JOURNAL OF MODERN DYNAMICS
VOLUME 15, 2019, 209–236
doi: 10.3934/jmd.2019019

THE LOCAL-GLOBAL PRINCIPLE FOR INTEGRAL SODDY SPHERE PACKINGS

ALEX KONTOROVICH
(Communicated by Laura DeMarco)

ABSTRACT. Fix an integral Soddy sphere packing $\mathscr{P}$. Let $\mathscr{B}$ be the set of all bends in $\mathscr{P}$. A number n is called *represented* if $n \in \mathscr{B}$, that is, if there is a sphere in $\mathscr{P}$ with bend equal to n. A number n is called *admissible* if it is everywhere locally represented, meaning that $n \in \mathscr{B} (\mathrm{mod}\, q)$ for all q. It is shown that every sufficiently large admissible number is represented.

1. INTRODUCTION

This paper is concerned with a 3-dimensional analogue of an Apollonian circle packing in the plane, constructed as follows. Given four mutually tangent spheres with disjoint points of tangency (Figure 1a), a generalization to spheres of Apollonius's theorem says that

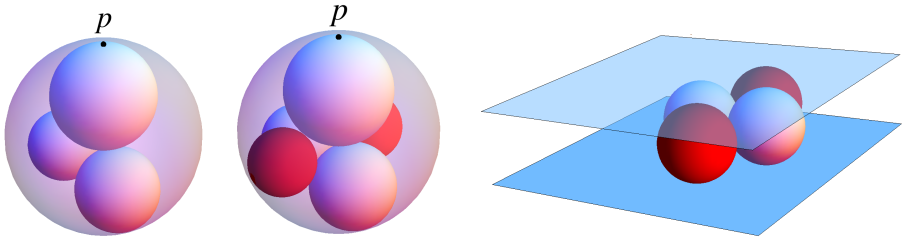
(1.1) there are exactly two spheres

tangent to the given ones (Figure 1b). For a proof of (1.1), take a point p of tangency of two given spheres and reflect the configuration through a sphere centered at p. Thus p is sent to ∞, and the resulting configuration (Figure 1c) consists of two tangent spheres wedged between two parallel planes; whence the two solutions claimed in (1.1) are obvious.

Returning to Figure 1b, one now has more configurations of tangent spheres, and can iteratively inscribe further spheres in this way (Figure 2a). Repeating this procedure *ad infinitum*, one obtains what we will call a *Soddy sphere packing* (Figure 2b).

The name refers to the radiochemist Frederick Soddy (1877–1956), who in 1936 wrote a *Nature* poem [27] in which he rediscovered Descartes's Circle Theorem [8, pp. 37–50] and a generalization to spheres, see Theorem 2.1. The latter was known already in 1886 to Lachlan [22], and appears in some form as early as 1798 in Japanese Sangaku problems [25]. We name the packings after Soddy

Received November 8, 2017; revised March 23, 2019.
2010 *Mathematics Subject Classification:* Primary: 11D85; Secondary: 11F06, 20H05.
Key words and phrases: Sphere packings, thin groups, hyperbolic geometry, arithmetic groups, quadratic forms, local-global principle.
The author is partially supported by an NSF CAREER grant DMS-1254788 and DMS-1455705, an NSF FRG grant DMS-1463940, an Alfred P. Sloan Research Fellowship, and a BSF grant.

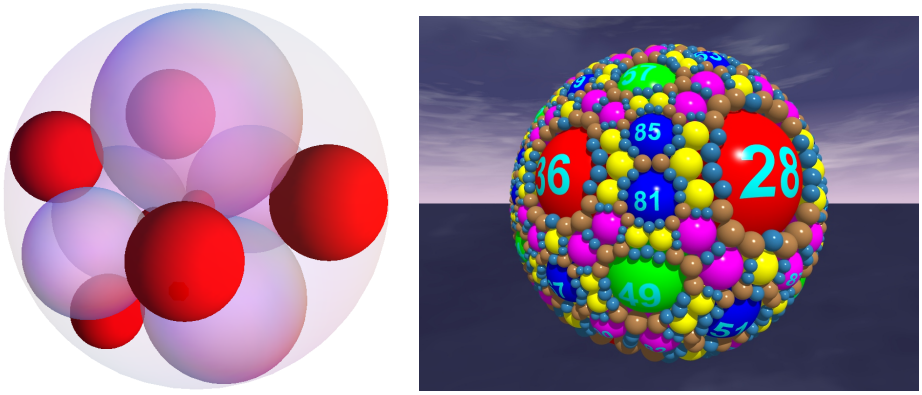


(a) Four tangent spheres

(b) Two more spheres

(c) Reflection of (b) through a sphere centered at p

FIGURE 1



(a) More tangent spheres

(b) A Soddy sphere packing. Image by Nicolas Hannachi, used with permission

FIGURE 2

because he was the first, as far as we know, to observe that there are configurations of circle and sphere packings in which all bends[1] are integers [28]; such a packing is called *integral*. The numbers illustrated in Figure 2b are some of the bends in that packing. In [28, p. 78], Soddy writes that he "discovered this [integrality] years ago for the simpler case of cylinders, or circles, in connection with the design of an actual mechanism," and provides a picture of a corresponding spherical mechanism, reproduced in Figure 3.

By rescaling an integral packing, we may assume that the only integers dividing all of the bends are ± 1; such a packing is called *primitive*. We restrict our attention henceforth to bounded, integral, primitive Soddy sphere packings. In fact, all of the salient features persist if one considers just the packing $\mathscr{P}_0$ illustrated in Figure 2b.

The goal of this paper is to address the question: What numbers appear in Figure 2b? For a sphere $S \in \mathscr{P}$, let $b(S)$ be its bend, and let $\mathscr{B} = \mathscr{B}(\mathscr{P})$ be the

[1]The "bend" of a circle or sphere is defined to be one over its radius.

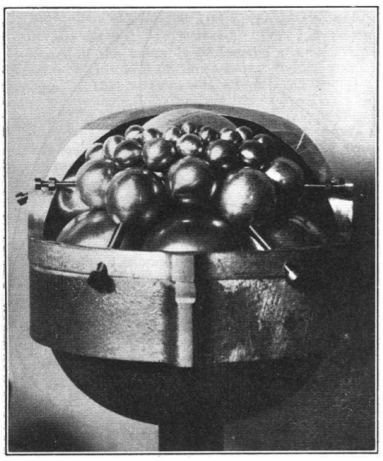


FIGURE 3. A reproduction from [28]

set of all bends in $\mathscr{P}$,

$$\mathscr{B} := \{n \in \mathbb{Z} : \exists S \in \mathscr{P},\ b(S) = n\}.$$

The bounding sphere is internally tangent to the others, so is given opposite orientation and negative bend. The first few bends in $\mathscr{P}_0$ are:

$$\mathscr{B} = \{-11, 21, 25, 27, 28, 34, 36, 40, 42, 43, 46, 48, 49, 51, 54, 57, 61, 63, \\ 64, 67, 69, 70, 72, 73, 75, 78, 79, 81, 82, 84, 85, 87, 90, \ldots\}. \tag{1.2}$$

A moment's inspection reveals that every bend in $\mathscr{P}_0$ is

$$\equiv 0 \text{ or } 1 \pmod 3, \tag{1.3}$$

that is, there are local obstructions. That such exist was already observed 40 years ago by Boyd [5, p. 376]. In analogy with Hilbert's 11th problem on representations of numbers by quadratic forms, we say that n is *represented* if $n \in \mathscr{B}$. Let $\mathscr{A} = \mathscr{A}(\mathscr{P})$ be the set of *admissible* numbers, that is, numbers n that are everywhere locally represented in the sense that

$$n \in \mathscr{B} \pmod q \text{ for all } q. \tag{1.4}$$

In our example, $\mathscr{A}$ is the set of all numbers satisfying (1.3). The set of admissible numbers for any primitive packing $\mathscr{P}$ satisfies either (1.3) or

$$\equiv 0 \text{ or } 2 \pmod 3, \tag{1.5}$$

see Lemma 2.2.

The number of spheres in $\mathscr{P}$ with bend at most N (counted with multiplicity) is asymptotically equal to a constant times N^δ, where δ is the Hausdorff dimension of the closure of the packing (see [16], which generalizes [19] to this setting). Soddy packings are rigid (one can be mapped to any other by a conformal transformation), and so δ is a universal constant; it is approximately (see [5, 2]) equal to

$$\delta \approx 2.4739\ldots.$$

Hence one expects, on grounds of randomness, that the multiplicity of a given admissible bend up to N is roughly $N^{\delta-1}$, which should be quite large. In particular, every sufficiently large admissible should be represented. The main purpose of this paper is to confirm this claim, giving the first instance of a local-global result for a "thin orbit" (see, e.g., [20, 21] for overviews of the theory).

THEOREM 1.1 (The Local-Global Theorem)**.** *The bends of a fixed primitive, integral Soddy sphere packing $\mathscr{P}$ satisfy a local-to-global principle.*

That is, there is an effectively computable $N_0 = N_0(\mathscr{P})$ so that, if $n > N_0$ and n is admissible, $n \in \mathscr{A}$, then n is represented, $n \in \mathscr{B}$.

Empirical evidence suggests (and could be verified with enough computation) that $N_0(\mathscr{P}_0) = 330$ suffices.

Theorem 1.1 is the analogue to Soddy sphere packings of the local-global conjecture for integral Apollonian circle packings [11, 10]. While the local-global problem for circle packings, despite some recent advances [3, 4], remains out of reach at present, the same for sphere packings is solvable, as above, due to having access to "more variables" in higher dimension. Here is a sketch of the ideas.

Outline of the proof. We study what we call the *Soddy group*, $\Gamma < \mathrm{Isom}(\mathbb{H}^4)$, consisting of symmetries of the sphere packing $\mathscr{P}$, the latter sitting in the boundary $\partial\mathbb{H}^4 = \mathbb{R}^3 \cup \{\infty\}$. This group is conjugate to an infinite index subgroup of the full integral orthogonal group preserving a particular rational quadratic form of signature $(4,1)$. That is, the quotient $\Gamma\backslash\mathbb{H}^4$ is an infinite volume hyperbolic 4-fold, and $\mathscr{P}$ is its limit set. After a calculation, we show that the subgroup of Γ which stabilizes a single sphere is an arithmetic and moreover, *congruence*, Bianchi group $\Xi < \mathrm{Isom}(\mathbb{H}^3)$, see Lemma 3.5. Further calculations show, as a consequence, that the set $\mathscr{B}$ of bends contains the "primitive" values of a shifted quaternary quadratic form (and moreover an infinite family of such). Here "primitive" is not a standard notion; this quaternary form in the integers is actually a binary Hermitian form in a pair of Eisenstein integers, and primitive refers to this pair being coprime, see Corollary 3.7.

Thus far, everything is a more-or-less direct generalization to sphere packings of the following related result in one lower dimension due to Sarnak [26]: the bends in an integral, primitive Apollonian circle packing contain the primitive values of a shifted *binary* quadratic form (over the rationals). It is in this sense that we have more variables: instead of binary forms, sphere packings contain values of quaternary forms. While binary forms represent very few numbers, it goes back to methods of Kloosterman [17] that quaternary forms essentially satisfy local-global theorems, so, at least, in principle, we should be done.

A relatively minor technical problem is to deal with the above-mentioned non-standard "primitivity" notion. A more serious issue has to do with ramification in the discriminants of the arising quadratic forms. Our main innovation here is a series of maneuvers which bypass the ramification altogether, leading to the Local-Global Theorem 1.1; see §4. Note that it should be possible, with

more work, to make this argument more robust and not rely on such maneuvers, along the lines of the circle method involving both the thin group Γ and the congruence group Ξ as in [4]. We plan to return to this approach later.

In dimension $n \geq 4$, one can start with a configuration of n tangent hyperspheres, repeating the above-described generating procedure. Unfortunately this does not give rise to a packing, as the hyperspheres eventually overlap [6].[2] Moreover there are no longer any such configurations in which all bends are integral (they can be S-integral, with the set S of localized primes depending on the dimension n); this follows from Gossett's [13] generalization (also in verse) of Soddy's Theorem 2.1 to n-space.[3]

Notation. The following notation for parentheses is used throughout. We sometimes write $x \equiv y(z)$ for $x \equiv y (\mathrm{mod}\, z)$. We will use bold parentheses $\mathbf{(}x, y\mathbf{)}$ for the ideal generated by x and y, not to be confused with the gcd, denoted simply by (x, y). The indicator function $\mathbf{1}_{\{X\}}$ is 1 if X holds and 0 otherwise.

