DISCRETE ANALYSIS, 20XX:XX, 27 pp.
www.discreteanalysisjournal.com

Beyond Expansion IV: Traces of Thin Semigroups

Jean Bourgain [*] Alex Kontorovich [†]

Received XX Month 20XX; Revised XX Month 20XX; Published XX Month 20XX

Abstract: This paper constitutes Part IV in our study of particular instances of the Affine Sieve, producing levels of distribution beyond those attainable from expansion alone. Motivated by McMullen's Arithmetic Chaos Conjecture regarding low-lying closed geodesics on the modular surface defined over a given number field, we study the set of traces for certain sub-semi-groups of $\mathrm{SL}_2(\mathbb{Z})$ corresponding to absolutely Diophantine numbers (see §1.2). In particular, we are concerned with the level of distribution for this set. While the standard Affine Sieve procedure, combined with Bourgain-Gamburd-Sarnak's resonance-free region for the resolvent of a "congruence" transfer operator, produces *some* exponent of distribution $\alpha > 0$, we are able to produce the exponent $\alpha = 1/3 - \varepsilon$. This recovers unconditionally the same exponent as what one would obtain under a Ramanujan-type conjecture for thin groups. A key ingredient, of independent interest, is a bound on the additive energy of $\mathrm{SL}_2(\mathbb{Z})$.

Key words and phrases: thin groups, affine sieve, additive energy

1 Introduction

In this paper, we reformulate McMullen's (Classical) Arithmetic Chaos Conjecture (see Conjecture 4) as a local-global problem for the set of traces in certain thin semigroups, see Conjecture 11. Our main goal is to make some partial progress towards this conjecture by establishing strong levels of distribution for this trace set, see §1.4.

[*]Supported by NSF grant DMS-1301619.

[†]Supported by an NSF CAREER grant DMS-1455705, an NSF FRG grant DMS-1463940, an Alfred P. Sloan Research Fellowship, and a BSF grant. Some of this work was carried out thanks to support from a Yale Junior Faculty Fellowship and the Ellentuck Fund at IAS.

DOI: 10.19086/daXXX

1.1 Low-Lying Closed Geodesics With Fixed Discriminant

This paper is motivated by the study of long closed geodesics on the modular surface defined over a given number field, which do not have high excursions into the cusp. Let us make this precise.

To set notation, let $\mathbb{H}$ denote the upper half plane, and let

$$\mathcal{X} = T^1(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}) \cong \mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{SL}_2(\mathbb{R})$$

be the unit tangent bundle of the modular surface. A closed geodesic γ on $\mathcal{X}$ corresponds to a hyperbolic matrix $M \in \mathrm{SL}_2(\mathbb{Z})$ (more precisely its conjugacy class). Let $\alpha_M \in \partial\mathbb{H}$ be one of the two fixed points of M, the other being its Galois conjugate $\overline{\alpha_M}$; then γ is the projection mod $\mathrm{SL}_2(\mathbb{Z})$ of the geodesic connecting α_M and $\overline{\alpha_M}$. We will say that γ is defined over the (real quadratic) field $K = \mathbb{Q}(\alpha_M)$. Let Δ_M be the discriminant of K; this number is (up to factors of 4) the square-free part of

$$D_M := (\mathrm{tr}\, M)^2 - 4. \tag{1}$$

To study excursions into the cusp, let $\mathscr{Y}(\gamma)$ denote the largest imaginary part of γ in the standard upper-half plane fundamental domain for the modular surface. Given a "height" $C > 1$, we say that the closed geodesic γ is **low-lying** (of height C) if $\mathscr{Y}(\gamma) < C$. By the well-known connection [Hum16, Art24, Ser85] between continued fractions and the cutting sequence of the geodesic flow on $\mathcal{X}$, the condition that γ be low-lying can be reformulated as a Diophantine property on the fixed point α_M of M, as follows. Write the (eventually periodic) continued fraction expansion

$$\alpha_M = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}} = [a_0, a_1, a_2, \ldots],$$

as usual, where the numbers a_j are called partial quotients. Given any $A \geq 1$, we say that α_M is **Diophantine** (of height A) if all its partial quotients a_j are bounded by A. Then α_M being Diophantine of height A is essentially equivalent to γ being low-lying of height $C = C(A)$.

