Invent math (2014) 196:589–650
DOI 10.1007/s00222-013-0475-y

On the local-global conjecture for integral Apollonian gaskets

With an appendix by Péter P. Varjú

Jean Bourgain · Alex Kontorovich

Received: 24 May 2012 / Accepted: 27 May 2013 / Published online: 10 July 2013

Abstract We prove that a set of density one satisfies the local-global conjecture for integral Apollonian gaskets. That is, for a fixed integral, primitive Apollonian gasket, almost every (in the sense of density) admissible (passing local obstructions) integer is the curvature of some circle in the gasket.

Contents

Bourgain is partially supported by NSF grant DMS-0808042.
Kontorovich is partially supported by NSF grants DMS-1209373, DMS-1064214 and DMS-1001252.
Varjú is partially supported by the Simons Foundation and the European Research Council (Advanced Research Grant 267259).

J. Bourgain
IAS, Princeton, NJ 08540, USA
e-mail: bourgain@ias.edu

A. Kontorovich (✉)
Yale University, New Haven, CT 06511, USA
e-mail: alex.kontorovich@yale.edu

1 Introduction

1.1 The local-global conjecture

Let $\mathscr{G}$ be an Apollonian gasket, see Fig. 1. The number $b(C)$ shown inside a circle $C \in \mathscr{G}$ is its curvature, that is, the reciprocal of its radius (the bounding circle has negative orientation). Soddy [46] first observed the existence of *integral* gaskets $\mathscr{G}$, meaning ones for which $b(C) \in \mathbb{Z}$ for all $C \in \mathscr{G}$. Let

$$\mathscr{B} = \mathscr{B}_{\mathscr{G}} := \left\{ b(C) : C \in \mathscr{G} \right\}$$

be the set of all curvatures in $\mathscr{G}$. We call a gasket *primitive* if $\gcd(\mathscr{B}) = 1$. From now on, we restrict our attention to a fixed primitive integral Apollonian gasket $\mathscr{G}$.

Graham, Lagarias, Mallows, Wilks, and Yan [26, 34] initiated a detailed study of Diophantine properties of $\mathscr{B}$, with two separate families of problems (see also e.g. [23, 33, 43]): studying $\mathscr{B}$ with multiplicity (that is, studying circles), or without multiplicity (studying the integers which arise). In the present paper, we are concerned with the latter.

In particular, the following striking local-to-global conjecture for $\mathscr{B}$ is given in [26, p. 37], [23]. Let $\mathscr{A} = \mathscr{A}_{\mathscr{G}}$ denote the *admissible* integers, that is, those passing all local (congruence) obstructions:

$$\mathscr{A} := \left\{ n \in \mathbb{Z} : n \in \mathscr{B} (\mathrm{mod}\, q), \text{ for all } q \geq 1 \right\}.$$

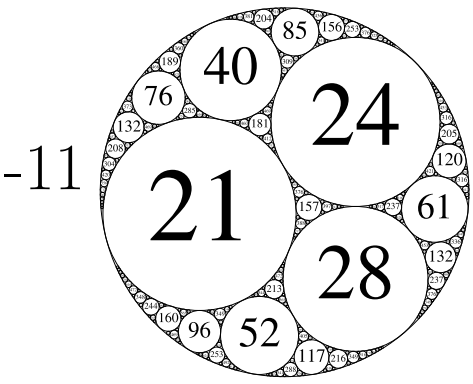

Fig. 1 The Apollonian gasket with root quadruple $v_0 = (-11, 21, 24, 28)^t$

Conjecture 1.1 (Local-Global Conjecture) *Fix a primitive, integral Apollonian gasket $\mathscr{G}$. Then every sufficiently large admissible number is the curvature of a circle in $\mathscr{G}$. That is, if $n \in \mathscr{A}$ and $n \gg 1$, then $n \in \mathscr{B}$.*

The purpose of this paper is to prove the following

Theorem 1.2 *Almost every admissible number is the curvature of a circle in $\mathscr{G}$. Quantitatively, the number of exceptions up to N is bounded by $O(N^{1-\eta})$, where $\eta > 0$ is effectively computable.*

Admissibility is completely explained in Fuchs's thesis [22], and is a condition restricting to certain residue classes modulo 24, cf. Lemma 2.3. E.g. for the gasket in Fig. 1, $n \in \mathscr{A}$ iff

$$n \equiv 0, 4, 12, 13, 16, \text{ or } 21 \pmod{24}. \tag{1.1}$$

Thus $\mathscr{A}$ contains one of every four numbers (six admissible residue classes out of 24), and Theorem 1.2 can be restated in this case as

$$\#\big(\mathscr{B} \cap [1, N]\big) = \frac{N}{4}\big(1 + O\big(N^{-\eta}\big)\big).$$

In general, the local obstructions are easily determined (see Remark 2.4) from the so-called *root quadruple*

$$v_0 = v_0(\mathscr{G}), \tag{1.2}$$

which is the column vector of the four smallest curvatures in $\mathscr{B}$. For the gasket in Fig. 1, $v_0 = (-11, 21, 24, 28)$.

The history of this problem is as follows. The first progress towards the Conjecture was already made in [26], who showed that

$$\#\big(\mathscr{B} \cap [1, N]\big) \gg N^{1/2}. \tag{1.3}$$

Sarnak [42] improved this to

$$\#\big(\mathscr{B} \cap [1, N]\big) \gg \frac{N}{(\log N)^{1/2}}, \tag{1.4}$$

and then Fuchs [22] showed

$$\#\big(\mathscr{B} \cap [1, N]\big) \gg \frac{N}{(\log N)^{0.150\ldots}}.$$

Finally Bourgain and Fuchs [4] settled the so-called "Positive Density Conjecture," that

$$\#\big(\mathscr{B} \cap [1, N]\big) \gg N.$$

1.2 Methods

Our main approach is through the Hardy-Littlewood circle method, combining two new ingredients. The first, applied to the major arcs, is effective bisector counting in infinite volume hyperbolic 3-folds, recently achieved by I. Vinogradov [49], as well as the uniform spectral gap over congruence towers of such, see the Appendix by Péter Varjú. The second ingredient is the minor arcs analysis, inspired by that given recently by the first-named author in [3], where it was proved that the prime curvatures in a gasket constitute a positive proportion of the primes. (Obviously Theorem 1.2 implies that 100 % of the admissible prime curvatures appear.)

1.3 Plan for the paper

A more detailed outline of the proof, as well as the setup of some relevant exponential sums, is given in Sect. 3. Before we can do this, we need to recall the Apollonian group and some of its subgroups in Sect. 2. After the outline in Sect. 3, we use Sect. 4 to collect some background from the spectral and representation theory of infinite volume hyperbolic quotients. Then some lemmata are reserved for Sect. 5, the major arcs are estimated in Sect. 6, and the minor arcs are dealt with in Sects. 7–9. The Appendix, by Péter Varjú, extracts the spectral gap property for the Apollonian group from that of its arithmetic subgroups.

1.4 Notation

We use the following standard notation. Set $e(x) = e^{2\pi i x}$ and $e_q(x) = e(\frac{x}{q})$. We use $f \ll g$ and $f = O(g)$ interchangeably; moreover $f \asymp g$ means $f \ll g \ll f$. Unless otherwise specified, the implied constants may depend at most on the gasket $\mathscr{G}$ (or equivalently on the root quadruple v_0), which is treated as fixed. The symbol $\mathbf{1}_{\{\cdot\}}$ is the indicator function of the event $\{\cdot\}$. The greatest common divisor of n and m is written (n, m), their least common multiple is $[n, m]$, and $\omega(n)$ denotes the number of distinct prime factors of n. The cardinality of a finite set S is denoted $|S|$ or $\#S$. The transpose of a matrix g is written g^t. The prime symbol $'$ in $\sum'_{r(q)}$ means the range of $r \pmod q$ is restricted to $(r, q) = 1$. Finally, $p^j \| q$ denotes $p^j \mid q$ and $p^{j+1} \nmid q$.

2 Preliminaries I: the Apollonian group and its subgroups

2.1 Descartes theorem and consequences

Descartes' Circle Theorem states that a quadruple v of (oriented) curvatures of four mutually tangent circles lies on the cone

$$F(v) = 0, \tag{2.1}$$

where F is the Descartes quadratic form:

$$F(a,b,c,d) = 2\left(a^2+b^2+c^2+d^2\right) - (a+b+c+d)^2. \tag{2.2}$$

Note that F has signature $(3,1)$ over $\mathbb{R}$, and let

$$G := \mathrm{SO}_F(\mathbb{R}) = \left\{g \in \mathrm{SL}(4,\mathbb{R}) : F(gv) = F(v), \text{ for all } v \in \mathbb{R}^4\right\}$$

be the real special orthogonal group preserving F.

It follows immediately that for b, c and d fixed, there are two solutions a, a' to (2.1), and

$$a + a' = 2(b+c+d).$$

Hence we observe that a can be changed into a' by a reflection, that is,

$$(a,b,c,d)^t = S_1 \cdot \left(a',b,c,d\right)^t,$$

where the reflections

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 1 & & & \\ 2 & -1 & 2 & 2 \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

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

generate the so-called *Apollonian group*

$$\mathcal{A} = \langle S_1, S_2, S_3, S_4 \rangle. \tag{2.3}$$

It is a Coxeter group, free except for the relations $S_j^2 = I$, $1 \le j \le 4$. We immediately pass to the index two subgroup

$$\Gamma := \mathcal{A} \cap \mathrm{SO}_F$$

of orientation preserving transformations, that is, even words in the generators. Then Γ is freely generated by S_1S_2, S_2S_3 and S_3S_4. It is known that Γ is Zariski dense in G but *thin*, that is, of infinite index in $G(\mathbb{Z})$; equivalently, the Haar measure of $\Gamma\backslash G$ is infinite.

2.2 Arithmetic subgroups

Now we review the arguments from [26, 42] which lead to (1.3) and (1.4), as our setup depends critically on them.

Recall that for any fixed gasket $\mathscr{G}$, there is a root quadruple v_0 of the four smallest curvatures in $\mathscr{G}$, cf. (1.2). It follows from (2.1) and (2.3) that the set $\mathscr{B}$ of all curvatures can be realized as the orbit of the root quadruple v_0 under $\mathcal{A}$. Let

$$\mathscr{O} = \mathscr{O}_{\mathscr{G}} := \Gamma \cdot v_0$$

be the orbit of v_0 under Γ. Then the set of all curvatures certainly contains

$$\mathscr{B} \supset \bigcup_{j=1}^{4} \langle e_j, \mathscr{O} \rangle = \bigcup_{j=1}^{4} \langle e_j, \Gamma \cdot v_0 \rangle, \tag{2.4}$$

where $e_1 = (1, 0, 0, 0)^t, \ldots, e_4 = (0, 0, 0, 1)^t$ constitute the standard basis for $\mathbb{R}^4$, and the inner product above is the standard one. Recall we are treating $\mathscr{B}$ as a set, that is, without multiplicities.

It was observed in [26] that Γ contains unipotent elements, and hence one can use these to furnish an injection of affine space in the otherwise intractable orbit $\mathscr{O}$, as follows. Note first that

$$C_1 := S_4 S_3 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ 2 & 2 & -1 & 2 \\ 6 & 6 & -2 & 3 \end{pmatrix} \in \Gamma, \tag{2.5}$$

and after conjugation by

$$J := \begin{pmatrix} 1 & & & \\ -1 & 1 & & \\ -1 & 1 & -2 & 1 \\ -1 & & & 1 \end{pmatrix},$$

we have

$$\tilde{C}_1 := J^{-1} \cdot C_1 \cdot J = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & 2 & 1 & \\ & 4 & 4 & 1 \end{pmatrix}.$$

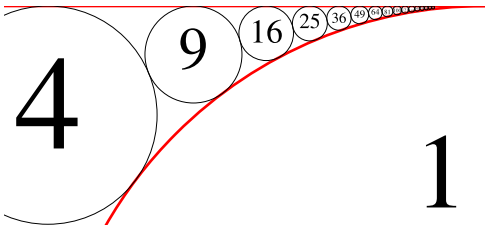

Fig. 2 Circles tangent to two fixed circles

Recall the spin homomorphism $\rho : \mathrm{SL}_2 \to \mathrm{SO}(2,1)$, embedded for our purposes in SL_4, given explicitly by

$$\rho : \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} 1 & & & \\ & \alpha^2 & 2\alpha\gamma & \gamma^2 \\ & \alpha\beta & \alpha\delta + \beta\gamma & \gamma\delta \\ & \beta^2 & 2\beta\delta & \delta^2 \end{pmatrix}. \tag{2.6}$$

In fact SL_2 is a double cover of $\mathrm{SO}(2,1)$ under ρ, with kernel $\pm I$. It is clear from inspection that

$$\rho : \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} =: T_1 \mapsto \tilde{C}_1.$$

Since $T_1^n = \left(\begin{smallmatrix} 1 & 2n \\ 0 & 1 \end{smallmatrix}\right)$, for each $n \in \mathbb{Z}$, Γ contains the element

$$C_1^n = J \cdot \rho\left(T_1^n\right) \cdot J^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 4n^2 - 2n & 4n^2 - 2n & 1 - 2n & 2n \\ 4n^2 + 2n & 4n^2 + 2n & -2n & 2n + 1 \end{pmatrix}.$$

(Of course this can be seen directly from (2.5); these transformations will be more enlightening below.)

Thus if $v = (a, b, c, d)^t \in \mathscr{O}$ is a quadruple in the orbit, then $\mathscr{O}$ also contains $C_1^n \cdot v$ for all n. From (2.4), we then have that the set $\mathscr{B}$ of curvatures contains

$$\mathscr{B} \ni \left\langle e_4, C_1^n \cdot v \right\rangle = 4(a+b)n^2 + 2(a+b-c+d)n + d. \tag{2.7}$$

The circles thus generated are all tangent to two fixed circles, which explains the square curvatures in Fig. 2. Of course (2.7) immediately implies (1.3).

Observe further that

$$C_2 := S_2 S_3 = \begin{pmatrix} 1 & & & \\ 6 & 3 & -2 & 6 \\ 2 & 2 & -1 & 2 \\ & & & 1 \end{pmatrix}$$

is another unipotent element, with

$$\tilde{C}_2 := J^{-1} \cdot C_2 \cdot J = \begin{pmatrix} 1 & & & \\ & 1 & 4 & 4 \\ & & 1 & 2 \\ & & & 1 \end{pmatrix},$$

and

$$\rho : \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} =: T_2 \mapsto \tilde{C}_2.$$

Since T_1 and T_2 generate $\Lambda(2)$, the principal 2-congruence subgroup of $\mathrm{PSL}(2, \mathbb{Z})$, we see that the Apollonian group Γ contains the subgroup

$$\Xi := \langle C_1, C_2 \rangle = J \cdot \rho\big(\Lambda(2)\big) \cdot J^{-1} < \Gamma. \tag{2.8}$$

In particular, whenever $(2x, y) = 1$, there is an element

$$\begin{pmatrix} * & 2x \\ * & y \end{pmatrix} \in \Lambda(2),$$

and thus Ξ contains the element

$$\begin{aligned} \xi_{x,y} &:= J \cdot \rho \begin{pmatrix} * & 2x \\ * & y \end{pmatrix} \cdot J^{-1} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ 4x^2 + 2xy + y^2 - 1 & 4x^2 + 2xy & -2xy & 2xy + y^2 \end{pmatrix}. \end{aligned} \tag{2.9}$$

Write

$$\begin{aligned} w_{x,y} &= \xi_{x,y}^t \cdot e_4 \\ &= \big(4x^2 + 2xy + y^2 - 1, 4x^2 + 2xy, -2xy, 2xy + y^2\big)^t. \end{aligned} \tag{2.10}$$

Then again by (2.4), we have shown the following

Lemma 2.1 ([42]) *Let $x, y \in \mathbb{Z}$ with $(2x, y) = 1$, and take any element $\gamma \in \Gamma$ with corresponding quadruple*

$$v_\gamma = (a_\gamma, b_\gamma, c_\gamma, d_\gamma)^t = \gamma \cdot v_0 \in \mathscr{O}. \tag{2.11}$$

Then the number

$$\langle e_4, \xi_{x,y} \cdot \gamma \cdot v_0 \rangle = \langle w_{x,y}, \gamma \cdot v_0 \rangle = 4A_\gamma x^2 + 4B_\gamma xy + C_\gamma y^2 - a_\gamma \tag{2.12}$$

is the curvature of some circle in $\mathscr{G}$, where we have defined

$$\begin{aligned} A_\gamma &:= a_\gamma + b_\gamma, \\ B_\gamma &:= \frac{a_\gamma + b_\gamma - c_\gamma + d_\gamma}{2}, \\ C_\gamma &:= a_\gamma + d_\gamma. \end{aligned} \tag{2.13}$$

Note from (2.1) that B_γ is integral.

Observe that, by construction, the value of a_γ is unchanged under the orbit of the group (2.8), and the circles whose curvatures are generated by (2.12) are all tangent to the circle corresponding to a_γ. It is classical (see [2]) that the number of distinct primitive values up to N assumed by a positive-definite binary quadratic form is of order at least $N(\log N)^{-1/2}$, proving (1.4).

To fix notation, we define the binary quadratic appearing in (2.12) and its shift by

$$f_\gamma(x, y) := A_\gamma x^2 + 2B_\gamma xy + C_\gamma y^2, \qquad \mathfrak{f}_\gamma(x, y) := f_\gamma(x, y) - a_\gamma, \tag{2.14}$$

so that

$$\langle w_{x,y}, \gamma \cdot v_0 \rangle = \mathfrak{f}_\gamma(2x, y). \tag{2.15}$$

Note from (2.13) and (2.1) that the discriminant of f_γ is

$$\Delta_\gamma = 4\big(B_\gamma^2 - A_\gamma C_\gamma\big) = -4a_\gamma^2. \tag{2.16}$$

When convenient, we will drop the subscripts γ in all the above.

2.3 Congruence subgroups

For each $q \geq 1$, define the "principal" q-congruence subgroup

$$\Gamma(q) := \big\{\gamma \in \Gamma : \gamma \equiv I \,(\mathrm{mod}\, q)\big\}. \tag{2.17}$$

These groups all have infinite index in $G(\mathbb{Z})$, but finite index in Γ. The quotients $\Gamma/\Gamma(q)$ have been determined completely by Fuchs [22] by proving

an explicit Strong Approximation theorem (see [37]), Goursat's Lemma, and other ingredients, as we explain below. Since G does not itself have the Strong Approximation Property, we pass to its connected spin double cover $\mathrm{SL}_2(\mathbb{C})$. We will need the covering map explicitly later, so record it here.

First change variables from the Descartes form F to

$$\tilde{F}(x, y, z, w) := xw + y^2 + z^2.$$

Then there is a homomorphism $\iota_0 : \mathrm{SL}(2, \mathbb{C}) \to \mathrm{SO}_{\tilde{F}}(\mathbb{R})$, sending

$$g = \begin{pmatrix} a + \alpha i & b + \beta i \\ c + \gamma i & d + \delta i \end{pmatrix} \in \mathrm{SL}(2, \mathbb{C})$$

to

$$\frac{1}{|\det(g)|^2} \times \begin{pmatrix} a^2 + \alpha^2 & 2(ac + \alpha\gamma) & 2(c\alpha - a\gamma) & -c^2 - \gamma^2 \\ ab + \alpha\beta & bc + ad + \beta\gamma + \alpha\delta & d\alpha + c\beta - b\gamma - a\delta & -cd - \gamma\delta \\ a\beta - b\alpha & -d\alpha + c\beta - b\gamma + a\delta & -bc + ad - \beta\gamma + \alpha\delta & d\gamma - c\delta \\ -b^2 - \beta^2 & -2(bd + \beta\delta) & 2(b\delta - d\beta) & d^2 + \delta^2 \end{pmatrix}.$$

To map from $\mathrm{SO}_{\tilde{F}}$ to SO_F, we apply a conjugation, see [26, (4.1)]. Let

$$\iota : \mathrm{SL}(2, \mathbb{C}) \to \mathrm{SO}_F(\mathbb{R}) \tag{2.18}$$

be the composition of this conjugation with ι_0. Let $\tilde{\Gamma}$ be the preimage of Γ under ι.

Lemma 2.2 ([22, 27]) *The group $\tilde{\Gamma}$ is generated by*

$$\pm\begin{pmatrix} 1 & 4i \\ & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} -2 & i \\ i & \end{pmatrix}, \qquad \pm\begin{pmatrix} 2 + 2i & 4 + 3i \\ -i & -2i \end{pmatrix}.$$

With this explicit realization of $\tilde{\Gamma}$ (and hence Γ), Fuchs was able to explicitly determine the images of $\tilde{\Gamma}$ in $\mathrm{SL}(2, \mathbb{Z}[i]/(q))$, and hence understand the quotients $\Gamma/\Gamma(q)$ for all q.