2. PRELIMINARIES

Let $\mathscr{S} = (S_1, S_2, S_3, S_4, S_5)$ be a configuration of five mutually tangent spheres, and let

$$\mathbf{b}_0 = \mathbf{b}(\mathscr{S}) = (b_1, b_2, b_3, b_4, b_5)$$

be the corresponding quintuple of bends, with $b_j = b(S_j)$. Any four tangent spheres, say S_1, S_2, S_3, S_4 have six cospherical points of tangency, and determine a *dual sphere* $\tilde{S}_5$ passing through these points. Similarly, for $j = 1, \ldots, 4$, let $\tilde{S}_j$ be the dual sphere orthogonal to all those in $\mathscr{S}$ except S_j, and call $\tilde{\mathscr{S}} = (\tilde{S}_1, \ldots, \tilde{S}_5)$ the *dual configuration*. Reflection through $\tilde{S}_5$ fixes S_1, S_2, S_3, S_4, and sends S_5 to S_5', the other sphere satisfying (1.1), see Figure 4a. The same holds for the other $\tilde{S}_j$, and iteratively reflecting the original configuration through the $\tilde{S}_j$ *ad infinitum* yields the Soddy packing $\mathscr{P} = \mathscr{P}(\mathscr{S})$ corresponding to $\mathscr{S}$. Observe that unlike the Apollonian case, the dual spheres in $\tilde{\mathscr{S}}$ are not tangent, but intersect non-trivially, see Figure 4b.

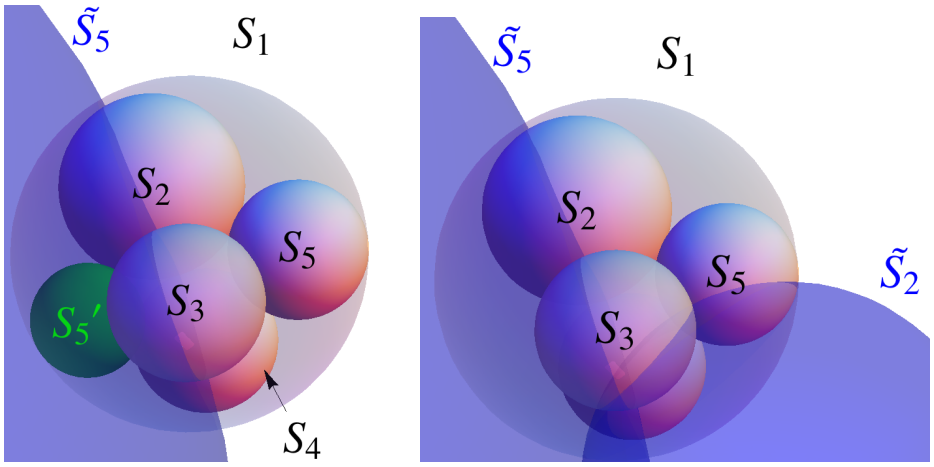
Extend the reflections through dual spheres to hyperbolic 4-space,

$$\mathscr{H}^4 := \{(x_1, x_2, x_3, y) : x_1, x_2, x_3 \in \mathbb{R}, y > 0\}, \tag{2.1}$$

replacing the action of the dual sphere $\tilde{S}_j$ by a reflection through a hyper(hemi)-sphere $\mathfrak{s}_j$ whose equator (at $y = 0$) is $\tilde{S}_j$ (with $j = 1, \ldots, 5$). We abuse notation,

[2] Added in print: See Baragar [1] for an alternate construction with non-overlapping hyperspheres. An even more general collection of higher dimensional "crystallographic" sphere packings is discovered in [18].

[3] Added in print: The tangency graph of a quintuple of mutually tangent spheres generating a Soddy sphere packing is isomorphic to the 1-skeleton of a 4-dimensional simplex. A further generalization in 3-dimensional sphere packings is to consider configurations coming from the 1-skeleton of a 4-orthoplex; the results here have been extended to this setting independently by Dias [9] and Nakamura [24]. For the corresponding generalization of classical Apollonian packings, see Zhang [29].



(a) Five tangent spheres and a dual reflection to a sixth

(b) Dual spheres intersect

FIGURE 4

writing $\mathfrak{s}_j$ for both the hypersphere and the conformal map reflecting through $\mathfrak{s}_j$. The group

$$\mathscr{A} := \langle \mathfrak{s}_1, \mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4, \mathfrak{s}_5 \rangle < \mathrm{Isom}(\mathscr{H}^4), \tag{2.2}$$

generated by these reflections acts discretely on $\mathscr{H}^4$. The $\mathscr{A}$-orbit of any given base point in $\mathscr{H}^4$ has a limit set in the boundary $\partial\mathscr{H}^4 \cong \mathbb{R}^3 \cup \{\infty\}$, which is the closure of the original sphere packing. A fundamental domain for this action is the exterior in $\mathscr{H}^4$ of the five dual hyperspheres $\mathfrak{s}_j$. Hence the quotient hyperbolic 4-fold $\mathscr{A}\backslash\mathscr{H}^4$ is geometrically finite (with orbifold singularities corresponding to non-trivial intersections of the dual spheres $\tilde{S}_j$), and has infinite hyperbolic volume with respect to the hyperbolic measure

$$y^{-4}dx_1dx_2dx_3dy$$

in the coordinates (2.1). The group $\mathscr{A}$ is the symmetry group of all conformal transformations fixing $\mathscr{P}$.

For an algebraic realization of $\mathscr{A}$, we need the following

THEOREM 2.1 ([22, 27])**.** *Given a configuration $\mathscr{S}$ of five tangent spheres, the quintuple $\mathbf{b} = (b_1, b_2, b_3, b_4, b_5)$ of their bends lies on the cone*

$$Q(\mathbf{b}) = 0, \tag{2.3}$$

where Q is the quinternary quadratic form

$$Q(b_1, \ldots, b_5) := 3(b_1^2 + \cdots + b_5^2) - (b_1 + \cdots + b_5)^2. \tag{2.4}$$

Recall again that a bounding sphere was negative bend. Arguably the nicest formulation of Theorem 2.1 is the last line of the following excerpt from Soddy's aforementioned poem [27]:

> 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.*

If $b_1,\dots,b_4$ are given, it then follows from (2.3) that the variable b_5 satisfies a quadratic equation, and hence there are two solutions. This is an algebraic proof of (1.1). Writing b_5 and b_5' for the two solutions, it is elementary from (2.3) that

$$b_5 + b_5' = b_1 + b_2 + b_3 + b_4.$$

In other words, if the quintuple $(b_1, b_2, b_3, b_4, b_5)$ is given, then one obtains the quintuple with b_5 replaced by b_5' via a linear action:

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ 1 & 1 & 1 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5' \end{pmatrix}.$$

This is an algebraic realization of the geometric action of $\tilde{S}_5$ (or $\mathfrak{s}_5$) on a quintuple. Call the above 5×5 matrix M_5. One can similarly replace other b_j by b_j' keeping the four complementary bends fixed, via the matrices

$$M_1 = \begin{pmatrix} -1 & 1 & 1 & 1 & 1 \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & & & & \\ 1 & -1 & 1 & 1 & 1 \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ 1 & 1 & -1 & 1 & 1 \\ & & & 1 & \\ & & & & 1 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ 1 & 1 & 1 & -1 & 1 \\ & & & & 1 \end{pmatrix}. \tag{2.5}$$

Let Γ be the group generated by the M_j:

$$\Gamma := \langle M_1, M_2, M_3, M_4, M_5 \rangle. \tag{2.6}$$

By construction, each generator M_j (and hence also Γ) lies inside the orthogonal group O_Q preserving the form Q,

$$O_Q := \left\{ g \in \mathrm{GL}_5 : Q(g\cdot\mathbf{b}) = Q(\mathbf{b}),\ \forall \mathbf{b} \right\}.$$

Moreover the Soddy group Γ is clearly contained in the group $O_Q(\mathbb{Z})$ of integer matrices. The fact that $\mathscr{A}$ has infinite co-volume is equivalent to Γ having infinite index in $O_Q(\mathbb{Z})$. That is, Γ is a "thin" group. The generators of Γ satisfy the relations: $M_j^2 = I$ and $(M_j M_k)^3 = I$ [12, Theorem 5.1]. Geometrically, these relations correspond, respectively, to reflections being involutions, and to the non-trivial intersections of the dual spheres (recall Figure 4b).

The orbit

$$\mathscr{O} := \Gamma \cdot \mathbf{b} \tag{2.7}$$

of the quintuple $\mathbf{b} = \mathbf{b}(\mathscr{S})$ under the Soddy group Γ consists of all quintuples corresponding to bends of five mutually tangent spheres in the packing $\mathscr{P}$. Hence the set $\mathscr{B}$ of all bends in $\mathscr{P}$ is simply the union of sets of the form

$$\mathscr{B} = \bigcup_{\mathbf{w} \in \{\mathbf{e}_1, \dots, \mathbf{e}_5\}} \langle \mathbf{w}, \Gamma \cdot \mathbf{b} \rangle, \tag{2.8}$$

as $\mathbf{w}$ ranges through the standard basis vectors

$$\mathbf{e}_1 = (1,0,0,0,0), \dots, \mathbf{e}_5 = (0,0,0,0,1).$$

The inner product $\langle \cdot, \cdot \rangle$ in (2.8) is the standard one on $\mathbb{R}^5$.

This explains the integrality of all bends in Figure 2b: the group Γ has only integer matrices, so if the initial quintuple $\mathbf{b}_0$ (or for that matter, any bends of five mutually tangent spheres in $\mathscr{P}$) is integral, then the bends in $\mathscr{P}$ are all integers (as first observed by Soddy [28]).

From (2.8) it is elementary to see the local obstruction claimed in (1.3). For the packing $\mathscr{P}_0$ of Figure 2b, one can choose to generate from the "root" quintuple (meaning it consists of the bends of the five largest tangent spheres, see [11, §3])

$$\mathbf{b}_0 := (-11, 21, 25, 27, 28). \tag{2.9}$$

The orbit under Γ, reduced mod 3, is then elementarily computed. In general we have the following

LEMMA 2.2. *For $\mathscr{B}$ the set of bends of an integral, primitive Soddy packing $\mathscr{P}$, there is always a local obstruction* mod 3*, either of the form* (1.3) *or* (1.5)*. In particular, there is an $\varepsilon = \varepsilon(\mathscr{P}) \in \{\pm 1\}$ so that, for any quintuple $\mathbf{b}$ in the cone* (2.3) *over $\mathbb{Z}$, two entries are $\equiv 0 \pmod 3$ and three entries are $\equiv \varepsilon \pmod 3$.*

Note that we are not (yet) claiming that these are the *only* local obstructions; this will follow from our proof of the local-to-global theorem.

Proof. One may first attempt to understand the cone (2.3) over $\mathbb{Z}/3\mathbb{Z}$, but the form Q in (2.4) reduced mod 3 is highly degenerate. So instead consider the cone over $\mathbb{Z}/9\mathbb{Z}$. Disregarding the origin (since the packing is assumed to be primitive), there are 140 vectors mod 9, not counting permutations. Reducing these mod 3 leaves only the two vectors $(0,0,\varepsilon,\varepsilon,\varepsilon)$, $\varepsilon \in \{\pm 1\}$, and their permutations. The action of $\Gamma \pmod 3$ on these is trivial: each vector is fixed. This is all verified by direct computation. □

It is convenient to also record here the following

LEMMA 2.3. *The set $\mathscr{B}$ of bends of an integral, primitive Soddy packing $\mathscr{P}$ always contains an element $b \equiv \varepsilon \pmod 6$, and an element $b \equiv 3+\varepsilon \pmod 6$.*

Proof. The cone (2.3) mod 36 has 30,576 vectors, not counting permutations. Reducing these mod 6 leaves 15 vectors, of which 5 are imprimitive, the remaining ones being:

$$\text{if } \varepsilon(\mathscr{P}) = +1\text{:} \quad \begin{pmatrix} 0\\0\\1\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\1\\3 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\3\\4 \end{pmatrix}, \begin{pmatrix} 1\\1\\3\\3\\4 \end{pmatrix}, \begin{pmatrix} 1\\3\\3\\4\\4 \end{pmatrix}$$

$$\text{if } \varepsilon(\mathscr{P}) = -1\text{:} \quad \begin{pmatrix} 0\\0\\5\\5\\5 \end{pmatrix}, \begin{pmatrix} 0\\3\\5\\5\\5 \end{pmatrix}, \begin{pmatrix} 0\\2\\3\\5\\5 \end{pmatrix}, \begin{pmatrix} 2\\2\\3\\3\\5 \end{pmatrix}, \begin{pmatrix} 2\\3\\3\\5\\5 \end{pmatrix}.$$

They plainly each have at least one element $\equiv 1$ or $5 \pmod 6$, giving the first claim.

