A PROOF OF THE POSITIVE DENSITY CONJECTURE FOR INTEGER APOLLONIAN CIRCLE PACKINGS

JEAN BOURGAIN AND 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. In this paper, we compute a lower bound for the number $\kappa(P,X)$ of integers less than X occurring as curvatures in a bounded integer ACP P, and prove a conjecture of Graham, Lagarias, Mallows, Wilkes, and Yan that the ratio $\kappa(P,X)/X$ is greater than 0 for X tending to infinity.

1. INTRODUCTION

In the first picture in Figure 1 there are three mutually tangent circles packed in a large circle on the outside, with four curvilinear triangles in-between – such a configuration of circles is called a *Descartes configuration*, and is the starting point for a bounded Apollonian circle packing (ACP). One may also consider is an unbounded Apollonian circle packing in which the original Descartes configuration consists of four circles which are all externally tangent to each other, or where one or two of the circles are in fact straight lines. One such configuration is depicted in the first picture of Figure 2 – the two parallel lines can be thought of as circles of infinite radius tangent at infinity. This is the only kind of unbounded packing we consider. Once a Descartes configuration is given, one constructs an ACP by inscribing a circle into each of the four triangular interstices in the original Descartes configuration as in the second picture of both Figure 1 and Figure 2. This results in 12 new triangular interstices which are in turn filled with circles. An ACP is then a packing of infinitely many circles obtained by continuing this process indefinitely.

We note that this construction is well defined once the original four circles are given. An old theorem (circa 200 BC) of Apollonius of Perga states that there are precisely two circles tangent to all of the circles in a triple of mutually tangent circles or lines. It follows that each triangular interstice arising in the construction above can be packed with precisely one circle.

Key words and phrases. Apollonian packings, number theory, quadratic forms, sieve methods, circle method.
The first author is supported in part by NSF.

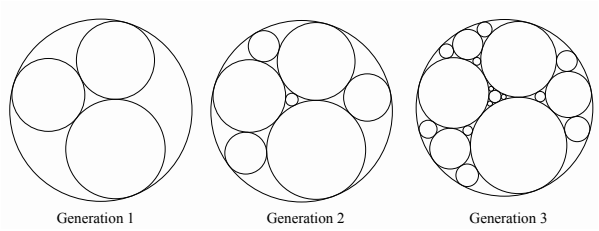

FIGURE 1. Bounded Apollonian circle packing

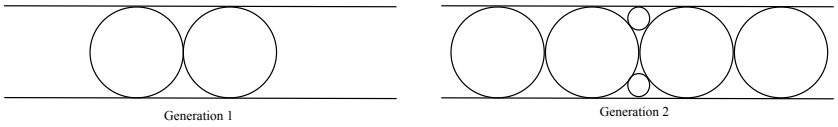

FIGURE 2. Unbounded Apollonian circle packing

A remarkable feature of these packings, believed to be noted first by Nobel Prize Laureate F. Soddy in 1936, is that if any quadruple of mutually tangent circles in an ACP have integer curvature (reciprocal of the radius), all of the circles in the packing will have integer curvature as well. Such a packing is called an integer ACP, and a *primitive* integer ACP is one in which the curvatures of the circles in the packing do not all share a factor greater than 1. One such primitive ACP, generated by starting with circles of curvatures $1,2,2$, and 3, is illustrated in Figure 3. We recall the following theorem from [GLMWY] regarding unbounded integer ACP's:

Theorem 1.1 (Graham, Lagarias, Malows, Wilks, Yan 2004)**.** *The only unbounded primitive integer ACP is the packing depicted in Figure 4, generated by starting with circles of curvatures* $0,0,1,1$.

The packings in Figures 3 and 4 are in fact two of infinitely many primitive integer ACP's (see [F], section 1.2 for an explanation), and it is thus natural and interesting to consider several number-theoretic questions related to such packings.

The various problems associated to the diophantine properties of integer ACP's were first addressed in [GLMWY] by the five authors Graham, Lagarias, Mallows, Wilks, and Yan. They make considerable progress in treating these problems and ask several fundamental questions many of which are now solved and discussed further in [S1], [F], [FS], and [KO].

In all of these papers, ACP's are studied using a convenient representation of the curvatures appearing in an ACP as maximum-norms of vectors in an orbit of a specific subgroup A of the orthogonal group $\mathrm{O}(3,1)$. We introduce this group in Section 1.1 and will use it throughout. In regards to counting the number of integers represented in a given ACP, Graham et. al. exploit the existence of unipotent elements of A in [GLMWY] to establish the lower bound below for the number $\kappa(P,X)$ of distinct

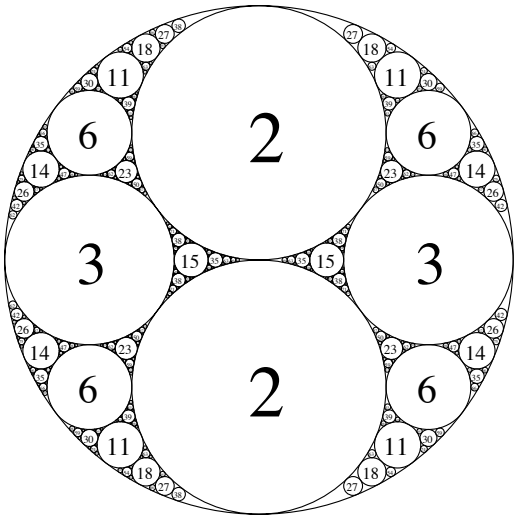

FIGURE 3. Apollonian Circle Packing $(-1,2,2,3)$

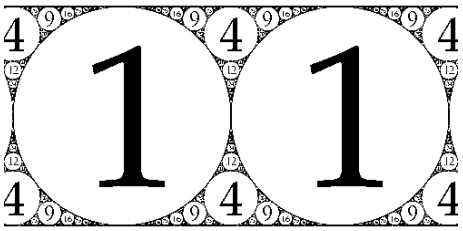

FIGURE 4. Apollonian Circle Packing $(0,0,1,1)$

curvatures less than X of circles in an integer packing P:

$$\kappa(P,X) \gg_{c_1} \sqrt{X} \tag{1.1}$$

where the notation

$$y \gg_c z \text{ or } y \ll_c z$$

in this paper is taken to mean that there exists a constant $c > 0$ such that

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

Graham et. al. suggest in [GLMWY] that the lower bound in (1.1) 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 provide experimental data in support of this.