Lemma 2.3 [22]

(1) *The quotient groups $\Gamma/\Gamma(q)$ are multiplicative, that is, if q factors as*

$$q = p_1^{\ell_1} \cdots p_r^{\ell_r},$$

then

$$\Gamma/\Gamma(q) \cong \Gamma/\Gamma\left(p_1^{\ell_1}\right) \times \cdots \times \Gamma/\Gamma\left(p_r^{\ell_r}\right).$$

(2) *If* $(q, 6) = 1$ *then*

$$\Gamma/\Gamma(q) \cong \mathrm{SO}_F(\mathbb{Z}/q\mathbb{Z}). \tag{2.19}$$

(3) *If* $q = 2^\ell$, $\ell \geq 3$, *then* $\Gamma/\Gamma(q)$ *is the full preimage of* $\Gamma/\Gamma(8)$ *under the projection* $\mathrm{SO}_F(\mathbb{Z}/q\mathbb{Z}) \to \mathrm{SO}_F(\mathbb{Z}/8\mathbb{Z})$. *That is, the powers of* 2 *stabilize at* 8. *Similarly, the powers of* 3 *stabilize at* 3, *meaning that for* $q = 3^\ell$, $\ell \geq 1$, *the quotient* $\Gamma/\Gamma(q)$ *is the preimage of* $\Gamma/\Gamma(3)$ *under the corresponding projection map.*

Remark 2.4 This of course explains all local obstructions, cf. (1.1). The admissible numbers are precisely those residue classes (mod 24) which appear as some entry in the orbit of v_0 under $\Gamma/\Gamma(24)$.

3 Setup and Outline of the Proof

In this section, we introduce the main exponential sum and give an outline of the rest of the argument. Recall the fixed gasket $\mathscr{G}$ having curvatures $\mathscr{B}$ and root quadruple v_0. Let Γ be the Apollonian subgroup with subgroup Ξ, see (2.8). Let $\delta \approx 1.3$ be the Hausdorff dimension of the gasket $\mathscr{G}$; see Sect. 4 for the important role played by this geometric invariant. Recall also from (2.12) that for any $\gamma \in \Gamma$ and $\xi \in \Xi$,

$$\langle e_4, \xi\gamma v_0\rangle \in \mathscr{B}.$$

Our approach, mimicking [8, 9], is to exploit the bilinear (or multilinear) structure above.

We first give an informal description of the main ensemble from which we will form an exponential sum. Let N be our main growing parameter. We construct our ensemble by decomposing a ball in Γ of norm N into two balls, a small one in all of Γ of norm T, and a larger one of norm X^2 in Ξ, corresponding to $x, y \asymp X$. Specifically, we take

$$T = N^{1/100} \quad \text{and} \quad X = N^{99/200}, \quad \text{so that } TX^2 = N. \tag{3.1}$$

See (9.8) and (9.11) where these numbers are used.

We further need the technical condition that in the T-ball, the value of $a_\gamma = \langle e_1, \gamma\, v_0\rangle$ (see (2.11)) is of order T. This is used crucially in (7.8) and (5.41).

Finally, for technical reasons (see Lemma 5.2 below), we need to further split the T-ball into two: a small ball of norm T_1, and a big ball of norm T_2. Write

$$T = T_1 T_2, \quad T_2 = T_1^{\mathcal{C}}, \tag{3.2}$$

where $\mathcal{C}$ is a large constant depending only on the spectral gap for Γ; it is determined in (5.11). We now make formal the above discussion.

3.1 Introducing the main exponential sum

Let N, X, T, T_1, and T_2 be as in (3.1) and (3.2). Define the family

$$\mathfrak{F} = \mathfrak{F}_T := \left\{ \gamma = \gamma_1\gamma_2 : \begin{array}{c} \gamma_1, \gamma_2 \in \Gamma, \\ T_1 < \|\gamma_1\| < 2T_1, \\ T_2 < \|\gamma_2\| < 2T_2, \\ \langle e_1, \gamma_1\,\gamma_2\, v_0\rangle > T/100 \end{array} \right\}. \tag{3.3}$$

From Lax-Phillips [35] (or see (4.10)), we have the bound

$$\#\mathfrak{F}_T \ll T^{\delta}. \tag{3.4}$$

From (2.15), we can identify $\gamma \in \mathfrak{F}$ with a shifted binary quadratic form $\mathfrak{f}_\gamma$ of discriminant $-4a_\gamma^2$ via

$$\mathfrak{f}_\gamma(2x, y) = \langle w_{x,y}, \gamma\, v_0\rangle.$$

Recall from (2.12) that whenever $(2x, y) = 1$, the above is a curvature in the gasket. We sometimes drop γ, writing simply $\mathfrak{f} \in \mathfrak{F}$; then the latter can also be thought of as a family of shifted quadratic forms. Note also that the decomposition $\gamma = \gamma_1\gamma_2$ in (3.3) need not be unique, so some forms may appear with multiplicity.

One final technicality is to smooth the sum on $x, y \asymp X$. To this end, we fix a smooth, nonnegative function Υ, supported in $[1, 2]$ and having unit mass, $\int_{\mathbb{R}} \Upsilon(x)dx = 1$.

Our main object of study is then the representation number

$$\mathcal{R}_N(n) := \sum_{\mathfrak{f}\in\mathfrak{F}_T} \sum_{(2x,y)=1} \Upsilon\left(\frac{2x}{X}\right)\Upsilon\left(\frac{y}{X}\right)\mathbf{1}_{\{n=\mathfrak{f}(2x,y)\}}, \tag{3.5}$$

and the corresponding exponential sum, its Fourier transform

$$\widehat{\mathcal{R}_N}(\theta) := \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{(2x,y)=1} \Upsilon\left(\frac{2x}{X}\right)\Upsilon\left(\frac{y}{X}\right)e\big(\theta\,\mathfrak{f}(2x, y)\big). \tag{3.6}$$

Clearly $\mathcal{R}_N(n) \neq 0$ implies that $n \in \mathscr{B}$. Note also from (3.4) that the total mass satisfies

$$\widehat{\mathcal{R}_N}(0) \ll T^{\delta}X^2. \tag{3.7}$$

The condition $(2x, y) = 1$ will be a technical nuisance, and can be freed by a standard use of the Möbius inversion formula. To this end, we introduce another parameter

$$U = N^{\mathfrak{u}}, \tag{3.8}$$

a small power of N, with $\mathfrak{u} > 0$ depending only on the spectral gap of Γ; it is determined in (6.3). Then by truncating Möbius inversion, define

$$\widehat{\mathcal{R}_N^U}(\theta) := \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{x,y\in\mathbb{Z}} \Upsilon\left(\frac{2x}{X}\right)\Upsilon\left(\frac{y}{X}\right) e\big(\theta\,\mathfrak{f}(2x, y)\big) \sum_{\substack{u|(2x,y)\\ u<U}} \mu(u), \tag{3.9}$$

with corresponding "representation function" $\mathcal{R}_N^U$ (which could be negative).

3.2 Reduction to the circle method

We are now in position to outline the argument in the rest of the paper. Recall that $\mathscr{A}$ is the set of admissible numbers. We first reduce our main Theorem 1.2 to the following

Theorem 3.1 *There exists an $\eta > 0$ and a function $\mathfrak{S}(n)$ with the following properties. For $\frac{1}{2}N < n < N$, the singular series $\mathfrak{S}(n)$ is nonnegative, vanishes only when $n \notin \mathscr{A}$, and is otherwise $\gg_\varepsilon N^{-\varepsilon}$ for any $\varepsilon > 0$. Moreover, for $\frac{1}{2}N < n < N$ and admissible,*

$$\mathcal{R}_N^U(n) \gg \mathfrak{S}(n)T^{\delta-1}, \tag{3.10}$$

except for a set of cardinality $\ll N^{1-\eta}$.

Proof of Theorem 1.2 assuming Theorem 3.1 We first show that the difference between $\mathcal{R}_N$ and $\mathcal{R}_N^U$ is small in ℓ^1. Using (3.4) we have

$$\begin{aligned}
&\sum_{n<N} \big|\mathcal{R}_N(n) - \mathcal{R}_N^U(n)\big| \\
&= \sum_{n<N} \Bigg|\sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{x,y\in\mathbb{Z}} \Upsilon\left(\frac{2x}{X}\right)\Upsilon\left(\frac{y}{X}\right)\mathbf{1}_{\{n=\mathfrak{f}(2x,y)\}} \sum_{\substack{u|(2x,y)\\ u\geq U}} \mu(u)\Bigg| \\
&\ll \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{u\geq U} \sum_{\substack{y\ll X\\ y\equiv 0 (\mathrm{mod}\, u)}} \sum_{\substack{x\ll X\\ 2x\equiv 0 (\mathrm{mod}\, u)}} 1 \\
&\ll T^\delta \frac{X^2}{U},
\end{aligned}$$

for any $\varepsilon > 0$. Recall from (3.8) that U is a fixed power of N, so the above saves a power from the total mass (3.7).

Now let Z be the "exceptional" set of admissible $n < N$ for which $\mathcal{R}_N(n) = 0$. Furthermore, let W be the set of admissible $n < N$ for which (3.10) is satisfied. Then

$$T^{\delta}\frac{X^2}{U} \gg \sum_{n<N} \left|\mathcal{R}_N^U(n) - \mathcal{R}_N(n)\right| \geq \sum_{n\in Z\cap W} \left|\mathcal{R}_N^U(n) - \mathcal{R}_N(n)\right|$$
$$\gg_{\varepsilon} |Z \cap W| \cdot T^{\delta-1}N^{-\varepsilon}.$$

Note also from Theorem 3.1 that $|Z \cap W^c| \leq |W^c| \ll N^{1-\eta}$. Hence by (3.1) and (3.8),

$$|Z| = \left|Z \cap W^c\right| + |Z \cap W| \ll_{\varepsilon} N^{1-\eta} + \frac{N^{1+\varepsilon}}{U}, \tag{3.11}$$

which is a power savings since $\varepsilon > 0$ is arbitrary. This completes the proof. □

To establish (3.10), we decompose $\mathcal{R}_N^U$ into "major" and "minor" arcs, reducing Theorem 3.1 to the following

Theorem 3.2 *There exists an $\eta > 0$ and a decomposition*

$$\mathcal{R}_N^U(n) = \mathcal{M}_N^U(n) + \mathcal{E}_N^U(n) \tag{3.12}$$

with the following properties. For $\frac{1}{2}N < n < N$ and admissible, $n \in \mathscr{A}$, we have

$$\mathcal{M}_N^U(n) \gg \mathfrak{S}(n)T^{\delta-1}, \tag{3.13}$$

except for a set of cardinality $\ll N^{1-\eta}$. The singular series $\mathfrak{S}(n)$ is the same as in Theorem 3.1. Moreover,

$$\sum_{n<N} \left|\mathcal{E}_N^U(n)\right|^2 \ll N\,T^{2(\delta-1)}N^{-\eta}. \tag{3.14}$$

Proof of Theorem 3.1 assuming Theorem 3.2 We restrict our attention to the set of admissible $n < N$ so that (3.13) holds (the remainder having sufficiently small cardinality). Let Z denote the subset of these n for which $\mathcal{R}_N^U(n) < \frac{1}{2}\mathcal{M}_N^U(n)$; hence for $n \in Z$,

$$1 \ll \frac{|\mathcal{E}_N^U(n)|}{N^{-\varepsilon}T^{\delta-1}}.$$

Then by (3.14),

$$|Z| \ll_\varepsilon \sum_{n<N} \frac{|\mathcal{E}_N^U(n)|^2}{N^{-\varepsilon} T^{2(\delta-1)}} \ll N^{1-\eta+\varepsilon},$$

whence the claim follows, since $\varepsilon > 0$ is arbitrary. □

3.3 Decomposition into major and minor arcs

Next we explain the decomposition (3.12). Let M be a parameter controlling the depth of approximation in Dirichlet's theorem: for any irrational $\theta \in [0, 1]$, there exists some $q < M$ and $(r, q) = 1$ so that $|\theta - r/q| < 1/(qM)$. We will eventually set

$$M = XT, \tag{3.15}$$

see (7.7) where this value is used. (Note that M is a bit bigger than $N^{1/2} = XT^{1/2}$.)

Writing $\theta = r/q + \beta$, we introduce parameters

$$Q_0, \quad K_0, \tag{3.16}$$

small powers of N as determined in (6.2), so that the "major arcs" correspond to $q < Q_0$ and $|\beta| < K_0/N$. In fact, we need a smooth version of this decomposition.

To this end, recall the "hat" function and its Fourier transform

$$\mathfrak{t}(x) := \min(1 + x, 1 - x)^+, \qquad \widehat{\mathfrak{t}}(y) = \left(\frac{\sin(\pi y)}{\pi y}\right)^2. \tag{3.17}$$

Localize $\mathfrak{t}$ to the width K_0/N, periodize it to the circle, and put this spike on each fraction in the major arcs:

$$\mathfrak{T}(\theta) = \mathfrak{T}_{N,Q_0,K_0}(\theta) := \sum_{q<Q_0} \sum_{(r,q)=1} \sum_{m\in\mathbb{Z}} \mathfrak{t}\left(\frac{N}{K_0}\left(\theta + m - \frac{r}{q}\right)\right). \tag{3.18}$$

By construction, $\mathfrak{T}$ lives on the circle $\mathbb{R}/\mathbb{Z}$ and is supported within K_0/N of fractions r/q with small denominator, $q < Q_0$, as desired.

Then define the "main term"

$$\mathcal{M}_N^U(n) := \int_0^1 \mathfrak{T}(\theta)\widehat{\mathcal{R}_N^U}(\theta)e(-n\theta)d\theta, \tag{3.19}$$

and "error term"

$$\mathcal{E}_N^U(n) := \int_0^1 \big(1 - \mathfrak{T}(\theta)\big)\widehat{\mathcal{R}_N^U}(\theta)e(-n\theta)d\theta, \tag{3.20}$$

so that (3.12) obviously holds.

Since $\mathcal{R}_N^U$ could be negative, the same holds for $\mathcal{M}_N^U$. Hence we will establish (3.13) by first proving a related result for

$$\mathcal{M}_N(n) := \int_0^1 \mathfrak{T}(\theta)\widehat{\mathcal{R}_N}(\theta)e(-n\theta)d\theta, \tag{3.21}$$

and then showing that $\mathcal{M}_N$ and $\mathcal{M}_N^U$ cannot differ by too much for too many values of n. This is the same (but in reverse) as the transfer from $\mathcal{R}_N$ to $\mathcal{R}_N^U$ in (3.11). See Theorem 6.1 for the lower bound on $\mathcal{M}_N$, and Theorem 6.2 for the transfer.

To prove (3.14), we apply Parseval and decompose dyadically:

$$\begin{aligned}\sum_n \left|\mathcal{E}_N^U(n)\right|^2 &= \int_0^1 \left|1-\mathfrak{T}(\theta)\right|^2\left|\widehat{\mathcal{R}_N^U}(\theta)\right|^2 d\theta \\ &\ll \mathcal{I}_{Q_0,K_0} + \mathcal{I}_{Q_0} + \sum_{\substack{Q_0\le Q<M\\ \text{dyadic}}} \mathcal{I}_Q,\end{aligned}$$

where we have dissected the circle into the following regions (using that $|1-\mathfrak{t}(x)| = |x|$ on $[-1,1]$):

$$\mathcal{I}_{Q_0,K_0} := \int_{\substack{\theta=\frac{r}{q}+\beta\\ q<Q_0,(r,q)=1,|\beta|<K_0/N}} \left|\beta\frac{N}{K_0}\right|^2 \left|\widehat{\mathcal{R}_N^U}(\theta)\right|^2 d\theta, \tag{3.22}$$

$$\mathcal{I}_{Q_0} := \int_{\substack{\theta=\frac{r}{q}+\beta\\ q<Q_0,(r,q)=1,K_0/N<|\beta|<1/(qM)}} \left|\widehat{\mathcal{R}_N^U}(\theta)\right|^2 d\theta, \tag{3.23}$$

$$\mathcal{I}_Q := \int_{\substack{\theta=\frac{r}{q}+\beta\\ Q\le q<2Q,(r,q)=1,|\beta|<1/(qM)}} \left|\widehat{\mathcal{R}_N^U}(\theta)\right|^2 d\theta. \tag{3.24}$$

Bounds of the quality (3.14) are given for (3.22) and (3.23) in Sect. 7, see Theorem 7.3. Our estimation of (3.24) decomposes further into two cases, whether $Q < X$ or $X \le Q < M$, and are handled separately in Sect. 8 and Sect. 9; see Theorems 8.5 and 9.5, respectively.

We point out again that our averaging on n in the minor arcs makes this quite crude as far as individual n's (the subject of Conjecture 1.1) are concerned.

3.4 The rest of the paper

The only section not yet described is Sect. 5, where we furnish some lemmata which are useful in the sequel. These decompose into two categories: one set

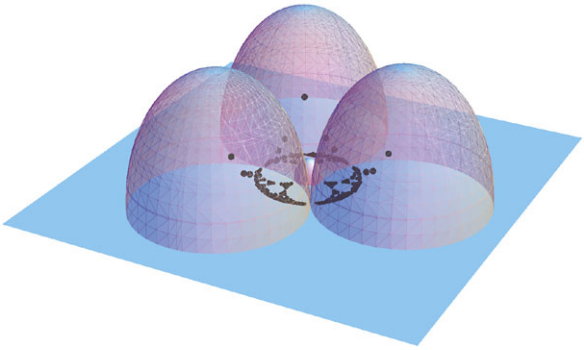

Fig. 3 The orbit of a point in hyperbolic space under the Apollonian group

of lemmata is related to some infinite-volume counting problems, for which the background in Sect. 4 is indispensable. The other lemma is of a classical flavor, corresponding to a local analysis for the shifted binary form $\mathfrak{f}$; this studies a certain exponential sum which is dealt with via Gauss and Kloosterman/Salié sums.

This completes our outline of the rest of the paper.

4 Preliminaries II: automorphic forms and representations

4.1 Spectral theory

Recall the general spectral theory in our present context. We abuse notation (in this section only), passing from $G = \mathrm{SO}_F(\mathbb{R})$ to its spin double cover $G = \mathrm{SL}(2, \mathbb{C})$. Let $\Gamma < G$ be a geometrically finite discrete group. (The Apollonian group is such, being a Schottky group, see Fig. 3.) Then Γ acts discontinuously on the upper half space $\mathbb{H}^3$, and any Γ orbit has a limit set Λ_Γ in the boundary $\partial\mathbb{H}^3 \cong S^2$ of some Hausdorff dimension $\delta = \delta(\Gamma) \in [0, 2]$. We assume that Γ is non-elementary (not virtually Abelian), so $\delta > 0$, and moreover that Γ is not a lattice, that is, the quotient $\Gamma\backslash\mathbb{H}^3$ has infinite hyperbolic volume; then $\delta < 2$. The hyperbolic Laplacian Δ acts on the space $L^2(\Gamma\backslash\mathbb{H}^3)$ of functions automorphic under Γ and square integrable on the quotient; we choose the Laplacian to be positive definite. The spectrum is controlled via the following, see [35, 38, 47].

Theorem 4.1 (Patterson, Sullivan, Lax-Phillips) *The spectrum above* 1 *is purely continuous, and the spectrum below* 1 *is purely discrete. The latter is empty unless* $\delta > 1$, *in which case, ordering the eigenvalues by*

$$0 < \lambda_0 < \lambda_1 \leq \cdots \leq \lambda_{max} < 1, \tag{4.1}$$

the base eigenvalue λ_0 *is given by*

$$\lambda_0 = \delta(2 - \delta).$$

Remark 4.2 In our application to the Apollonian group, the limit set is precisely the underlying gasket, see Fig. 3. It has dimension

$$\delta \approx 1.3\ldots > 1. \tag{4.2}$$

Corresponding to λ_0 is the Patterson-Sullivan base eigenfunction, φ_0, which can be realized explicitly as the integral of a Poisson kernel against the so-called Patterson-Sullivan measure μ. Roughly speaking, μ is the weak* limit as $s \to \delta^+$ of the measures

$$\mu_s(x) := \frac{\sum_{\gamma\in\Gamma} \exp(-s\, d(\mathfrak{o}, \gamma\cdot\mathfrak{o}))\mathbf{1}_{x=\gamma\mathfrak{o}}}{\sum_{\gamma\in\Gamma} \exp(-s\, d(\mathfrak{o}, \gamma\cdot\mathfrak{o}))}, \tag{4.3}$$

where $d(\cdot,\cdot)$ is the hyperbolic distance, and $\mathfrak{o}$ is any fixed point in $\mathbb{H}^3$.

4.2 Spectral gap

We assume henceforth that Γ moreover satisfies $\Gamma < \mathrm{SL}(2,\mathcal{O})$, where $\mathcal{O} = \mathbb{Z}[i]$. Then we have a tower of congruence subgroups: for any integer $q \geq 1$, define $\Gamma(q)$ to be the kernel of the projection map $\Gamma \to \mathrm{SL}(2,\mathcal{O}/\mathfrak{q})$, with $\mathfrak{q} = (q)$ the principal ideal. As in (4.1), write

$$0 < \lambda_0(q) < \lambda_1(q) \leq \cdots \leq \lambda_{max(q)}(q) < 1, \tag{4.4}$$

for the discrete spectrum of $\Gamma(q)\backslash\mathbb{H}^3$. The groups $\Gamma(q)$, while of infinite covolume, have finite index in Γ, and hence

$$\lambda_0(q) = \lambda_0 = \delta(2-\delta). \tag{4.5}$$

But the second eigenvalues $\lambda_1(q)$ could *a priori* encroach on the base. The fact that this does not happen is the spectral gap property for Γ.