Next observe that the orbit under $\Gamma \pmod 6$ plus permutations acts transitively on each row (of course, Γ cannot change $\varepsilon(\mathscr{P})$). This gives the second claim, that one can always make either 2 or 4 appear as one of the entries mod 6. □

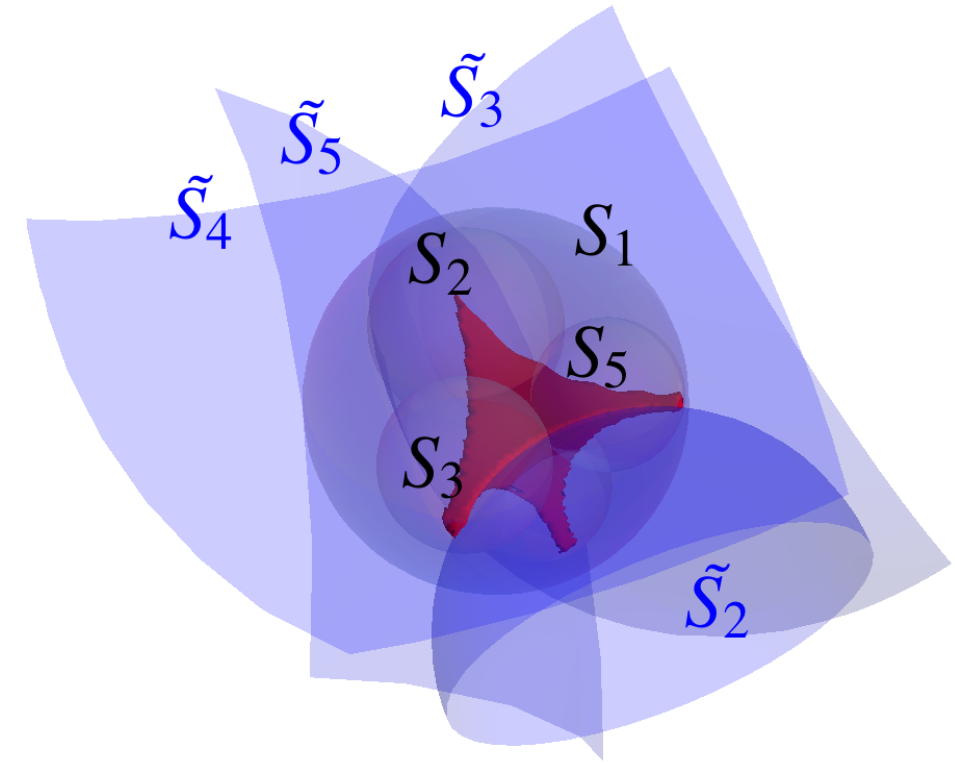
3. BENDS AS PRIMITIVE VALUES OF QUATERNARY FORMS

In this section, we show that a subset of the bends $\mathscr{B}$ in a Soddy packing can be obtained as "primitive" (which has a non-standard meaning here; see below) values of certain shifted quaternary quadratic forms. Our first goal is to prove that the Soddy group Γ, while being infinite index in $O_Q \cong O(4,1)$, contains a congruence Kleinian subgroup. The method is a generalization of Sarnak's observation in [26].

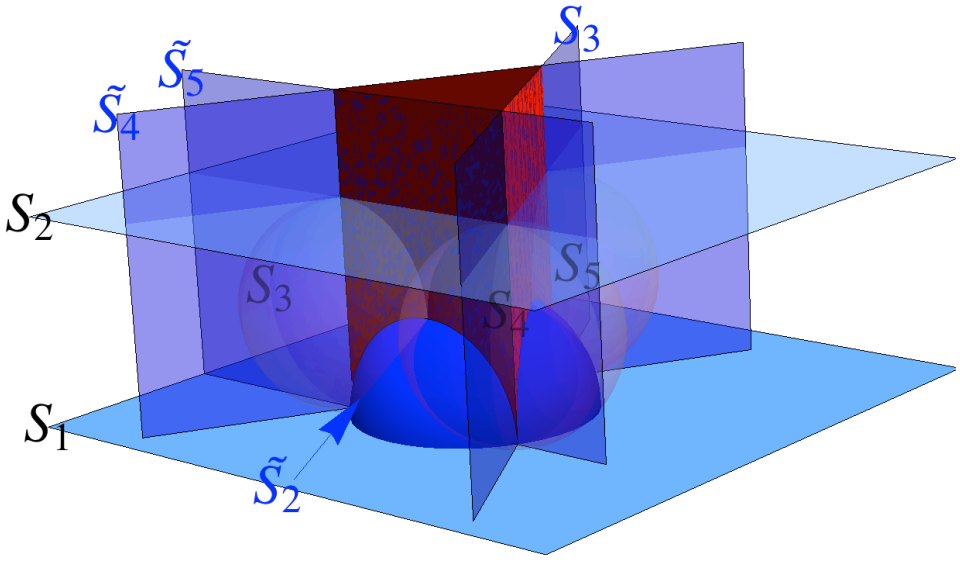
Recall the configuration $\mathscr{S} = (S_1, \ldots, S_5)$ of five mutually tangent spheres and the group $\mathscr{A}$ in (2.2) of reflections through spheres in the configuration $\tilde{\mathscr{S}}$ dual to $\mathscr{S}$. Let

$$\mathscr{A}_1 = \langle \mathfrak{s}_2, \ldots, \mathfrak{s}_5 \rangle$$

be the subgroup of $\mathscr{A}$ which fixes the sphere S_1 in $\mathscr{S}$. It acts discontinuously on the interior of S_1, which we now consider as the ball model for hyperbolic 3-space $\mathscr{H}^3$. A fundamental domain for the quotient $\mathscr{A}_1 \backslash \mathscr{H}^3$ is the curvilinear regular ideal tetrahedron interior to S_1 and exterior to the dual spheres $\tilde{S}_2, \ldots, \tilde{S}_5$, see Figure 5a. This is easier seen by first applying the same transformation as in Figure 1c, see Figure 5b. In particular, the quotient has finite volume, and at any vertex, the three edges meet at dihedral angles all equal to $\pi/3$. Then the



(a) A fundamental domain for the action of $\mathscr{A}_1$



(b) The same domain on sending two spheres to planes

FIGURE 5

volume can be computed via the dilogarithm, or equivalently, Lobachevsky's function

$$\text{Л}(\theta) := -\int_0^\theta \log|2\sin u|\, du,$$

see, e.g., [23, Lemma 2]. Namely, the volume of this domain is $3\,\text{Л}(\pi/3)$. Then its index-2 orientation preserving subgroup, a gluing of two such tetrahedra, has co-volume

$$\text{vol}((\mathscr{A}_1 \cap \text{Isom}^+)\backslash\mathscr{H}^3) = 6\,\text{Л}(\pi/3). \tag{3.1}$$

REMARK 3.1. Curt McMullen asked (private communication) whether this quotient is then the figure eight knot complement; recall that Thurston showed the latter can be triangulated by two maximal tetrahedra. It turns out that, like the knot complement, our quotient is indeed arithmetic; but the two are not isomorphic, see Remark 3.4 below.

To realize this geometric action algebraically, let

$$\Gamma_1 := \langle M_2, \cdots, M_5\rangle \tag{3.2}$$

be the corresponding subgroup of Γ, where the M_j are given in (2.5). We immediately pass again to the index-2 orientation preserving subgroup, setting

$$\Xi := \Gamma_1 \cap \text{SL}_5\,. \tag{3.3}$$

Then Ξ is generated by

$$\Xi = \langle \xi_1, \xi_2, \xi_3\rangle\,, \tag{3.4}$$

where

$$\xi_1 := M_2M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 2 & 0 & -1 & 2 & 2\\ 1 & 1 & -1 & 1 & 1\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},\ \xi_2 := M_2M_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 2 & 0 & 2 & -1 & 2\\ 0 & 0 & 1 & 0 & 0\\ 1 & 1 & 1 & -1 & 1\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and

$$\xi_3 := M_2M_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 2 & 0 & 2 & 2 & -1\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 1 & 1 & 1 & 1 & -1 \end{pmatrix}.$$

It will turn out that Ξ is in fact a *congruence* group, as a form of $\text{SL}_2(\mathbb{C})$. To see this, we make a number of transformations.

LEMMA 3.2. *Let*

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1 & 0\\ 1/3 & 1/3 & -2/3 & 1/3 & 1/3\\ 1/3 & -2/3 & 1/3 & 1/3 & 1/3\\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then for $j = 1,2,3$, the conjugates

$$\tilde{\xi}_j := J \cdot \xi_j \cdot J^{-1} \tag{3.5}$$

are given by

$$\tilde{\xi}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \tilde{\xi}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & -3 & 3 \\ 0 & 0 & -1 & -1 & 2 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$
$$\text{and} \quad \tilde{\xi}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & -1 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 3 & -3 & -3 & 1 \end{pmatrix}. \tag{3.6}$$

Proof. Of course this can be verified by direct computation. But we elucidate the role of J as follows.

Let $\mathbf{b} = \mathbf{b}(\mathscr{S}) = (b_1, \dots, b_5)$ be the quintuple of bends corresponding to $\mathscr{S}$. Write the form Q in (2.4) as

$$\begin{aligned} Q(b_1, b_2, \dots, b_5) &= 3(b_1^2 + b_2^2 + \cdots + b_5^2) - (b_1 + b_2 + \cdots + b_5)^2 \\ &= 2(\widetilde{Q}(\mathbf{y}) + 3b_1^2), \end{aligned}$$

where

$$\mathbf{y} = (y_2, \dots, y_5) := (b_2, \dots, b_5) + (b_1, b_1, b_1, b_1), \tag{3.7}$$

and

$$\widetilde{Q}(\mathbf{y}) := y_2^2 + \cdots + y_5^2 - y_2 y_3 - y_2 y_4 - \cdots - y_4 y_5.$$

The affine action of Ξ on $(b_2, \dots, b_5)$ is conjugated by the above to a linear action $\Xi' < \mathrm{SO}_{\widetilde{Q}}$. Since $\mathbf{b}$ was assumed to be primitive, $\mathbf{y}$ is a primitive point on the quadric

$$\widetilde{Q}(\mathbf{y}) = -3b_1^2. \tag{3.8}$$

For later convenience, we make another change of variables. It turns out that, despite beginning with a problem in the (rational) integers, we will need to work in the number field

$$K := \mathbb{Q}(\sqrt{-3})$$

with its ring of (Eisenstein) integers

$$\mathscr{O} := \mathbb{Z}[\omega].$$

Here

$$\omega := e^{\pi i/3}$$

is a primitive *sixth* root of unity (it turns out to be more convenient to use the sixth root than the cube root). We will conjugate $\widetilde{Q}$ to the form

$$F(\mathbf{a}) := B^2 + BC + C^2 - AD, \tag{3.9}$$

where $\mathbf{a} = (A, B, C, D)$. The determinant of the Hermitian matrix

$$X := \begin{pmatrix} A & B+\omega C \\ B+\bar{\omega} C & D \end{pmatrix} \tag{3.10}$$

is easily seen to be $-F(\mathbf{a})$. Let

$$y_2 = A - B - 2C + D,\ y_3 = A - 2B - C + D,\ y_4 = A,\ y_5 = D,$$

or equivalently, make the change of variables

$$A = y_4,\ B = \frac{y_2 - 2y_3 + y_4 + y_5}{3},\ C = \frac{-2y_2 + y_3 + y_4 + y_5}{3},\ D = y_5.$$

We claim that B and C are integers; indeed, returning to the b variables in (3.7), we have

$$\begin{aligned} A &= b_1 + b_4, \\ B &= \frac{1}{3}(b_1 + b_2 - 2b_3 + b_4 + b_5), \\ C &= \frac{1}{3}(b_1 - 2b_2 + b_3 + b_4 + b_5), \\ D &= b_1 + b_5. \end{aligned} \tag{3.11}$$

But reducing (2.3), (2.4) mod 3 shows that $b_1 + \cdots + b_5 \equiv 0 (\mathrm{mod}\, 3)$, and hence B and C are integers.

