text{ for some } s,t \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$$

and let

$$B(x,q,a) = \sum_{\substack{n \leq x \\ n \equiv a\,(q)}} b(n)$$

For $2 \leq q \leq x$, $(a,q=1)$, and $a \equiv 1$ mod $(4,q)$ we have

$$B(x,q,a) = \frac{c_q}{q} \cdot \frac{x}{\sqrt{\log x}} \left[1 + O\left[\left(\frac{\log q}{\log x} \right)^{\frac{1}{7}} \right) \right]$$

where the implied constant is absolute and $c_q \ll \log\log q$ is a positive constant.

We note that the statement in Lemma 2.6 is much stronger than what we need – we require only an upper bound on $B(x,q,a)$, which could be proven using an upper bound sieve. Since our set $\mathscr{A}$ is obtained via the fixed quadratic form of discriminant $-4a_0^2$ from Section 1, such an upper bound implies the following in our case.

LEMMA 2.7. *Let $\mathscr{A}$, X, and η be as before. Then we have*

$$\sum_{\substack{a \in \mathscr{A} \\ a \equiv r(q)}} \frac{1}{a} \ll \frac{\log\log q}{q} \cdot \eta$$

where $1 < q < \log X$ is a square free integer.

PROOF. With the definition of $\mathscr{A}^{(k)}$ in (2.3), we may bound above the sum in Lemma 2.7 as a sum over k for which $(\log X)^2 \leq 2^k, 2^{k+1} \leq (\log X)^3$:

$$\sum_k \frac{1}{2^k} \sum_{\substack{a \in \mathscr{A}_0 \\ a \in [2^k, 2^k + \eta \frac{2^k}{\sqrt{k}}] \\ a \equiv r(q)}} 1 \tag{2.23}$$

By Lemma 2.6, the inner sum is bounded above (up to a constant) by

$$\eta \frac{c_q}{q} \frac{2^k}{k} \left[1 + \mathrm{O}\left(\left(\frac{\log q}{\log\log q} \right)^{\frac{1}{7}} \right) \right]$$

Since $c_q \ll \log\log q$, substituting this into (2.23) we have

$$\sum_k \eta \frac{c_q}{qk} \left[1 + \mathrm{O}\left(\left(\frac{\log q}{\log\log q} \right)^{\frac{1}{7}} \right) \right] \ll \eta \frac{\log\log q}{q}$$

as desired. □

With this in mind, we may evaluate the sum in (2.22) as follows.

$$\sum_{a\neq a'\in\mathscr{A}} |S_a\cap S_{a'}| \ll X\cdot \sum_{a\neq a'\in\mathscr{A}} \frac{1}{aa'}2^{\omega((a,a'))} \prod_{\substack{p|aa'(a-a')\\ p\nmid(a,a')}} \left(1+\frac{1}{p}\right) \tag{2.24}$$

$$\ll X\cdot \sum_{q_0,q_1,q_1',q_2} \frac{2^{\omega(q_2)}}{q_1q_1'q_2} \sum_{\substack{q_0q_1|a\\ q_0q_1'|a'\\ q_2|a-a'}} \frac{1}{aa'} \tag{2.25}$$

where q_0,q_1,q_1',q_2 are square free and relatively prime. We may restrict to primes $p<(\log X)^{\frac{1}{100}}$ in the product in (2.24), we may restrict in (2.25) the summation to $q_0,q_1,q_1',q_2<(\log X)^{\frac{1}{10}}$. We bound the sum

$$\sum_{\substack{q_0q_1|a\\ q_0q_1'|a'\\ q_2|a-a'}} \frac{1}{aa'}$$

using Lemma 2.7. First fix a and sum over a' subject to the restrictions $q_0q_1'|a'$ and $a\equiv a' \bmod q_2$. From Lemma 2.7, we have

$$\sum_{\substack{a'\in\mathscr{A}\\ q_0q_1'|a'\\ q_2|a-a'}} \frac{1}{a'} \ll \frac{\log\log(q_0q_1'q_2)}{q_0q_1'q_2}\cdot\eta$$

and

$$\sum_{q_0q_1|a} \frac{1}{a} \ll \frac{\log(q_0q_1)}{q_0q_1}\cdot\eta$$

so

$$\sum_{\substack{q_0q_1|a\\ q_0q_1'|a'\\ q_2|a-a'}} \frac{1}{aa'} \ll \frac{(\log\log(q_0+q_1+q_1'+q_2))^2}{q_0^2q_1q_1'q_2}\cdot\eta^2 \tag{2.26}$$