Theorem 4.3 *Given Γ as above, there exists some $\varepsilon = \varepsilon(\Gamma) > 0$ such that for all $q \geq 1$,*

$$\lambda_1(q) \geq \lambda_0 + \varepsilon. \tag{4.6}$$

This is proved in the Appendix by Péter Varjú.

4.3 Representation theory and mixing rates

By the Duality Theorem of Gelfand, Graev, and Piatetski-Shapiro [24], the spectral decomposition above is equivalent to the decomposition into irreducibles of the right regular representation acting on $L^2(\Gamma\backslash G)$. That is, we identify $\mathbb{H}^3 \cong G/K$, with $K = \mathrm{SU}(2)$ a maximal compact subgroup, and lift

functions from $\mathbb{H}^3$ to (right K-invariant) functions on G. Corresponding to (4.1) is the decomposition

$$L^2(\Gamma\backslash G) = V_{\lambda_0} \oplus V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_{max}} \oplus V_{temp}. \tag{4.7}$$

Here V_{temp} contains the tempered spectrum (for $\mathrm{SL}_2(\mathbb{C})$, every non-spherical irreducible representation is tempered), and each V_{λ_j} is an infinite dimensional vector space, isomorphic as a G-representation to a complementary series representation with parameter $s_j \in (1, 2)$ determined by $\lambda_j = s_j(2 - s_j)$. Obviously, a similar decomposition holds for $L^2(\Gamma(q)\backslash G)$, corresponding to (4.4).

We also have the following well-known general fact about mixing rates of matrix coefficients, see e.g. [20]. First we recall the relevant Sobolev norm. Let (π, V) be a unitary G-representation, and let $\{X_j\}$ denote an orthonormal basis of the Lie algebra $\mathfrak{k}$ of K with respect to an Ad-invariant scalar product. For a smooth vector $v \in V^\infty$, define the (second order) Sobolev norm $\mathcal{S}$ of v by

$$\mathcal{S}v := \|v\|_2 + \sum_j \left\|d\pi(X_j).v\right\|_2 + \sum_j \sum_{j'} \left\|d\pi(X_j)d\pi(X_{j'}).v\right\|_2.$$

Theorem 4.4 ([33, Prop. 5.3]) *Let $\Theta > 1$ and (π, V) be a unitary representation of G which does not weakly contain any complementary series representation with parameter $s > \Theta$. Then for any smooth vectors $v, w \in V^\infty$,*

$$\left|\langle \pi(g).v, w\rangle\right| \ll \|g\|^{-2(2-\Theta)} \cdot \mathcal{S}v \cdot \mathcal{S}w. \tag{4.8}$$

Here $\|\cdot\|$ is the standard Frobenius matrix norm.

4.4 Effective bisector counting

The next ingredient which we require is the recent work by Vinogradov [49] on effective bisector counting for such infinite volume quotients. Recall the following sub(semi)groups of G:

$$A = \left\{a_t := \begin{pmatrix} e^{t/2} & \\ & e^{-t/2} \end{pmatrix} : t \in \mathbb{R}\right\}, \qquad A^+ = \{a_t : t \geq 0\},$$

$$M = \left\{\begin{pmatrix} e^{2\pi i\theta} & \\ & e^{-2\pi i\theta} \end{pmatrix} : \theta \in \mathbb{R}/\mathbb{Z}\right\}, \qquad K = \mathrm{SU}(2).$$

We have the Cartan decomposition $G = KA^+K$, unique up to the normalizer M of A in K. We require it in the following more precise form. Identify K/M

with the sphere $S^2 \cong \partial\mathbb{H}^3$. Then for every $g \in G$ not in K, there is a unique decomposition

$$g = s_1(g) \cdot a(g) \cdot m(g) \cdot s_2(g)^{-1} \tag{4.9}$$

with $s_1, s_2 \in K/M$, $a \in A^+$ and $m \in M$, corresponding to

$$G = K/M \times A^+ \times M \times M\backslash K,$$

see, e.g., [49, (3.4)]. The following theorem follows easily from [49, Theorem 2.2].

Theorem 4.5 ([49]) *Let $\Phi, \Psi \subset S^2$ be spherical caps and let $\mathcal{I} \subset \mathbb{R}/\mathbb{Z}$ be an interval. Then under the above hypotheses on Γ (in particular $\delta > 1$), and using the decomposition* (4.9), *we have*

$$\sum_{\gamma\in\Gamma} \mathbf{1}\left\{\begin{array}{c} s_1(\gamma) \in \Phi \\ s_2(\gamma) \in \Psi \\ \|a(\gamma)\|^2 < T \\ m(\gamma) \in \mathcal{I} \end{array}\right\} = c_\delta \cdot \mu(\Phi)\mu(\Psi)\ell(\mathcal{I})T^\delta + O\big(T^\Theta\big), \tag{4.10}$$

as $T \to \infty$. Here $c_\delta > 0$, $\|\cdot\|$ is the Frobenius norm, ℓ is Lebesgue measure, μ is Patterson-Sullivan measure (*cf.* (4.3)), *and*

$$\Theta < \delta \tag{4.11}$$

depends only on the spectral gap for Γ. The implied constant does not depend on Φ, Ψ, or $\mathcal{I}$.

This generalizes from $\mathrm{SL}(2,\mathbb{R})$ to $\mathrm{SL}(2,\mathbb{C})$ the main result of [12], which is itself a generalization (with weaker exponents) to our infinite volume setting of [25, Theorem 4].

5 Some lemmata

5.1 Infinite volume counting statements

Equipped with the tools of Sect. 4, we isolate here some consequences which will be needed in the sequel. We return to the notation $G = \mathrm{SO}_F$, with F the Descartes form (2.2), $\Gamma = \mathcal{A} \cap G$, the orientation preserving Apollonian subgroup, and $\Gamma(q)$ its principal congruence subgroups. Moreover, we import all the notation from the previous section.

First we use the spectral gap to see that summing over a coset of a congruence group can be reduced to summing over the original group.

Lemma 5.1 *Fix $\gamma_1 \in \Gamma, q \geq 1$, and any "congruence" group $\tilde{\Gamma}(q)$ satisfying*

$$\Gamma(q) < \tilde{\Gamma}(q) < \Gamma. \tag{5.1}$$

Then as $Y \to \infty$,

$$\#\big\{\gamma \in \tilde{\Gamma}(q) : \|\gamma_1 \gamma\| < Y\big\} \tag{5.2}$$

$$= \frac{1}{[\Gamma : \tilde{\Gamma}(q)]} \cdot \#\big\{\gamma \in \Gamma : \|\gamma\| < Y\big\} + O\big(Y^{\Theta_0}\big), \tag{5.3}$$

where $\Theta_0 < \delta$ depends only on the spectral gap for Γ. The implied constant above does not depend on q or γ_1. The same holds with $\gamma_1\gamma$ in (5.2) replaced by $\gamma\gamma_1$.

This simple lemma follows from a more-or-less standard argument. We give a sketch below, since a slightly more complicated result will be needed later, cf. Lemma 5.3, but with essentially no new ideas. After proving the lemma below, we will use the argument as a template for the more complicated statement.

Sketch of Proof Denote the left hand side (5.2) by $\mathcal{N}_q$, and let $\mathcal{N}_1/[\Gamma : \tilde{\Gamma}(q)]$ be the first term of (5.3). For $g \in G$, let

$$f(g) = f_Y(g) := \mathbf{1}_{\{\|g\| < Y\}}, \tag{5.4}$$

and define

$$F_q(g, h) := \sum_{\gamma \in \tilde{\Gamma}(q)} f\big(g^{-1}\gamma h\big), \tag{5.5}$$

so that

$$\mathcal{N}_q = F_q\big(\gamma_1^{-1}, e\big). \tag{5.6}$$

By construction, F_q is a function on $\tilde{\Gamma}(q)\backslash G \times \tilde{\Gamma}(q)\backslash G$, and we smooth F_q in both copies of $\tilde{\Gamma}(q)\backslash G$, as follows. Let $\psi \geq 0$ be a smooth bump function supported in a ball of radius $\eta > 0$ (to be chosen later) about the origin in G with $\int_G \psi = 1$, and automorphize it to

$$\Psi_q(g) := \sum_{\gamma \in \tilde{\Gamma}(q)} \psi(\gamma g).$$

Then clearly Ψ_q is a bump function in $\tilde{\Gamma}(q)\backslash G$ with $\int_{\tilde{\Gamma}(q)\backslash G} \Psi_q = 1$. Let

$$\Psi_{q,\gamma_1}(g) := \Psi_q(g\gamma_1).$$

Smooth the variables g and h in F_q by considering

$$\mathcal{H}_q := \langle F_q, \Psi_{q,\gamma_1} \otimes \Psi_q \rangle = \int_{\tilde{\Gamma}(q)\backslash G} \int_{\tilde{\Gamma}(q)\backslash G} F_q(g,h)\Psi_{q,\gamma_1}(g)\Psi_q(h)dg\,dh$$
$$= \sum_{\gamma \in \tilde{\Gamma}(q)} \int_{\tilde{\Gamma}(q)\backslash G} \int_{\tilde{\Gamma}(q)\backslash G} f\big(\gamma_1 g^{-1}\gamma h\big)\Psi_q(g)\Psi_q(h)dg\,dh.$$

First we estimate the error from smoothing:

$$\mathcal{E} = |\mathcal{N}_q - \mathcal{H}_q|$$
$$\leq \sum_{\gamma \in \Gamma} \int_{\tilde{\Gamma}(q)\backslash G} \int_{\tilde{\Gamma}(q)\backslash G} \big| f\big(\gamma_1 g^{-1}\gamma h\big) - f(\gamma_1\gamma)\big|\Psi_q(g)\Psi_q(h)dg\,dh,$$

where we have increased γ to run over all of Γ. The analysis splits into three ranges.

(1) If γ is such that

$$\|\gamma_1\gamma\| > Y(1+10\eta), \tag{5.7}$$

then both $f(\gamma_1 g^{-1}\gamma h)$ and $f(\gamma_1\gamma)$ vanish.

(2) In the range

$$\|\gamma_1\gamma\| < Y(1-10\eta), \tag{5.8}$$

both $f(\gamma_1 g^{-1}\gamma h)$ and $f(\gamma_1\gamma)$ are 1, so their difference vanishes.

(3) In the intermediate range, we apply [35], bounding the count by

$$\ll Y^{\delta}\eta + Y^{\delta-\varepsilon}, \tag{5.9}$$

where $\varepsilon > 0$ depends on the spectral gap for Γ.

Thus it remains to analyze $\mathcal{H}_q$.

Use a simple change of variables (see [12, Lemma 3.7]) to express $\mathcal{H}_q$ via matrix coefficients:

$$\mathcal{H}_q = \int_G f(g)\big\langle \pi(g)\Psi_q, \Psi_{q,\gamma_1}\big\rangle_{\tilde{\Gamma}(q)\backslash G} dg.$$

Decompose the matrix coefficient into its projection onto the base irreducible V_{λ_0} in (4.7) and an orthogonal term, and bound the remainder by the mixing rate (4.8) using the uniform spectral gap $\varepsilon > 0$ in (4.6). The functions ψ are bump functions in six real dimensions, so can be chosen to have second-order Sobolev norms bounded by $\ll \eta^{-5}$. Of course the projection onto the base representation is just $[\Gamma : \tilde{\Gamma}(q)]^{-1}$ times the same projection at level

one, cf. (4.5). Running the above argument in reverse at level one (see [12, Proposition 4.18]) gives:

$$\mathcal{N}_q = \frac{1}{[\Gamma : \tilde{\Gamma}(q)]} \cdot \mathcal{N}_1 + O\big(\eta Y^{\delta} + Y^{\delta-\varepsilon}\big) + O\big(Y^{\delta-\varepsilon}\eta^{-10}\big). \tag{5.10}$$

Optimizing η and renaming $\Theta_0 < \delta$ in terms of the spectral gap ε gives the claim. □

Next we exploit the previous lemma and the product structure of the family $\mathfrak{F}$ in (3.3) to save a small power of q in the following modular restriction. Such a bound is needed at several places in Sect. 8.

Lemma 5.2 *Let Θ_0 be as in (5.3). Define $\mathcal{C}$ in (3.2) by*

$$\mathcal{C} := \frac{10^{30}}{\delta - \Theta_0}, \tag{5.11}$$

hence determining T_1 and T_2. There exists some $\eta_0 > 0$ depending only on the spectral gap of Γ so that for any $1 \le q < N$ and any $r \pmod q$,

$$\sum_{\gamma \in \mathfrak{F}} \mathbf{1}_{\{\langle e_1, \gamma v_0\rangle \equiv r \,(\mathrm{mod}\, q)\}} \ll \frac{1}{q^{\eta_0}} T^{\delta}. \tag{5.12}$$

The implied constant is independent of r.

Proof Dropping the condition $\langle e_1, \gamma_1 \gamma_2 v_0\rangle > T/100$ in (3.3), bound the left hand side of (5.12) by

$$\sum_{\substack{\gamma_1 \in \Gamma \\ \|\gamma_1\| \asymp T_1}} \sum_{\substack{\gamma_2 \in \Gamma \\ \|\gamma_2\| \asymp T_2}} \mathbf{1}_{\{\langle e_1, \gamma_1\gamma_2 v_0\rangle \equiv r \,(\mathrm{mod}\, q)\}}. \tag{5.13}$$

We decompose the argument into two ranges of q.

Case 1: q small In this range, we fix γ_1, and follow a standard argument for γ_2. Let $\tilde{\Gamma}(q) < \Gamma$ denote the stabilizer of $v_0 \pmod q$, that is

$$\tilde{\Gamma}(q) := \big\{\gamma \in \Gamma : \gamma v_0 \equiv v_0 \,(\mathrm{mod}\, q)\big\}. \tag{5.14}$$

Clearly (5.1) is satisfied, and it is elementary that

$$\big[\Gamma : \tilde{\Gamma}(q)\big] \asymp q^2, \tag{5.15}$$

cf. (2.19). Decompose $\gamma_2 = \gamma_2'\gamma_2''$ with $\gamma_2'' \in \tilde{\Gamma}(q)$ and $\gamma_2' \in \Gamma/\tilde{\Gamma}(q)$. Then by (5.3) and [35], we have

$$(5.13) = \sum_{\substack{\gamma_1 \in \Gamma \\ \|\gamma_1\| \asymp T_1}} \sum_{\gamma_2' \in \Gamma/\tilde{\Gamma}(q)} \mathbf{1}_{\{\langle e_1, \gamma_1\gamma_2' v_0\rangle \equiv r (\mathrm{mod}\, q)\}} \sum_{\substack{\gamma_2'' \in \tilde{\Gamma}(q) \\ \|\gamma_2'\gamma_2''\| \asymp T_2}} 1$$

$$\ll T_1^{\delta} q \left(\frac{1}{q^2}\, T_2^{\delta} + T_2^{\Theta_0} \right).$$

Hence we have saved a whole power of q, as long as

$$q < T_2^{(\delta - \Theta_0)/2}. \tag{5.16}$$

Case 2: $q \geq T_2^{\frac{\delta - \Theta_0}{2}}$ Then by (5.11) and (3.2), q is actually a very large power of T_1,

$$q \geq T_1^{10^{29}}. \tag{5.17}$$

In this range, we exploit Hilbert's Nullstellensatz and effective versions of Bezout's theorem; see a related argument in [7, Proof of Proposition 4.1].

Fixing γ_2 in (5.13) (with $\ll T_2^{\delta}$ choices), we set

$$v := \gamma_2 v_0,$$

and play now with γ_1. Let S be the set of γ_1's in question (and we now drop the subscript 1):

$$S = S_{v,q}(T_1) := \big\{ \gamma \in \Gamma : \|\gamma\| \asymp T_1, \langle e_1, \gamma v\rangle \equiv r (\mathrm{mod}\, q) \big\}.$$

This congruence restriction is to a modulus much bigger than the parameter, so we

Claim *There is an integer vector $v_* \neq 0$ and an integer z_* such that*

$$\langle e_1, \gamma v_*\rangle = z_* \tag{5.18}$$

holds for all $\gamma \in S$. That is, the modular condition can be lifted to an exact equality.

First we assume the Claim and complete the proof of (5.12). Let q_0 be a prime of size $\asymp T_1^{(\delta - \Theta_0)/2}$, say, such that $v_* \not\equiv 0 (\mathrm{mod}\, q_0)$; then

$$|S| \ll \#\big\{ \|\gamma_1\| < T_1 : \langle e_1, \gamma v_*\rangle \equiv z_* (\mathrm{mod}\, q_0) \big\}$$

$$\ll q_0\left(\frac{1}{q_0^2}T_1^{\delta}+T_1^{\Theta_0}\right)\ll \frac{1}{q_0}T_1^{\delta},$$

by the argument in Case 1. Recall we assumed that $q < N$. Since q_0 above is a small power of N, the above saves a tiny power of q, as desired.

It remains to establish the Claim. For each $\gamma \in S$, consider the condition

$$\langle e_1, \gamma\, v\rangle = \sum_{1\le j\le 4} \gamma_{1,j}\, v_j \equiv r \,(\mathrm{mod}\, q).$$

First massage the equation into one with no trivial solutions. Since v is a primitive vector, after a linear change of variables we may assume that $(v_1, q) = 1$. Then multiply through by $\bar{v}_1$, where $v_1\bar{v}_1 \equiv 1 (\mathrm{mod}\, q)$, getting

$$\gamma_{1,1} + \sum_{2\le j\le 4} \gamma_{1,j}\, v_j \bar{v}_1 \equiv r\bar{v}_1 (\mathrm{mod}\, q). \tag{5.19}$$

Now, for variables $V = (V_2, V_3, V_4)$ and Z, and each $\gamma \in S$, consider the (linear) polynomials $P_\gamma \in \mathbb{Z}[V, Z]$:

$$P_\gamma(V, Z) := \gamma_{1,1} + \sum_{2\le j\le 4} \gamma_{1,j}\, V_j - Z,$$

and the affine variety

$$\mathcal{V} := \bigcap_{\gamma\in S}\{P_\gamma = 0\}.$$

If this variety $\mathcal{V}(\mathbb{C})$ is non-empty, then there is clearly a rational solution, $(V^*, Z^*) \in \mathcal{V}(\mathbb{Q})$. Hence we have found a rational solution to (5.18), namely $v^* = (1, V_2^*, V_3^*, V_4^*) \neq 0$ and $z^* = Z^*$. Since (5.18) is homogeneous, we may clear denominators, getting an integral solution, v_*, z_*.

Thus we henceforth assume by contradiction that the variety $\mathcal{V}(\mathbb{C})$ is empty. Then by Hilbert's Nullstellensatz, there are polynomials $Q_\gamma \in \mathbb{Z}[V, Z]$ and an integer $\mathfrak{d} \ge 1$ so that

$$\sum_{\gamma\in S} P_\gamma(V, Z)Q_\gamma(V, Z) = \mathfrak{d}, \tag{5.20}$$

for all $(V, Z) \in \mathbb{C}^4$. Moreover, Hermann's method [29] (see [36, Theorem IV]) gives effective bounds on the heights of Q_γ and $\mathfrak{d}$ in the above Bezout equation. Recall the height of a polynomial is the logarithm of its largest coefficient (in absolute value); thus the polynomials P_γ are linear in four variables with height $\le \log T_1$. Then Q_γ and $\mathfrak{d}$ can be found so that

$$\mathfrak{d} \le e^{8^{4\cdot 2^{4-1}-1}(\log T_1 + 8\log 8)} \ll T_1^{10^{28}}. \tag{5.21}$$

(Much better bounds are known, see e.g. [1, Theorem 5.1], but these suffice for our purposes.)

On the other hand, reducing (5.20) modulo q and evaluating at

$$V_0 = (v_2\bar{v}_1, v_3\bar{v}_1, v_4\bar{v}_1), \qquad Z_0 = r\bar{v}_1,$$

we have

$$\sum_{\gamma\in S} P_\gamma(V_0, Z_0)\, Q_\gamma(V_0, Z_0) \equiv 0 \equiv \mathfrak{d} (\mathrm{mod}\, q),$$

by (5.19). But then since $\mathfrak{d} \geq 1$, we in fact have $\mathfrak{d} \geq q$, which is incompatible with (5.21) and (5.17). This furnishes our desired contradiction, completing the proof. □

Next we need a slight generalization of Lemma 5.1, which will be used in the major arcs analysis, see (6.6).

Lemma 5.3 *Let $1 < K \leq T_2^{1/10}$, fix $|\beta| < K/N$, and fix $x, y \asymp X$. Then for any $\gamma_0 \in \Gamma$, any $q \geq 1$, and any group $\tilde{\Gamma}(q)$ satisfying (5.1), we have*

$$\sum_{\gamma\in\mathfrak{F}\cap\{\gamma_0\tilde{\Gamma}(q)\}} e\big(\beta\, \mathfrak{f}_\gamma(2x, y)\big) = \frac{1}{[\Gamma : \tilde{\Gamma}(q)]} \sum_{\gamma\in\mathfrak{F}} e\big(\beta\, \mathfrak{f}_\gamma(2x, y)\big) + O\big(T^{\Theta} K\big), \tag{5.22}$$

where $\Theta < \delta$ depends only on the spectral gap for Γ, and the implied constant does not depend on q, γ_0, β, x or y.