Question 2. Given a real quadratic field K and a height C, can one find longer and longer primitive closed geodesics defined over K which are low-lying of height C? Equivalently, given a fixed fundamental discriminant $\Delta > 0$ and a height $A \geq 1$, we wish to find larger and larger (non-conjugate, primitive, hyperbolic) matrices M so that their fixed points α_M are Diophantine of height A, and so that $t = \mathrm{tr}(M)$ solves the Pell equation $t^2 - \Delta s^2 = 4$; cf. (1). If solutions exist, how rare/ubiquitous are they?

1.2 Arithmetic Chaos

On one hand, the answer to Question 2 is, on average, negative. Indeed, generic long closed geodesics equidistribute, so must have high excursions into the cusp. On the other hand, McMullen's (Classical) Arithmetic Chaos Conjecture (see [McM09, McM12] for the dynamical perspective and origin of this problem) predicts that solutions exist, and moreover have positive entropy:

Conjecture 3 (Arithmetic Chaos [McM12])**.** *There exists an absolute height $A \geq 2$ so that, for any fixed real quadratic field K, the cardinality of the set*

$$\left\{ [\overline{a_0, a_1, \dots, a_\ell}] \in K \quad : \quad 1 \leq a_j \leq A \right\} \tag{4}$$

grows exponentially, as $\ell \to \infty$.

Remark 5. Though we have stated the conjecture with some absolute height A, McMullen formulated this problem with $A = 2$ (of course $A = 1$ only produces the golden mean). He further suggested it should also hold whenever the corresponding growth exponent exceeds $1/2$, see Remark 13.

Remark 6. As pointed out to us by McMullen, one can also formulate a $\mathrm{GL}_n(\mathbb{Z})$ version of Arithmetic Chaos by strengthening [McM09, Conjecture 1.7 (3)] so as to postulate exponential growth of periodic points instead of just infinitude.

It is not currently known whether the following much weaker statement is true: for some A and every K, the cardinality of the set (4) is unbounded. Even worse, it is not known whether (4) is eventually non-empty, that is, whether there exists an $A \geq 2$ so that any K contains at least one element which is Diophantine of height A.

Some progress towards Conjecture 3 appears in [Woo78, Wil80, McM09, Mer12], where special periodic patterns of partial quotients are constructed to lie in certain prescribed real quadratic fields. These results prove that for any K, there exists an $A = A(K)$ so that the cardinality of (4) is unbounded with ℓ; but exponential growth is not known in a single case.

In light of this conjecture, we call a number **absolutely Diophantine** if it is Diophantine of height A for some absolute constant $A \geq 1$. That is, when we speak of a number being absolutely Diophantine, the height A is fixed in advance. In the next subsection, we describe a certain "local-global" conjecture which has the Arithmetic Chaos Conjecture as a consequence.

1.3 The Local-Global Conjecture

First we need some more notation. Consider a finite subset $\mathcal{A} \subset \mathbb{N}$, which we call an **alphabet**, and let

$$\mathfrak{C}_{\mathcal{A}} = \{[a_0, a_1, \dots] : a_j \in \mathcal{A}\}$$

denote the set of all $\alpha \in \mathbb{R}$ with all partial quotients in $\mathcal{A}$. If $\max \mathcal{A} \leq A$ for an absolute constant A, then every $\alpha \in \mathfrak{C}_{\mathcal{A}}$ is clearly absolutely Diophantine. Assuming $2 \leq |\mathcal{A}| < \infty$, each $\mathfrak{C}_{\mathcal{A}}$ is a Cantor set of some Hausdorff dimension

$$0 < \delta_{\mathcal{A}} < 1,$$

and by choosing $\mathcal{A}$ appropriately (for example, $\mathcal{A} = \{1, 2, \dots, A\}$ with A large), one can make $\delta_{\mathcal{A}}$ arbitrarily close to 1 [Hen92].