In these coordinates, (3.8) becomes

$$F(\mathbf{a}) = -b_1^2. \tag{3.12}$$

The action $\Xi' < \mathrm{SO}_{\tilde{Q}}$ on $\mathbf{y}$ is then conjugated to an action $\widetilde{\Xi} < \mathrm{SO}_F$ on $\mathbf{a}$. The matrix J is then simply the change of variables matrix from $\mathbf{b}$ to $(b_1, \mathbf{a})$. □

The convenience of this conjugation is made apparent in the following

LEMMA 3.3. *The quadratic form F in (3.9) has signature $(3,1)$. The connected component of the identity of the special orthogonal group $\mathrm{SO}_F(\mathbb{R})$ has spin double cover isomorphic to $\mathrm{PSL}_2(\mathbb{C})$. There is a homomorphism $\rho : \mathrm{PSL}_2(\mathbb{C}) \to \mathrm{SO}_F(\mathbb{R})$ given explicitly (for our purposes embedded in GL_5) by mapping*

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{C}) \tag{3.13}$$

to

(3.14)

$$\frac{1}{|\det(g)|^2} \times \begin{pmatrix} 1 & & & \\ & |\alpha|^2 & 2\mathfrak{Re}(\beta\bar{\alpha}) & 2\mathfrak{Re}(\alpha\omega\bar{\beta}) & |\beta|^2 \\ & \frac{2}{\sqrt{3}}\mathfrak{Im}(\gamma\omega\bar{\alpha}) & \frac{2}{\sqrt{3}}\mathfrak{Im}(\omega(\delta\bar{\alpha}+\gamma\bar{\beta})) & \frac{2}{\sqrt{3}}\mathfrak{Im}(\gamma\bar{\beta}\omega^2+\delta\bar{\alpha}) & \frac{2}{\sqrt{3}}\mathfrak{Im}(\delta\omega\bar{\beta}) \\ & \frac{2}{\sqrt{3}}\mathfrak{Im}(\alpha\bar{\gamma}) & \frac{2}{\sqrt{3}}\mathfrak{Im}(\beta\bar{\gamma}+\alpha\bar{\delta}) & \frac{2}{\sqrt{3}}\mathfrak{Im}(\omega(\alpha\bar{\delta}-\gamma\bar{\beta})) & \frac{2}{\sqrt{3}}\mathfrak{Im}(\beta\bar{\delta}) \\ & |\gamma|^2 & 2\mathfrak{Re}(\gamma\bar{\delta}) & 2\mathfrak{Re}(\gamma\omega\bar{\delta}) & |\delta|^2 \end{pmatrix}.$$

The preimages under ρ of the matrices $\tilde{\xi}_1, \tilde{\xi}_2, \tilde{\xi}_3$ in (3.6) are $\pm\mathfrak{t}_1, \pm\mathfrak{t}_2, \pm\mathfrak{t}_3$, respectively, where:

$$\mathfrak{t}_1 = \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}, \quad \mathfrak{t}_2 = \begin{pmatrix} \omega^{-2} & \omega\varrho \\ 0 & \omega^2 \end{pmatrix}, \quad \mathfrak{t}_3 = \begin{pmatrix} \omega & 0 \\ \omega\varrho & \omega^{-1} \end{pmatrix}. \tag{3.15}$$

Here

$$\varrho := 1 + \omega$$

is the prime in $\mathcal{O}$ above the ramified rational prime 3, which factors as $3 = \bar{\omega}\varrho^2$.

Proof. The signature of F is computed directly, and its spin group being $\mathrm{PSL}_2(\mathbb{C})$ is a general fact in the theory of quadratic forms, see e.g. [7, Ch. 10]. We construct ρ explicitly as follows. Return to the Hermitian matrix X in (3.10) with determinant $-F(\mathbf{a})$. Then for $g \in \mathrm{PSL}_2(\mathbb{C})$,

$$X' := g \cdot X \cdot \bar{g}^t = \begin{pmatrix} A' & B' + \omega C' \\ B' + \bar{\omega} C' & D' \end{pmatrix}$$

is also Hermitian with the same determinant. This gives a linear action sending (A, B, C, D) to (A', B', C', D'), which can be computed explicitly in the coordinates (3.13). The result (embedded in GL_5) is (3.14). The preimages (3.15) are then computed directly. □

Let

$$\Lambda = \langle \pm\mathfrak{t}_1, \pm\mathfrak{t}_2, \pm\mathfrak{t}_3 \rangle / \langle \pm I \rangle \ < \ \mathrm{PSL}_2(\mathbb{C}) \tag{3.16}$$

be the group generated by (3.15).

Then Λ is clearly a subgroup of the Bianchi group $\mathrm{PSL}_2(\mathcal{O})$. The full group $\mathrm{PSL}_2(\mathcal{O})$ is well-known to have co-volume

$$\mathrm{vol}(\mathrm{PSL}_2(\mathcal{O}) \backslash \mathscr{H}^3) = \frac{1}{2} \Pi(\pi/3),$$

see e.g. [23, p. 21]. Combined with (3.1), this gives us the index

$$[\mathrm{PSL}_2(\mathcal{O}) : \Lambda] = 12,$$

since $\Lambda \cong \Xi \cong \mathscr{A}_1 \cap \mathrm{Isom}^+$.

REMARK 3.4. This fact was already known to Grunewald-Schwermer, who list a conjugate of the generators (3.15) in their table [14, p. 76], calling the group "$\Gamma_{-3}(12, 7)$". In the same table [p. 75], the figure eight knot complement is listed as "$\Gamma_{-3}(12, 1)$"; so these are not isomorphic, cf. Remark 3.1.

The next lemma, crucial for our purposes, states that our group is not just arithmetic, but *congruence*.

LEMMA 3.5. *The group Λ is equal to the following congruence subgroup of $\mathrm{PSL}_2(\mathcal{O})$,*

$$\left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}) : \beta, \gamma \equiv 0 (\mathrm{mod}\, \varrho) \right\}. \tag{3.17}$$

Proof. The inclusion

$$\Lambda < (3.17) \tag{3.18}$$

is clear from the generators (3.15). For the opposite inclusion, is it an elementary computation that (3.17) has index 12 in $\mathrm{PSL}_2(\mathscr{O})$, as does Λ. □

The point is that, since Λ is now realized as an congruence group, its elements can be parametrized, giving an injection of affine space into the otherwise intractable thin Soddy group Γ. (In the Apollonian circle packing setting, the analogous idea was exploited extensively in, e.g., [26, 3, 4].)

PROPOSITION 3.6. *For any $\gamma, \delta \in \mathscr{O}$ with*

$$\gamma \equiv 0 (\mathrm{mod}\, \varrho), \qquad (\gamma, \delta) = \mathscr{O}, \tag{3.19}$$

there is an element

$$\xi_{\gamma,\delta} := J^{-1} \cdot \rho \begin{pmatrix} * & * \\ \gamma & \delta \end{pmatrix} \cdot J \in \Xi < \Gamma_1 < \Gamma,$$

where

$$\xi_{\gamma,\delta} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ V & W & X & Y & Z \end{pmatrix},$$

and

$$\begin{aligned} V &= \frac{2}{3} \mathfrak{Re}\left(\varrho \gamma \bar{\delta}\right) + |\gamma|^2 + |\delta|^2 - 1, \\ W &= -\frac{2}{3} \mathfrak{Re}\left(\omega \varrho \gamma \bar{\delta}\right), \\ X &= -\frac{2}{3} \mathfrak{Re}\left(\bar{\varrho} \gamma \bar{\delta}\right), \\ Y &= \frac{2}{3} \mathfrak{Re}\left(\varrho \gamma \bar{\delta}\right) + |\gamma|^2, \\ Z &= \frac{2}{3} \mathfrak{Re}\left(\varrho \gamma \bar{\delta}\right) + |\delta|^2. \end{aligned}$$

Proof. This follows directly from (3.17), (3.5), (3.4), (3.3) and (3.2). □

Recall that $\mathscr{O} = \Gamma \cdot \mathbf{b}$ in (2.7) is the orbit under the Soddy group Γ of a quintuple $\mathbf{b} = (b_1, \ldots, b_5)$ of bends. According to Lemma 2.2, there is an $\varepsilon = \varepsilon(\mathscr{P}) \in \{\pm 1\}$ so that every bend in $\mathscr{B}$ is $\equiv 0$ or $\varepsilon (\mathrm{mod}\, 3)$.

Recalling that the set $\mathscr{B}$ of bends contains sets of the form (2.8), and setting $\mathbf{w} = \mathbf{e}_5$, Proposition 3.6 immediately implies the following key

COROLLARY 3.7. *Let $\mathbf{b} \in \mathscr{O}$ be a quintuple of bends, and assume that $\gamma, \delta \in \mathscr{O}$ satisfy (3.19). Then the integer*

$$\mathfrak{F}_{\mathbf{b}}(\gamma, \delta) := \left\langle \mathbf{e}_5, \xi_{\gamma,\delta} \cdot \mathbf{b} \right\rangle \tag{3.20}$$

is in the set $\mathscr{B}$ of bends. Setting

$$\mathfrak{f}_{\mathbf{b}} := \mathfrak{F}_{\mathbf{b}} + b_1, \tag{3.21}$$

we have that $\mathfrak{f}_{\mathbf{b}}$ is a homogeneous quaternary quadratic form given by:

$$\begin{aligned}\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta) = 3A(\gamma_1^2+\gamma_1\gamma_2+\gamma_2^2) + 3B(\gamma_1\delta_1+\gamma_2\delta_2) - 3C\gamma_2\delta_1 \\ + 3(B+C)\gamma_1\delta_2 + D(\delta_1^2+\delta_1\delta_2+\delta_2^2).\end{aligned} \tag{3.22}$$

Here the coefficients A,B,C,D are as in (3.11), and $\gamma = \gamma_1+\gamma_2\omega$, $\delta = \delta_1+\delta_2\omega$ with $\gamma_j,\delta_j \in \mathbb{Z}$.

Abusing notation, we write

$$\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) = \mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta), \tag{3.23}$$

where $\mathbf{x} := (\gamma_1,\gamma_2,\delta_1,\delta_2)$. The (classically integral) symmetric matrix (that is, Hessian) corresponding to $\mathfrak{f}_{\mathbf{b}}(\mathbf{x})$ is

$$\mathbf{A} := \begin{pmatrix} 6A & 3A & 3B & 3(B+C) \\ 3A & 6A & -3C & 3B \\ 3B & -3C & 2D & D \\ 3(B+C) & 3B & D & 2D \end{pmatrix}, \tag{3.24}$$

so that $\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta) = \frac{1}{2}\mathbf{x}\mathbf{A}\mathbf{x}^t$. By (2.3), the discriminant of $\mathfrak{f}_{\mathbf{b}}$ is

$$\operatorname{discr}(\mathfrak{f}_{\mathbf{b}}) = |\mathbf{A}| = 9\left(\frac{1}{2}Q(\mathbf{b}) - 3b_1^2\right)^2 = (3b_1)^4. \tag{3.25}$$

Assume further that

$$b_1 \le b_2 \le b_3 \le b_4 \le b_5, \quad \text{and} \quad b_2 \ge 0. \tag{3.26}$$

Then the form $\mathfrak{f}_{\mathbf{b}}$ is positive definite iff $b_1 \neq 0$ (otherwise it is positive semidefinite).