Proof The proof follows with minor changes that of Lemma 5.1, so we give a sketch; see also [12, Sect. 4].

According to the construction (3.3) of $\mathfrak{F}$, the γ's in question satisfy $\gamma = \gamma_1\gamma_2 \in \gamma_0\tilde{\Gamma}(q)$, and hence we can write

$$\gamma_2 = \gamma_1^{-1}\gamma_0\gamma_2',$$

with $\gamma_2' \in \tilde{\Gamma}(q)$. Then $\gamma_2' = \gamma_0^{-1}\gamma_1\gamma_2$, and using (2.15), we can write the left hand side of (5.22) as

$$\sum_{\substack{\gamma_1\in\Gamma \\ T_1<\|\gamma_1\|<2T_1}} \sum_{\substack{\gamma_2'\in\tilde{\Gamma}(q) \\ T_2<\|\gamma_1^{-1}\gamma_0\gamma_2'\|<2T_2}} \mathbf{1}_{\{\langle e_1, \gamma_0\gamma_2' v_0\rangle > T/100\}}\, e\big(\beta\, \langle w_{x,y}, \gamma_0\gamma_2' v_0\rangle\big).$$

Now we fix γ_1 and mimic the proof of Lemma 5.1 in γ_2'.

Replace (5.4) by

$$f(g) := \mathbf{1}_{\{T_2 < \|\gamma_1^{-1} g\| < 2T_2\}} \mathbf{1}_{\{\langle e_1, g\, v_0\rangle > T/100\}}\, e\big(\beta\, \langle w_{x,y}, g\, v_0\rangle\big).$$

Then (5.5)–(5.7) remains essentially unchanged, save cosmetic changes such as replacing (5.6) by $F_q(\gamma_1\gamma_0^{-1}, e)$. Then in the estimation of the difference $|\mathcal{N}_q - \mathcal{H}_q|$ by splitting the sum on γ_2' into ranges, the argument now proceeds as follows.

(1) The range (5.7) should be replaced by

$$\big\|\gamma_1\gamma_0^{-1}\gamma_2'\big\| < T_2(1-10\eta), \quad \text{or} \quad \big\|\gamma_1\gamma_0^{-1}\gamma_2'\big\| > 2T_2(1+10\eta),$$
$$\text{or} \quad \big\langle e_1, \gamma_1\gamma_0^{-1}\gamma_2'\, v_0\big\rangle < \frac{T}{100}(1-10\eta).$$

(2) The range (5.8) should be replaced by the range

$$T_2(1+10\eta) < \big\|\gamma_1\gamma_0^{-1}\gamma_2'\big\| < 2T_2(1-10\eta), \quad \text{and}$$
$$\big\langle e_1, \gamma_1\gamma_0^{-1}\gamma_2'\, v_0\big\rangle > \frac{T}{100}(1+10\eta),$$

in which f is differentiable. Here instead of the difference $|f(\gamma_1\gamma_0^{-1} \cdot g\gamma_2' h) - f(\gamma_1\gamma_0^{-1}\gamma_2')|$ vanishing, it is now bounded by

$$\ll \eta K,$$

for a net contribution to the error of $\ll \eta K T^{\delta}$.

(3) In the remaining range, (5.9) remains unchanged, using $|f| \le 1$.

The error in (5.10) is then replaced by

$$O\big(\eta\, K\, T_2^{\delta} + T_2^{\delta-\varepsilon}\eta^{-10}\big).$$

Optimizing η and renaming Θ gives the bound $O(T_2^{\Theta} K^{10/11})$, which is better than claimed in the power of K. Rename Θ once more using (3.2) and (5.11), giving (5.22). □

The following is our last counting lemma, showing a certain equidistribution among the values of $\mathfrak{f}_\gamma(2x, y)$ at the scale N/K. This bound is used in the major arcs, see the proof of Theorem 6.1.

Lemma 5.4 *Fix $N/2 < n < N$, $1 < K \le T_2^{1/10}$, and $x, y \asymp X$. Then*

$$\sum_{\gamma\in\mathfrak{F}} \mathbf{1}_{\{|\mathfrak{f}_\gamma(2x,y)-n|<\frac{N}{K}\}} \gg \frac{T^{\delta}}{K} + T^{\Theta}, \tag{5.23}$$

where $\Theta < \delta$ only depends on the spectral gap for Γ. The implied constant is independent of x, y, and n.

Sketch The proof is an explicit calculation nearly identical to the one given in [12, Sect. 5]; we give only a sketch here. Write the left hand side of (5.23) as

$$\sum_{\substack{\gamma_1\in\Gamma\\ T_1<\|\gamma_1\|<2T_1}}\ \sum_{\substack{\gamma_2\in\Gamma\\ T_2<\|\gamma_2\|<2T_2}} \mathbf{1}_{\{\langle e_1,\gamma_1\gamma_2 v_0\rangle > T/100\}}\mathbf{1}_{\{|\langle w_{x,y},\gamma_1\gamma_2 v_0\rangle - n|<N/K\}}.$$

Fix γ_1 and express the condition on γ_2 as $\gamma_2 \in R \subset G$, where R is the region

$$R = R_{\gamma_1,x,y,n} := \left\{ g\in G: \begin{array}{c} T_2 < \|g\| < 2T_2 \\ \langle \gamma_1^t e_1, g\, v_0\rangle > T/100 \\ |\langle \gamma_1^t w_{x,y}, g\, v_0\rangle - n| < \frac{N}{K} \end{array} \right\}.$$

Lift $G = \mathrm{SO}_F(\mathbb{R})$ to its spin cover $\tilde{G} = \mathrm{SL}_2(\mathbb{C})$ via the map ι of (2.18). Let $\tilde{R} \subset \tilde{G}$ be the corresponding pullback region, and decompose $\tilde{G}$ into Cartan KAK coordinates according to (4.9). Note that ι is quadratic in the entries, so, e.g., the condition

$$\|g\|^2 \asymp T \quad \text{gives } \big\|\iota(g)\big\| \asymp T, \tag{5.24}$$

explaining the factor $\|a(g)\|^2$ appearing in (4.10).

Then chop $\tilde{R}$ into spherical caps and apply Theorem 4.5. The same argument as in [12, Sect. 5] then leads to (5.23), after renaming Θ; we suppress the details. □

5.2 Local analysis statements

In this subsection, we study a certain exponential sum which arises in a crucial way in our estimates. Fix $\mathfrak{f} \in \mathfrak{F}$, and write $\mathfrak{f} = f - a$ with

$$f(x, y) = Ax^2 + 2Bxy + Cy^2$$

according to (2.14). Let $q_0 \geq 1$, fix r with $(r, q_0) = 1$, and fix $n, m \in \mathbb{Z}$. (The notation is meant to be consistent with its later use; there will be another parameter q, and q_0 will be a divisor of q.) Define the exponential sum

$$\mathcal{S}_f(q_0, r; n, m) := \frac{1}{q_0^2} \sum_{k(q_0)} \sum_{\ell(q_0)} e_{q_0}\big(rf(k, \ell) + nk + m\ell\big). \tag{5.25}$$

This sum appears naturally in many places in the minor arcs analysis, see e.g. (7.4) and (9.2). Our first lemma is completely standard, see, e.g. [30, Sect. 12.3].

Lemma 5.5 *With the above conditions*,

$$\left|\mathcal{S}_f(q_0, r; n, m)\right| \leq q_0^{-1/2}. \tag{5.26}$$

Remark 5.6 Being a sum in two variables, one might expect square-root cancellation in each, giving a savings of q_0^{-1}; indeed this is what we obtain, modulo some coprimality conditions, see (5.29). For some of our applications, saving just one square-root is plenty, and we can ignore the coprimality; hence the cleaner statement in (5.26).

Proof Write $\mathcal{S}_f$ for $\mathcal{S}_f(q_0, r; n, m)$. Note first that $\mathcal{S}_f$ is multiplicative in q_0, so we study the case $q_0 = p^j$ is a prime power. Assume for simplicity $(q_0, 2) = 1$; similar calculations are needed to handle the 2-adic case.

First we re-express $\mathcal{S}_f$ in a more convenient form. By Descartes theorem (2.1), primitivity of the gasket $\mathscr{G}$, and (2.13), we have that $(A, B, C) = 1$; assume henceforth that $(C, q_0) = 1$, say. Write $\bar{x}$ for the multiplicative inverse of x (the modulus will be clear from context). Recall throughout that $(r, q_0) = 1$.

Looking at the terms in the summand of $\mathcal{S}_f$, we have

$$\begin{aligned}
&rf(k,\ell) + nk + m\ell \pmod{q_0} \\
&\quad \equiv r\left(Ak^2 + 2Bk\ell + C\ell^2\right) + nk + m\ell \\
&\quad \equiv rC(\ell + B\bar{C}k)^2 + r\bar{C}k^2\left(AC - B^2\right) + nk + m\ell \\
&\quad \equiv rC(\ell + B\bar{C}k)^2 + a^2 r\bar{C}k^2 + nk + m\ell \\
&\quad \equiv rC(\ell + B\bar{C}k + \overline{2rC}m)^2 - \overline{4rC}m^2 + a^2 r\bar{C}k^2 + k(n - B\bar{C}m),
\end{aligned}$$

where we used (2.16). Hence we have

$$\begin{aligned}
\mathcal{S}_f = \frac{1}{q_0^2} e_{q_0}\left(-\overline{4rC}m^2\right) \sum_{k(q_0)} e_{q_0}\left(a^2 r\bar{C}k^2 + k(n - B\bar{C}m)\right) \\
\times \sum_{\ell(q_0)} e_{q_0}\left(rC(\ell + B\bar{C}k + \overline{2rC}m)^2\right),
\end{aligned}$$

and the ℓ sum is just a classical Gauss sum. It can be evaluated explicitly, see e.g. [30, Eq. (3.38)]. Let

$$\varepsilon_{q_0} := \begin{cases} 1 & \text{if } q_0 \equiv 1 \pmod 4 \\ i & \text{if } q_0 \equiv 3 \pmod 4. \end{cases}$$

Then the Gauss sum on ℓ is $\varepsilon_{q_0}\sqrt{q}_0(\frac{rC}{q_0})$, where $(\frac{\cdot}{q_0})$ is the Legendre symbol. Thus we have

$$\mathcal{S}_f = \frac{\varepsilon_{q_0}}{q_0^{3/2}}\left(\frac{rC}{q_0}\right)e_{q_0}\big(-\overline{4rC}m^2\big)\sum_{k(q_0)} e_{q_0}\big(a^2r\bar{C}k^2 + k(n - B\bar{C}m)\big).$$

Let

$$\tilde{q}_0 := \big(a^2, q_0\big), \qquad q_1 := q_0/\tilde{q}_0, \quad \text{and} \quad a_1 := a^2/\tilde{q}_0, \tag{5.27}$$

so that $a^2/q_0 = a_1/q_1$ in lowest terms. Break the sum on $0 \le k < q_0$ according to $k = k_1 + q_1\tilde{k}$, with $0 \le k_1 < q_1$ and $0 \le \tilde{k} < \tilde{q}_0$. Then

$$\begin{aligned}\mathcal{S}_f = \frac{\varepsilon_{q_0}}{q_0^{3/2}}\left(\frac{rC}{q_0}\right)&e_{q_0}\big(-\overline{4rC}m^2\big)\\ &\times \sum_{k_1(q_1)} e_{q_1}\big(a_1r\bar{C}(k_1)^2\big)e_{q_0}\big(k_1(n - B\bar{C}m)\big)\\ &\times \sum_{\tilde{k}(\tilde{q}_0)} e_{\tilde{q}_0}\big(\tilde{k}(n - B\bar{C}m)\big).\end{aligned}$$

The last sum vanishes unless $n - B\bar{C}m \equiv 0 \pmod{\tilde{q}_0}$, in which case it is $\tilde{q}_0$. In the latter case, define L by

$$L := (Cn - Bm)/\tilde{q}_0. \tag{5.28}$$

Then we have

$$\begin{aligned}\mathcal{S}_f = \mathbf{1}_{nC\equiv mB(\tilde{q}_0)}&\frac{\varepsilon_{q_0}}{q_0^{3/2}}\left(\frac{rC}{q_0}\right)e_{q_0}\big(-\overline{4rC}m^2\big)\\ &\times e_{q_1}\big(-\overline{4a_1rC}L^2\big)\Bigg[\sum_{k_1(q_1)} e_{q_1}\big(a_1r\bar{C}(k_1 + \overline{2a_1r}L)^2\big)\Bigg]\tilde{q}_0.\end{aligned}$$

The Gauss sum in brackets is again evaluated as $\varepsilon_{q_1}q_1^{1/2}(\frac{a_1r\bar{C}}{q_1})$, so we have

$$\begin{aligned}\mathcal{S}_f(q_0, r; n, m) = \mathbf{1}_{nC\equiv mB(\tilde{q}_0)}&\frac{\varepsilon_{q_0}\varepsilon_{q_1}\tilde{q}_0^{1/2}}{q_0}e_{q_0}\big(-\overline{4rC}m^2\big)\\ &\times e_{q_1}\big(-\overline{4a_1rC}L^2\big)\left(\frac{rC}{q_0}\right)\left(\frac{a_1r\bar{C}}{q_1}\right).\end{aligned} \tag{5.29}$$

The claim then follows trivially. □

Next we introduce a certain average of a pair of such sums. Let f, q_0, r, n, and m be as before, and fix $q \equiv 0 \pmod{q_0}$ and $(u_0, q_0) = 1$. Let $\mathfrak{f}' \in \mathfrak{F}$ be another shifted form $\mathfrak{f}' = f' - a'$, with

$$f'(x, y) = A'x^2 + 2B'xy + C'y^2.$$

Also let $n', m' \in \mathbb{Z}$. Then define

$$\begin{aligned}\mathcal{S} &= \mathcal{S}\big(q, q_0, f, f', n, m, n', m'; u_0\big) \\ &:= \sideset{}{'}\sum_{r(q)} \mathcal{S}_f(q_0, ru_0; n, m)\overline{\mathcal{S}_{f'}\big(q_0, ru_0; n', m'\big)}e_q\big(r\big(a' - a\big)\big). \quad (5.30)\end{aligned}$$

This sum also appears naturally in the minor arcs analysis, see (8.2) and (9.4).

Lemma 5.7 *With the above notation, we have the estimate*

$$|\mathcal{S}| \ll (q/q_0)^2 \frac{\{(a^2, q_0) \cdot ((a')^2, q_0)\}^{1/2}}{q^{5/4}}\big(a - a', q\big)^{1/4}. \quad (5.31)$$

Remark 5.8 Treating all gcd's above as 1 and pretending $q = q_0$, the trivial bound here (after having saved essentially a whole q from each of the two $\mathcal{S}_f$ sums) is $1/q$, since the r sum is unnormalized. So (5.31) saves an extra $q^{1/4}$ in the r sum. (In fact we could have saved the expected $q^{1/2}$, but this does not improve our final estimates.)

Proof Observe that $\mathcal{S}$ is multiplicative in q, so we again consider the prime power case $q = p^j$, $p \neq 2$; then q_0 is also a prime power, since $q_0 \mid q$. As before, we may assume $(C, q_0) = (C', q_0) = 1$.

Recall a_1, $\tilde{q}_0$, and L given in (5.27) and (5.28), and let a_1', $\tilde{q}_0'$ and L' be defined similarly. Inputting the analysis from (5.29) into both $\mathcal{S}_f$ and $\mathcal{S}_{f'}$, we have

$$\begin{aligned}\mathcal{S} = \mathbf{1}_{\substack{nC \equiv 2mB(\tilde{q}_0) \\ n'C' \equiv 2m'B'(\tilde{q}_0')}} &\frac{\varepsilon_{q_1}\bar{\varepsilon}_{q_1'}(\tilde{q}_0\tilde{q}_0')^{1/2}}{q_0^2}\left(\frac{CC'}{q_0}\right)\left(\frac{a_1u_0\bar{C}}{q_1}\right)\left(\frac{a_1'u_0\bar{C}'}{q_1'}\right) \\ &\times \Bigg[\sideset{}{'}\sum_{r(q)}\left(\frac{r}{q_1}\right)\left(\frac{r}{q_1'}\right)e_q\big(r\{a' - a\}\big) \\ &\times e_{q_0}\left(\overline{4ru_0}\left\{\overline{C'}\big(m'\big)^2 - \overline{C}m^2 + \overline{a_1'C'}\big(L'\big)^2\tilde{q}' - \overline{a_1C}L^2\tilde{q}\right\}\right)\Bigg]. \quad (5.32)\end{aligned}$$

The term in brackets $[\cdot]$ is a Kloosterman- or Salié-type sum, for which we have an elementary bound [32] to the power 3/4:

$$|\mathcal{S}| \ll \frac{(\tilde{q}_0\tilde{q}_0')^{1/2}}{q_0^2} q^{3/4}\big(a-a', q\big)^{1/4},$$

giving the claim. (There is no improvement in our use of this estimate from appealing to Weil's bound instead of Kloosterman's; any power gain suffices.) □

In the case $a = a'$, (5.31) only saves one power of q, and in Sect. 9 we will need slightly more; see the proof of (9.10). We get a bit more cancellation in the special case $f(m,-n) \neq f'(m',-n')$ below.

Lemma 5.9 *Assuming $a = a'$ and $f(m,-n) \neq f'(m',-n')$, we have the estimate*

$$|\mathcal{S}| \ll (q/q_0)^5 \frac{(a^2, q_0)}{q^{9/8}} \cdot \big|f(m,-n) - f'\big(m',-n'\big)\big|^{1/2}. \tag{5.33}$$

Proof Assume first that q (and hence q_0) is a prime power, continuing to omit the prime 2. Returning to the definition of $\mathcal{S}$ in (5.30), it is clear in the case $a = a'$ that

$$\sideset{}{'}\sum_{r(q)} = (q/q_0) \sideset{}{'}\sum_{r(q_0)}.$$

Hence we again apply Kloosterman's 3/4th bound to (5.32), getting

$$\begin{aligned}|\mathcal{S}| \ll \mathbf{1}_{\substack{nC\equiv 2mB(\tilde{q}_0)\\ n'C'\equiv 2m'B'(\tilde{q}_0')}} (q/q_0)^{9/2} \frac{(a^2,q_0)}{q^{5/4}} \\ \times \prod_{p^j \| q_0} \big(p^j, \bar{4}\{\overline{C'}(m')^2 - \overline{C}m^2 + \overline{a_1}(a^2, p^j)\big(\overline{C'}(L')^2 - \overline{C}L^2\big)\}\big)^{1/4},\end{aligned} \tag{5.34}$$

which is valid now without the assumption that q_0 is a prime power. (Here a_1 satisfies $a^2 = a_1(a^2, p^j)$ as in (5.27), and L is given in (5.28), so both depend on p^j.)

Break the primes diving q_0 into two sets, $\mathcal{P}_1$ and $\mathcal{P}_2$, defining $\mathcal{P}_1$ to be the set of those primes p for which

$$\overline{C}m^2 + \overline{C}L^2\overline{a_1}(a^2, p^j) \equiv \overline{C'}(m')^2 + \overline{C'}(L')^2\overline{a_1}(a^2, p^j) \pmod{p^{\lceil j/2\rceil}}, \tag{5.35}$$

and $\mathcal{P}_2$ the rest. For the latter, the gcd in $(p^j, \dots)$ of (5.34) is at most $p^{j/2}$, so we clearly have

$$\prod_{\substack{p^j \| q_0 \\ p \in \mathcal{P}_2}} (p^j, \dots)^{1/4} \leq \prod_{p^j \| q_0} p^{j/8} = q_0^{1/8}. \tag{5.36}$$

For $p \in \mathcal{P}_1$, we multiply both sides of (5.35) by

$$a^2 = AC - B^2 = A'C' - (B')^2 = a_1(a^2, p^j),$$

giving

$$\begin{aligned} &(AC - B^2)\overline{C}m^2 + \overline{C}L^2(a^2, p^j)^2 \\ &\quad \equiv (A'C' - (B')^2)\overline{C'}(m')^2 + \overline{C'}(L')^2(a^2, p^j)^2 \pmod{p^{\lceil j/2 \rceil}}. \end{aligned} \tag{5.37}$$

Using (5.28) that

$$nC - mB = (a^2, p^j)L, \qquad n'C' - m'B' = (a^2, p^j)L'$$

and subtracting a from both sides of (5.37), we have shown that

$$f'(m', -n') \equiv f(m, -n) \pmod{p^{\lceil j/2 \rceil}}. \tag{5.38}$$

Let

$$Z = |f(m, -n) - f'(m', -n')|.$$

By assumption $Z \neq 0$. Moreover (5.38) implies that

$$\left(\prod_{p \in \mathcal{P}_1} p^{\lceil j/2 \rceil} \right) \mid Z,$$

and hence

$$\prod_{\substack{p^j \| q_0 \\ p \in \mathcal{P}_1}} p^{j/4} \leq Z^{1/2}. \tag{5.39}$$

Combining (5.39) and (5.36) in (5.34) gives the claim. □

Finally we need some savings in the case $a = a'$ and $f(m, -n) = f'(m', -n')$. This will no longer come from $\mathcal{S}$ itself, but from the following supplementary lemmata.