It is easy to see that the matrix

$$M = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_\ell & 1 \\ 1 & 0 \end{pmatrix} \tag{7}$$

(of determinant ± 1) fixes the quadratic irrational

$$\alpha_M = [\overline{a_0, a_1, \dots, a_\ell}],$$

so we introduce the semi-group[1]

$$\mathcal{G}_{\mathcal{A}} := \left\langle \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \,:\, a \in \mathcal{A} \right\rangle^{+} \quad \subset \quad \mathrm{GL}_2(\mathbb{Z}) \tag{8}$$

of all such matrices whose fixed points α_M lie in $\mathfrak{C}_{\mathcal{A}}$. Preferring to work in SL_2, we immediately pass to the even-length (determinant-one) sub-semi-group

$$\Gamma_{\mathcal{A}} := \mathcal{G}_{\mathcal{A}} \cap \mathrm{SL}_2(\mathbb{Z}), \tag{9}$$

which is (finitely) generated by the products $\left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} b & 1 \\ 1 & 0 \end{smallmatrix}\right)$, for $a, b \in \mathcal{A}$.

Having accounted for the "low-lying" (or Diophantine) criterion, we must study the discriminants, or what is essentially the same, the set

$$\mathcal{T}_{\mathcal{A}} := \{\mathrm{tr}\, M \,:\, M \in \Gamma_{\mathcal{A}}\} \quad \subset \quad \mathbb{Z}$$

of traces in $\Gamma_{\mathcal{A}}$. Borrowing language from Hilbert's 11^{th} problem on numbers represented by quadratic forms, we call an integer t **admissible** (for the alphabet $\mathcal{A}$) if for every $q \geq 1$,

$$t \in \mathcal{T}_{\mathcal{A}} (\mathrm{mod}\, q),$$

that is, if t passes all finite local obstructions.

Remark 10. If $\{1,2\} \subseteq \mathcal{A}$, then, allowing inverses, the *group* $\langle \Gamma_{\mathcal{A}} \rangle$ generated by the semigroup $\Gamma_{\mathcal{A}}$ is all of $\mathrm{SL}_2(\mathbb{Z})$, and hence every integer is admissible. In general, Strong Approximation [MVW84] shows that admissibility can be checked using a single modulus $q(\mathcal{A})$.

We say t is **represented** if $t \in \mathcal{T}_{\mathcal{A}}$, and let $\mathcal{M}_{\mathcal{A}}(t)$ denote its **multiplicity**,

$$\mathcal{M}_{\mathcal{A}}(t) := \#\{M \in \Gamma_{\mathcal{A}} : \mathrm{tr}\, M = t\}.$$

Since the entries of $\Gamma_{\mathcal{A}}$ are all positive, the multiplicity is always finite.

The following conjecture seems plausible.

Conjecture 11 (Local-Global Conjecture for Traces)**.** *Let $\mathcal{A}$ be an alphabet for which the dimension $\delta_{\mathcal{A}}$ exceeds $1/2$. Then the set $\mathcal{T}_{\mathcal{A}}$ of traces contains every sufficiently large admissible integer. Moreover, the multiplicity $\mathcal{M}_{\mathcal{A}}(t)$ of an admissible $t \in [N, 2N)$ is at least*

$$\mathcal{M}_{\mathcal{A}}(t) > N^{2\delta_{\mathcal{A}} - 1 - o(1)}. \tag{12}$$

Remark 13. It is now clear how to generalize Conjecture 3; the same should hold for a_j restricted to any alphabet $\mathcal{A}$, as long as $\delta_{\mathcal{A}} > 1/2$.

A direct attack on this conjecture seems out of reach of current technology. Therefore we shift our focus to the study of the arithmetic properties of the trace set, more specifically to its equidistribution along progressions, with applications to almost primes. Our main goal is to make some progress in this direction.

[1] The superscript $+$ in (8) denotes generation as a semigroup, that is, no inverses.

1.4 Statements of the Main Theorems

In this subsection, we state our main theorems, though we defer the precise (and somewhat technical) definitions to the next section.

For several applications, an important barometer of our understanding of a sequence is its *level of distribution*, defined roughly as follows. In our context, we wish to know that the traces in $\mathcal{T}_{\mathcal{A}}$ up to some growing parameter N are equi-distributed along multiples of integers q, with q as large as possible relative to N. That is, the quantity

$$\#\{t \in \mathcal{T}_{\mathcal{A}} : t < N,\ t \equiv 0(q)\},$$

counted with multiplicity, should be "close" to

$$\frac{1}{q} \times \#\{t \in \mathcal{T}_{\mathcal{A}} : t < N\},$$

in the sense that their difference should be much smaller than the total number of $t \in \mathcal{T}_{\mathcal{A}}$ up to N. This proximity cannot be expected once q is as large as N, say, but perhaps can be established with q of size $N^{1/2}$ or more generally N^{α} for some $\alpha > 0$. If this is the case, in an average sense, then N^{α} is called a **level of distribution** for $\mathcal{T}_{\mathcal{A}}$, and α is called an **exponent of distribution**. Let us make matters a bit more precise.