It is important to note that this question is different from one recently addressed in [KO] 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 this paper. In fact, the results in [KO] suggest that the integers occurring as curvatures in a given ACP arise with significant multiplicity. Specifically, Kontorovich and Oh find that $N_P(X)$ is asymptotic to $c \cdot x^{\delta}$, where $\delta = 1.3056\ldots$ is the Hausdorff dimension of the limit set of any Apollonian circle packing (see [**?**] for a discussion of the Hausdorff dimension of ACP's). Kontorovich and Oh's techniques, however, do not appear to extend in any obvious way to proving that the integers represented by curvatures in an ACP make up a positive fraction in $\mathbb{N}$.

As far as counting integers without multiplicity is concerned, in his unpublished letter to Lagarias ([S1]), Sarnak uses the existence of arithmetic Fuchsian subgroups of A to get a bound of

$$\kappa(P,X) \gg_{c_2} \frac{X}{\sqrt{\log X}} \tag{1.2}$$

towards Graham.et.al.'s positive density conjecture. This method is the crucial starting point to the argument in this paper, and we give a detailed exposition of it in Section 2. It was further improved to yield a bound of

$$\kappa(P,X) \gg_{c_3} \frac{X}{(\log X)^{\varepsilon}}$$

where $\varepsilon = 0.150\ldots$ by the second author in a preprint [F1].

In this paper, we refine this Fuchsian subgroup method in a number of ways and settle the positive density question of Graham et.al. in the following theorem:

Theorem 1.2. *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 there exists a constant $c > 0$ depending on P such that*

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

We treat this question by counting curvatures in different subpackings of a given ACP. Namely, we fix a circle C_{a_0} of curvature a_0 and investigate which integers occur as curvatures of circles tangent to C_{a_0}. This gives the preliminary lower bound in (1.2) which was first proven by Sarnak in [S1]. The essential observation which leads to this lower bound is that the set of integers appearing as curvatures of circles tangent to C_{a_0} contain the integers represented by a shifted binary quadratic form

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

where f_{a_0} has discriminant $-4a_0^2$, which we introduce in (2.8) – its coefficients depend only on a_0 and the curvatures of the largest three circles tangent to C_{a_0}. This specific relationship between ACP's and

binary quadratic forms was also observed by Graham et. al. in Theorem 4.2 of [GLMWY], where they note that primitive root quadruples[1] (see (v) of Theorem 1.4) of Apollonian packings are in one-to-one correspondence with a certain family of positive definite binary quadratic forms. They use this relationship to analyze the number of primitive root quadruples whose smallest (negative) coordinate is n – this is a different question from the one addressed in this paper. The binary forms of their Theorem 4.2 are precisely the binary forms f_{a_0} in this paper.

Our approach in Section 3 is to repeat the method for a subset of the circles which we find are tangent to C_{a_0} in this way. Namely, denoting by

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

we have that for every $a \in \mathscr{A}_0$ there is a circle of curvature a tangent to C_{a_0}. Fixing a circle C_a of curvature a obtained in this way we count circles tangent to it by using the process above: we produce a shifted binary quadratic form

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

whose coefficients again depend only on a and the curvatures of the largest four circles tangent to C (see (3.1)). Notably, the discriminant of f_a is $-4a^2$ and so we can obtain a family of binary quadratic forms of discriminant depending only on a, where a varies over $\mathscr{A}_0$. Our strategy is to count integers represented by several forms in this family: we consider $f_a - a$ for $a \in \mathscr{A}_0$ in a suitably reduced subset of $[(\log X)^2, (\log X)^3]$ and count the integers $\leq X$ represented by $f_a - a$ for a in this subset (the importance of taking this subset of $\mathscr{A}_0$ will become apparent in Section 3).

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 $-\lambda^2$. In fact, f_a and $f_{a'}$ represent practically the same integers (see [F1] 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 the purpose of proving Theorem 1.2. We note that while this method proves that the integers appearing as curvatures in a given integer ACP make up a positive fraction of all integers, we do not strive to compute or optimize the fraction itself. There are conjectures as to what this fraction should be (see the discussion on the local to global principle in ACP's in [FS]), and proving a result towards such conjectures would be very interesting.

[1]For a detailed discussion of root quadruples, see [GLMWY]. A root quadruple of a packing is essentially the quadruple of curvatures of the four largest circles in the packing

Acknowledgements: We thank Peter Sarnak and Jeffrey Lagarias for introducing this problem to us, and for many insightful comments and conversations. We thank Alex Kontorovich for sharing his program for drawing Apollonian circle packings, and the referee for helpful comments on a previous version of this paper.

1.1. **The Apollonian group.** We recall an old theorem of Descartes which gives a relationship between the curvatures of four mutually tangent circles:

Theorem 1.3 (Descartes, 1643)**.** *Given four externally tangent circles of curvatures x_1, x_2, x_3, and x_4, we have*

$$Q(x_1,x_2,x_3,x_4) = 2(x_1^2+x_2^2+x_3^2+x_4^2)-(x_1+x_2+x_3+x_4)^2 = 0 \tag{1.3}$$

A proof of this can be found in [Cx]. This equation also holds for four mutually tangent circles when three of the circles are internally tangent (or inscribed) to the fourth circle as in the case of ACP's. However, because the outside circle is internally tangent to the other three, we assign to it a negative curvature in order for the equation to hold (see [GLMWY1] for a discussion of this). Note that fixing three of the curvatures (say x_2,x_3,x_4) above yields a quadratic equation which has two solutions $x_1 = x_1^+, x_1^-$ such that

$$x_1^+ + x_1^- = 2(x_2+x_3+x_4).$$

In fact, the circles $C_{x_1^+}$ and $C_{x_1^-}$ of curvatures x_1^+ and x_1^-, respectively, are precisely the two circles tangent to all three of the mutually tangent circles of curvature x_2,x_3, and x_4.