Lemma 5.10 *Fix an equivalence class $\mathcal{K}$ of primitive binary quadratic forms of discriminant $-4a^2$. We claim that the number of equivalent forms $f \in \mathcal{K}$ with $\mathfrak{f} = f - a \in \mathfrak{F}$ is bounded, that is,*

$$\#\{\mathfrak{f} \in \mathfrak{F} : f \in \mathcal{K}\} = O(1). \tag{5.40}$$

Proof From (2.13), (3.3), and (2.16), we have that $f(m,n) = Am^2 + 2Bmn + Cn^2$ has coefficients of size

$$A, B, C \ll T,$$

and $AC - B^2 = a^2$, with $a \asymp T$. It follows that $AC \asymp T^2$, and hence

$$A, C \asymp T. \tag{5.41}$$

Now suppose we have $\mathfrak{f} = f - a$ and $\mathfrak{f}' = f' - a$ with f as above and f' having coefficients A', B', C'. If f and f' are equivalent then there is an element $\left(\begin{smallmatrix} g & h \\ i & j \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ so that

$$\begin{aligned} A' &= g^2 A + 2gi B + i^2 C, \\ B' &= ghA + (gj + hi)B + ijC, \\ C' &= h^2 A + 2hj B + j^2 C. \end{aligned} \tag{5.42}$$

The first line can be rewritten as

$$A' = C(i + gB/C)^2 + g^2 \frac{4a^2}{C},$$

so that

$$g^2 \le A' \frac{C}{4a^2} \ll 1.$$

Similarly,

$$(i + gB/C)^2 \le \frac{A'}{C} \ll 1,$$

and hence $|i| \ll 1$. In a similar fashion, we see that $|h|$ and $|j|$ are also bounded, thus the number of equivalent forms in $\mathcal{K}$ is bounded, as claimed. □

Lemma 5.11 *For a fixed large integer z, the number of inequivalent classes $\mathcal{K}$ of primitive quadratic forms of determinant $-4a^2$ which represent z is*

$$\ll_\varepsilon z^\varepsilon \cdot \left(z, 4a^2\right)^{1/2}, \quad \text{for any } \varepsilon > 0. \tag{5.43}$$

Proof If $f \in \mathcal{K}$ represents z, say $f(m,n) = z$, then, setting $w = (m,n)$, f represents $z_1 := z/w^2$ primitively. We see from (5.42) that f is then in the same class as $f_1(m,n) = z_1 m^2 + 2Bmn + Cn^2$, with

$$-4a^2 = z_1 C - B^2.$$

Moreover, by a unipotent change of variables preserving z_1, we can force B into the range $[0, z_1)$, that is, B is determined mod z_1. So the number of inequivalent such f_1 is equal to

$$\#\big\{B(\bmod z_1) : B^2 \equiv -4a^2(z_1)\big\} = \prod_{p^e \| z_1} \#\big\{B^2 \equiv -p^{2f}\big(p^e\big)\big\}, \tag{5.44}$$

where $p^f \,||\, 2a$. If $2f \geq e$, then the number of local solutions is at most $p^{e/2}$. Otherwise, write $B = B_1 p^f$; then there are at most 2 solutions to $B_1^2 \equiv -1 (\bmod p^{e-2f})$, and there are p^f values for B once B_1 is determined. Hence the number of local solutions is at most $2 \cdot \min(p^{e/2}, p^f)$, so the number of solutions to (5.44) is at most

$$2^{\omega(z)}\big(z_1, 4a^2\big)^{1/2} \ll_\varepsilon z^\varepsilon \big(z, 4a^2\big)^{1/2}.$$

The number of divisors z_1 of z is $\ll_\varepsilon z^\varepsilon$, completing the proof. □

Lemma 5.12 *Fix $(A,B,C) = 1$ and $d \mid AC - B^2$. Then there are integers k, ℓ with $(k, \ell, d) = 1$ so that, whenever $Am^2 + 2Bmn + Cn^2 \equiv 0(d)$, we have*

$$(mk + n\ell)^2 \equiv 0(d). \tag{5.45}$$

Proof We will work locally, then lift to a global solution. Let $p^e \,||\, d$.

Case 1: If $(p, A) = 1$, then $Am^2 + 2Bmn + Cn^2 \equiv 0(p^e)$ implies

$$(m + \bar{A}Bn)^2 - \bar{A}^2 B^2 n^2 + \bar{A}Cn^2 \equiv (m + \bar{A}Bn)^2 \equiv 0\big(p^e\big).$$

In this case, we set $k_p := 1$, and $\ell_p := \bar{A}B$.

Case 2: If $(p, A) > 1$, then by primitivity, $(p, C) = 1$. As before, we have $(n + \bar{C}Bm)^2 \equiv 0(p^e)$, and we choose $k_p = \bar{C}B$, $\ell_p := 1$.

By the Chinese Remainder Theorem, there are integers k and ℓ so that $k \equiv k_p (\bmod p^e)$, and similarly with ℓ. By construction, we have $(k, \ell, d) = 1$, as claimed. □

Lemma 5.13 *Given large M, $(A, B, C) = 1$ and $d \mid AC - B^2$,*

$$\#\{m, n < M : Am^2 + 2Bmn + Cn^2 \equiv 0(d)\} \ll_\varepsilon d^\varepsilon \left(\frac{M^2}{d^{1/2}} + M\right). \tag{5.46}$$

Proof As in Lemma 5.12, A, B, C and d determine k, ℓ so that

$$\sum_{m,n<M} \mathbf{1}_{\{Am^2+2Bmn+Cn^2\equiv 0(d)\}} \le \sum_{m,n<M} \mathbf{1}_{\{(mk+n\ell)^2\equiv 0(d)\}}.$$

But then there is a $d_1 \mid d$, with $d \mid d_1^2$ so that $mk + n\ell \equiv 0(d_1)$. Let $w = (\ell, d_1)$; then $mk \equiv 0(w)$ implies $m \equiv 0(w)$ since $(k, \ell, d) = 1$. There are at most $1 + M/w$ such m up to M. With m fixed, n is uniquely determined mod d_1/w. Hence we get the bound

$$\begin{aligned}(5.46) &\le \sum_{\substack{d_1\mid d\\ d\mid d_1^2}} \sum_{w\mid d_1} \sum_{m,n<M} \mathbf{1}_{\{m\equiv 0(\mathrm{mod}\, w)\}} \mathbf{1}_{\{n\equiv -\frac{\overline{\ell}}{w}\frac{m}{w}k(\mathrm{mod}\, \frac{d_1}{w})\}} \\ &\ll \sum_{\substack{d_1\mid d\\ d\mid d_1^2}} \sum_{w\mid d_1} \left(\frac{M}{w} + 1\right)\left(\frac{wM}{d_1} + 1\right) \ll_\varepsilon d^\varepsilon \left(\frac{M^2}{d^{1/2}} + M\right),\end{aligned}$$

as claimed. □

Finally we collect the above lemmata into our desired estimate, essential in the proof of (9.12).

Proposition 5.14 *For large M and $\mathfrak{f} = f - a \in \mathfrak{F}$ fixed,*

$$\#\left\{ \begin{matrix} \mathfrak{f}' \in \mathfrak{F} \\ m, n, m', n' < M \end{matrix} \;\middle|\; \begin{matrix} a' = a \\ \mathfrak{f}(m, -n) = \mathfrak{f}'(m', -n') \end{matrix} \right\} \ll_\varepsilon (TM)^\varepsilon \left(M^2 + TM\right), \tag{5.47}$$

for any $\varepsilon > 0$.

Proof Once f, m, n, and $\mathfrak{f}' = f' - a \in \mathfrak{F}$ are determined, it is elementary that there are $\ll_\varepsilon M^\varepsilon$ values of m', n' with $f(m, -n) = f'(m', -n')$. Decomposing f' into classes and applying (5.40), (5.43), and (5.46), in succession, we have

$$\sum_{m,n<M} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F}\\ a'=a}} \sum_{m',n'<M} \mathbf{1}_{\{f(m,-n)=f'(m',-n')\}}$$

$$
\begin{aligned}
&\ll_\varepsilon \sum_{m,n<M} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F}\\ a'=a}} \mathbf{1}_{\{f' \text{ represents } f(m,-n)\}} M^\varepsilon \\
&\ll M^\varepsilon \sum_{m,n<M} \sum_{\substack{\text{classes } \mathcal{K}\\ \text{representing } f(m,-n)}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F}\\ a'=a,\, f'\in\mathcal{K}}} 1 \\
&\ll_\varepsilon (TM)^\varepsilon \sum_{m,n<M} \left(f(m,-n), 4a^2\right)^{1/2} \\
&\ll (TM)^\varepsilon \sum_{d\mid 4a^2} d^{1/2} \sum_{m,n<M} \mathbf{1}_{\{f(m,-n)\equiv 0(d)\}} \\
&\ll (TM)^\varepsilon \sum_{d\mid 4a^2} d^{1/2}\left(\frac{M^2}{d^{1/2}} + M\right) \\
&\ll (TM)^\varepsilon \left(M^2 + Ma\right),
\end{aligned}
$$

from which the claim follows since $a \ll T$. □

6 Major arcs

We return to the setting and notation of Sect. 3 with the goal of establishing (3.13). Thanks to the counting lemmata in Sect. 5.1, we can now define the major arcs parameters Q_0 and K_0 from (3.16). First recall the two numbers $\Theta < \delta$ appearing in (5.22), (5.23), and define

$$1 < \Theta_1 < \delta \tag{6.1}$$

to be the larger of the two. Then set

$$Q_0 = T^{(\delta-\Theta_1)/20}, \quad K_0 = Q_0^2. \tag{6.2}$$

We may now also set the parameter U from (3.8) to be

$$U = {Q_0}^{(\eta_0)^2/100}, \tag{6.3}$$

where $0 < \eta_0 < 1$ is the number which appears in Lemma 5.2.

Let $\mathcal{M}_N^{(U)}(n)$ denote either $\mathcal{M}_N(n)$ or $\mathcal{M}_N^U(n)$ from (3.21), (3.19), respectively. Putting (3.18) and (3.6) (resp. (3.9)) into (3.21) (resp. (3.19)), making a change of variables $\theta = r/q + \beta$, and unfolding the integral from $\sum_m \int_0^1$ to $\int_{\mathbb{R}}$ gives

$$\mathcal{M}_N^{(U)}(n) = \sum_{x,y\in\mathbb{Z}} \Upsilon\left(\frac{2x}{X}\right)\Upsilon\left(\frac{y}{X}\right) \cdot \mathfrak{M}(n) \cdot \sum_u \mu(u), \tag{6.4}$$

where in the last sum, u ranges over $u \mid (2x, y)$ (resp. and $u < U$). Here we have defined

$$\begin{aligned}\mathfrak{M}(n) &= \mathfrak{M}_{x,y}(n)\\ &:= \sum_{q<Q_0}\sum_{r(q)}{}'\sum_{\gamma\in\mathfrak{F}} e_q\big(r\big(\langle w_{x,y}, \gamma v_0\rangle - n\big)\big)\\ &\quad\times \int_{\mathbb{R}} \mathfrak{t}\left(\frac{N}{K_0}\beta\right) e\big(\beta\big(\mathfrak{f}_\gamma(2x, y) - n\big)\big)d\beta,\end{aligned} \tag{6.5}$$

using (2.15).

As in (5.14), let $\tilde{\Gamma}(q)$ be the stabilizer of $v_0 (\mathrm{mod}\, q)$. Decompose the sum on $\gamma \in \mathfrak{F}$ in (6.5) as a sum on $\gamma_0 \in \Gamma/\tilde{\Gamma}(q)$ and $\gamma \in \mathfrak{F} \cap \gamma_0\tilde{\Gamma}(q)$. Applying Lemma 5.3 to the latter sum, using the definition of Θ_1 in (6.1), and recalling the estimate (5.15) gives

$$\mathfrak{M}(n) = \mathfrak{S}_{Q_0}(n)\cdot\mathfrak{W}(n) + O\left(\frac{T^{\Theta_1}}{N}K_0^2Q_0^4\right), \tag{6.6}$$

where

$$\mathfrak{S}_{Q_0}(n) := \sum_{q<Q_0}\sum_{r(q)}{}'\sum_{\gamma_0\in\Gamma/\tilde{\Gamma}(q)} \frac{e_q(r(\langle w_{x,y}, \gamma_0 v_0\rangle - n))}{[\Gamma : \tilde{\Gamma}(q)]},$$

$$\mathfrak{W}(n) := \frac{K_0}{N}\sum_{\mathfrak{f}\in\mathfrak{F}} \widehat{\mathfrak{t}}\left(\big(\mathfrak{f}(2x, y) - n\big)\frac{K_0}{N}\right).$$

Clearly we have thus split $\mathfrak{M}$ into "modular" and "Archimedean" components. It is now a simple matter to prove the following

Theorem 6.1 *For $\frac{1}{2}N < n < N$, there exists a function $\mathfrak{S}(n)$ as in Theorem 3.1 so that*

$$\mathcal{M}_N(n) \gg \mathfrak{S}(n)T^{\delta-1}. \tag{6.7}$$

Proof First we discuss the modular component. Write $\mathfrak{S}_{Q_0}$ as

$$\mathfrak{S}_{Q_0}(n) = \sum_{q<Q_0}\frac{1}{[\Gamma : \tilde{\Gamma}(q)]}\sum_{\gamma_0\in\Gamma/\tilde{\Gamma}(q)} c_q\big(\langle w_{x,y}, \gamma_0 v_0\rangle - n\big),$$

where c_q is the Ramanujan sum, $c_q(m) = \sum_{r(q)}{}' e_q(rm)$. By (2.19), the analysis now reduces to a classical estimate for the singular series. We may use the transitivity of the γ_0 sum to replace $\langle w_{x,y}, \gamma_0 v_0\rangle$ by $\langle e_4, \gamma_0 v_0\rangle$, extend the

sum on q to all natural numbers, and use multiplicativity to write the sum as an Euler product. Then the resulting singular series

$$\mathfrak{S}(n) := \prod_p \left[1 + \sum_{k\geq 1} \frac{1}{[\Gamma : \Gamma_0(p^k)]} \sum_{\gamma_0 \in \Gamma/\Gamma_0(p^k)} c_{p^k}\big(\langle e_4, \gamma_0 v_0\rangle - n\big) \right]$$

vanishes only on non-admissible numbers, and can easily be seen to satisfy

$$N^{-\varepsilon} \ll_\varepsilon \mathfrak{S}(n) \ll_\varepsilon N^\varepsilon, \tag{6.8}$$

for any $\varepsilon > 0$. See, e.g. [8, Sect. 4.3].

Next we handle the Archimedean component. By our choice of $\mathfrak{t}$ in (3.17), specifically that $\widehat{\mathfrak{t}} > 0$ and $\widehat{\mathfrak{t}}(y) > 2/5$ for $|y| < 1/2$, we have

$$\mathfrak{W}(n) \gg \frac{K_0}{N} \sum_{\mathfrak{f}\in\mathfrak{F}} \mathbf{1}_{\{|\mathfrak{f}(2x,y)-n| < \frac{N}{2K_0}\}} \gg \frac{T^\delta}{N} + \frac{T^{\Theta_1} K_0}{N},$$

using Lemma 5.4.

Putting everything into (6.6) and then into (6.4) gives (6.7), using (6.2) and (3.1). □

Next we derive from the above that the same bound holds for $\mathcal{M}_N^U$ (most of the time).

Theorem 6.2 *There is an $\eta > 0$ such that the bound (6.7) holds with $\mathcal{M}_N$ replaced by $\mathcal{M}_N^U$, except on a set of cardinality $\ll N^{1-\eta}$.*

Proof Putting (6.6) into (6.4) gives

$$\begin{aligned}
&\sum_{n<N} \big|\mathcal{M}_N(n) - \mathcal{M}_N^U(n)\big| \\
&\ll \sum_{x,y\asymp X} \sum_{n<N} \big|\mathfrak{M}(n)\big| \sum_{\substack{u|(2x,y)\\ u\geq U}} 1 \\
&\ll_\varepsilon \sum_{y<X} \sum_{\substack{u|y\\ u\geq U}} \sum_{\substack{x<X\\ 2x\equiv 0 (\mathrm{mod}\, u)}} \left\{ N^\varepsilon \sum_{\mathfrak{f}\in\mathfrak{F}} \frac{K_0}{N} \left[\sum_{n<N} \widehat{\mathfrak{t}}\left(\big(\mathfrak{f}(2x,y) - n\big)\frac{K_0}{N} \right) \right] \right. \\
&\qquad \left. + K_0^2 Q_0^4 T^{\Theta_1} \right\} \\
&\ll N^\varepsilon X \frac{X}{U} T^\delta,
\end{aligned}$$

using (6.8) and (6.2). The rest of the argument is identical to that leading to (3.11). □

This establishes (3.13), and hence completes our Major Arcs analysis; the rest of the paper is devoted to proving (3.14).

7 Minor arcs I: case $q < Q_0$

We keep all the notation of Sect. 3, our goal in this section being to bound (3.22) and (3.23). First we return to (3.9) and reverse orders of summation, writing

$$\widehat{\mathcal{R}_N^U}(\theta) = \sum_{u<U} \mu(u) \sum_{\mathfrak{f}\in\mathfrak{F}} e(-a\theta)\widehat{\mathcal{R}}_{f,u}(\theta), \tag{7.1}$$

where $\mathfrak{f} = f - a$ according to (2.14), and we have set

$$\widehat{\mathcal{R}}_{f,u}(\theta) := \sum_{2x\equiv 0(u)} \sum_{y\equiv 0(u)} \Upsilon\left(\frac{2x}{X}\right)\Upsilon\left(\frac{y}{X}\right)e\big(\theta f(2x,y)\big).$$

If u is even, then we have

$$\widehat{\mathcal{R}}_{f,u}(\theta) = \sum_{x,y\in\mathbb{Z}} \Upsilon\left(\frac{xu}{X}\right)\Upsilon\left(\frac{yu}{X}\right)e\big(\theta f(xu,yu)\big). \tag{7.2}$$

If u is odd, we have

$$\widehat{\mathcal{R}}_{f,u}(\theta) = \sum_{x,y\in\mathbb{Z}} \Upsilon\left(\frac{2xu}{X}\right)\Upsilon\left(\frac{yu}{X}\right)e\big(\theta f(2xu,yu)\big).$$

From now on, we focus exclusively on the case u is even, the other case being handled similarly. We first massage $\widehat{\mathcal{R}}_{f,u}$ further.

Since f is homogeneous quadratic, we have

$$f(xu,yu) = u^2 f(x,y).$$

Hence expressing $\theta = \frac{r}{q} + \beta$, we will need to write u^2/q as a reduced fraction; to this end, introduce the notation

$$\tilde{q} := \big(u^2, q\big) \qquad u_0 := u^2/\tilde{q}, \qquad q_0 := q/\tilde{q}, \tag{7.3}$$

so that $u^2/q = u_0/q_0$ in lowest terms, $(u_0, q_0) = 1$.

Lemma 7.1 *Recalling the notation* (5.25), *we have*

$$\widehat{\mathcal{R}}_{f,u}\Big(\frac{r}{q}+\beta\Big)=\frac{1}{u^2}\sum_{n,m\in\mathbb{Z}}\mathcal{J}_f\Big(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\Big)\mathcal{S}_f(q_0,ru_0;n,m),\quad(7.4)$$

where we have set

$$\mathcal{J}_f\Big(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\Big):=\iint\limits_{x,y\in\mathbb{R}}\Upsilon\Big(\frac{x}{X}\Big)\Upsilon\Big(\frac{y}{X}\Big)e\Big(\beta f(x,y)-\frac{n}{uq_0}x-\frac{m}{uq_0}y\Big)dxdy.\quad(7.5)$$

Proof Returning to (7.2), we have

$$\begin{aligned}\widehat{\mathcal{R}}_{f,u}\Big(\frac{r}{q}+\beta\Big)&=\sum_{x,y\in\mathbb{Z}}\Upsilon\Big(\frac{ux}{X}\Big)\Upsilon\Big(\frac{uy}{X}\Big)e_{q_0}\big(ru_0f(x,y)\big)e\big(\beta u^2f(x,y)\big)\\&=\sum_{k(q_0)}\sum_{\ell(q_0)}e_{q_0}\big(ru_0f(k,\ell)\big)\\&\quad\times\Big[\sum_{\substack{x\in\mathbb{Z}\\x\equiv k(q_0)}}\sum_{\substack{y\in\mathbb{Z}\\y\equiv\ell(q_0)}}\Upsilon\Big(\frac{ux}{X}\Big)\Upsilon\Big(\frac{uy}{X}\Big)e\big(\beta u^2f(x,y)\big)\Big].\end{aligned}$$

Apply Poisson summation to the bracketed term above:

$$\begin{aligned}[\cdot]&=\sum_{x,y\in\mathbb{Z}}\Upsilon\Big(\frac{u(q_0x+k)}{X}\Big)\Upsilon\Big(\frac{u(q_0y+\ell)}{X}\Big)e\big(\beta u^2f(q_0x+k,q_0y+\ell)\big)\\&=\sum_{n,m\in\mathbb{Z}}\iint\limits_{x,y\in\mathbb{R}}\Upsilon\Big(\frac{u(q_0x+k)}{X}\Big)\Upsilon\Big(\frac{u(q_0y+\ell)}{X}\Big)\\&\quad\times e\big(\beta u^2f(q_0x+k,q_0y+\ell)\big)\\&\quad\times e(-nx-my)dxdy\\&=\frac{1}{u^2q_0^2}\sum_{n,m\in\mathbb{Z}}e_{q_0}(nk+m\ell)\mathcal{J}_f\Big(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\Big).\end{aligned}$$

Inserting this in the above, the claim follows immediately. □

We are now in position to prove the following

Proposition 7.2 *With the above notation,*

$$\left|\widehat{\mathcal{R}}_{f,u}\left(\frac{r}{q}+\beta\right)\right| \ll u\big(\sqrt{q}|\beta|T\big)^{-1}. \tag{7.6}$$

Proof By (non)stationary phase (see, e.g., [30, §8.3]), the integral in (7.5) has negligible contribution unless

$$\frac{|n|}{uq_0}, \frac{|m|}{uq_0} \ll |\beta|\cdot|\nabla f| \ll |\beta|\cdot TX,$$

so the n, m sum can be restricted to

$$|n|, |m| \ll |\beta|\cdot TX\cdot uq_0 \ll u. \tag{7.7}$$

Here we used $|\beta| \ll (qM)^{-1}$ with M given by (3.15). In this range, stationary phase gives

$$\begin{aligned}\left|\mathcal{J}_f\left(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\right)\right| &\ll \min\left(X^2, \frac{1}{|\beta|\cdot|\operatorname{discr}(f)|^{1/2}}\right)\\ &\ll \min\left(X^2,\frac{1}{|\beta|T}\right),\end{aligned} \tag{7.8}$$

using (2.16) and (3.4) that $|\operatorname{discr}(f)| = 4|B^2-AC| = 4a^2 \gg T^2$.