Looking at traces up to N counted with multiplicity is essentially the same as looking at matrices in the semigroup $\Gamma_{\mathcal{A}}$ of norm at most N. Writing

$$r_q(N) := \sum_{\substack{\gamma \in \Gamma_{\mathcal{A}} \\ \|\gamma\| < N}} \mathbf{1}_{\{\operatorname{tr}\gamma \equiv 0(q)\}} - \frac{1}{q} \sum_{\substack{\gamma \in \Gamma_{\mathcal{A}} \\ \|\gamma\| < N}} 1$$

for the "remainder" terms, we will say, again roughly, that $\mathcal{T}_{\mathcal{A}}$ has level of distribution $\mathcal{Q}$ if

$$\sum_{q < \mathcal{Q}} |r_q(N)| = o\left(\sum_{\substack{\gamma \in \Gamma_{\mathcal{A}} \\ \|\gamma\| < N}} 1 \right). \tag{14}$$

In applications it is enough to consider only square-free q in the sum. If (14) can be established with $\mathcal{Q}$ as large as N^{α}, then we will say $\mathcal{T}_{\mathcal{A}}$ has exponent of distribution α. See §2.1 for a precise definition of level and exponent of distribution.

Remark 15. Note that a level and exponent of distribution is not a quantity intrinsic to $\mathcal{T}_{\mathcal{A}}$, but rather a function of what one can prove about $\mathcal{T}_{\mathcal{A}}$. The larger this exponent, the more control one has on the distribution of $\mathcal{T}_{\mathcal{A}}$ on such arithmetic progressions.

Remark 16. The set $\mathcal{T}_{\mathcal{A}}$ is of Affine Sieve type; see [BK15] for a definition. As such, the general Affine Sieve procedure introduced in [BGS06, BGS10], combined with the "expansion property" established in [BGS11], shows that $\mathcal{T}_{\mathcal{A}}$ has *some* exponent of distribution $\alpha > 0$, see §2.2. In fact, if one replaces the known expansion by a Ramanujan-type conjecture for the spectral gap, one obtains an exponent $\alpha = 1/3 - \varepsilon$, see Remark 36.

Our main goal in this paper is to make some partial progress towards Conjecture 11 by establishing levels of distribution for $\mathcal{T}_{\mathcal{A}}$ beyond those available from expansion alone.

Theorem 17. *For any small $\eta > 0$, there is an effectively computable $\delta_0 = \delta_0(\eta) < 1$ so that, if the dimension $\delta_{\mathcal{A}}$ of the alphabet $\mathcal{A}$ exceeds δ_0, then the set $\mathcal{T}_{\mathcal{A}}$ has exponent of distribution*

$$\alpha = \frac{1}{3} - \eta. \tag{18}$$

That is, we recover unconditionally a Ramanujan-quality exponent. Applying standard sieve theory [Gre86], these levels of distribution have the following immediate corollary on almost primes. Recall that a number is R-almost-prime if it has at most R prime factors.

Corollary 19. *There exists an effectively computable $\delta_0 < 1$ so that, if the dimension $\delta_{\mathcal{A}}$ of the alphabet $\mathcal{A}$ exceeds δ_0, then the set $\mathcal{T}_{\mathcal{A}}$ of traces contains an infinitude of R-almost-primes, with $R = 4$.*

As an afterthought, we explore what can be said about R-almost-primes, not in the set $\mathcal{T}_{\mathcal{A}}$ of traces, but in the set of discriminants which arise. To this end, recalling (1), we define

$$\mathcal{D}_{\mathcal{A}} := \{\mathrm{sqf}(t^2-4) : t \in \mathcal{T}_{\mathcal{A}}\}, \tag{20}$$

where $\mathrm{sqf}(\cdot)$ denotes the square-free part. As explained in §7, an easy consequence of Mercat's thesis [Mer12], combined with our work [BK14a] on Zaremba's Conjecture and Iwaniec's theorem [Iwa78], gives the following

Theorem 21. *For the alphabet $\mathcal{A} = \{1, \dots, 50\}$, the set $\mathcal{D}_{\mathcal{A}}$ contains an infinitude of R-almost-primes with $R = 2$.*

The proof of the main Theorem 17 is based on the following result on additive energy in $\mathrm{SL}_2(\mathbb{Z})$ of independent interest.