Therefore, if we assign to every set of 4 mutually tangent circles in a packing P a vector $\mathbf{v} \in \mathbb{Z}^4$ of the circles' curvatures, we can use Descartes' equation to express any ACP as an orbit of the group A generated by

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

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

acting on $\mathbf{v}$. This group, called the *Apollonian group*, was introduced by Hirst in 1967 (see [H]). We summarize the relevant properties of this group in the following theorem:

Theorem 1.4. *Let A be the group generated by S_1,S_2,S_3,S_4 in (1.4), and let Q be as in (1.3).*

(i) *For $1 \leq i \leq 4$, we have $S_i^2 = I$, the identity.*

(ii) *A is an infinite-index subgroup of the orthogonal group $O_Q(\mathbb{Z})$ fixing Q.*

(iii) *Q is of signature $(3,1)$, so we have $A \subset O_{\mathbb{R}}(3,1)$, the group of isometries of hyperbolic 3-space $\mathbb{H}^3$. The group A can thus be realized as a group acting on $\mathbb{H}^3$.*

(iv) *Let (a,b,c,d) be the curvatures of some quadruple of mutually tangent circles in a packing P. Then any quadruple (x_1,x_2,x_3,x_4) of curvatures of mutually tangent circles in the packing is an element of the orbit $A(a,b,c,d)^t$.*

(v) *A quadruple of curvatures of mutually tangent circles $\mathbf{v} = (a,b,c,d)$ with $a+b+c+d > 0$ is defined to be a* root quadruple *if $a \leq 0 \leq b \leq c \leq d$ and $a+b+c \geq d$. Every ACP has a unique root quadruple* $\mathbf{v}$.

The statements in (ii),(iii), and (iv) are proven in [F]. The notion of the root quadruple in (v) was developed in [GLMWY], and its uniqueness for a given ACP is proven there as well.

From this point on, we denote by $\mathbf{v}_P$ the root quadruple of the packing P, and assume that P is primitive – the gcd of the coordinates of any $\mathbf{w} \in A\mathbf{v}_P^t$ in the orbit is 1.

We briefly discuss the action of A on hyperbolic 3-space here. We summarize the insightful description of this action from Section 2.2 of [KO]. We consider the model

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

with measure hich is bounded by $\mathbb{C} \cup \infty$. In this model, we consider an ACP lying in $\mathbb{C}$, and the action of A is realized as follows.

For any triple of mutually tangent circles (C_1,C_2,C_3) there is a unique *dual circle* or line which passes through the tangency points of the three. The generators of A are precisely 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 Figure 5. The shaded circle on the inside is the image of the outside circle under reflection through the smallest of the dual circles. The action of A on $\mathbb{H}^3$ is then realized as reflections through the hemispheres lying above the dual circles (which are embedded in the boundary $\mathbb{C} \cup \infty$ of $\mathbb{H}^3$) of the packing, and a fundamental domain for this action is the union of the exteriors of the hemispheres lying above to the dual circles corresponding to the root quadruple of the packing. This is further discussed in Section 2.2 of [KO]. This fundamental domain has infinite volume (see [F]), 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 can be conjugated to subgroups of corresponding $\mathrm{O}(2,1)$'s as we show in Section 2. To this end, denote by A_i the subgroup of A generated by three of the four generators as follows:

$$A_i := (\{S_1,S_2,S_3,S_4\} - \{S_i\}) \tag{1.5}$$

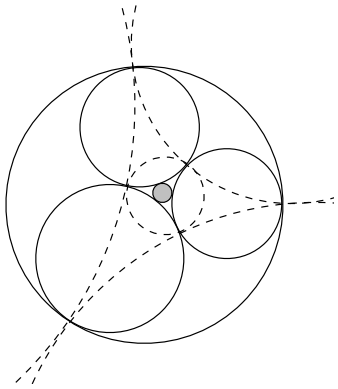

FIGURE 5. Dual circles in an Apollonian circle packing

This group is generated by reflections in the three dual circles intersecting the ith circle in the root quadruple and perpendicular to the initial circles in the packing; in particular, the ith circle C_i is fixed under this action. In Section 2 we conjugate the action of A_1 on $\mathbb{H}^3$ to the action of a lattice subgroup Γ of $\mathrm{O}_{\mathbb{R}}(2,1)$ on $\mathbb{H}$. In the context of the fundamental domain of A described above, Γ is acting on $\mathbb{H}$ which is realized as the disk bounded by the fixed circle C_i sitting in $\mathbb{C}$ as above and its fundamental domain is then a triangle bounded by the three dual circles intersecting C_i; since this is a hyperbolic triangle in which all angles are 0, by the Gauss-Bonnet formula it has hyperbolic area π (see Theorem 1.4.2 of [K]).

2. A PRELIMINARY LOWER BOUND

In this section, we recall the method used in [S1] to count integers appearing in a given integer orbit of the group A_i in (1.5). 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.

Lemma 2.1. *Let $\mathbf{v}_P$ be the root quadruple of the packing P, and let A_i be as in (1.5). For $X \in \mathbb{N}$, let*

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

be the set of positive integers appearing in the orbit $A_i\mathbf{v}_P^t$.

(1) *If P is bounded, write $\mathbf{v}_P = (a_0,b,c,d)$, and let C_{a_0} denote the circle of curvature a_0 in this quadruple.*
(2) *If P is unbounded, write $\mathbf{v}_P = (b,c,d,a_0)$ and let C_{a_0} denote the circle of curvature a_0 in this quadruple.*

Let $f_{a_0}(\zeta,\nu) = A_0\zeta^2 + 2B_0\zeta\nu + C_0\nu^2$, *where*

$$A_0 = b + a_0, B_0 = \frac{a_0+b+d-c}{2}, C_0 = d + a_0 \tag{2.1}$$

and let

$$\mathscr{A}_0 = \{a \in \mathbb{N} \mid a \leq X,\ a = f_{a_0}(\zeta,\nu) - a_0 \text{ for some } \zeta,\nu \in \mathbb{Z}, gcd(\zeta,\nu) = 1\} \tag{2.2}$$