Proof. All direct computation. This should also elucidate the choice of the change of variables in (3.11). □

DEFINITION 3.8. We say that $\mathfrak{F}_{\mathbf{b}}$ "$\mathscr{O}$-primitively" represents an integer n if there exist $\gamma,\delta \in \mathscr{O}$ satisfying (3.19) so that $\mathfrak{F}_{\mathbf{b}}(\gamma,\delta) = n$.

We have thus shown that $\mathscr{B}$ contains all the $\mathscr{O}$-primitive values of the shifted quaternary quadratic form $\mathfrak{F}_{\mathbf{b}}$. In the next section, we show that enough numbers are represented by such forms to produce a local-global principle in $\mathscr{B}$.

4. PROOF OF THE LOCAL-GLOBAL THEOREM

Recall from Lemma 2.2 that, to a primitive integral Soddy packing $\mathscr{P}$, one assigns the number $\varepsilon = \varepsilon(\mathscr{P}) \in \{\pm 1\}$, so that every bend in $\mathscr{B} = \mathscr{B}(\mathscr{P})$ is congruent either 0 or ε modulo 3. The analysis turns out to require that the odd primes dividing b_1 be congruent 1 mod 3, so we first claim that this can always be arranged.

THEOREM 4.1. *If $\varepsilon(\mathscr{P})=+1$, then there exists a (rational) prime*

$$\mathfrak{p}\equiv 1 \pmod 3 \tag{4.1}$$

which is a bend in $\mathscr{P}$. If $\varepsilon(\mathscr{P})=-1$, then $2\mathfrak{p}$ is a bend.

Before giving the proof, we explain how this fact will be used. By Corollary 3.7, we turn our attention to numbers $\mathscr{O}$-primitively represented by $\mathfrak{F}_{\mathbf{b}}$, as these are guaranteed to be in the bend set $\mathscr{B}$. It turns out that these are all $\equiv b_5 \pmod 3$, which is fine for our purposes, since we can make $b_5\equiv 0$ or $\varepsilon \pmod 3$ by a choice of the quintuple $\mathbf{b}=(b_j)$. Changing to the homogeneous form $\mathfrak{f}_{\mathbf{b}}$ as in (3.21), it will then suffice to show the following

THEOREM 4.2. *Assume that the quintuple $\mathbf{b}$ has $b_1=\mathfrak{p}\equiv 1 \pmod 3$ or $b_1=2\mathfrak{p}$, and is ordered, that is, satisfies (3.26). Then every sufficiently large $n\equiv b_1+b_5 \pmod 3$ is $\mathscr{O}$-primitively represented by $\mathfrak{f}_{\mathbf{b}}$.*

Let

$$\mathscr{R}_{\mathbf{b}}(n):=\sum_{\substack{\gamma,\delta\in\mathscr{O}\\(\varrho\gamma,\delta)=\mathscr{O}}}\mathbf{1}_{\{n=\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta)\}} \tag{4.2}$$

be the number of $\mathscr{O}$-primitive representations of n by $\mathfrak{f}_{\mathbf{b}}$. The study of this function will prove both theorems, with most of the tools going into the proof of the first also being useful for the second. The key proposition which follows is essentially Kloosterman's method for representations by quaternary forms (as championed in this generality by Malyshev).

For an integer $m\geq 1$ and a prime power p^a, define the p-adic local density $\sigma_p(m;\mathbf{b})$ by

$$\sigma_p(m;\mathbf{b}):=\lim_{a\to\infty}\frac{1}{p^{3a}}\#\{\mathbf{x}\in(\mathbb{Z}/p^a\mathbb{Z})^4:\mathfrak{f}_{\mathbf{b}}(\mathbf{x})\equiv m \pmod{p^a}\}, \tag{4.3}$$

where we have used the convention (3.23).

PROPOSITION 4.3. *If $n\equiv b_1+b_5 \pmod 3$ and $(b_1,3)=1$, then*

$$\mathscr{R}_{\mathbf{b}}(n) \;=\; n\frac{\pi^2}{9b_1^2}\mathfrak{S}_0(n;\mathbf{b})\mathfrak{S}_1(n;\mathbf{b})\mathfrak{S}_2(n;\mathbf{b})+O_{\mathbf{b},\epsilon}\left(n^{3/4+\epsilon}\right), \tag{4.4}$$

with an effective implied constant. Here

$$\begin{aligned}\mathfrak{S}_0(n;\mathbf{b}) &:= \prod_p \sigma_p(n;\mathbf{b}),\quad \mathfrak{S}_1(n;\mathbf{b}) := \prod_{\substack{p\equiv 1(3)\\ p\mid n}}\sigma_p^{(1)}(n;\mathbf{b}),\\ \mathfrak{S}_2(n;\mathbf{b}) &:= \prod_{\substack{p\equiv 2(3)\\ p^2\mid n}}\sigma_p^{(2)}(n;\mathbf{b}),\end{aligned} \tag{4.5}$$

where

$$\sigma_p^{(1)}(n;\mathbf{b}) := \left(1-\frac{2}{p}\frac{\sigma_p\left(\frac{n}{p};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}+\mathbf{1}_{\{p^2\mid n\}}\frac{1}{p^2}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\right), \tag{4.6}$$

and

$$\sigma_p^{(2)}(n;\mathbf{b}) := \left(1-\frac{1}{p^2}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\right). \tag{4.7}$$

We will call the terms arising in $\mathfrak{S}_j$ "Type j", and refer to primes p as "Good" or "Bad" depending on whether $(p, 2\cdot 3\cdot b_1) = 1$ or not. While the proof largely uses standard techniques, a few of the manipulations are somewhat delicate, so we give the details.

Proof. Recall that the Dedekind zeta function of K is

$$\zeta_K(s) := \sum_{\mathfrak{m}} \frac{1}{\mathbb{N}\mathfrak{m}^s} = \prod_{\mathfrak{p}} \left(1-\frac{1}{\mathbb{N}\mathfrak{p}^s}\right)^{-1},$$

where $\mathbb{N}$ is the norm, the sum is over non-zero integral ideals $\mathfrak{m}$ of K, and the product is over prime ideals $\mathfrak{p}$. We define the K-Möbius function μ_K via

$$\frac{1}{\zeta_K(s)} = \prod_{\mathfrak{p}} \left(1-\frac{1}{\mathbb{N}\mathfrak{p}^s}\right) = \sum_{\mathfrak{m}} \frac{\mu_K(\mathfrak{m})}{\mathbb{N}\mathfrak{m}^s}.$$

Thus μ_K is multiplicative, supported on non-zero, square-free integral ideals, and takes the value -1 on prime ideals. Möbius inversion now reads:

$$\sum_{\mathfrak{d}\supset\mathfrak{m}} \mu_K(\mathfrak{d}) = \begin{cases} 1 & \text{if } \mathfrak{m} = \mathscr{O}, \\ 0 & \text{otherwise.} \end{cases}$$

Möbius inversion works on the level of ideals, but $\mathfrak{f}_{\mathbf{b}}$ in (4.2) is a function on elements of $\mathscr{O}$, not ideals (i.e. it is *not* invariant under units in each variable γ, δ separately). So we will have to pass from ideals to elements, and back again. Begin by writing

$$\begin{aligned} \mathscr{R}_{\mathbf{b}}(n) &= \sum_{\gamma,\delta\in\mathscr{O}} \mathbf{1}_{\{n=\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta)\}} \sum_{\mathfrak{d}\supset(\varrho\gamma,\delta)} \mu_K(\mathfrak{d}) \\ &= \sum_{\mathfrak{d}} \mu_K(\mathfrak{d}) \sum_{\substack{\gamma,\delta\in\mathscr{O} \\ (\varrho\gamma)\subset\mathfrak{d},(\delta)\subset\mathfrak{d}}} \mathbf{1}_{\{n=\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta)\}}. \end{aligned}$$

The field K is a principal ideal domain with a finite group of units, $|\mathscr{O}^\times| = 6$, so the non-zero integral ideals of K are in 1-to-6 correspondence with non-zero elements of $\mathscr{O}$. So we can write $\mathfrak{d} = (\eta)$ with $\eta \in \mathscr{O} \smallsetminus 0$, whence

$$\mathscr{R}_{\mathbf{b}}(n) = \frac{1}{|\mathscr{O}^\times|} \sum_{\eta\in\mathscr{O}} \mu_K((\eta)) \sum_{\substack{\gamma,\delta\in\mathscr{O} \\ \varrho\gamma\equiv 0(\mathrm{mod}\,\eta),\delta\equiv 0(\mathrm{mod}\,\eta)}} \mathbf{1}_{\{n=\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta)\}}.$$

Now comes a little trick which will allow us to replace $\varrho\gamma \equiv 0(\eta)$ by just $\gamma \equiv 0(\eta)$. Indeed, an easy calculation shows that

$$\mathfrak{f}_{\mathbf{b}}(\eta\gamma',\eta\delta') = \mathbb{N}\eta\cdot\mathfrak{f}_{\mathbf{b}}(\gamma',\delta'). \tag{4.8}$$

So $n = \mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta)$, together with $\varrho\gamma,\delta \equiv 0(\mathrm{mod}\,\eta)$, implies that $\mathbb{N}\eta$ divides n. But $b_1 \equiv \varepsilon(\mathrm{mod}3)$, $b_5 \equiv 0$ or $\varepsilon(\mathrm{mod}3)$, and $n \equiv b_1 + b_5(\mathrm{mod}3)$ together imply that

$n \equiv \varepsilon$ or $2\varepsilon \pmod 3$. In particular, $(n,3)=1$, hence $(\mathbb{N}\eta,3)=1$, so ϱ is coprime to η. Now we have:

$$\mathscr{R}_{\mathbf{b}}(n) = \frac{1}{|\mathscr{O}^\times|}\sum_{\substack{\eta\in\mathscr{O}\\ \mathbb{N}\eta\mid n}} \mu_K((\eta)) \sum_{\gamma,\delta\in\mathscr{O}} \mathbf{1}_{\{\frac{n}{\mathbb{N}\eta}=\mathfrak{f}_{\mathbf{b}}(\varrho\gamma,\delta)\}}.$$

Having freed the variables γ,δ, we may return to ideals, and use the convention (3.23) to write

$$\mathscr{R}_{\mathbf{b}}(n) = \sum_{\mathbb{N}\mathfrak{d}\mid n} \mu_K(\mathfrak{d})\mathscr{R}_{\mathbf{b}}\left(\frac{n}{\mathbb{N}\mathfrak{d}}\right), \tag{4.9}$$

where

$$\mathscr{R}_{\mathbf{b}}(m) := \sum_{\mathbf{x}\in\mathbb{Z}^4} \mathbf{1}_{\{m=\mathfrak{f}_{\mathbf{b}}(\mathbf{x})\}}$$

is now a classical representation quantity.

Combining (3.25) with [15, (11.57), (11.62), (11.19)], we have, for any $\epsilon>0$ (not to be confused with $\varepsilon(\mathscr{P})\in\{\pm1\}$),

$$\mathscr{R}_{\mathbf{b}}(m) = \frac{\pi^2}{9b_1^2}\, m\mathfrak{S}_0(m,\mathbf{b}) \;+\; O_{\mathbf{b},\epsilon}(m^{3/4+\epsilon}), \tag{4.10}$$

where the singular series $\mathfrak{S}_0(m,\mathbf{b})$ is as in (4.5). The implied constant is effective. Inserting (4.10) into (4.9) gives

$$\mathscr{R}_{\mathbf{b}}(n) = n\frac{\pi^2}{9b_1^2}\sum_{\mathbb{N}\mathfrak{d}\mid n}\frac{\mu_K(\mathfrak{d})}{\mathbb{N}\mathfrak{d}}\mathfrak{S}_0\left(\frac{n}{\mathbb{N}\mathfrak{d}},\mathbf{b}\right) + O_{\mathbf{b},\epsilon}\left(n^{3/4+\epsilon}\sum_{\mathbb{N}\mathfrak{d}\mid n}1\right). \tag{4.11}$$

We clearly have $\sum_{\mathbb{N}\mathfrak{d}\mid n}1 \ll_\epsilon n^\epsilon$, so the error term is as claimed in (4.4). It remains to control the local densities.