Putting (7.7), (7.8) and (5.26) into (7.4), we have

$$\left|\widehat{\mathcal{R}}_{f,u}\left(\frac{r}{q}+\beta\right)\right| \ll \frac{1}{u^2}\sum_{|n|,|m|\ll u}\frac{1}{|\beta|T}\cdot\frac{1}{\sqrt{q_0}},$$

from which the claim follows, using (7.3). □

Finally, we prove the desired estimates of the strength (3.14).

Theorem 7.3 *Recall the integrals $\mathcal{I}_{Q_0,K_0}$, $\mathcal{I}_{Q_0}$ from (3.22), (3.23). There is an $\eta>0$ so that*

$$\mathcal{I}_{Q_0,K_0},\ \mathcal{I}_{Q_0} \ll N\,T^{2(\delta-1)}\,N^{-\eta},$$

as $N\to\infty$.

Proof We first handle $\mathcal{I}_{Q_0,K_0}$. Returning to (7.1) and applying (7.6) gives

$$\left|\widehat{\mathcal{R}_N^U}\left(\frac{r}{q}+\beta\right)\right| \ll \sum_{u<U}\sum_{\mathfrak{f}\in\mathfrak{F}} u\big(\sqrt{q}|\beta|T\big)^{-1} \ll U^2T^{\delta-1}\big(\sqrt{q}|\beta|\big)^{-1}.$$

Inserting this into (3.22) and using (6.2), (6.3) gives

$$\mathcal{I}_{Q_0,K_0} \ll \sum_{q<Q_0} \sideset{}{'}\sum_{r(q)} \int_{|\beta|<K_0/N} \left|\beta \frac{N}{K_0}\right|^2 U^4 T^{2(\delta-1)} \frac{1}{q|\beta|^2} d\beta$$
$$\ll Q_0 \frac{N}{K_0} U^4 T^{2(\delta-1)} \ll N T^{2(\delta-1)} N^{-\eta}.$$

Next we handle

$$\mathcal{I}_{Q_0} \ll \sum_{q<Q_0} \sideset{}{'}\sum_{r(q)} \int_{\frac{K_0}{N}<|\beta|<\frac{1}{qM}} U^4 T^{2(\delta-1)} \frac{1}{q|\beta|^2} d\beta$$
$$\ll Q_0 U^4 T^{2(\delta-1)} \left(\frac{N}{K_0} + Q_0 M\right)$$
$$\ll N T^{2(\delta-1)} \frac{Q_0 U^4}{K_0},$$

which is again a power savings. □

8 Minor arcs II: case $Q_0 \le Q < X$

Keeping all the notation from the last section, we now turn our attention to the integrals $\mathcal{I}_Q$ in (3.24). It is no longer sufficient just to get cancellation in $\widehat{\mathcal{R}}_{f,u}$ alone, as in (7.6); we must use the fact that $\mathcal{I}_Q$ is an L^2-norm.

To this end, recall the notation (7.3), and put (7.4) into (7.1), applying Cauchy-Schwarz in the u-variable:

$$\left|\widehat{\mathcal{R}_N^U}\left(\frac{r}{q}+\beta\right)\right|^2 \ll U \sum_{u<U} \left|\sum_{\mathfrak{f}\in\mathfrak{F}} e_q(-ra) e(-a\beta)\right.$$
$$\left. \times \frac{1}{u^2} \sum_{n,m\in\mathbb{Z}} \mathcal{J}_f\left(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\right) \mathcal{S}_f(q_0, ru_0; n, m)\right|^2. \tag{8.1}$$

Recall from (2.14) that $\mathfrak{f} = f - a$. Insert (8.1) into (3.24) and open the square, setting $\mathfrak{f}' = f' - a'$. This gives

$$\begin{aligned}\mathcal{I}_Q &\ll U\sum_{u<U}\frac{1}{u^4}\sum_{q\asymp Q}{\sum_{r(q)}}'\int_{|\beta|<\frac{1}{qM}}\Big|\sum_{\mathfrak{f}\in\mathfrak{F}}e_q(-ra)e(-a\beta)\\ &\quad\times\sum_{n,m\in\mathbb{Z}}\mathcal{J}_f\Big(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\Big)\mathcal{S}_f(q_0,ru_0;n,m)\Big|^2d\beta\\ &= U\sum_{u<U}\frac{1}{u^4}\sum_{n,m,n',m'\in\mathbb{Z}}\sum_{\mathfrak{f},\mathfrak{f}'\in\mathfrak{F}}\sum_{q\asymp Q}\Big[{\sum_{r(q)}}'\mathcal{S}_f(q_0,ru_0;n,m)\\ &\quad\times\overline{\mathcal{S}_{f'}(q_0,ru_0;n',m')}e_q\big(r(a'-a)\big)\Big]\\ &\quad\times\Big[\int_{|\beta|<\frac{1}{qM}}\mathcal{J}_f\Big(X,\beta;\frac{n}{uq_0},\frac{m}{uq_0}\Big)\\ &\quad\times\overline{\mathcal{J}_{f'}\Big(X,\beta;\frac{n'}{uq_0},\frac{m'}{uq_0}\Big)}e\big(\beta(a'-a)\big)d\beta\Big].\end{aligned}\tag{8.2}$$

Note that again the sum has split into "modular" and "Archimedean" pieces (collected in brackets, respectively), with the former being exactly equal to $\mathcal{S}$ in (5.30).

Decompose (8.2) as

$$\mathcal{I}_Q \ll \mathcal{I}_Q^{(=)}+\mathcal{I}_Q^{(\neq)},\tag{8.3}$$

where, once $\mathfrak{f}$ is fixed, we collect $\mathfrak{f}'$ according to whether $a'=a$ (the "diagonal" case) and the off-diagonal $a'\neq a$.

Lemma 8.1 *Assume $Q<X$. For $\square\in\{=,\neq\}$, we have*

$$\mathcal{I}_Q^{(\square)}\ll U^6\frac{X^2}{T}\sum_{\mathfrak{f}\in\mathfrak{F}}\sum_{\substack{\mathfrak{f}'\in\mathfrak{F}\\ a'\square a}}\sum_{q\asymp Q}\frac{\{(a^2,q)\cdot((a')^2,q)\}^{1/2}(a-a',q)^{1/4}}{q^{5/4}}.\tag{8.4}$$

Proof Apply (5.31) and (7.7), (7.8) to (8.2), giving

$$\begin{aligned}\mathcal{I}_Q^{(\square)}&\ll U\sum_{u<U}\frac{1}{u^4}\\ &\quad\times\sum_{|n|,|m|,|n'|,|m'|\ll u}\sum_{\substack{\mathfrak{f},\mathfrak{f}'\in\mathfrak{F}\\ a'\square a}}\sum_{q\asymp Q}\frac{u^4\{(a^2,q)\cdot((a')^2,q)\}^{1/2}(a-a',q)^{1/4}}{q^{5/4}}\\ &\quad\times\int_{|\beta|<1/(qM)}\min\Big(X^2,\frac{1}{|\beta|T}\Big)^2d\beta,\end{aligned}$$

where we used (7.3). The claim then follows immediately from (3.15) and $Q < X$. □

We treat $\mathcal{I}_Q^{(=)}$, $\mathcal{I}_Q^{(\neq)}$ separately, starting with the former; we give bounds of the quality claimed in (3.14).

Proposition 8.2 *There is an $\eta > 0$ such that*

$$\mathcal{I}_Q^{(=)} \ll N T^{2(\delta-1)} N^{-\eta}, \tag{8.5}$$

as $N \to \infty$.

Proof From (8.4), we have

$$\begin{aligned}
\mathcal{I}_Q^{(=)} &\ll U^6 \frac{X^2}{T} \sum_{\mathfrak{f} \in \mathfrak{F}} \sum_{\substack{\mathfrak{f}' \in \mathfrak{F} \\ a' = a}} \sum_{q \asymp Q} \frac{(a^2, q)}{q} \\
&\ll \frac{U^6 X^2}{QT} \sum_{\mathfrak{f} \in \mathfrak{F}} \sum_{\substack{\tilde{q}_1 \mid a^2 \\ \tilde{q}_1 \ll Q}} \tilde{q}_1 \sum_{\substack{q \asymp Q \\ q \equiv 0 (\tilde{q}_1)}} \sum_{\substack{\mathfrak{f}' \in \mathfrak{F} \\ a' = a}} 1 \\
&\ll_\varepsilon \frac{U^6 X^2}{T} \sum_{\mathfrak{f} \in \mathfrak{F}} T^\varepsilon \sum_{\substack{\mathfrak{f}' \in \mathfrak{F} \\ a' = a}} 1.
\end{aligned}$$

Recalling that $a = a_\gamma = \langle e_1, \gamma v_0 \rangle$, replace the condition $a' = a$ with $a' \equiv a (\mathrm{mod} \lfloor Q_0 \rfloor)$, and apply (5.12):

$$\mathcal{I}_Q^{(=)} \ll_\varepsilon \frac{U^6 X^2}{T} T^\delta T^\varepsilon \frac{T^\delta}{Q_0^{\eta_0}}.$$

Then (6.3) and (3.1) imply the claimed power savings. □

Next we turn our attention to $\mathcal{I}_Q^{(\neq)}$, the off-diagonal contribution. We decompose this sum further according to whether $\gcd(a, a')$ is large or not. To this end, introduce a parameter H, which we will eventually set to

$$H = U^{10/\eta_0} = {Q_0}^{\eta_0/10}, \tag{8.6}$$

where, as in (6.3), the constant $\eta_0 > 0$ comes from Lemma 5.2. Write

$$\mathcal{I}_Q^{(\neq)} = \mathcal{I}_Q^{(\neq,>)} + \mathcal{I}_Q^{(\neq,\leq)}, \tag{8.7}$$

corresponding to whether $(a, a') > H$ or $(a, a') \leq H$, respectively. We deal first with the large gcd.

Proposition 8.3 *There is an $\eta > 0$ such that*

$$\mathcal{I}_Q^{(\neq,>)} \ll N\, T^{2(\delta-1)} N^{-\eta}, \tag{8.8}$$

as $N \to \infty$.

Proof Writing $(a, a') = h > H$, $\tilde{q}_1 = (a^2, q)$, $\tilde{q}_1' = ((a')^2, q)$, and using $(a - a', q) \le q$ in (8.4), we have

$$\begin{aligned}
\mathcal{I}_Q^{(\neq,>)} &\ll U^6 \frac{X^2}{T} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\neq a,(a,a')>H}} \sum_{q\asymp Q} \frac{\{(a^2,q)\cdot((a')^2,q)\}^{1/2}(a-a',q)^{1/4}}{q^{5/4}} \\
&\ll U^6 \frac{X^2}{T} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{h\mid a \\ h>H}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\equiv 0 (\mathrm{mod}\, h)}} \sum_{\substack{\tilde{q}_1\mid a^2 \\ \tilde{q}_1\ll Q}} \sum_{\substack{\tilde{q}_1'\mid (a')^2 \\ [\tilde{q}_1,\tilde{q}_1']\ll Q}} \left(\tilde{q}_1\tilde{q}_1'\right)^{1/2} \sum_{\substack{q\asymp Q \\ q\equiv 0([\tilde{q}_1,\tilde{q}_1'])}} \frac{1}{Q} \\
&\ll_\varepsilon U^6 \frac{X^2}{T} T^\varepsilon \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{h\mid a \\ h>H}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\equiv 0(\mathrm{mod}\, h)}} 1,
\end{aligned}$$

where we used $[n, m] > (nm)^{1/2}$. Apply (5.12) to the innermost sum, getting

$$\mathcal{I}_Q^{(\neq,>)} \ll_\varepsilon U^6 \frac{X^2}{T} T^\varepsilon T^\delta \frac{1}{H^{\eta_0}} T^\delta.$$

By (8.6) and (6.3), this is a power savings, as claimed. □

Finally, we handle small gcd.

Proposition 8.4 *There is an $\eta > 0$ such that*

$$\mathcal{I}_Q^{(\neq,\le)} \ll N\, T^{2(\delta-1)} N^{-\eta}, \tag{8.9}$$

as $N \to \infty$.

Proof First note that

$$\begin{aligned}
\mathcal{I}_Q^{(\neq,\le)} &= U^6 \frac{X^2}{T} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\neq a,(a,a')\le H}} \sum_{q\asymp Q} \frac{\{(a^2,q)\cdot((a')^2,q)\}^{1/2}(a-a',q)^{1/4}}{q^{5/4}} \\
&\ll U^6 \frac{X^2}{T} \frac{1}{Q^{5/4}} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\neq a,(a,a')\le H}} \sum_{q\asymp Q} (a,q)\left(a',q\right)\left(a-a',q\right)^{1/4}.
\end{aligned}$$

Write $g = (a, q)$ and $g' = (a', q)$, and let $h = (g, g')$; observe then that $h \mid (a, a')$ and $h \ll Q$. Hence we can write $g = hg_1$ and $g' = hg_1'$ so that $(g_1, g_1') = 1$. Note also that $h \mid (a - a', q)$, so we can write $(a - a', q) = h\tilde{g}$; thus g_1, g_1', and $\tilde{g}$ are pairwise coprime, implying

$$\big[hg_1, hg_1', h\tilde{g}\big] \geq g_1 g_1' \tilde{g}.$$

Then we have

$$\begin{aligned}
\mathcal{I}_Q^{(\neq,\leq)} &\ll U^6 \frac{X^2}{T} \frac{1}{Q^{5/4}} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\neq a,(a,a')\leq H}} \sum_{\substack{h\mid(a,a') \\ h\leq H}} \sum_{\substack{g_1\mid a \\ g_1\ll Q}} \sum_{\substack{g_1'\mid a' \\ g_1'\ll Q}} \\
&\quad \times \sum_{\substack{\tilde{g}\mid(a-a') \\ [hg_1,hg_1',h\tilde{g}]\ll Q}} (hg_1)\big(hg_1'\big)(h\tilde{g})^{1/4} \sum_{\substack{q\asymp Q \\ q\equiv 0([hg_1,hg_1',h\tilde{g}])}} 1 \\
&\ll_\varepsilon U^6 \frac{X^2}{T} \frac{H^{9/4}}{Q^{5/4}} \sum_{\mathfrak{f},\mathfrak{f}'\in\mathfrak{F}} T^\varepsilon \sum_{\substack{g_1\mid a \\ g_1\ll Q}} \sum_{\substack{g_1'\mid a' \\ g_1'\ll Q}} \sum_{\substack{\tilde{g}\mid(a-a') \\ \tilde{g}\ll Q}} g_1\, g_1'\, \tilde{g}^{1/4} \frac{Q}{g_1 g_1' \tilde{g}} \\
&\ll U^6 \frac{X^2}{T} \frac{H^{9/4}}{Q^{1/4}} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\tilde{g}\ll Q} \frac{1}{\tilde{g}^{3/4}} T^\varepsilon \sum_{\substack{\mathfrak{f}'\in\mathfrak{F} \\ a'\equiv a(\mathrm{mod}\,\tilde{g})}} 1.
\end{aligned}$$

To the last sum, we again apply Lemma 5.2, giving

$$\mathcal{I}_Q^{(\neq,\leq)} \ll_\varepsilon U^6 \frac{X^2}{T} \frac{H^{9/4}}{Q^{1/4}} T^\delta \sum_{\tilde{g}\ll Q} \frac{1}{\tilde{g}^{3/4}} T^\varepsilon \frac{1}{\tilde{g}^{\eta_0}} T^\delta \ll U^6 \frac{X^2}{T} \frac{H^{9/4}}{Q_0^{\eta_0}} T^\delta T^\varepsilon T^\delta,$$

since $Q \geq Q_0$. By (8.6) and (6.3), this is again a power savings, as claimed. □

Putting together (8.3), (8.5), (8.7), (8.8), and (8.9), we have proved the following

Theorem 8.5 *For $Q_0 \leq Q < X$, there is some $\eta > 0$ such that*

$$\mathcal{I}_Q \ll N\, T^{2(\delta-1)}\, N^{-\eta},$$

as $N \to \infty$.

9 Minor arcs III: case $X \leq Q < M$

In this section, we continue our analysis of $\mathcal{I}_Q$ from (3.24), but now we need different methods to handle the very large Q situation. In particular, the range

of x, y in (7.2) is now such that we have incomplete sums, so our first step is to complete them.

To this end, recall the notation (7.3) and introduce

$$\lambda_f\Big(X,\beta;\frac{n}{q_0},\frac{m}{q_0},u\Big):=\sum_{x,y\in\mathbb{Z}}\Upsilon\Big(\frac{ux}{X}\Big)\Upsilon\Big(\frac{uy}{X}\Big)e\Big(-\frac{n}{q_0}x-\frac{m}{q_0}y\Big)\times e\big(\beta u^2 f(x,y)\big),\tag{9.1}$$

so that, using (5.25), an elementary calculation gives

$$\widehat{\mathcal{R}}_{f,u}\Big(\frac{r}{q}+\beta\Big)=\sum_{n(q_0)}\sum_{m(q_0)}\lambda_f\Big(X,\beta;\frac{n}{q_0},\frac{m}{q_0},u\Big)\mathcal{S}_f(q_0,ru_0;n,m).\tag{9.2}$$

Put (9.2) into (7.1) and apply Cauchy-Schwarz in the u-variable:

$$\Big|\widehat{\mathcal{R}_N^U}\Big(\frac{r}{q}+\beta\Big)\Big|^2\ll U\sum_{u<U}\Big|\sum_{\mathfrak{f}\in\mathfrak{F}}e_q(-ra)e(-a\beta)\times\sum_{0\le n,m<q_0}\lambda_f\Big(X,\beta;\frac{n}{q_0},\frac{m}{q_0},u\Big)\mathcal{S}_f(q_0,ru_0;n,m)\Big|^2.\tag{9.3}$$

As before, open the square, setting $\mathfrak{f}'=f'-a'$, and insert the result into (3.24):

$$\begin{aligned}\mathcal{I}_Q\ll U\sum_{u<U}\sum_{q\asymp Q}\sum_{n,m,n',m'<q_0}\sum_{\mathfrak{f},\mathfrak{f}'\in\mathfrak{F}}\Big[\sum_{r(q)}{}'\mathcal{S}_f(q_0,ru_0;n,m)\\ \times\overline{\mathcal{S}_{f'}(q_0,ru_0;n',m')}e_q\big(r(a'-a)\big)\Big]\\ \times\Big[\int_{|\beta|<1/(qM)}\lambda_f\Big(X,\beta;\frac{n}{q_0},\frac{m}{q_0},u\Big)\overline{\lambda_{f'}\Big(X,\beta;\frac{n'}{q_0},\frac{m'}{q_0},u\Big)}\\ \times e\big(\beta(a-a')\big)d\beta\Big].\end{aligned}\tag{9.4}$$

Yet again the sum has split into modular and Archimedean components with the former being exactly equal to $\mathcal{S}$ in (5.30). As before, decompose $\mathcal{I}_Q$ according to the diagonal ($a=a'$) and off-diagonal terms:

$$\mathcal{I}_Q\ll\mathcal{I}_Q^{(=)}+\mathcal{I}_Q^{(\neq)}.\tag{9.5}$$

Lemma 9.1 *Assume $Q \geq X$. For $\square \in \{=, \neq\}$, we have*

$$\mathcal{I}_Q^{(\square)} \ll \frac{UX^3}{QT} \sum_{u<U} \frac{1}{u^4} \sum_{q \asymp Q} \sum_{n,m,n',m' \ll \frac{UQ}{X}} \sum_{\mathfrak{f} \in \mathfrak{F}} \sum_{\substack{\mathfrak{f}' \in \mathfrak{F} \\ a' \square a}} |\mathcal{S}|. \tag{9.6}$$

Proof Consider the sum λ_f in (9.1). Since $x, y \asymp X/u$, $|\beta| < 1/(qM)$, $X \leq Q$, and using (3.15), we have that

$$\left|\beta u^2 f(x, y)\right| \ll \frac{1}{QM} u^2 T \left(\frac{X}{u}\right)^2 = \frac{X}{Q} \leq 1.$$

Hence there is contribution only if $nx/q_0, my/q_0 \ll 1$, that is, we may restrict to the range

$$n, m \ll uq_0/X.$$

In this range, we give λ_f the trivial bound of X^2/u^2. Putting this analysis into (9.4), the claim follows. □

We handle the off-diagonal term first.