If P is as in (1), we have

$$\mathscr{A}_0 \subset K_1(P).$$

If P is as in (2), we have

$$\mathscr{A}_0 \subset K_4(P).$$

Proof. For P bounded we have that the first coordinate a_0 of $\mathbf{v}_P$ is fixed throughout the orbit $A_1\mathbf{v}_P^t$. The other coordinates of points in the orbit of A_1 vary to satisfy

$$Q(a_0,x_2,x_3,x_4) = 2(a_0^2+x_2^2+x_3^2+x_4^2) - (a_0+x_2+x_3+x_4)^2 = 0, \tag{2.3}$$

where Q is the Descartes form in (1.3). In the case of an unbounded packing P, the fourth coordinate a_0 is fixed throughout the orbit $A_4\mathbf{v}_P^t$, and the other coordinates then vary to satisfy $Q(x_1,x_2,x_3,a_0) = 0$. To prove Lemma 2.1, we note that A_1, respectively A_4 in the unbounded case, is isomorphic to a subgroup of $\mathrm{O}_{\mathbb{R}}(2,1)$. We show this by conjugating A_1 (or A_4) to a group Γ which is obviously isomorphic to a subgroup of $\mathrm{O}_{\mathbb{R}}(2,1)$. We do this in detail for the case of the bounded packing below, and note that the proof is identical in the unbounded case.

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 in (2.3) as

$$g(\mathbf{y}) + 4a_0^2 = 0, \tag{2.4}$$

where $g(\mathbf{y}) = y_2^2+y_3^2+y_4^2-2y_2y_3-2y_2y_4-2y_3y_4$. In the context of the orbit, this change of variables is equivalent to conjugating the group A_1 to $A_1' = W^{-1}A_1W$ where

$$W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

The group A_1' is isomorphic to the group $\Gamma \subset \mathrm{GL}_3$ generated by

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

The group Γ fixes g in (2.4), so $\Gamma \subset \mathrm{O}_g(\mathbb{Z})$, the orthogonal group fixing g. Note that the orbit $A_1\mathbf{v}_P^t$ is related to the orbit $\Gamma(\mathbf{v}')^t$ where

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

by

$$A_1\mathbf{v}_P^t = (a_0, [\mathbf{v}' - (a_0,a_0,a_0)]\Gamma^t)^t$$

where $\Gamma^t = \{\gamma^t \mid \gamma \in \Gamma\}$, so the number of integers appearing in the orbit of A_1 is the same as the number of integers in the orbit of Γ. We change variables once again by letting

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

Claim: In the notation above, $A,B,C \in \mathbb{Z}$ and $\gcd(A,B,C)$=1.

Proof. We first prove the integrality: since $a_0,x_2,x_3,x_4 \in \mathbb{Z}$, we have $y_i = x_i + a_0 \in \mathbb{Z}$ for $2 \leq i \leq 4$. Therefore $A,C,2B \in \mathbb{Z}$. To see that $B \in \mathbb{Z}$, note that $Q(x_1,x_2,x_3,x_4) = 0$ and $\gcd(x_1,x_2,x_3,x_4) = 1$ implies that exactly two of the x_i must be even (see [S] for a detailed proof). Therefore we must have that exactly one of y_2,y_3,y_4 is even, and so $2B = y_2 + y_4 - y_3$ is even as well, giving $B \in \mathbb{Z}$.

To prove primitivity, recall that $\gcd(a_0,x_2,x_3,x_4) = 1$. Suppose $\gcd(y_2,y_3,y_4) = q > 1$. So

$$(a_0,x_2,x_3,x_4) = (a_0, y_2'q - a_0, y_3'q - a_0, y_4'q - a_0) \text{ for some } y_2',y_3',y_4' \in \mathbb{Z}$$

If $q|a_0$, we have a contradiction to the primitivity of the packing. Suppose $q \not| a_0$. Then we have

$$Q(a_0,x_2,x_3,x_4) \equiv 4a_0^2 \not\equiv 0 \pmod{q}$$

and so we have a contradiction to (2.3). Therefore $\gcd(y_2,y_3,y_4) = 1$, and so $\gcd(A,B,C) = 1$ as well. □

In this way, the action of Γ on v' is related to the action of a group Γ' on $(A_0,B_0,C_0)^t$ where

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

and Γ' is generated by

$$s_1 = \begin{pmatrix} 1 & -4 & 4 \\ 0 & -1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, s_3 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & 0 \\ 4 & -4 & 1 \end{pmatrix}.$$

Under this change of variables, the expression in (2.4) becomes

$$\Delta(A,B,C) = 4(B^2 - AC) = -4a_0^2 \tag{2.5}$$

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 [EGM]) to be SL_2, and is obtained via

the homomorphism

$$\begin{array}{ccc} \rho : \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SO}_\Delta(\mathbb{Z}) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \overset{\rho}{\longmapsto} & \frac{1}{\alpha\delta-\beta\gamma} \cdot \begin{pmatrix} \alpha^2 & 2\alpha\gamma & \gamma^2 \\ \alpha\beta & \alpha\delta+\beta\gamma & \gamma\delta \\ \beta^2 & 2\beta\delta & \delta^2 \end{pmatrix} \end{array} \tag{2.6}$$

written here over $\mathbb{Z}$ as this is the situation we work with.

Claim: Let $\tilde{\Gamma}$ and ρ be as before. Let I denote the identity matrix, and let

$$\Lambda(2) = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1,\ M \equiv I \pmod 2\}$$

be the principal congruence 2-subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then the preimage of $\tilde{\Gamma}$ in $\mathrm{SL}_2(\mathbb{Z})$ under ρ is $\Lambda(2)$.