Substituting (2.26) into (2.25) gives the desired bound

$$\sum_{a\neq a'\in\mathscr{A}} |S_a\cap S_{a'}| \ll \eta^2X \sum_{q_0,q_1,q_1',q_2} 2^{\omega(q_2)}\cdot\frac{(\log\log(q_0+q_1+q_1'+q_2))^2}{(q_0q_1q_1'q_2)^2}$$

$$< c\eta^2X \tag{2.27}$$

□

Note that $\eta-\eta^2>0$ since $0<\eta<1$.We may take η small enough so that (2.12) and (2.10) imply

$$\left|\bigcup_{a\in\mathscr{A}} S_a\right| \gg (\eta-c\eta^2)X \gg X$$

as desired. □

The local to global conjecture, as well as the data in the case of several different integral ACP's in [**19**] suggest that $\kappa(P,X)$ is in fact either $\frac{X}{3}$ or $\frac{X}{4}$, depending on the mod 24 reduction of the packing P. It would be of great interest to prove this is true.

Finally, we note that the methods used here are easily generalizable to many discrete linear algebraic groups acting on $\mathbb{H}^3$ with an integral orbit. If the group contains several Fuchsian subgroups as in the case of the Apollonian group, we may restrict to the orbits of these subgroups as in Section 1. We would again utilize the subgroup's preimage in the spin double cover of SO to relate the problem to integers represented by a binary quadratic form. This would yield a comparable lower bound on the number of integers less than X in the orbit of the group. One might ask in what general case one would be able to prove a positive density statement using the techniques used in this chapter – the answer would probably include a rather wide range of algebraic groups.

CHAPTER 5

Appendix

In this section we clarify why the two binary quadratic forms f_a and $f_{a'}$ described in Chapter 1.3 represent approximately the same integers up to x. We begin by pointing out that, no matter what the form, primes congruent to 3 mod 4 can only divide the represented integers in even powers.

PROPOSITION 0.8. *Let $f_a(x,y) = Ax^2 + 2Bxy + cy^2$, with $B^2 - AC = -a^2$ as before. Suppose $n \in \mathbb{Z}$ is represented by f_a, and let $p|n$ denote a prime not dividing a, with $p \cong 3\ (4)$. Then we have that $n = n'p^{2v}$, where $p \not| n'$ and v is an integer.*

PROOF. We diagonalize the form $f_{a'}$ to

$$F(x,y) = A'x^2 + C'y^2,$$

where we know $A'C' = a^2$. Let p be a prime as above. Then, since $p \not| a$, p does not divide either A' or C'. Now suppose we have that

$$A'x^2 + C'y^2 \equiv 0\ (p^w),$$

for some pair of integers (x,y). If $p|x$ and $p|y$, we have that w must be even, and we are done.

Suppose this is not the case. Then, wlog, we have that $p \not| y$, and there exists an integer z such that

$$yz \equiv 1\ (p^w),$$

and so we have that

$$A'(xz)^2 + C'(yz)^2 \equiv 0\ (p^w),$$

or

$$A'(xz)^2 \equiv -C'\ (p^w).$$

Since $p \not| A'$, there is an integer $(A')^{-1}$ such that $(A')^{-1}A' \equiv 1\ (p)$, and we can rewrite the equation above as

$$(xz)^2 \equiv -(A')^{-1}C'\ (p^w). \tag{0.28}$$

Since $A'C' = a^2$, we have that $-(A')^{-1}C' = -((A')^{-1})^2a^2$. This, together with 0.28, implies -1 is a square modulo p^w, and so w must be even. □

With this in mind, we can now specify exactly which integers are represented by our forms.