Proposition 9.2 *Assuming $X \leq Q < M$, there is some $\eta > 0$ such that*

$$\mathcal{I}_Q^{(\neq)} \ll N T^{2(\delta-1)} N^{-\eta}, \tag{9.7}$$

as $N \to \infty$.

Proof Since (5.31) is such a large savings in $q > X$, we can afford to lose in the much smaller variable T. Hence put (5.31) into (9.6), estimating $(a - a', q) \leq |a - a'|$ (since $a \neq a'$):

$$\begin{aligned}
\mathcal{I}_Q^{(\neq)} &\ll \frac{UX^3}{QT} \sum_{u<U} \frac{1}{u^4} \sum_{q \asymp Q} \sum_{n,m,n',m' \ll \frac{UQ}{X}} \sum_{\mathfrak{f},\mathfrak{f}' \in \mathfrak{F}} u^4 \frac{a \cdot a'}{q^{5/4}} \left|a - a'\right|^{1/4} \\
&\ll \frac{U^6 X^3}{T} \left(\frac{Q}{X}\right)^4 T^{2\delta} \frac{T^2}{Q^{5/4}} T^{1/4} \\
&\ll U^6 X^{7/4} T^{2\delta} T^4 = X^2 T\, T^{2(\delta-1)} \left(U^6 X^{-1/4} T^5\right),
\end{aligned}$$

where we used (7.3), $Q < M$, and (3.15). Using (3.1) we have that

$$X^{-1/4} T^5 = N^{-59/800}, \tag{9.8}$$

so together with (6.3), this is clearly a substantial power savings. □

Lastly, we deal with the diagonal term. We no longer save enough from $a = a'$ alone. But recall that here more cancellation can be gotten from (5.33) in the special case that $\mathfrak{f}(m, -n) \neq \mathfrak{f}'(m', -n')$. Hence we return to (9.6) and, once n, m, and $\mathfrak{f}$ are determined, separate n', m', and $\mathfrak{f}'$ into cases corresponding to whether $\mathfrak{f}(m, -n) = \mathfrak{f}'(m', -n')$ or not. Accordingly, write

$$\mathcal{I}_Q^{(=)} = \mathcal{I}_Q^{(=,=)} + \mathcal{I}_Q^{(=,\neq)}. \tag{9.9}$$

We now estimate $\mathcal{I}_Q^{(=,\neq)}$ using the extra cancellation in (5.33).

Proposition 9.3 *Assuming $Q < XT$, there is some $\eta > 0$ such that*

$$\mathcal{I}_Q^{(=,\neq)} \ll N\, T^{2(\delta-1)}\, N^{-\eta}, \tag{9.10}$$

as $N \to \infty$.

Proof Returning to (9.6), apply (5.33):

$$\begin{aligned}
\mathcal{I}_Q^{(=,\neq)} &\ll \frac{UX^3}{QT} \sum_{u<U} \frac{1}{u^4} \sum_{\mathfrak{f}\in\mathfrak{F}} \sum_{\substack{\mathfrak{f}'\in\mathfrak{F}\\ a'=a}} \sum_{q\asymp Q} \sum_{n,m\ll \frac{UQ}{X}} \sum_{\substack{n',m'\ll \frac{UQ}{X}\\ \mathfrak{f}(m,-n)\neq\mathfrak{f}'(m',-n')}} |\mathcal{S}| \\
&\ll \frac{UX^3}{QT} \sum_{u<U} \frac{1}{u^4} \sum_{\mathfrak{f},\mathfrak{f}'\in\mathfrak{F}} \sum_{\substack{\tilde{q}_1 | a^2\\ \tilde{q}_1 \ll Q}} \sum_{\substack{q\asymp Q\\ q\equiv 0(\tilde{q}_1)}} \sum_{n,m,n',m'\ll \frac{UQ}{X}} u^{10} \frac{\tilde{q}_1}{Q^{9/8}} \\
&\quad \times \left(T\left(\frac{UQ}{X}\right)^2 \right)^{1/2} \\
&\ll_\varepsilon \frac{U^8X^3}{T} T^{2\delta}\, T^\varepsilon \left(\frac{UQ}{X}\right)^4 \frac{1}{Q^{9/8}} T^{1/2} \frac{UQ}{X} \\
&\ll X^2T\; T^{2(\delta-1)} \left(X^{-1/8} T^{35/8} U^{13} T^\varepsilon\right),
\end{aligned}$$

where we used that $\mathfrak{f}(m, n) \ll T(UQ/X)^2$ and $Q < XT$. From (3.1), we have

$$X^{-1/8} T^{35/8} = N^{-29/1600}, \tag{9.11}$$

so we have again a power savings, as claimed. □

Lastly, we turn to the case $\mathcal{I}_Q^{(=,=)}$, with $\mathfrak{f}(m, -n) = \mathfrak{f}'(m', -n')$. We exploit this condition to get savings using (5.47).

Proposition 9.4 *Assuming $Q < XT$, there is some $\eta > 0$ such that*

$$\mathcal{I}_Q^{(=,=)} \ll N\, T^{2(\delta-1)}\, N^{-\eta}, \tag{9.12}$$

as $N \to \infty$.

Proof Returning to (9.6), apply (5.31), and (5.47):

$$\begin{aligned}
\mathcal{I}_Q^{(=,=)} &\ll \frac{UX^3}{QT} \sum_{u<U} \frac{1}{u^4} \sum_{q \asymp Q} \sum_{n,m \ll \frac{UQ}{X}} \sum_{\mathfrak{f} \in \mathfrak{F}} \sum_{\substack{\mathfrak{f}' \in \mathfrak{F} \\ a'=a}} \sum_{\substack{n',m' \ll UQ/X \\ \mathfrak{f}(m,-n)=\mathfrak{f}'(m',-n')}} u^4 \frac{(a^2,q)}{q^{5/4}} q^{1/4} \\
&\ll \frac{UX^3}{Q^2T} \sum_{u<U} \sum_{\mathfrak{f} \in \mathfrak{F}} \sum_{\substack{\tilde{q}_1 \mid a^2 \\ \tilde{q}_1 \ll Q}} \tilde{q}_1 \sum_{\substack{q \asymp Q \\ q \equiv 0 (\tilde{q}_1)}} \Bigg[\sum_{n,m \ll \frac{UQ}{X}} \sum_{\substack{\mathfrak{f}' \in \mathfrak{F} \\ a'=a}} \sum_{\substack{n',m' \ll UQ/X \\ \mathfrak{f}(m,-n)=\mathfrak{f}'(m',-n')}} 1 \Bigg] \\
&\ll_\varepsilon N^\varepsilon \frac{UX^3}{Q^2T} UT^\delta Q \left[\left(\frac{UQ}{X} \right)^2 + T \frac{UQ}{X} \right] \\
&\ll_\varepsilon N^\varepsilon U^4 X^2 T^\delta \ll X^2 T\, T^{2(\delta-1)} \left(T^{1-\delta} U^4 N^\varepsilon \right).
\end{aligned}$$

From (4.2), this is a power savings. □

Combining (9.5), (9.7), (9.9), (9.10), and (9.12), we have the following

Theorem 9.5 *If $X \leq Q < M$, then there is some $\eta > 0$ so that*

$$\mathcal{I}_Q \ll N\, T^{2(\delta-1)}\, N^{-\eta},$$

as $N \to \infty$.

Finally, Theorems 7.3, 8.5, and 9.5 together complete the proof of (3.14), and hence Theorem 1.2 is proved.

Acknowledgements The authors are grateful to Peter Sarnak for illuminating discussions, and many detailed comments improving the exposition of an earlier version of this paper. We thank Tim Browning, Sam Chow, Hee Oh, Xin Zhang, and the referee for numerous corrections and suggestions.

Appendix: Spectral gap for the Apollonian group (by Péter P. Varjú[1])

In recent years some spectacular advances were made on estimating spectral gaps (to be defined below) of infinite co-volume subgroups of $\mathrm{SL}(d, \mathbb{Z})$.

[1] P.P. Varjú
University of Cambridge, Cambridge CB3 0WA, UK
e-mail: pv270@dpmms.cam.ac.uk

Bourgain and Gamburd [6] proved uniform spectral gap estimates for Zariski-dense subgroups of $\mathrm{SL}(2,\mathbb{Z})$ under the additional assumption that the modulus q is prime. One of the crucial ideas in their paper is the application of Helfgott's triple-product theorem [28]. The result in [6] was generalized in a series of papers [5, 7, 10, 11, 48] and [40]. Some of these require the generalization of [28] obtained independently by Breuillard, Green and Tao [14] and Pyber and Szabó [39].

In particular, Bourgain and Varjú [10, Theorem 1] proved the spectral gap for Zariski-dense subgroups of $\mathrm{SL}(d,\mathbb{Z})$ without any restriction for the modulus q. Salehi Golsefidy and Varjú [40, Theorem 1] obtained the result for Zariski-dense subgroups of perfect arithmetic groups, but only for square-free q. Unfortunately, these results do not cover Theorem 4.3; the first one is not applicable to the Apollonian group, the second one is restricted for the moduli.

In this appendix, we present an approach which differs from those discussed above. This is much simpler and probably would give better numerical results, but we do not pursue explicit bounds. However, our method depends on special properties of the Apollonian group and does not apply to general Zariski-dense subgroups.

Recall from Sect. 2 that the preimage of the Apollonian group under the homomorphism

$$\iota : \mathrm{SL}(2,\mathbb{C}) \to \mathrm{SO}_F(\mathbb{R})$$

is generated by the matrices

$$\pm\begin{pmatrix} 1 & 4i \\ 0 & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} 2 & -i \\ -i & 0 \end{pmatrix}, \qquad \pm\begin{pmatrix} 2+2i & 4+3i \\ -i & -2i \end{pmatrix}. \tag{A.1}$$

We describe an automorphism of $\mathrm{SL}(2,\mathbb{Z}[i])$ which transforms the above generators to matrices that will be more convenient to work with. Set $A := \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$. A simple calculation shows that the image of the matrices (A.1) under the map $g \mapsto A^{-1} g A$ are

$$\pm\begin{pmatrix} 1 & 4i \\ 0 & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} 1 & 0 \\ -i & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} 1+2i & 4i \\ -i & 1-2i \end{pmatrix}.$$

We put

$$\gamma_1 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \qquad \gamma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \gamma_3 = \begin{pmatrix} 1+2i & 4 \\ 1 & 1-2i \end{pmatrix}. \tag{A.2}$$

These are the image of (A.1) under the product of two isomorphism: first conjugation by A and then multiplication of the off-diagonal elements by $-i$

and i. We denote by $\bar{\Gamma}$ the group generated by $\bar{S} = \{\pm\gamma_1^{\pm 1}, \pm\gamma_2^{\pm 1}, \pm\gamma_3^{\pm 1}\}$. This is isomorphic to the group denoted by the same symbol in the paper.

First we recall two different notions of spectral gap. The notion, "geometric" spectral gap, has already been explained in Sect. 4.2. Recall that for an integer q, $\bar{\Gamma}(q)$ denotes the kernel of the projection map $\bar{\Gamma} \to \mathrm{SL}(2, \mathbb{Z}[i]/(q))$. We consider the Laplace Beltrami operator Δ on the hyperbolic orbifolds $\bar{\Gamma}(q)\backslash\mathbb{H}^3$. We denote by $\lambda_0(q) \leq \lambda_1(q)$ the two smallest eigenvalues of Δ on $\bar{\Gamma}(q)\backslash\mathbb{H}^3$. The geometric spectral gap is an inequality of the form $\lambda_1(q) > \lambda_0(q) + \varepsilon$ for some $\varepsilon > 0$ independent of q.

The other notion, "combinatorial" spectral gap is defined as follows. Let G be a finite group, and S a symmetric set of generators. Let $T_{G,S}$ be the Markov operator on the space $L^2(G)$ defined by

$$T_{G,S} f(g) = \frac{1}{|S|} \sum_{\gamma \in S} f(\gamma g)$$

for $f \in L^2(G)$ and $g \in G$. We denote by

$$\lambda'_n(G, S) \leq \cdots \leq \lambda'_1(G, S) \leq \lambda'_0(G, S) = 1$$

the eigenvalues of $T_{G,S}$ in increasing order.

The operator $Id - T_{\bar{\Gamma}/\bar{\Gamma}(q)}$ is a discrete analogue of the Laplacian Δ on $\bar{\Gamma}(q)\backslash\mathbb{H}^3$. So by combinatorial spectral gap we mean the inequality

$$\lambda'_1\big(\bar{\Gamma}/\bar{\Gamma}(q), \bar{S}\big) < 1 - \varepsilon$$

for some $\varepsilon > 0$ independent of q. To simplify notation, we will write $\lambda'_1(q) = \lambda'_1(\bar{\Gamma}/\bar{\Gamma}(q), \bar{S})$.

The relation between the two notions is not just an analogy. It was shown by Brooks [15, Theorem 1] and Burger [17–19] that they are equivalent for the fundamental groups of a family of covers of a compact manifold. The orbifolds $\bar{\Gamma}(q)\backslash\mathbb{H}^3$ are not compact, they even have infinite volume, however the equivalence can be extended to cover our example, see [13, Theorems 1.2 and 2.1].

We show that the congruence subgroups $\bar{\Gamma}(q)$ of the Apollonian group have combinatorial spectral gap which implies Theorem 4.3 in light of [13, Theorems 1.2 and 2.1].

Theorem A.1 *Let $\bar{\Gamma}$ be the Apollonian group and $\lambda'_1(q)$ be as above. There is an absolute constant $c > 0$ such that $\lambda'_1(q) < 1 - c$ for all q. I.e. the Apollonian group has combinatorial spectral gap.*

Denote by Γ_1 and Γ_2 respectively, the groups generated by $\{\gamma_1, \gamma_2\}$ and $\{\gamma_1, \gamma_3\}$ respectively. Denote by $\mathbf{G}_1$ and $\mathbf{G}_2$ the Zariski-closures of Γ_1 and Γ_2 in $\mathrm{Res}_{\mathbb{R}|\mathbb{C}}\,\mathrm{SL}(2,\mathbb{C})$, i.e. in $\mathrm{SL}(2,\mathbb{C})$ considered an algebraic group over $\mathbb{R}$.

As we will see later, $\mathbf{G}_1$ and $\mathbf{G}_2$ are isomorphic to $\mathrm{SL}(2,\mathbb{R})$. Moreover Γ_1 and Γ_2 are lattices inside them. This feature of the Apollonian group was pointed out by Sarnak [42]. We exploit it heavily in our approach.

Due to a result going back to Selberg [44], Γ_1 and Γ_2 have geometric spectral gaps with respect to the congruence subgroups. From here we can deduce the combinatorial spectral gap using Brooks [15, Theorem 1] (see also [16, Theorem 1], where the non-compact case is considered.)

We transfer the combinatorial spectral gap property of Γ_1 and Γ_2 to the Apollonian group $\bar{\Gamma}$ and conclude Theorem A.1. This is done in following two Lemmata:

Lemma A.2 *Let G be a finite group and $S \subset G$ a finite symmetric generating set. Let $G_1, G_2, \ldots, G_k$ be subgroups of G such that for every $g \in G$ there are $g_1 \in G_1, \ldots, g_k \in G_k$ such that $g = g_1 \cdots g_k$. Then*

$$1 - \lambda_1'(G,S) \geq \min_{1\leq i\leq k} \left\{ \frac{|S \cap G_i|}{|S|} \cdot \frac{1 - \lambda_1'(G_i, S \cap G_i)}{2k^2} \right\}.$$

The above Lemma and its proof below is closely related to the well-known fact that if G is generated by S in k steps then one has $\lambda_1'(G,S) \leq 1 - 1/|S|k^2$. This can be found for example in [21, Corollary 1 on page 2138]. After circulating an earlier version of this appendix, it was pointed out to me that an idea similar to Lemma A.2 has been used by Sarnak [41, Sect. 2.4], by Shalom [45], and also by Kassabov, Lubotzky and Nikolov [31].

Lemma A.3 *Let $q \geq 2$ be an integer. Then for every $g \in \bar{\Gamma}/\bar{\Gamma}(q)$, there are $g_1, \ldots, g_{10^{13}} \in \Gamma_1/\Gamma_1(q)$ and $h_1, \ldots, h_{10^{13}} \in \Gamma_2/\Gamma_2(q)$ such that $g = g_1 h_1 \cdots g_{10^{13}} h_{10^{13}}$.*

Lemma A.3 enables us to apply Lemma A.2 with $k = 2 \cdot 10^{13}$ and $G_i = \Gamma_1/\Gamma_1(q)$ for odd i and $G_i = \Gamma_2/\Gamma_2(q)$ for even i. Now [44] and [16, Theorem 1] provides us with lower bounds on

$$1 - \lambda_1'\big(\Gamma_1/\Gamma_1(q), \{\pm\gamma_1^{\pm 1}, \pm\gamma_2^{\pm 1}\}\big) \quad \text{and}$$
$$1 - \lambda_1'\big(\Gamma_2/\Gamma_2(q), \{\pm\gamma_1^{\pm 1}, \pm\gamma_3^{\pm 1}\}\big).$$

Therefore Theorem A.1 is proved once the two Lemmata are proved.

Before we proceed with the proofs, we make two remarks. First, we note that instead of [44] we could just as well use [10, Theorem 1]. Second, we suggest that the constant 10^{13} in Lemma A.3 is not optimal. In particular, the

argument we present would give 72 if the statement is checked for $q = 2^7 \cdot 3$, e.g. by a computer program. Certainly there is further room for improvement but we make no efforts to optimize the constants.

Proof of Lemma A.2 Denote by π the regular representation of G, i.e. we write

$$\pi(g_0) f(g) = f\left(g_0^{-1} g\right)$$

for $f \in L^2(G)$ and $g, g_0 \in G$. Let $T_{G,S}$ be the Markov operator defined above. Let $f_0 \in L^2(G)$ be an eigenfunction with $\|f_0\|_2 = 1$ corresponding to $\lambda_1'(G, S)$. It is orthogonal to the constant and

$$\langle T_{G,S} f_0, f_0 \rangle = \lambda_1'(G, S).$$

Since f_0 is orthogonal to the constant, we have

$$\sum_{g \in G} \langle \pi(g) f_0, f_0 \rangle = \left| \langle f_0, 1 \rangle \right|^2 = 0.$$

Thus there is $g_0 \in G$ such that $\langle \pi(g_0) f_0, f_0 \rangle \leq 0$ and hence $\|\pi(g_0) f_0 - f_0\|_2 \geq \sqrt{2}$.

By the hypothesis of the lemma, there are $g_i \in G_i$ for $1 \leq i \leq k$ such that $g_0 = g_1 \cdots g_k$. By the triangle inequality, there is some $1 \leq i_0 \leq k$ such that

$$\left\| \pi(g_1 \cdots g_{i_0 - 1}) f_0 - \pi(g_1 \cdots g_{i_0}) f_0 \right\|_2 \geq \sqrt{2}/k.$$

Since π is unitary, we have $\| f_0 - \pi(g_{i_0}) f_0 \|_2 \geq \sqrt{2}/k$.

We write $f_0 = f_1 + f_2$ such that f_1 is invariant under the elements of G_{i_0} in the regular representation π and f_2 is orthogonal to the space of functions invariant under G_{i_0}. Then

$$\sqrt{2}/k \leq \left\| f_0 - \pi(g_{i_0}) f_0 \right\|_2 = \left\| f_2 - \pi(g_{i_0}) f_2 \right\|_2 \leq 2 \| f_2 \|_2.$$

Thus $\| f_2 \|_2 \geq 1/\sqrt{2}k$.