Proof. Note that $\Lambda(2)$ is generated by

$$M_1 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

Since $\rho(M_1) = s_2 s_1$, and $\rho(M_2) = s_2 s_3$ where s_1, s_2, s_3 are the generators of Γ' above, we have that

$$\Lambda(2) \subset \rho^{-1}(\tilde{\Gamma}) \tag{2.7}$$

Recall that since the fundamental domain of A_1 acting on $\mathbb{H}$ is a hyperbolic triangle where all the angles are 0, the hyperbolic area of $A_1\backslash\mathbb{H}$ is π. Since $\mathrm{SO}_\Delta(\mathbb{Z}) \bigcap \Gamma'$ contains exactly those elements of Γ' which have even word length when written via the generators of Γ', the group $\tilde{\Gamma}$ is of index 2 in Γ'. Therefore the hyperbolic area of $\tilde{\Gamma}\backslash\mathbb{H}$ is 2π, which is also known to be the hyperbolic area of $\Lambda(2)\backslash\mathbb{H}$ (see [K]). Combining this with (2.7), we have that 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. By the claim above, we have that the $\rho^{-1}(\tilde{\Gamma})$ consists of matrices in SL_2 of the form

$$\begin{pmatrix} 2k+1 & 2l \\ 2m & 2n+1 \end{pmatrix}$$

and under the spin homomorphism in (2.6) we have that the values of $A, A+C-2B$, and C respectively are of the form

- $A_0(2k+1)^2 + 2B_0(2k+1)(2m) + C_0(2m)^2$

- $A_0(2k+1-2l)^2+2B_0(2k+1-2l)(2m-2n-1)+C_0(2m-2n-1)^2$
- $A_0(2l)^2+2B_0(2l)(2n+1)+C_0(2n+1)^2$

Note that the collection of all three of these is precisely the set of integers represented primitively by the binary quadratic form

$$f_{a_0}(\zeta,\nu)=A_0\zeta^2+2B_0\zeta\nu+C_0\nu^2, \tag{2.8}$$

where $(\zeta,\nu)=1$, and A_0,B_0,C_0 are as in (2.1). The vectors in the orbit of A_1 are of the form $(a_0,A-a_0,A+C-2B-a_0,C-a_0)$, and so the integers appearing as coordinates of these vectors are at least those which can be written in the form

$$f_{a_0}(\zeta,\nu)-a_0, \tag{2.9}$$

where f_{a_0} is as in (2.8), so for a bounded packing P we have $\mathscr{A}_0\subset K_1(P)$ as desired. The proof in the case of an unbounded packing P that $\mathscr{A}_0\subset K_3(P)$ runs identically. □

By Lemma 2.1, we have

$$\kappa(P,X)\gg\#\{m\in\mathbb{N}\,|\,f_{a_0}(x,y)-a_0=m \text{ for some } x,y\in\mathbb{Z},(x,y)=1\} \tag{2.10}$$

and we need only to count the integers represented by f_{a_0} in order to get a bound on $\kappa(P,X)$. We note that the discriminant of the form f_{a_0} is

$$D(f_{a_0})=(2B_0)^2-4A_0C_0=-4a_0^2 \tag{2.11}$$

and for $a_0\neq 0$ this is not a square. The problem of counting integers represented by a binary quadratic form of discriminant $-D<0$ is classical. For example, we have the following theorem from [Be]:

Theorem 2.2 (Bernays, 1912)**.** *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

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

where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi-Kronecker symbol.

Note that Theorem 2.2 paired with (2.10) immediately yields the preliminary lower bound on $\kappa(P,X)$ from [S1]:

Proposition 2.3 (Sarnak, 2007)**.** *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 for some $c_2 > 0$ we have*

$$\kappa(P,X) \gg_{c_2} \frac{X}{\sqrt{\log X}}.$$

3. Proof of Theorem 1.2

Our computation in Section 2 concerns only those integers which occur as curvatures of circles which are tangent to a fixed circle C_{a_0} in P. It is thus natural to count some of the omitted curvatures here. Specifically, we repeat the method from Section 2 several times, fixing a different circle C each time and counting the integers occurring as curvatures of circles tangent to C.

Recall that to prove Proposition 2.3 we fixed a circle of curvature a_0, and associated curvatures of circles tangent to it with the set $\mathscr{A}_0$ of integers represented by $f_{a_0}(x,y) - a_0$. Let $a \in \mathscr{A}_0$ such that $a \neq 0$. By Lemma 2.1, there is a circle C_a of curvature a which is tangent to C_{a_0}, and, without loss of generality[2], there is a vector $\mathbf{v}_a = (a, b', c', d')$ such that $\mathbf{v}_a^t \in A\mathbf{v}_P^t$.

Lemma 3.1. *Let $a \in \mathscr{A}_0$, $a \neq 0$, and let P, C_a, and $\mathbf{v}_a$ be as above. Let*

$$f_a(x,y) = A_0'x^2 + 2B_0'y^2 + C_0'z^2 \tag{3.1}$$

where

$$A_0' = b' + a, B_0' = \frac{a + b' + d' - c'}{2}, C_0' = d' + a$$

and let S_a denote the set of integers less than X represented by $f_a - a$:

$$S_a = \{n \in \mathbb{N} \,|\, n \leq X, n = f_a(x,y) - a,\ x,y \geq 0,\ gcd(x,y) = 1\} \tag{3.2}$$

Then the set of integers $\leq X$ which occur as curvatures of circles tangent to C_a in the packing P are at least those which are in the set S_a.

This can be seen immediately by replacing the root quadruple $\mathbf{v}_P$ in Lemma 2.1 by $\mathbf{v}_a$.

Note that the discriminant of f_a is $-D = -4a^2$ and that the sets S_a depend only on a_0, the curvature of the original circle C_{a_0} which we fixed. One important consideration in counting the integers $\leq X$ represented by the forms f_a (i.e. computing $|S_a|$) 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 Theorem 2.2 is not uniform in D so we use more recent results of Blomer and Granville in [BG]

[2] a may not be in the first coordinate of a vector in the orbit of A. However, if it appears in the ith coordinate where $i \neq 1$ we simply consider orbits $A_i\mathbf{v}_a^t$ in what follows rather than $A_1\mathbf{v}_a^t$ and the argument runs analogously.

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[3].

By Lemma 3.1, we have that

$$\kappa(P,X) \gg \left| \bigcup_{a \in \mathscr{A}_0} S_a \right| \tag{3.3}$$

We wish to compute this bound using the first step of inclusion-exclusion:

$$\left| \bigcup_{a \in \mathscr{A}_0} S_a \right| \geq \sum_a |S_a| - \sum_{a,a'} |S_a \cap S_{a'}|$$

In Section 3.1, we use the results in [BG] to produce 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 $a \neq a'$ in Section 3.2, and thus get a lower bound for $\kappa(P,X)$ from (3.3).