PROPOSITION 0.9. *Let f_a be a binary quadratic form as before, with discriminant $-a^2$. Then if $f_a(x,y) = N$ for some integers x and y where N is relatively prime to a, we have that can be written as $N = v^2 n$, where n is square free and has no prime divisors congruent to* 3 *modulo* 4.

PROOF. We begin, again, by diagonalizing our form to

$$F(x,y) = A'x^2 + C'y^2.$$

Since n has no prime divisors congruent to 3 mod 4, we know that $\left(\frac{-1}{n}\right) = 1$. In particular, this means that

$$-a^2 \equiv w^2 \ (n)$$

for some integer w. We rewrite this as

$$nk - a^2 = w^2, \text{ or}$$

$$nk - w^2 = a^2.$$

So the binary form $F'(x,y) = nx^2 + wxy + ky^2$ has discriminant $-a^2$, and is equivalent to $F(x,y)$. Since F' represents n in the obvious way, we have that F represents it as well. Thus F will represent any integer of the form $v^2 n$ above. □

So we see that a binary quadratic form of discriminant $-a^2$ will represent almost the same integers as a binary quadratic form of discriminant $-a'^2$, the difference coming only from the prime divisors of a and a'.

Bibliography

[1] S. Balaji, S. Meyn, *Multiplicative ergodic theorems and large deviations for an irreducible Markov chain*, Stochastic processes and their applications, **90** (1), pp. 123-144 (2000)

[2] 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)

[3] V. Blomer, *Binary quadratic forms with large discriminants and sums of two squareful numbers*, J. reine angew. Math. **569**, pp. 213-214 (2004)

[4] V. Blomer, A. Granville, *Estimates for representation numbers of quadratic forms*, Duke Mathematical Journal, **135**, No 2, pp. 261-302 (2006)

[5] P. Bougerol, J. Lacroix, *Products of Random Matrices with Applications to Schroedinger Operators*, Birkhauser (1985)

[6] J. Bourgain, E. Fuchs *A proof of the positive density conjecture for integer Apollonian circle packings*, preprint (2010)

[7] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** No. 3, pp. 559-644 (2010)

[8] J. Bourgain, A. Gamburd, *Uniform Expansion Bounds for Cayley Graphs of $SL_2(\mathbb{F}_p)$*, Annals of Math, **167** (2008)

[9] J.W.S. Cassels, *Rational Quadratic Forms*, Dover Publications, Inc., Mineola, NY (1978)

[10] J. Cogdell, *On Sums of Three Squares*, J. Thèor. Nombres Bordeaux, **15** (2003)

[11] H.S.M. Coxeter, *An absolute property of four mutually tangent circles*, *Non-Euclidean Geometries, Jaános Bolyai Memorial Volume* (eds. A. Prékopa and E. Molnàr), Kluwer Academic Pub. (2005)

[12] G. Davidoff, P. Sarnak, A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, Cambridge University Press, Cambridge UK (2003)

[13] W. Duke, Z. Rudnick, and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. **71** No. 1, pp. 143Ð179 (1993)

[14] W. Duke, R. Schulze-Pillot, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids.* Invent. Math. **99**, pp. 49-57 (1990)

[15] J. Elstrodt, F. Grunewald, J. Mennicke, *Groups Acting on Hyperbolic Space*, Springer Verlag Berlin Heidelberg (1998)

[16] T. Estermann, *A new application of the Hardy - Littlewood - Kloosterman method*, Proc. London. Math. Soc. **12**, pp. 425-444 (1962)

[17] J. Friedlander, H. Iwaniec, *Opera de Cribro*, unpublished manuscript (2009)

[18] E. Fuchs, *A note on the density of Apollonian curvatures in $\mathbb{Z}$*, preprint.

[19] E. Fuchs, K. Sanden, *Some experiments with integral Apollonian circle packings*, Experiment. Math., to appear.