Recall that $\mathfrak{d}$ is a square-free ideal. Let p be a rational prime dividing $\mathbb{N}\mathfrak{d}$; then $p\neq 3$. If $p\equiv 2(3)$ is inert, then $\mathbb{N}(p)=p^2$ and we can write $\mathfrak{d}=(p)\mathfrak{d}'$, where $(\mathbb{N}\mathfrak{d}',p)=1$; thus $\mathrm{ord}_p(\mathbb{N}\mathfrak{d})=2$. If $p\equiv 1(3)$ splits in $\mathscr{O}$ as $(p)=\pi\bar\pi$, then we have $\mathrm{ord}_p(\mathbb{N}\mathfrak{d})=2$ or 1, depending on whether both π and $\bar\pi$ divide $\mathfrak{d}$ or just one. Either way, we can write

$$\mathfrak{d} = \mathfrak{p}_0\mathfrak{d}' \quad \text{with} \quad (\mathbb{N}\mathfrak{d}',p)=1.$$

Extend this notation to rational primes p not dividing $\mathbb{N}\mathfrak{d}$ by setting $\mathfrak{p}_0=\mathscr{O}$ and $\mathfrak{d}'=\mathfrak{d}$. We claim that:

$$\sigma_p\left(\frac{n}{\mathbb{N}\mathfrak{d}};\mathbf{b}\right) = \sigma_p\left(\frac{n}{\mathbb{N}\mathfrak{p}_0};\mathbf{b}\right). \tag{4.12}$$

Indeed, let $\mathfrak{d}'=(\eta')$. Applying (4.8) in reverse together with (4.3), we see that the density $\sigma_p\left(\frac{n}{\mathbb{N}\mathfrak{d}};\mathbf{b}\right)$ is counting the number of solutions to

$$\mathfrak{f}_{\mathbf{b}}(\eta'\varrho(\gamma_1+\gamma_2\omega),\eta'(\delta_1+\delta_2\omega)) \equiv \frac{n}{\mathbb{N}\mathfrak{p}_0} \pmod{p^a}.$$

The linear map

$$(\varrho(\gamma_1+\gamma_2\omega),\delta_1+\delta_2\omega) \mapsto (\eta'\varrho(\gamma_1+\gamma_2\omega),\eta'(\delta_1+\delta_2\omega))$$

has determinant $(\mathbb{N}\mathfrak{d}')^2$, and hence is invertible since $(p,\mathbb{N}\mathfrak{d}')=1$. Thus the two densities agree and we have proved (4.12).

In particular, we have

$$\sum_{\mathbb{N}\mathfrak{d}|n}\frac{\mu_K(\mathfrak{d})}{\mathbb{N}\mathfrak{d}}\mathfrak{S}_0\left(\frac{n}{\mathbb{N}\mathfrak{d}},\mathbf{b}\right)=\mathfrak{S}_0(n,\mathbf{b})\sum_{\mathbb{N}\mathfrak{d}|n}\frac{\mu_K(\mathfrak{d})}{\mathbb{N}\mathfrak{d}}h(\mathfrak{d}), \tag{4.13}$$

where

$$h(\mathfrak{d}):=\prod_{\substack{p|\mathbb{N}\mathfrak{d}\\ p\equiv 2(3)}}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\prod_{\substack{p|\mathbb{N}\mathfrak{d}\\ p\equiv 1(3)}}\frac{\sigma_p\left(\frac{n}{p^{\mathrm{ord}_p(\mathbb{N}\mathfrak{d})}};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})},$$

assuming the denominators do not vanish. Note that this function is *not* multiplicative on ideals. Nevertheless, we do have a factorization with respect to rational primes of the following form:

(4.14)

$$\begin{aligned}\sum_{\mathbb{N}\mathfrak{d}|n}\frac{\mu_K(\mathfrak{d})}{\mathbb{N}\mathfrak{d}}h(\mathfrak{d})&=\prod_{\substack{p\equiv 2(3)\\ p^2|n}}\left(1+\frac{\mu_K((p))}{\mathbb{N}(p)}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\right)\\ &\times\prod_{\substack{p\equiv 1(3)\\ p|n,(p)=\pi\bar{\pi}}}\left(1+\frac{\mu_K(\pi)}{\mathbb{N}\pi}\frac{\sigma_p\left(\frac{n}{p};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}+\frac{\mu_K(\bar{\pi})}{\mathbb{N}\bar{\pi}}\frac{\sigma_p\left(\frac{n}{p};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}+\mathbf{1}_{\{p^2|n\}}\frac{\mu_K(\pi\bar{\pi})}{\mathbb{N}(\pi\bar{\pi})}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\right)\\ &=\prod_{\substack{p\equiv 2(3)\\ p^2|n}}\left(1-\frac{1}{p^2}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\right)\prod_{\substack{p\equiv 1(3)\\ p|n}}\left(1-\frac{2}{p}\frac{\sigma_p\left(\frac{n}{p};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}+\mathbf{1}_{\{p^2|n\}}\frac{1}{p^2}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})}\right).\end{aligned}$$

The problem has now returned back to the rational integers $\mathbb{Z}$ after the detour through the Eisenstein ones $\mathcal{O}$. Inserting (4.14) and (4.13) into (4.11) gives (4.4), as claimed. □

It remains to analyze the Type 0, 1, and 2 factors for both Good and Bad primes. First the Good.

LEMMA 4.4. *Let n and b_1 as in Proposition 4.3, and assume that p is Good, that is, $(p,2\cdot 3\cdot b_1)=1$. Then*

$$\sigma_p(n;\mathbf{b})=\begin{cases}1+\frac{1}{p}+O(\frac{1}{p^2}) & \text{if } p\mid n,\\ 1-\frac{1}{p^2} & \text{otherwise,}\end{cases} \tag{4.15}$$

$$\sigma_p^{(1)}(n;\mathbf{b})=\begin{cases}1+O(\frac{1}{p}) & \text{if } p\mid n,\\ 1 & \text{otherwise,}\end{cases}$$

$$\sigma_p^{(2)}(n;\mathbf{b})=1+O\left(\frac{1}{p^2}\right),$$

and none of these local factors vanish.

Proof. Write $p^k \| n$. We first handle $\sigma_p(n;\mathbf{b})$. Apply [15, (11.69), (11.70), (11.72)], giving

$$\sigma_p(n;\mathbf{b}) = \frac{\left(1-\frac{\chi(p)}{p^2}\right)\left(1-\frac{\chi(p^{k+1})}{p^{k+1}}\right)}{\left(1-\frac{\chi(p)}{p}\right)}.$$

Here $\chi(m) := \left(\frac{|\mathbf{A}|}{m}\right)$ is the quadratic character modulo the discriminant $|\mathbf{A}| = (3b_1)^4$ of $\mathfrak{f}_\mathbf{b}$, cf. (3.25). Since the latter is a square and $(p,|\mathbf{A}|) = 1$, we have that $\chi(p) = \chi(p^k) = 1$; hence

$$\sigma_p(n;\mathbf{b}) = \left(1+\frac{1}{p}\right)\left(1-\frac{1}{p^{k+1}}\right). \tag{4.16}$$

This clearly never vanishes, and (4.15) is readily verified.

Next we deal with $\sigma_p^{(2)}$. Then $p \equiv 2(3)$ and $p^2 \mid n$, that is, $p^k \| n$ with $k \geq 2$. Inserting (4.16) into (4.7) gives

$$\sigma_p^{(2)}(n;\mathbf{b}) = 1 - \frac{1}{p^2}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})} = 1 - \frac{1}{p^2}\frac{\left(1-\frac{1}{p^{k-1}}\right)}{\left(1-\frac{1}{p^{k+1}}\right)} = 1 - \frac{p^{k-1}-1}{p^{k+1}-1}.$$

This factor clearly never vanishes, and for p large is of size $1+O\left(\frac{1}{p^2}\right)$, so is harmless.

Finally we handle $\sigma_p^{(1)}$. Here $p \equiv 1(3)$ and there are two cases depending on whether $k = 1$, or $k \geq 1$. If $k = 1$, then the factor is

$$\sigma_p^{(1)}(n;\mathbf{b}) = 1 - \frac{2}{p}\frac{\sigma_p\left(\frac{n}{p};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})} = 1 - \frac{2}{p}\frac{\left(1-\frac{1}{p}\right)}{\left(1-\frac{1}{p^2}\right)} = 1 - \frac{2}{p+1},$$

which doesn't vanish. If $k \geq 2$, then the factor is

$$\begin{aligned} 1 - \frac{2}{p}\frac{\sigma_p\left(\frac{n}{p};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})} + \frac{1}{p^2}\frac{\sigma_p\left(\frac{n}{p^2};\mathbf{b}\right)}{\sigma_p(n;\mathbf{b})} &= 1 - \frac{2}{p}\frac{\left(1-\frac{1}{p^k}\right)}{\left(1-\frac{1}{p^{k+1}}\right)} + \frac{1}{p^2}\frac{\left(1-\frac{1}{p^{k-1}}\right)}{\left(1-\frac{1}{p^{k+1}}\right)} \\ &= 1 - \frac{2p^k - p^{k-1} - 1}{p^{k+1}-1}. \end{aligned}$$

This again does not vanish, and is asymptotically of size $1+O(\frac{1}{p})$. This completes the proof. □

To deal with the Bad primes, we first record Hensel's Lemma. Recall from (3.24) that $\mathbf{A}$ is the Hessian of $\mathfrak{f}_\mathbf{b}$.

LEMMA 4.5 (Hensel's Lemma)**.** *Assume that*

$$\mathfrak{f}_\mathbf{b}(\mathbf{x}) \equiv n (\mathrm{mod}\, p^k)$$

for $\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^4$ *with* $\mathbf{x}\mathbf{A} \neq 0 \pmod p$. *Then the set of "lifts"* $\mathbf{y} \in (\mathbb{Z}/p^{k+1}\mathbb{Z})^4$ *with* $\mathbf{y} \equiv \mathbf{x} \pmod{p^k}$ *having*

$$\mathfrak{f}_{\mathbf{b}}(\mathbf{y}) \equiv n \pmod{p^{k+1}}, \tag{4.17}$$

has cardinality exactly p^3.

If on the other hand $\mathbf{x}\mathbf{A} \equiv 0 \pmod p$, *then the number of lifts is either* p^4 *or* 0, *depending on whether* $\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv n \pmod{p^{k+1}}$ *or not.*

Proof. Write $\mathbf{y} = \mathbf{x} + p^k\mathbf{a}$ with $\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^4$. The equation

$$\mathfrak{f}_{\mathbf{b}}(\mathbf{x} + p^k\mathbf{a}) \;=\; \mathfrak{f}_{\mathbf{b}}(\mathbf{x}) + p^k\mathbf{x}\mathbf{A}\mathbf{a}^t + p^{2k}\mathfrak{f}_{\mathbf{b}}(\mathbf{a})$$

is valid in the integers, and hence also valid mod p^{k+1}, even for $p = 2$. Write

$$n - \mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv p^k m \qquad (\mathrm{mod}\, p^{k+1}).$$

Then the equation (4.17) becomes

$$m = \mathbf{x}\mathbf{A}\mathbf{a}^t \pmod p. \tag{4.18}$$

If $\mathbf{x}\mathbf{A}$ is not the zero vector mod p, then there are exactly p^3 solutions for $\mathbf{a}$, and hence for $\mathbf{y}$, as claimed.

If, on the other hand, $\mathbf{x}\mathbf{A} \equiv 0 \pmod p$, then (4.18) has either p^4 or 0 solutions, depending on whether $m \equiv 0$ or not, that is, whether $\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv n \pmod{p^{k+1}}$ or not. □

This is already sufficient to deal conclusively with the crucial prime $p = 3$, for which there is only Type 0, and the only relevant n's are those coprime to 3.