A crucial ingredient to computing this and proving Theorem 1.2 (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 3.1 we specify how we choose the a's used in our computation, and compute the first sum, $\sum_a |S_a|$. In Section 3.2, we compute an upper bound on $\sum_{a,a'} |S_a \cap S_{a'}|$ for $a \neq a'$ to prove Theorem 1.2.

3.1. **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 [BG] – this will become clear in the computations preceding (3.13). 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.

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

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 Theorem 2.2, we have

$$\left|\mathscr{A}_0 \cap [2^k, 2^{k+1}]\right| \gg \frac{2^k}{\sqrt{k}} \tag{3.4}$$

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 3.4. 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

$$\mathbb{E}_n \left(\left| \mathscr{A}_0 \cap [2^k + n \cdot \eta \frac{2^k}{\sqrt{k}}, 2^k + (n+1) \cdot \eta \frac{2^k}{\sqrt{k}}] \right| \right) \gg \eta \frac{2^k}{k} \tag{3.5}$$

by (3.4). Thus for every value of k there exists an $0 \leq n \leq \sqrt{k}\eta^{-1}$ for which the intersection in (3.5) contains $\gg \eta \frac{2^k}{k}$ integers. For simplicity of notation, we assume without loss of generality[4] that $n = 0$, and define $\mathscr{A}^{(k)}$ to be

$$\mathscr{A}^{(k)} = \mathscr{A}_0 \cap [2^k, 2^k + \eta \frac{2^k}{\sqrt{k}}] \tag{3.6}$$

where we have

$$|\mathscr{A}^{(k)}| \gg \eta \frac{2^k}{k} \tag{3.7}$$

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

$$\mathscr{A} = \bigcup \mathscr{A}^{(k)} \tag{3.8}$$

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

Lemma 3.2. *Let $\mathscr{A}$ be as in (3.8) and S_a be as in (3.2). Then we have*

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

To prove Lemma 3.2, we recall the notation and relevant theorem from [BG]. Let f be a binary quadratic form of discriminant $-D$, and let $r'_f(n)$ be the number of representations[5] of n by f:

$$r'_f(n) = \#\{(m_1, m_2) \in \mathbb{Z}^2 - \{\mathbf{0}\} \mid gcd(m_1, m_2) = 1, f(m_1, m_2) = n\} \tag{3.9}$$

[4]One can in fact extend Theorem 2.2 to show that this holds for *every* n. Friedlander and Iwaniec do this for $a_0 = 1$ in Theorem 14.4 of [FI]. However, it is not necessary here.

[5]In [BG], the authors consider $r_f(n)$, the number of *inequivalent* representations of n by f, which is slightly different from $r'_f(n)$. Note, however, that $(r_f(n))^0 = (r'_f(n))^0$, so the notation $U_f^0(X)$ in (3.10) is the same in this paper as it is in [BG].

Let $r'_f(n)^0 = 1$ if $r'_f(n) > 0$, and 0 otherwise. Denote by

$$U_f^0(X) = \sum_{n \leq X} r'_f(n)^0 \tag{3.10}$$

the number of integers less than X represented by f, counting without multiplicity. In [BG], 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. Denote by $L(1,\chi_{-D})$ the Dirichlet L-function at 1 with character $\chi_{-D}(n) = \left(\frac{-D}{n}\right)$ where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi-Kronecker symbol, and let ϕ be the Euler totient function. Letting $\ell = \ell_{-D} = L(1,\chi_{-D})(\phi(D)/D)$, Blomer and Granville create a parameter

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

where $h/g = D^{1/2+o(1)}$. Their bounds for $U_f^0(X)$ are then uniform in D for each range below (see Theorem 3.3):

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

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 Bernays' result in Theorem 2.2, and is used to show that

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

in [F1]. Our results and the statement in Lemma 3.2 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 [BG], which is summarized below.

Theorem 3.3. *(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*

$$U_f^0(X) = \pi \cdot \left(1 - \frac{1}{2u}\right) \cdot \frac{X}{\sqrt{D}} + E_0(X,D) \tag{3.11}$$

where

$$E_0(X,D) \ll \sqrt{\frac{X}{s}} + \tau(D) \cdot \left(\frac{X\log X}{D} + \frac{X}{D^{\frac{3}{4}}}\right) \tag{3.12}$$

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 3.2.

Proof of Lemma 3.2:

We use Theorem 3.3 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

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

Thus we have that the error $E_0(X,D) \ll \frac{X}{D^{3/4-\varepsilon}}$ for any $\varepsilon > 0$, and thus Theorem 3.3 implies

$$U_f^0(X) \gg \frac{X}{\sqrt{D}} \tag{3.13}$$

where the implied constant does not depend on D. Since $D = -4a^2$, it follows from (3.13) that the number of distinct values less than X represented by f_a is $\gg \frac{X}{a}$ and we have

$$\begin{aligned} \sum_{a \in \mathscr{A}} |S_a| &\gg \sum_{a \in \mathscr{A}} \frac{X}{a} \\ &\gg \eta \cdot X \cdot \sum_{\substack{2^{k+1} < (\log X)^3 \\ 2^k > (\log X)^2}} \frac{1}{k} \\ &\gg \eta \cdot X \end{aligned} \tag{3.14}$$

as desired. □

The sum in Lemma 3.2 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 1.2, we obtain an upper bound on the number of integers we have counted twice in this way in the next section.

3.2. **Integers in the intersections.** To prove Theorem 1.2 we would like to show

$$\left| \bigcup_{a \in \mathscr{A}} S_a \right| \gg X \tag{3.15}$$

since this union is a subset of all curvatures less than X in the packing P. By Lemma 3.2, we may estimate the size of this union as follows:

$$\begin{aligned} \left| \bigcup_{a \in \mathscr{A}} S_a \right| &\geq \sum_{a \in \mathscr{A}} |S_a| - \sum_{a \neq a' \in \mathscr{A}} |S_a \cap S_{a'}| \\ &\gg \eta X - \sum_{a \neq a' \in \mathscr{A}} |S_a \cap S_{a'}| \end{aligned} \tag{3.16}$$

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

$$f_a(x,y) = \frac{(\alpha x + \beta y)^2 + 4a^2y^2}{\alpha} \tag{3.17}$$

we can define a region

$$B_a = \{(x,y) \in \mathbb{R}^2 \text{ s.t. } |\alpha x + \beta y| \ll \sqrt{|\alpha|} \text{ and } |y| \ll \frac{\sqrt{|\alpha|}}{a}\} \tag{3.18}$$

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 3.4. *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*

$$\sum_{a \neq a' \in \mathscr{A}} |S_a \cap S_{a'}| \leq c'' \eta^2 X \tag{3.19}$$

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 3.2.