Theorem 22. *Let $\mathcal{S}_N = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \|\gamma\| < N\}$. For any sufficiently small $\kappa > 0$ and $\varepsilon > 0$, there is a subset $\mathcal{S}'_N \subset \mathcal{S}_N$ satisfying*

$$|\mathcal{S}_N \setminus \mathcal{S}'_N| < N^{2-\kappa}, \tag{23}$$

having additive energy

$$E(\mathcal{S}'_N) = \#\{(\gamma_1, \gamma_2, \gamma_3, \gamma_4) \in (\mathcal{S}'_N)^4 : \gamma_1 + \gamma_2 = \gamma_3 + \gamma_4\} \ll N^{4+2\kappa+\varepsilon}. \tag{24}$$

1.5 Organization

In §2, we give precise definitions of level and exponent of distribution, thus making unambiguous the statement of Theorem 17. There we also discuss the main ingredients involved in the proofs. We spend §3 constructing the sifting sequence $\mathfrak{A}$, and we execute the main term analysis in §4. The error analysis is handled in §5, thus proving Theorem 17 modulo the proof of Theorem 22; the latter is postponed to §6. Finally, Theorem 21 is proved quickly in §7.

1.6 Notation

We use the following notation throughout. Set $e(x) = e^{2\pi i x}$ and $e_q(x) = e(\frac{x}{q})$. We use the symbol $f \sim g$ to mean $f/g \to 1$. The symbols $f \ll g$ and $f = O(g)$ are used interchangeably to mean the existence of an implied constant $C > 0$ so that $f(x) \le Cg(x)$ holds for all $x > C$; moreover $f \asymp g$ means $f \ll g \ll f$. The letters c, C denote positive constants, not necessarily the same in each occurrence. Unless otherwise specified, implied constants may depend at most on $\mathcal{A}$, which is treated as fixed. The letter $\varepsilon > 0$ is an arbitrarily small constant, not necessarily the same at each occurrence. When it appears in an inequality, the implied constant may also depend on ε without further specification. The symbol $\mathbf{1}_{\{\cdot\}}$ is the indicator function of the event $\{\cdot\}$. The trace of a matrix γ is denoted $\operatorname{tr}\gamma$. The greatest common divisor of n and m is written (n,m) and their least common multiple is $[n,m]$. The function $\nu(n)$ 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 ${}^t g$. When there can be no confusion, we use the shorthand $r(q)$ for $r(\mathrm{mod}\, q)$. The prime symbol $'$ in $\sum_{r(q)}'$ means the range of $r(\mathrm{mod}\, q)$ is restricted to $(r,q) = 1$.

2 Levels of Distribution and Ingredients

2.1 Levels of Distribution

In this subsection, we give precise definitions of level and exponent of distribution. Fix the alphabet $\mathcal{A}$ and let $\mathcal{T}_{\mathcal{A}}$ be the set of traces of $\Gamma_{\mathcal{A}}$. First we assume that the set of traces is **primitive**, that is,

$$\gcd(\mathcal{T}_{\mathcal{A}}) = 1. \tag{25}$$

If not,[2] then replace $\mathcal{T}_{\mathcal{A}}$ by $\mathcal{T}_{\mathcal{A}}/\gcd(\mathcal{T}_{\mathcal{A}})$. Given a large parameter N, let $\mathfrak{A} = \{a_N(n)\}$ be a sequence of non-negative numbers supported on $\mathcal{T}_{\mathcal{A}} \cap [1,N]$, and set

$$|\mathfrak{A}| = \sum_n a_N(n).$$

We require that $\mathfrak{A}$ is well-distributed on average over multiples of square-free integers $\mathfrak{q}$. More precisely, setting

$$|\mathfrak{A}_{\mathfrak{q}}| := \sum_{n \equiv 0(\mathfrak{q})} a_N(n),$$

we insist that

$$|\mathfrak{A}_{\mathfrak{q}}| = \beta(\mathfrak{q})|\mathfrak{A}| + r(\mathfrak{q}), \tag{26}$$