LEMMA 4.6. *Let* n *and* b_1 *as in Proposition 4.3. Then*

$$\sigma_3(n; \mathbf{b}) \;\gg\; 1.$$

Proof. Reducing (3.22) mod 3 shows that $\mathfrak{f}_{\mathbf{b}}(\varrho\gamma, \delta) \equiv (b_1 + b_5)\mathbb{N}(\delta)$, where $\mathbb{N}(\delta) = \delta_1^2 + \delta_1\delta_2 + \delta_2^2$. As ϱ and δ are coprime, $\mathbb{N}(\delta) \equiv 1 \pmod 3$. Hence $\mathfrak{f}_{\mathbf{b}}(\varrho\gamma, \delta)$ is always

$$\equiv b_1 + b_5 \pmod 3.$$

Having assumed that $b_1 \equiv \varepsilon \pmod 3$, we have that $D = b_1 + b_5 \equiv \varepsilon$ or $2\varepsilon \pmod 3$, in either case this is coprime to 3. Hence Hensel's lemma applies and solutions can be lifted to the 3-adic integers $\mathbb{Z}_3$. □

Next we record that for Bad primes $p \neq 3$, the Hessian $\mathbf{A}$ cannot vanish completely.

LEMMA 4.7. *Assume* $p \mid 2b_1$ *and* $p \neq 3$. *Then* $\mathbf{A}$ *is not identically zero mod* p.

Proof. For $p = 2$, this is a direct calculation. Indeed, if $\mathbf{A} \equiv 0 \pmod p$, then

$$A \equiv B \equiv C \equiv D \equiv B + C, \tag{4.19}$$

which forces the b_j's to either be all 0 or all 1. The former is impossible by the primitivity of $\mathbf{b}$. The latter is also impossible from looking at the cone (2.3) mod 4.

If instead $p \mid b_1$, then (4.19) forces the b_j to all be $\equiv 0 \pmod p$, which again is impossible by primitivity. □

By Lemma 4.7, the Hessian $\mathbf{A}$ has a non-zero entry; assume that $A \neq 0 \pmod p$, the other cases being similar. For Bad primes $p \geq 5$, that is, those diving b_1, the following is a convenient normal basis for studying the quadratic space of $\mathfrak{f}_{\mathbf{b}}$.

LEMMA 4.8. *Assume $p \mid b_1$, $p \geq 5$, and $A \neq 0 \pmod p$. Then the following vectors*

$$\mathbf{u}_1 = (1,0,0,0),\ \mathbf{u}_2 = (1,-2,0,0),$$

$$\mathbf{u}_3 = (-B-2C,-B+C,0,3A),\ \mathbf{u}_4 = (-2B-C,B+2C,3A,0),$$

form a basis for $\mathbb{F}_p^4$ which is normal, that is, $\mathbf{u}_j \mathbf{A} \mathbf{u}_k \equiv 0$ if $j \neq k$.

Moreover,

$$\mathfrak{f}_{\mathbf{b}}(\mathbf{u}_1) = 3A,\ \mathfrak{f}_{\mathbf{b}}(\mathbf{u}_2) = 9A,\ \mathfrak{f}_{\mathbf{b}}(\mathbf{u}_3) = \mathfrak{f}_{\mathbf{b}}(\mathbf{u}_4) = -9A \cdot F(\mathbf{a}), \tag{4.20}$$

where $F(\mathbf{a})$ is given in (3.9). Hence writing any $\mathbf{x} \in \mathbb{F}_p^4$ as

$$\mathbf{x} = a\mathbf{u}_1 + b\mathbf{u}_2 + c\mathbf{u}_3 + d\mathbf{u}_4, \tag{4.21}$$

we have that

$$\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \ \equiv\ 3Aa^2 + 9Ab^2 \ \equiv\ 3A(a^2+3b^2) \pmod p. \tag{4.22}$$

Proof. By (3.12),

$$F(\mathbf{a}) \ =\ B^2 + BC + C^2 - AD \ \equiv\ 0 \pmod p,$$

whence $\mathbf{u}_3$ and $\mathbf{u}_4$ are null vectors for $\mathbf{A}$, that is,

$$\mathbf{u}_3\mathbf{A} \equiv \mathbf{u}_4\mathbf{A} \equiv 0 \pmod p.$$

The rest is readily verified by computation. □

The appearance of the binary form a^2+3b^2 in (4.22) explains why we want b_1 to contain only primes $p \equiv 1 \pmod 3$ in Theorem 4.1; indeed, if there are Bad primes $p \equiv 2 \pmod 3$, then there *can* be further local obstructions mod p^2, and σ_p can vanish! But first, we are now in position to give a

4.1. **Proof of Theorem 4.1.**

Assume first that $\varepsilon = \varepsilon(\mathscr{P}) = +1$. By Lemma 2.3, we may arrange $\mathbf{b}$ so that

$$b_1 \equiv 3 + \varepsilon = 4 \pmod 6.$$

In particular, b_1 is even, and $b_1 \equiv 1 \pmod 3$. We may also assume that $b_5 \equiv \varepsilon \equiv 1 \pmod 3$, as can be arranged by Lemma 2.2. We first claim that $\mathfrak{f}_{\mathbf{b}}$, the homogeneous form, $\mathscr{O}$-primitively represents every sufficiently large

$$n \equiv 1 + 4b_1 \pmod{6b_1}. \tag{4.23}$$

Indeed, in this progression,

$$n \equiv 2 \equiv 2\varepsilon \equiv b_1 + b_5 \pmod 3,$$

so the conditions of Proposition 4.3 is satisfied. Moreover, n is coprime to $2b_1$, so there are no Bad factors of Type 1 or 2, and Hensel's lemma, together with Lemma 4.7, allows us to control the local densities at 2 and at primes dividing b_1. Then (4.4) is a true asymptotic, giving the claim.

Returning to the shifted quaternary form $\mathfrak{F}_{\mathbf{b}}$ in (3.20), we have from (3.21) that every sufficiently large value of

$$n - b_1 \equiv 1 + 3b_1 \pmod{6b_1} \tag{4.24}$$

is $\mathscr{O}$-primitively represented by $\mathfrak{F}_{\mathbf{b}}$, and hence appears in the set $\mathscr{B}$ of bends. Such numbers are all $\equiv 1 \pmod 6$, and this arithmetic progression has coprime modulus and shift (since b_1 is even), whence Dirichlet's theorem applies, showing that $\mathscr{B}$ contains a prime $\mathfrak{p} \equiv 1 \pmod 6$. This of course is equivalent to $\mathfrak{p} \equiv 1 \pmod 3$.

The argument for the case $\varepsilon(\mathscr{P}) = -1$ is similar, so we omit it. This completes the proof of Theorem 4.1.

4.2. **Proof of Theorem 4.2.**

Now we assume that $b_1 = \mathfrak{p}$ or $b_1 = 2\mathfrak{p}$ as in Theorem 4.1; clearly then $b_1 \equiv \varepsilon \pmod 3$. As before, if $n \equiv b_1 + b_5 \pmod 3$ is coprime to $2b_1$ and sufficiently large, then it is $\mathscr{O}$-primitively represented by $\mathfrak{f}_{\mathbf{b}}$. So if n is even, we need to handle the 2-adic densities, both of Type 0 and Type 2, and when $n \equiv 0 \pmod{\mathfrak{p}}$, we need control on the $\mathfrak{p}$-adic local factors of Type 0 and Type 1.

We begin by recording the following

LEMMA 4.9. *If $n \equiv 0 \pmod{\mathfrak{p}}$, then*

$$\#\{\mathbf{x} \in \mathbb{F}_{\mathfrak{p}}^4 \,:\, \mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv n,\ \mathbf{x}\mathbf{A} \neq 0 \pmod{\mathfrak{p}}\} \;=\; 2(\mathfrak{p}-1)\mathfrak{p}^2,$$

and

$$\#\{\mathbf{x} \in \mathbb{F}_{\mathfrak{p}}^4 \,:\, \mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv n,\ \mathbf{x}\mathbf{A} \equiv 0 \pmod{\mathfrak{p}}\} \;=\; \mathfrak{p}^2.$$

If $(n, \mathfrak{p}) = 1$, then

$$\#\{\mathbf{x} \in \mathbb{F}_{\mathfrak{p}}^4 \,:\, \mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv n \pmod{\mathfrak{p}}\} \;=\; (\mathfrak{p}-1)\mathfrak{p}^2.$$

Proof. This follows easily from Lemma 4.8. Indeed, assume that $A \neq 0 \pmod{\mathfrak{p}}$, and first check the case $n \equiv 0 \pmod{\mathfrak{p}}$. Then by (4.22), we need (since the values c and d in (4.21) are completely free) to count the number of $a^2 + 3b^2 \equiv 0 \pmod{\mathfrak{p}}$. Since $\mathfrak{p} \equiv 1 \pmod 3$, there are $2(\mathfrak{p}-1)$ such non-trivial solutions[4], plus one trivial, $(a,b) = (0,0)$. For any of these, $\mathbf{x}\mathbf{A} \equiv 0$ if and only if (a,b) is trivial, so the total number of solutions is as claimed.

If $(n, \mathfrak{p}) = 1$, then the number of solutions, say $\mathscr{N}$, is independent of n. By the counts for $\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv 0$ above, we then have that

$$(\mathfrak{p}-1)\mathscr{N} + \mathfrak{p}^2 + 2(\mathfrak{p}-1)\mathfrak{p}^2 \;=\; \mathfrak{p}^4,$$

since there are $\mathfrak{p}^4$ total choices for $\mathbf{x}$. Solving for $\mathscr{N}$ gives the claim. □

Lifting these solutions by Hensel's lemma, we completely control the Type 0 factors, as follows.

[4] In the language of [7, Ch. 2.2], the span of $\mathbf{u}_1$ and $\mathbf{u}_2$ in Lemma 4.8 is a regular, isotropic subspace of $\mathbb{F}_{\mathfrak{p}}^4$ when $\mathfrak{p} \equiv 1 \pmod 3$.

LEMMA 4.10. *If* $(n,\mathfrak{p})=1$, *then*

$$\sigma_{\mathfrak{p}}(n;\mathbf{b}) \;=\; \left(1-\frac{1}{\mathfrak{p}}\right). \tag{4.25}$$

If $\mathfrak{p}\|n$, *then*

$$\#\{\mathbf{x}\in(\mathbb{Z}/\mathfrak{p}^2\mathbb{Z})^4 \;:\; \mathfrak{f}_{\mathbf{b}}(\mathbf{x})\equiv n(\mathrm{mod}\,\mathfrak{p}^2)\} \;=\; 2(\mathfrak{p}-1)\mathfrak{p}^5,$$

whence

$$\sigma_{\mathfrak{p}}(n;\mathbf{b}) \;=\; 2\left(1-\frac{1}{\mathfrak{p}}\right). \tag{4.26}$$

If $\mathfrak{p}^2\mid n$, *then*

$$\#\{\mathbf{x}\in(\mathbb{Z}/\mathfrak{p}^2\mathbb{Z})^4 \;:\; \mathfrak{f}_{\mathbf{b}}(\mathbf{x})\equiv n(\mathrm{mod}\,\mathfrak{p}^2)\} \;=\; 2(\mathfrak{p}-1)\mathfrak{p}^5+\mathfrak{p}^6,$$

and

$$\sigma_{\mathfrak{p}}(n;\mathbf{b}) \;\geq\; 2\left(1-\frac{1}{\mathfrak{p}}\right). \tag{4.27}$$

Proof. If $(n,\mathfrak{p})=1$, then the last statement of Lemma 4.9 applies, and can be lifted by Hensel's Lemma, giving (4.25).

Next consider the case $\mathfrak{p}\|n$. By Lemma 4.9, there are $2(\mathfrak{p}-1)\mathfrak{p}^2$ "non-trivial" solutions mod $\mathfrak{p}$ (i.e., those with $\mathbf{xA}\neq 0$), and by Hensel's Lemma, these each lift to $\mathfrak{p}^3$ solutions mod $\mathfrak{p}^2$. We claim that the trivial mod $\mathfrak{p}$ solutions (those with $\mathbf{xA}\equiv 0$) have no lifts mod $\mathfrak{p}^2$. Indeed, (4.20) and (3.12) imply that $\mathfrak{f}_{\mathbf{b}}(\mathbf{u}_3)\equiv \mathfrak{f}_{\mathbf{b}}(\mathbf{u}_4)\equiv 0(\mathrm{mod}\,\mathfrak{p}^2)$, and $n/\mathfrak{p}$ is coprime to $\mathfrak{p}$, so the trivial solutions do not lift. This gives the asserted count, and also (4.26) by iterating Hensel's Lemma.