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

$$\begin{aligned} &|S_a \cap S_{a'}| \\ \leq\ &|\{(x,y,x',y') \in \mathscr{B}_{a,a'} \,|\, f_a(x,y) - f_{a'}(x',y') = a - a'\}| \end{aligned} \tag{3.20}$$

Although bounding (3.19) 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 [Kl] and Esterman in [E] or modular forms (see [DRS]). 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 [HB] and Niedermowwe's Theorem 5.6 in [N] determine representation numbers of a fixed indefinite quadratic form[6]. 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:

Theorem 3.5. *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

$$\begin{aligned} & R_{\chi_{a,a'}}(a-a') \\ &= |I_{\chi_{a,a'}}(a-a')| \cdot |\mathfrak{S}(a-a')| + O\left(\frac{X\cdot\Delta^{100}}{(\log X)^{\lambda}}\right) \end{aligned} \tag{3.21}$$

where the first factor is the singular integral

$$I_{\chi_{a,a'}} = \int_{-\infty}^{\infty} \left[\int_{\mathbb{R}^4} \chi_{a,a'}(x) e(z(F(x) - a + a')) dx \right] dz \tag{3.22}$$

and the second factor is the singular series

$$\mathfrak{S}(a-a') = \prod_p \sigma_p \tag{3.23}$$

where

$$\sigma_p = \lim_{k\to\infty} p^{-3k} \cdot \#\{\mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^4 \ s.t. \ F(\mathbf{x}) \equiv a - a' \ (p^k)\} \tag{3.24}$$

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

In the error term in (3.21), 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

[6]Note that in [HB] 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 [N] m is any nonzero integer.

in [HB] and [N] suffice. In particular, the argument in [N] 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 (3.21) via a power of the discriminant Δ of F. It is similarly important here that the distortion of B_a and $B_{a'}$ with respect to the standard cube discussed in [HB] and [N] is logarithmic in X.

To prove Proposition 3.4 it remains to evaluate the singular integral and singular series in (3.22) and (3.23). 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 (3.17) and (3.18), we have

$$\begin{aligned} I_{\chi_{a,a'}} &\ll \lim_{\varepsilon\to 0}\frac{1}{\varepsilon}\cdot \mathbf{V}\Big(\{(x,y,x',y')\in \sqrt{X}B_a\times\sqrt{X}B_{a'} \,|\, |f_a(x,y)-f_{a'}(x',y')-a+a'|<\varepsilon\}\Big) \\ &\ll \lim_{\varepsilon\to 0}\frac{1}{\varepsilon}\cdot\frac{\varepsilon}{\sqrt{|\alpha|X}}\cdot\frac{\sqrt{|\alpha|X}}{a}\cdot\sqrt{\frac{X}{|\alpha'|}}\cdot\frac{\sqrt{|\alpha'|X}}{a'} \\ &\ll \frac{X}{aa'} \qquad (3.25) \end{aligned}$$

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

Lemma 3.6. *Let $\mathfrak{S}(a-a')$ be the singular series defined in (3.23). We have*

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

where $\omega(n)$ denotes the number of distinct prime factors of n.

Proof. We compute an upper bound for the expression in the limit in (3.24) 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 (**??**). Therefore

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

and over $\mathbb{F}_p$, the number of nontrivial representations of 0 by F is bounded above by $2p^3$ (see [C] p. 31 ex.13, for example), so σ_p is bounded above by 2 in this case. In the other cases, we use exponential sum estimates – see Chapter 20.2 of [IK] for a detailed explanation of the equivalence of the expression below to that in (3.24). Bounding σ_p from above by letting $k=1$ as before, we have

$$p^3\cdot\sigma_p < \frac{1}{p}\sum_{r=0}^{p-1}\Big[\sum_{x,y}e_p(rf_a(x,y))\Big]\Big[\sum_{x',y'}e_p(-rf_{a'}(x',y'))\Big]e_p(r(a-a')) \qquad (3.26)$$

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

$$p^3 \cdot \sigma_p < p^3 + \frac{1}{p}\sum_{r=1}^{p-1}\left(\frac{\tilde{\alpha}r}{p}\right)^2\left(\frac{\tilde{\alpha}'r}{p}\right)^2 p^2 e_p(r(a-a')) = p^3 + \mathrm{o}(p)$$

since $(a-a',p)=1$.

Case 2: $p|a-a'$ and does not divide aa':

In this case we have $p^3 \cdot \sigma_p < p^3 + \mathrm{o}(p^2)$.

Case 3: $p|a$ and $p \not| a'$:

Diagonalizing $f_{a'}$, we obtain

$$p^3 \cdot \sigma_p < p^3 + \frac{1}{p}\sum_{r=1}^{p-1}\left(\frac{\alpha r}{p}\right) p\sqrt{p}\cdot p \cdot e_p(r(a-a')) < p^3 + \mathrm{o}(p^2)$$

From these bounds and Lemma 3.8, we obtain the desired result in Lemma 3.6. □

Combining our computation of the singular integral in (3.25) and the bound on the singular series in Lemma 3.6, the result of Niedermowwe in Theorem 3.5 yields

$$|S_a \cap S_{a'}| \ll \frac{X}{aa'} \cdot \prod_{\substack{p|aa'(a-a') \\ p\not|(a,a')}} \left(1+\frac{1}{p}\right) \cdot 2^{\omega((a,a'))} \tag{3.27}$$

where $\omega(n)$ is the number of distinct prime factors of n. Thus to evaluate the last sum in (3.16), 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 [FI] of Friedlander and Iwaniec regarding sums of squares in progressions below.[7].