Now we can write

$$\begin{aligned} \langle T_{G, S \cap G_{i_0}} f_0, f_0 \rangle &= \| f_1 \|_2^2 + \langle T_{G, S \cap G_{i_0}} f_2, f_2 \rangle \\ &\leq \| f_1 \|_2^2 + \lambda_1'(G_{i_0}, S \cap G_{i_0}) \| f_2 \|_2^2 \\ &= 1 - \left(1 - \lambda_1'(G_{i_0}, S \cap G_{i_0})\right) \| f_2 \|_2^2. \end{aligned} \tag{A.3}$$

Since

$$T_{G,S} = \frac{|S \cap G_{i_0}|}{|S|} T_{G, S \cap G_{i_0}} + \frac{|S \backslash G_{i_0}|}{|S|} T_{G, S \backslash G_{i_0}},$$

we have

$$\langle T_{G,S} f_0, f_0\rangle \le 1 - \frac{|S\cap G_{i_0}|}{|S|}\big(1 - \langle T_{G,S\cap G_{i_0}} f_0, f_0\rangle\big). \tag{A.4}$$

We combine (A.3), (A.4) and the estimate on $\|f_2\|_2$ and get

$$\langle T_{G,S} f_0, f_0\rangle \le 1 - \frac{|S\cap G_{i_0}|}{|S|}\cdot\frac{1-\lambda_1'(G_{i_0}, S\cap G_{i_0})}{2k^2}$$

which was to be proved. □

Now we turn to the proof of Lemma A.3. It will be convenient to write

$$A_k(q) = \big\{g_1h_1\cdots g_kh_k : g_1,\dots g_k \in \Gamma_1/\Gamma_1(q), h_1,\dots h_k \in \Gamma_2/\Gamma_2(q)\big\}.$$

First we consider the case when q is the power of a prime; the general case will be easy to deduce from this.

Lemma A.4 *Let p be a prime and m a positive integer. Then $A_{10^{13}}(p^m) = \bar\Gamma/\bar\Gamma(p^m)$.*

We use different methods when p is 2 or 3 compared to when it is larger. First we consider the latter situation.

Proof of Lemma A.4 for $p \ge 5$ It is well-known and easy to check that the group generated by γ_1 and γ_2 is

$$\Gamma_1 = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : b \equiv 0 \mod 4\right\}. \tag{A.5}$$

Thus $\Gamma_1/\Gamma_1(p^m) = \mathrm{SL}(2,\mathbb{Z}/p^m\mathbb{Z})$ for $p \ne 2$.

By simple calculation:

$$\begin{pmatrix} a^{-1} & 0\\ 0 & a\end{pmatrix}\begin{pmatrix} \frac12 & 0\\ \frac{-1}{8} & 2\end{pmatrix}\gamma_3^2\begin{pmatrix} 1 & 0\\ \frac18 & 1\end{pmatrix}\gamma_3^{-1}\begin{pmatrix} a & 0\\ 0 & a^{-1}\end{pmatrix} = \begin{pmatrix} 1 & 0\\ \frac{-3ia^2}{2} & 1\end{pmatrix}.$$

Since $p \ne 2$ we can divide by 2 in the ring $\mathbb{Z}/p^m\mathbb{Z}$, hence for $(a, p) = 1$, the matrices in the above calculation are in $\Gamma_1/\Gamma_1(p^m)$ except for γ_3. Therefore

$$\begin{pmatrix} 1 & 0\\ \frac{-3ia^2}{2} & 1\end{pmatrix} \in A_3\big(p^m\big).$$

Using this, we want to show that

$$\begin{pmatrix} 1 & 0\\ ai & 1\end{pmatrix} \in A_{12}\big(p^m\big) \tag{A.6}$$

for all $a \in \mathbb{Z}/p^m\mathbb{Z}$. To do this, we need to show that for every element $x \in \mathbb{Z}/p^m\mathbb{Z}$, we can find elements $a_1, \ldots, a_k \in \mathbb{Z}/p^m\mathbb{Z}$ for some $0 \leq k \leq 4$, such that $a_1, \ldots, a_k$ are not divisible by p and $x = a_1^2 + \cdots + a_k^2$. If $m = 1$, this simply follows from the fact that any positive integer is a sum of at most 4 squares, and the a_i can not be divisible by p since $0 < a_i \leq x \leq p$ and at least one of the inequalities are strict.

Suppose that $m > 1$, $x \in \mathbb{Z}/p^m\mathbb{Z}$ and $a_1^2 + \cdots + a_k^2 \equiv x \bmod p$ with none of $a_1 \ldots a_k$ divisible by p. Then by Hensel's lemma (recall that $p \neq 2$), there is an $a_1' \in \mathbb{Z}/p^m\mathbb{Z}$ such that

$$\left(a_1'\right)^2 = a_1^2 + \left(x - a_1^2 - \cdots - a_k^2\right).$$

This proves the claim for arbitrary $m \geq 1$.

Multiplying (A.6) by a suitable unipotent element of $\Gamma_1/\Gamma_1(p^m)$, we can get

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in A_{12}\left(p^m\right)$$

for $a \in \mathbb{Z}[i]/(p^m)$. We can prove the same for the upper triangular unipotents by a very similar argument.

Again, by simple calculation:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+ab & a+c+abc \\ b & 1+bc \end{pmatrix}.$$

This shows that

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in A_{36}\left(p^m\right)$$

for all $a', b', c', d' \in \mathbb{Z}[i]/(p^m)$, $a'd' - b'c' = 1$, provided c' is not divisible by a prime above p.

Thus, $A_{36}(p^m)$ contains more than half of the group $\bar{\Gamma}/\bar{\Gamma}(p^m)$, hence

$$A_{72}\left(p^m\right) = \bar{\Gamma}/\bar{\Gamma}\left(p^m\right).$$

□

Proof of Lemma A.4 for $p = 2$ and 3 We give the proof for $p = 2$ and then explain the differences for $p = 3$.

We prove by induction the following statement. For every $m \geq 7$ and $g \in \bar{\Gamma}(2^7)/\bar{\Gamma}(2^m)$, there are $g_1, g_2, g_3 \in \Gamma_1(2^2)/\Gamma_1(2^m)$ such that

$$g = g_1\gamma_3 g_2 {\gamma_3}^{-1}\gamma_3^2 g_3 {\gamma_3}^{-2}.$$

For $m = 7$ this is clear since we can take $g_1 = g_2 = g_3 = 1$. Now assume that $m > 7$ and the statement holds for $m - 1$. In this proof, we denote by 1 the multiplicative unit (identity matrix) and by 0 the matrix with all entries 0. Let $g \in \bar{\Gamma}(2^7)/\bar{\Gamma}(2^m)$ be arbitrary. By the induction hypothesis, there is $h_1, h_2, h_3 \in \Gamma_1(2^2)/\Gamma_1(2^m)$ such that

$$g - h_1\gamma_3 h_2 \gamma_3^{-1}\gamma_3^2 h_3 \gamma_3^{-2} = 2^{m-1}x,$$

where x can be considered as an element of $\mathrm{Mat}(2, \mathbb{Z}[i]/(2))$, i.e. a 2×2 matrix with elements in $\mathbb{Z}[i]/(2)$. Since g, h_1, h_2, h_3 has determinant 1 and congruent to the unit element mod 2, x has trace 0.

Now we look for suitable $x_1, x_2, x_3 \in \mathrm{Mat}(2, \mathbb{Z})$ such that

$$x_1 + \gamma_3 x_2 \gamma_3^{-1} + \gamma_3^2 x_3 \gamma_3^{-2} \equiv 2^{m-1}x \mod 2^m.$$

Moreover, we ensure that $x_i \equiv 0 \mod 2^{m-4}$ and that $\mathrm{Tr}(x_i) \equiv 0 \mod 2^m$ for all $i = 1, 2, 3$. Since $m \geq 8$, this implies that $h_i + x_i \equiv 1 \mod 4$ and $\det(h_i + x_i) \equiv 1 \mod 2^m$, hence $h_i + x_i \in \Gamma_1(2^2)/\Gamma_1(2^m)$. Recall (A.5) from the previous proof. If the matrices x_i satisfy the claimed properties then

$$\begin{aligned}&(h_1 + x_1)\gamma_3(h_2 + x_2)\gamma_3^{-1}\gamma_3^2(h_3 + x_3)\gamma_3^{-2}\\ &\quad\equiv h_1\gamma_3 h_2\gamma_3^{-1}\gamma_3^2 h_3\gamma_3^{-2} + x_1 + \gamma_3 x_2\gamma_3^{-1} + \gamma_3^2 x_3\gamma_3^{-2} \equiv g \mod 2^m.\end{aligned}$$

The matrices x_1, x_2, x_3 can be chosen to be a suitable linear combination of the matrices in the following calculations, and this finishes the induction:

$$2^{m-1}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \gamma_3 0 \gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2} \equiv 2^{m-1}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \mod 2^m,$$

$$2^{m-1}\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} + \gamma_3 0 \gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2} 2^{m-1} \equiv \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} \mod 2^m,$$

$$2^{m-1}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} + \gamma_3 0 \gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2} \equiv 2^{m-1}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \mod 2^m,$$

$$\begin{aligned}&2^{m-2}\begin{pmatrix}1 & 3\\ 1 & -1\end{pmatrix} + \gamma_3 2^{m-2}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2}\\ &\quad\equiv 2^{m-1}\begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix} \mod 2^m,\\ &2^{m-3}\begin{pmatrix}-4 & 0\\ 3 & 4\end{pmatrix} + \gamma_3 2^{m-3}\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2}\end{aligned}$$

$$\equiv 2^{m-1}\begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix} \mod 2^m,$$

$$2^{m-4}\begin{pmatrix} 2 & 15 \\ 4 & -2 \end{pmatrix} + \gamma_3 0 \gamma_3^{-1} + \gamma_3^2 2^{m-4}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\gamma_3^{-2}$$

$$\equiv 2^{m-1}\begin{pmatrix} -i & i \\ 0 & i \end{pmatrix} \mod 2^m.$$

Now we showed that

$$A_3\big(2^m\big) \supseteq \bar{\Gamma}\big(2^7\big)/\bar{\Gamma}\big(2^m\big).$$

The index of $\bar{\Gamma}(2^7)/\bar{\Gamma}(2^m)$ in $\bar{\Gamma}/\bar{\Gamma}(2^m)$ is at most

$$\big|\operatorname{SL}\big(2, \mathbb{Z}[i]/\big(2^7\big)\big)\big| = 46 \cdot 64^6.$$

This shows that

$$A_{10^{13}}\big(2^m\big) = \bar{\Gamma}/\bar{\Gamma}\big(2^m\big).$$

Now we turn to the case $p = 3$. By the same argument, one can show that for every $m \geq 1$ and $g \in \bar{\Gamma}(3)/\bar{\Gamma}(3^m)$, there are $g_1, g_2, g_3 \in \Gamma_1/\Gamma_1(3^m)$ such that

$$g = g_1 \gamma_3 g_2 \gamma_3^{-1} \gamma_3^2 g_3 \gamma_3^{-2}.$$

The only significant difference is that one needs to use the following identities:

$$3^{m-1}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} + \gamma_3 3^{m-1}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2}$$

$$\equiv 3^{m-1}\begin{pmatrix} i & i \\ 0 & -i \end{pmatrix} \mod 3^m,$$

$$3^{m-1}\begin{pmatrix} -4 & 16 \\ 3 & 4 \end{pmatrix} + \gamma_3 3^{m-1}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\gamma_3^{-1} + \gamma_3^2 0 \gamma_3^{-2}$$

$$\equiv 3^{m-1}\begin{pmatrix} i & 0 \\ -i & -i \end{pmatrix} \mod 3^m,$$

$$3^{m-1}\begin{pmatrix} 2 & 15 \\ 4 & -2 \end{pmatrix} + \gamma_3 0 \gamma_3^{-1} + \gamma_3^2 3^{m-1}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\gamma_3^{-2}$$

$$\equiv 3^{m-1}\begin{pmatrix} i & -i \\ 0 & -i \end{pmatrix} \mod 3^m.$$

Using this claim, one can finish the proof as above. □

Proof of Lemma A.3 Let q be an integer and $q = p_1^{m_1} \cdots p_n^{m_n}$ where p_i are primes. We prove that

$$A_{10^{13}}(q) = A_{10^{13}}\big(p_1^{m_1}\big) \times \cdots \times A_{10^{13}}\big(p_n^{m_n}\big).$$

Let $x \in A_{10^{13}}(p_1^{m_1}) \times \cdots \times A_{10^{13}}(p_n^{m_n})$ be arbitrary. By definition, for each k, we can find elements $g_1^{(k)}, \ldots, g_{10^{13}}^{(k)} \in \Gamma_1/\Gamma_1(q)$ and $h_1^{(k)}, \ldots, h_{10^{13}}^{(k)} \in \Gamma_2/\Gamma_2(q)$ such that

$$x \equiv g_1^{(k)} h_1^{(k)} \cdots g_{10^{13}}^{(k)} h_{10^{13}}^{(k)} \mod p_k^{m_k}.$$

Since $\Gamma_1/\Gamma_1(p^m)$ and $\Gamma_2/\Gamma_2(p^m)$ are the direct product of local factors, we can find elements $g_1, \ldots, g_{10^{13}} \in \Gamma_1/\Gamma_1(p^m)$ and $h_1, \ldots, h_{10^{13}} \in \Gamma_2/\Gamma_2(p^m)$ such that

$$g_i \equiv g_i^{(k)} \mod p_k^{m_k} \quad \text{and} \quad h_i \equiv h_i^{(k)} \mod p_k^{m_k}$$

for each i and k. Thus

$$x = g_1 h_1 \cdots g_{10^{13}} h_{10^{13}} \in A_{10^{13}}(q).$$

Using Lemma A.4 we get

$$\begin{aligned} \bar{\Gamma}/\bar{\Gamma}(q) \supset A_{10^{13}}(q) &\supset A_{10^{13}}\big(p_1^{m_1}\big) \times \cdots \times A_{10^{13}}\big(p_n^{m_n}\big) \\ &= \bar{\Gamma}/\bar{\Gamma}\big(p_1^{m_1}\big) \times \cdots \times \bar{\Gamma}/\bar{\Gamma}\big(p_n^{m_n}\big). \end{aligned}$$

Obviously

$$\bar{\Gamma}/\bar{\Gamma}(q) \subset \bar{\Gamma}/\bar{\Gamma}\big(p_1^{m_1}\big) \times \cdots \times \bar{\Gamma}/\bar{\Gamma}\big(p_n^{m_n}\big)$$

hence all these containments must be equality. □

References

1. Berenstein, C.A., Yger, A.: Effective Bezout identities in $\boldsymbol{Q}[z_1, \ldots, z_n]$. Acta Math. **166**(1–2), 69–120 (1991)
2. Bernays, P.: Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht quadratischen Diskriminante. PhD thesis, Georg-August-Universität, Göttingen, Germany (1912)
3. Bourgain, J.: Integral Apollonian circle packings and prime curvatures. J. Anal. Math. **118**(1), 221–249 (2012)
4. Bourgain, J., Fuchs, E.: A proof of the positive density conjecture for integer Apollonian circle packings. J. Am. Math. Soc. **24**(4), 945–967 (2011)
5. Bourgain, J., Gamburd, A.: Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I. J. Eur. Math. Soc. **10**(4), 987–1011 (2008)

6. Bourgain, J., Gamburd, A.: Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. Ann. Math. (2) **167**(2), 625–642 (2008)
7. Bourgain, J., Gamburd, A.: Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. II. J. Eur. Math. Soc. **11**(5), 1057–1103 (2009). With an appendix by Bourgain
8. Bourgain, J., Kontorovich, A.: On representations of integers in thin subgroups of SL(2, **Z**). Geom. Funct. Anal. **20**(5), 1144–1174 (2010)
9. Bourgain, J., Kontorovich, A.: On Zaremba's conjecture (2011). Preprint arXiv:1107.3776
10. Bourgain, J., Varjú, P.P.: Expansion in $SL_n(\mathbf{Z}/q\mathbf{Z})$, q arbitrary. Invent. Math. **188**(1), 151–173 (2012)
11. Bourgain, J., Gamburd, A., Sarnak, P.: Affine linear sieve, expanders, and sum-product. Invent. Math. **179**(3), 559–644 (2010)
12. Bourgain, J., Kontorovich, A., Sarnak, P.: Sector estimates for hyperbolic isometries. Geom. Funct. Anal. **20**(5), 1175–1200 (2010)
13. Bourgain, J., Gamburd, A., Sarnak, P.: Generalization of Selberg's 3/16 theorem and affine sieve. Acta Math. **207**, 255–290 (2011)
14. Breuillard, E., Green, B., Tao, T.: Approximate subgroups of linear groups. Geom. Funct. Anal. **21**(4), 774–819 (2011)
15. Brooks, R.: The spectral geometry of a tower of coverings. J. Differ. Geom. **23**(1), 97–107 (1986)
16. Brooks, R.: The spectral geometry of Riemannian surfaces. In: Monastyrsky, M.I. (ed.) Topology in Molecular Biology. Springer, Berlin (2007)
17. Burger, M.: Grandes valeurs propres du Laplacien et graphes. In: Séminaire de Théorie Spectrale et Géométrie, No. 4, Année 1985–1986, pp. 95–100. Univ. Grenoble I (1986)
18. Burger, M.: Petites valeurs propres du Laplacien et topologie de Fell. PhD thesis, EPFL (1986)
19. Burger, M.: Spectre du Laplacien, graphes et topologie de Fell. Comment. Math. Helv. **63**(2), 226–252 (1988)
20. Cowling, M., Haagerup, U., Howe, R.: Almost L^2 matrix coefficients. J. Reine Angew. Math. **387**, 97–110 (1988)
21. Diaconis, P., Saloff-Coste, L.: Comparison techniques for random walk on finite groups. Ann. Probab. **21**(4), 2131–2156 (1993)
22. Fuchs, E.: Arithmetic properties of Apollonian circle packings. Princeton University Thesis (2010)
23. Fuchs, E., Sanden, K.: Some experiments with integral Apollonian circle packings. Exp. Math. **20**(4), 380–399 (2011)
24. Gelfand, I.M., Graev, M.I., Pjateckii-Shapiro, I.I.: Teoriya Predstavlenii i Avtomorfnye Funktsii. Generalized Functions, vol. 6. Nauka, Moscow (1966)
25. Good, A.: Local Analysis of Selberg's Trace Formula. Lecture Notes in Mathematics, vol. 1040. Springer, Berlin (1983)
26. Graham, R.L., Lagarias, J.C., Mallows, C.L., Wilks, A.R., Yan, C.H.: Apollonian circle packings: number theory. J. Number Theory **100**(1), 1–45 (2003)
27. Graham, R.L., Lagarias, J.C., Mallows, C.L., Wilks, A.R., Yan, C.H.: Apollonian circle packings: geometry and group theory. I. The Apollonian group. Discrete Comput. Geom. **34**(4), 547–585 (2005)
28. Helfgott, H.A.: Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ann. Math. (2) **167**(2), 601–623 (2008)
29. Hermann, G.: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95**(1), 736–788 (1926)
30. Iwaniec, H., Kowalski, E.: Analytic Number Theory. American Mathematical Society Colloquium Publications, vol. 53. American Mathematical Society, Providence (2004)
31. Kassabov, M., Lubotzky, A., Nikolov, N.: Finite simple groups as expanders. Proc. Natl. Acad. Sci. USA **103**(16), 6116–6119 (2006)

32. Kloosterman, H.D.: On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. Acta Math. **49**(3–4), 407–464 (1927)
33. Kontorovich, A., Oh, H.: Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds. J. Am. Math. Soc. **24**(3), 603–648 (2011)
34. Lagarias, J.C., Mallows, C.L., Wilks, A.R.: Beyond the Descartes circle theorem. Am. Math. Mon. **109**(4), 338–361 (2002)
35. Lax, P.D., Phillips, R.S.: The asymptotic distribution of lattice points in Euclidean and non-Euclidean space. J. Funct. Anal. **46**, 280–350 (1982)
36. Masser, D.W., Wüstholz, G.: Fields of large transcendence degree generated by values of elliptic functions. Invent. Math. **72**(3), 407–464 (1983)
37. Matthews, C., Vaserstein, L., Weisfeiler, B.: Congruence properties of Zariski-dense subgroups. Proc. Lond. Math. Soc. **48**, 514–532 (1984)
38. Patterson, S.J.: The limit set of a Fuchsian group. Acta Math. **136**, 241–273 (1976)
39. Pyber, L., Szabó, E.: Growth in finite simple groups of lie type of bounded rank (2010). Preprint arXiv:1005.1858
40. Salehi Golsefidy, A., Varjú, P.: Expansion in perfect groups. Geom. Funct. Anal. **22**(6), 1832–1891 (2012)
41. Sarnak, P.: Some Applications of Modular Forms. Cambridge Tracts in Mathematics, vol. 99. Cambridge University Press, Cambridge (1990)
42. Sarnak, P.: Letter to J. Lagarias. web.math.princeton.edu/sarnak/AppolonianPackings.pdf (2007)
43. Sarnak, P.: Integral Apollonian packings. Am. Math. Mon. **118**(4), 291–306 (2011)
44. Selberg, A.: On the estimation of Fourier coefficients of modular forms. Proc. Symp. Pure Math. **VII**, 1–15 (1965)
45. Shalom, Y.: Bounded generation and Kazhdan's property (T). Publ. Math. Inst. Hautes Études Sci. **90**, 145–168 (1999)
46. Soddy, F.: The bowl of integers and the hexlet. Nature **139**, 77–79 (1937)
47. Sullivan, D.: Entropy, Hausdorff measures old and new, and limit sets of geometrically finite Kleinian groups. Acta Math. **153**(3–4), 259–277 (1984)
48. Varjú, P.P.: Expansion in $SL_d(O_K/I)$, I square-free. J. Eur. Math. Soc. **14**(1), 273–305 (2012)
49. Vinogradov, I.: Effective bisector estimate with application to Apollonian circle packings. IMRN (2013). Princeton University Thesis (2012). arXiv:1204.5498v1