[20] A. Gamburd, *On the spectral gap for infinite index "congruence" subgroups of $SL_2(\mathbb{Z})$*, Israel J. Math. **127**, pp. 157-200 (2002)

[21] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: geometry and group theory. I. The Apollonian group*, DOI:10.1007/s00454-005-1196-9 (2005)

[22] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: geometry and group theory. II. Super-Apollonian group and integral packings*, Discrete Comput. Geom. DOI: 10.1007/s00454-005-1195x (2005)

[23] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: geometry and group theory. III. Higher dimensions*, DOI: 10.1007/s00454-1197-8 (2005)

[24] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: number theory*, Journal of Number Theory **100**, pp. 1-45 (2003)

[25] H. Halberstam, H.E. Richert, *Sieve Methods*, London Mathematical Society, Academic Press Inc, London (1974)

[26] D.R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J.Reine Angew. Math. **481**, pp. 149-206 (1996)

[27] H. Hennion, *Limit theorems for products of positive random matrices*, Annals of Probability, **25** No.4, pp. 1545-1587 (1997)

[28] K.E. Hirst, *The Apollonian packing of circles*, Proc. Nat. Acad. Sci. USA, 29, 378-384 (1943)

[29] B. Huppert, *Endliche Gruppe I*, Springer-Verlag Berlin Heidelberg (1967)

[30] K.H. Indlekofer, *Scharfe untere Abschätzung für die Anzahlfunktion der B-Zwillinge*, Acta Arithmetica, XXVI, pp. 207-212 (1974)

[31] H. Iwaniec, *Spectral Methods of Automorphic Forms*, American Mathematical Society, Providence RI (2002)

[32] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications **53** (2004)

[33] R.D. James, *The Distribution of integers represented by quadratic forms*. American Journal of Mathematics, **60** No.3. pp. 737-744 (1938)

[34] H.D. Kloosterman, *On the representation of numbers of the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. **49**, pp. 407-464 (1926)

[35] A. Kontorovich, H. Oh, *Apollonian circle packings and closed horospheres on hyperbolic* 3*-manifolds*, http://arxiv.org/pdf/0811.2236 (2008)

[36] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Chelsea Pub Co, 3rd edition (1974)

[37] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. **13**, pp. 305-312 (1908)

[38] J. Liu, P. Sarnak, *Integral points on quadrics with in three variables whose coordinates have few prime factors*, preprint

[39] C. R. Matthews, L.N. Vaserstein, B. Weisfeiler, *Congruence properties of Zariski dense subgroups*, Proc. London Math Soc. (3) **48**, pp. 514-532 (1984)

[40] G. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica **2**, pp. 71-78 (1982)

[41] C.T. McMullen, *Hausdorff dimension and conformal dynamics. III. Computation of dimension*, Amer. J. of Math. **120** (4) (1998)

[42] N. Niedermowwe, *A version of the circle method for the representation of integers by quadratic forms*, preprint arXiv:0905.1229v1 (2009)

[43] G. Pall, *The Distribution of Integers Represented by Binary Quadratic Forms*, Bull. of Amer. Math. Soc. **49** No. 6, pp. 447-449 (1943)

[44] G.J. Rieger, *Aufeinanderfolgende Zahlen als Summen von zwei Quadraten*, Indag. Math. **27**, pp. 208-220 (1965)

[45] P. Sarnak, *Some Applications of Modular Forms*, Cambridge University Press, New York (1990)

[46] P. Sarnak, *Equidistribution and Primes*, Rademacher Lecture Series (2007)

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

[48] P. Sarnak, *What is an Expander?* Notices of the AMS **51**, pp.762-763 (2004)

[49] J-P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, Addison-Wesley Publishing Company, INC. The Advanced Book Program, New York (1989)

[50] D. Steinsaltz, *Convergence of moments in a Markov-chain central limit theorem*, Indag. Math., N.S. **12** (4), pp. 533-555 (2001)

[51] M. Suzuki, *Group theory*, Grundlehren der Mathematischen Wissenschaften **248**, Springer-Verlag, New York (1986)

[52] B. Weisfeiler, *Strong Approximation for Zariski dense subgroups of semi-simple algebraic groups*. Ann. of Math. **120** No. 2, pp. 271-315 (1984)