Theorem 3.7. *(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

$$B(x,q,a) = \sum_{\substack{n\le x \\ n\equiv a\,(q)}} b(n)$$

[7]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.

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 Theorem 3.7 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 2, such an upper bound implies the following in our case.

Lemma 3.8. *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 (3.6), we may bound above the sum in Lemma 3.8 as a sum over k for which $(\log X)^2 \leq 2^k, 2^{k+1} \leq (\log X)^3$:

$$\sum_k \frac{1}{2^k} \sum_{\substack{a \in \mathscr{A}_0 \\ a \in [2^k, 2^k + \eta \frac{2^k}{\sqrt{k}}] \\ a \equiv r(q)}} 1 \tag{3.28}$$

By Theorem 3.7, 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 (3.28) 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 (3.27) as follows.

$$\sum_{a\neq a'\in\mathscr{A}} |S_a\cap S_{a'}| \ll X\cdot \sum_{a\neq a'\in\mathscr{A}} \frac{1}{aa'}2^{\omega((a,a'))} \prod_{\substack{p|aa'(a-a')\\ p\nmid(a,a')}} \left(1+\frac{1}{p}\right) \tag{3.29}$$

$$\ll X\cdot \sum_{q_0,q_1,q_1',q_2} \frac{2^{\omega(q_2)}}{q_1q_1'q_2} \sum_{\substack{q_0q_1|a\\ q_0q_1'|a'\\ q_2|a-a'}} \frac{1}{aa'} \tag{3.30}$$

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 (3.29), we may restrict in (3.30) 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 3.8. First fix a and sum over a' subject to the restrictions $q_0q_1'|a'$ and $a\equiv a' \bmod q_2$. From Lemma 3.8, 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

$$\sum_{\substack{q_0q_1|a\\ q_0q_1'|a'\\ q_2|a-a'}} \frac{1}{aa'} \ll \frac{(\log\log(q_0+q_1+q_1'+q_2))^2}{q_0^2q_1q_1'q_2}\cdot\eta^2 \tag{3.31}$$

Substituting (3.31) into (3.30) gives the desired bound

$$\sum_{a\neq a'\in\mathscr{A}} |S_a\cap S_{a'}| \ll \eta^2X \sum_{q_0,q_1,q_1',q_2} 2^{\omega(q_2)}\cdot\frac{(\log\log(q_0+q_1+q_1'+q_2))^2}{(q_0q_1q_1'q_2)^2}$$

$$< c''\eta^2X \tag{3.32}$$

□

Note that c'' above is independent of η, and we may choose η small enough depending on c'' so that $\eta-c''\eta^2>0$ since $0<\eta<1$. Then (3.16) and (3.14) imply

$$\left|\bigcup_{a\in\mathscr{A}} S_a\right| \gg (\eta-c''\eta^2)X \gg_c X$$

where $c = \eta - c''\eta^2 > 0$ as desired. □

We note that the methods used here are easily generalizable to prove similar positive density theorems for integer orbits of subgroups of $\mathrm{O}(3,1)$. 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 2. 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 (counted without multiplicity).

REFERENCES

[Be] 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)

[BG] V. Blomer, A. Granville, *Estimates for representation numbers of quadratic forms*, Duke Mathematical Journal, Vol. 135, No 2, pp. 261-302 (2006)

[C] J.W.S. Cassels, *Rational Quadratic Forms*, Dover Publications, Inc., Mineola, NY (1978)

[Cx] 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)

[DRS] W. Duke, Z. Rudnick, and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. 71, no. 1, pp. 143179 (1993)

[EGM] J. Elstrodt, F. Grunewald, J. Mennicke, *Groups Acting on Hyperbolic Space*, Springer Verlag Berlin Heidelberg (1998)

[E] T. Estermann, *A new application of the Hardy - Littlewood - Kloosterman method*, Proc. London. Math. Soc. 12, pp. 425444 (1962)

[FI] J. Friedlander, H. Iwaniec, *Opera de Cribro*, preprint (2009)

[F] E. Fuchs, *Arithmetic properties of Apollonian circle packings*, Ph. D. Thesis, Princeton (2010)

[F1] E. Fuchs, *A note on the density of curvatures in integer Apollonian circle packings*, preprint, http://www.math.princeton.edu/~efuchs (2009)

[FS] E. Fuchs, K. Sanden, *Some experiments with integral Apollonian circle packings*, preprint, http://www.math.princeton.edu/~efuchs (2010)

[GLMWY] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: number theory*, J. of Number Theory, vol 100 (1) pp. 1-45 (2003)

[GLMWY1] 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*, Discrete Comput. Geom., 34(4):547585 (2005)

[HB] 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)

[H] K.E. Hirst, *The Apollonian packing of circles*, Proc. Nat. Acad. Sci. USA, 29, pp. 378-384 (1943)

[IK] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications **53** (2004)

[J] R.D. James, *The Distribution of integers represented by quadratic forms*, American Journal of Mathematics, Vol. 60, No.3. pp. 737-744 (1938)

[K] S. Katok, *Fuchsian Groups*, The University of Chicago Press (1992)

[Kl] 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)

[KO] A. Kontorovich, H. Oh, *Apollonian circle packings and closed horospheres on hyperbolic* 3*-manifolds*, preprint, http://arxiv.org/pdf/0811.2236 (2008)

[N] N. Niedermowwe, *A version of the circle method for the representation of integers by quadratic forms*, preprint arXiv:0905.1229v1 (2009)

[S] K. Sanden, *Prime number theorems for Apollonian circle packings*, Senior Thesis, Princeton University (2009)

[S1] P. Sarnak, *Letter to Lagarias*, http://www.math.princeton.edu/sarnak (2008)

[S2] P. Sarnak, *MAA Lecture on Apollonian Circle Packings*, http://www.math.princeton.edu/sarnak (2009)

INSTITUTE FOR ADVANCED STUDY, SCHOOL OF MATHEMATICS, EINSTEIN DRIVE, PRINCETON, NJ 08540 USA

E-mail address: bourgain@math.ias.edu

INSTITUTE FOR ADVANCED STUDY, SCHOOL OF MATHEMATICS, EINSTEIN DRIVE, PRINCETON, NJ 08540 USA

E-mail address: efuchs@math.ias.edu