If $\mathfrak{p}^2\mid n$, then the non-trivial mod $\mathfrak{p}$ solutions still each lift to $\mathfrak{p}^3$ solutions mod $\mathfrak{p}^2$. But now the trivial mod $\mathfrak{p}$ solutions also lift, and each has $\mathfrak{p}^4$ lifts, since $\mathbf{a}$ in (4.18) is completely free. The lower bound (4.27) comes from lifting just the non-trivial solutions. □

Thus the Type 0 local density is controlled. We can also now handle the Type 1 local density.

LEMMA 4.11. *If* $\mathfrak{p}\|n$, *then*

$$\sigma^{(1)}_{\mathfrak{p}}(n;\mathbf{b}) \;=\; 1-\frac{1}{\mathfrak{p}}.$$

If $p^2\mid n$, *then*

$$\sigma^{(1)}_{\mathfrak{p}}(n;\mathbf{b}) \;\geq\; 1-\frac{1}{\mathfrak{p}}.$$

Proof. If $p\|n$, then the claim follows trivially on combining (4.25) and (4.26) into (4.6), where there is no third term.

If $p^k\|n$ with $k\geq 2$, then there is a third term in (4.6), but we can drop it by positivity (since we're only claiming a lower bound). In the expression (4.3) for the local density $\sigma_{\mathfrak{p}}$, the limit stabilizes as soon as $a>k+\mathrm{ord}_{\mathfrak{p}}(|\mathbf{A}|)$, so we can take $a=k+3$, since $\mathrm{ord}_{\mathfrak{p}}(|\mathbf{A}|)=2$. Setting

$$\mathscr{N}_{\mathfrak{b}}(n;p^a) := \#\{\mathbf{x}\in(\mathbb{Z}/p^a\mathbb{Z})^4 : \mathfrak{f}_{\mathbf{b}}(\mathbf{x})\equiv m \pmod{p^a}\},$$

we see that, since $p^k \| n$,

$$\mathscr{N}_{\mathfrak{b}}(n; p^{k+3}) \;\geq\; \mathscr{N}_{\mathfrak{b}}(n/p; p^{k+3}),$$

since the former may have more "trivial" lifts. Hence $\sigma_{\mathfrak{p}}(n;\mathfrak{b}) \geq \sigma_{\mathfrak{p}}(n/p;\mathfrak{b})$, from which the claim follows. □

This completes our analysis for the special Bad prime $p = \mathfrak{p}$. It remains to handle $p = 2$.

LEMMA 4.12. *For $p = 2$,*

$$\sigma_2(n;\mathbf{b}) \;\gg\; 1, \qquad \sigma_2^{(2)}(n;\mathbf{b}) \;\gg\; 1.$$

Proof. Assume first that b_1, b_2, and b_3 are odd, and that b_4 is even, the other cases being similar. Reducing (3.11) mod 2 gives

$$A \equiv 1,\; B \equiv b_5,\; C \equiv b_5,\; B + C \equiv 0,\; D \equiv 1 + b_5.$$

For either possible value of b_5, there are six $\mathbf{x} \in \mathbb{F}_2^4$ with $\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv 1$ and the other ten have $\mathfrak{f}_{\mathbf{b}}(\mathbf{x}) \equiv 0$. One of the ten is of course the zero vector, and the remaining nine all have $\mathbf{x}\mathbf{A} \neq 0 (\mathrm{mod}\, 2)$. Hence they lift by Hensel's lemma, giving control on both σ_2 and $\sigma_2^{(2)}$. □

4.3. **Proof of Theorem 1.1.**

Now we put evertything together. By Theorem 4.1, we take $b_1 = \mathfrak{p}$ or $2\mathfrak{p}$, the arrange for the ordering (3.26) to be satisfied. By Theorem 4.2, $\mathfrak{f}_{\mathbf{b}}$ then $\mathscr{O}$-primitively represents every large $n \equiv b_1 + b_5 (\mathrm{mod}\, 3)$. Hence $\mathfrak{F}_{\mathbf{b}} = \mathfrak{f}_{\mathbf{b}} - b_1$, the shifted form, $\mathscr{O}$-primitively represents every large $n \equiv b_5 (\mathrm{mod}\, 3)$, and by Corollary 3.7, these numbers are all in $\mathscr{B}$. Since we can make $b_5 \equiv 0$ or ε mod 3, this covers all the local obstructions in Lemma 2.2. In particular, they are *a posteriori* all the local obstructions. This completes the proof of the Local-Global Theorem.

4.4. **Explicit example.**

We illustrate here the procedure described above for the example of the packing $\mathscr{P}_0$ having "root" quintuple $\mathbf{b}_0 = (-11, 21, 25, 27, 28)$ as in (2.9). In this case, $\varepsilon(\mathscr{P}) = +1$, but $b_1 = -11$ has prime factors (namely, 11) which are not $\equiv 1 (\mathrm{mod}\, 3)$, so we cannot apply Theorem 4.2 directly. Following the proof of Theorem 4.1, we first arrange for b_1 to be $\equiv 4 (\mathrm{mod}\, 6)$ and $b_5 \equiv 1 (\mathrm{mod}\, 3)$, by re-ordering $\mathbf{b}_0$ to $\mathbf{b}_1 = (28, 21, 25, 27, -11)$. This does not satisfy (3.26), so we apply $M_4 M_5 M_4 M_3 M_2 M_5$ in (2.5) to $\mathbf{b}_1$, giving

$$\mathbf{b}_2 = (28, 171, 313, 912, 997).$$

(Note that at no point are we changing the bends appearing in $\mathscr{P}_0$, and each quintuple still represents the bends of five mutually tangent spheres. We also only apply even length words in M_j, $j = 2, \ldots, 5$, so are staying within Ξ in (3.3).) Now we have $b_1 \equiv 4 (\mathrm{mod}\, 6)$ and $b_5 \equiv 1 (\mathrm{mod}\, 3)$, so can argue as in (4.24) to show that the set $\mathscr{B}$ of bends contains all sufficiently large values of the progression $85 (\mathrm{mod}\, 168)$. The smallest of these which is prime, $\mathfrak{p} = 421$, turns out to already

be in $\mathscr{B}$; in fact, applying $M_5M_3M_4M_3M_5M_4$ to $\mathbf{b}_2$, and reordering to make $b_1 = \mathfrak{p}$ gives

$$\mathbf{b}_3 = (421, 25, 28, 171, 309).$$

Now apply Γ some more to correct the ordering,

$$\mathbf{b}_4 = M_5M_4M_3M_2 \cdot \mathbf{b}_3 = (421, 904, 1777, 3240, 6033).$$

We are finally in position to apply Theorem 4.2; then every sufficiently large number

$$n \equiv b_5 \equiv 0 (\mathrm{mod}\, 3)$$

is $\mathscr{O}$-primitively represented by the shifted form $\mathfrak{F}_{\mathbf{b}}$, and hence appears in $\mathscr{B}$ by Corollary 3.7. Next we apply $M_5.M_3$ to $\mathbf{b}_4$ and reorder to obtain

$$\mathbf{b}_5 = (421, 904, 3240, 7353, 8821).$$

This has $b_5 \equiv 1 (\mathrm{mod}\, 3)$, and hence all large numbers $\equiv 1 (\mathrm{mod}\, 3)$ also appear in $\mathscr{B}$, as claimed.

Acknowledgments. The author wishes to express his gratitude to Dimitri Dias, Jeff Lagarias, Yair Minsky, Kei Nakamura, Alan Reid, and Peter Sarnak for enlightening conversations, comments and corrections. Thanks also to Stony Brook University, where the bulk of this text was completed, and the referee for comments.

REFERENCES

[1] A. Baragar, Higher dimensional Apollonian packings, revisited, *Geom. Dedicata*, **195** (2018), 137–161.
[2] M. Borkovec, W. de Paris and R. Peikert, The fractal dimension of the Apollonian sphere packing, *Fractals*, **2** (1994), 521–526.
[3] J. Bourgain and E. Fuchs, A proof of the positive density conjecture for integer Apollonian circle packings, *J. Amer. Math. Soc.*, **24** (2011), 945–967.
[4] J. Bourgain and A. Kontorovich, On the local-global conjecture for integral Apollonian gaskets, *Invent. Math.*, **196** (2014), 589–650.
[5] D. W. Boyd, An algorithm for generating the sphere coordinates in a three-dimensional osculatory packing, *Math. Comp.*, **27** (1973), 369–377.
[6] D. W. Boyd, The osculatory packing of a three dimensional sphere, *Can. J. Math.*, **25** (1973), 303–322.
[7] J. W. S. Cassels, *Rational Quadratic Forms*, London Mathematical Society Monographs, 13, Academic Press, London-New York, 1978.
[8] R. Descartes, *Œuvres*, volume 4, (eds. C. Adams and P. Tannery), Paris, 1901.
[9] D. Dias, The local-global principle for integral generalized Apollonian sphere packings, preprint, arXiv:1401.4789, (2014).
[10] E. Fuchs and K. Sanden, Some experiments with integral Apollonian circle packings, *Exp. Math.*, **20** (2011), 380–399.
[11] R. L. Graham, J. C. Lagarias, C. L. Mallows, A. R. Wilks and C. H. Yan, Apollonian circle packings: Number theory, *J. Number Theory*, **100** (2003), 1–45.
[12] R. L. Graham, J. C. Lagarias, C. L. Mallows, A. R. Wilks and C. H. Yan, Apollonian circle packings: Geometry and group theory. III. Higher dimensions, *Discrete Comput. Geom.*, **35** (2006), 37–72.
[13] T. Gossett, The kiss precise, *Nature*, **139** (1937), 62.

[14] F. Grunewald and J. Schwermer, Subgroups of Bianchi groups and arithmetic quotients of hyperbolic 3-space, *Trans. Amer. Math. Soc.*, **335** (1993), 47–78.
[15] H. Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics, 17, American Mathematical Society, Providence, RI, 1997.
[16] I. Kim, Counting, mixing and equidistribution of horospheres in geometrically finite rank one locally symmetric manifolds, *J. Reine Angew. Math.*, **704** (2015), 85–133.
[17] H. D. Kloosterman, On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, *Acta Math.*, **49** (1927), 407–464.
[18] A. Kontorovich and K. Nakamura, Geometry and arithmetic of crystallographic sphere packings, *Proc. Natl. Acad. Sci. USA*, **116** (2019), 436–441.
[19] A. Kontorovich and H. Oh, Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds, *J. Amer. Math. Soc.*, **24** (2011), 603–648.
[20] A. Kontorovich, From Apollonius to Zaremba: Local-global phenomena in thin orbits, *Bull. Amer. Math. Soc. (N.S.)*, **50** (2013), 187–228.
[21] A. Kontorovich, Applications of thin orbits, in *Dynamics and Analytic Number Theory*, London Math. Soc. Lecture Note Ser., 437, Cambridge Univ. Press, Cambridge, 2016, 289–317.
[22] R. Lachlan, On systems of circles and spheres, *Philos. Roy. Soc. London Ser. A*, **177** (1886), 481–625.
[23] J. Milnor, Hyperbolic geometry: The first 150 years, *Bull. Amer. Math. Soc. (N.S.)*, **6** (1982), 9–24.
[24] K. Nakamura, The local-global principle for integral bends in orthoplicial Apollonian sphere packings, preprint, arXiv:1401.2980, (2014).
[25] http://mathworld.wolfram.com/TangentSpheres.html.
[26] P. Sarnak, *Letter to J. Lagarias about integral Apollonian packings*, 2007. Available from: http://web.math.princeton.edu/sarnak/AppolonianPackings.pdf.
[27] F. Soddy, The kiss precise, *Nature*, **137** (1936), 1021.
[28] F. Soddy, The bowl of integers and the hexlet, *Nature*, **139** (1937), 77–79.
[29] X. Zhang, *On the local-global principle for integral Apollonian-3 Circle packings*, preprint, arXiv:1312.4650, (2013).

ALEX KONTOROVICH <alex.kontorovich@rutgers.edu>: Department of Mathematics, Rutgers University, 110 Frelinghuysen Rd., Piscataway, NJ 08854, USA