where

1. the "local density" β is a multiplicative function assumed to satisfy the "linear sieve" condition

$$\prod_{w \le p < z} (1 - \beta(p))^{-1} \le C \cdot \frac{\log z}{\log w}, \tag{27}$$

for some $C > 1$ and any $2 \le w < z$; and

[2] In fact, since the identity matrix has trace 2, the set of traces is not primitive if and only if the alphabet $\mathcal{A} \subset 2\mathbb{Z}$ consists entirely of even numbers (in which case the traces are all even and should be halved).

2. the "remainders" $r(\mathfrak{q})$ are small on average, in the sense that

$$\sum_{\mathfrak{q}<\mathcal{Q}} |r(\mathfrak{q})| \ll_K \frac{1}{(\log N)^K}|\mathfrak{A}|, \tag{28}$$

for some $\mathcal{Q} \geq 1$ and any $K \geq 1$. That is, we ask for an arbitrary power of log savings.

If a sequence $\mathfrak{A}$ exists for which the conditions (26)–(28) hold, then we say that $\mathcal{T}_{\mathcal{A}}$ has a **level of distribution** $\mathcal{Q}$. If (28) can be established with $\mathcal{Q}$ as large as a power,

$$\mathcal{Q} = N^{\alpha}, \qquad \alpha > 0, \tag{29}$$

then we say that $\mathcal{T}_{\mathcal{A}}$ has an **exponent of distribution** α.

2.2 The Main Ideas

This subsection is purely heuristic and expository. First we recall how the "standard" Affine Sieve procedure applies in this context, explaining Remark 16. Since $\delta_{\mathcal{A}}$ is assumed to be large, we must have $\{1,2\} \subset \mathcal{A}$, whence for all $\mathfrak{q} \geq 1$, the reduction $\Gamma_{\mathcal{A}} (\mathrm{mod}\, \mathfrak{q})$ is all of $\mathrm{SL}_2(\mathfrak{q})$; cf. Remark 10. Initially, we could construct the sequence $\mathfrak{A}$ by setting

$$a_N(n) := \sum_{\substack{\gamma \in \Gamma_{\mathcal{A}} \\ \|\gamma\| < N}} \mathbf{1}_{\{\mathrm{tr}\,\gamma = n\}}, \tag{30}$$

which is clearly supported on $n \in \mathcal{T}_{\mathcal{A}}$, $n \ll N$. Then work of Hensley [Hen89] gives

$$|\mathfrak{A}| = \#\{\gamma \in \Gamma_{\mathcal{A}} : \|\gamma\| < N\} \asymp N^{2\delta_{\mathcal{A}}}, \tag{31}$$

and $|\mathfrak{A}_{\mathfrak{q}}|$ can be expressed as

$$|\mathfrak{A}_{\mathfrak{q}}| = \sum_{\substack{\gamma \in \Gamma_{\mathcal{A}} \\ \|\gamma\| < N}} \mathbf{1}_{\{\mathrm{tr}\,\gamma \equiv 0 (\mathfrak{q})\}} = \sum_{\gamma_0 \in \mathrm{SL}_2(\mathfrak{q})} \mathbf{1}_{\{\mathrm{tr}\,\gamma_0 \equiv 0(\mathfrak{q})\}} \left[\sum_{\substack{\gamma \in \Gamma_{\mathcal{A}} \\ \|\gamma\| < N}} \mathbf{1}_{\{\gamma \equiv \gamma_0 (\mathfrak{q})\}} \right], \tag{32}$$

where we have decomposed the γ sum into residue classes mod $\mathfrak{q}$. A theorem of Bourgain-Gamburd-Sarnak [BGS11] in this context states very roughly (see Proposition 40 for a precise statement) that

$$\begin{aligned} &\#\{\gamma \in \Gamma_{\mathcal{A}} : \|\gamma\| < N,\ \gamma \equiv \gamma_0(\mathfrak{q})\} \\ &\qquad = \frac{1}{|\mathrm{SL}_2(\mathfrak{q})|}\#\{\gamma \in \Gamma_{\mathcal{A}} : \|\gamma\| < N\} + \text{“}O(\mathfrak{q}^C N^{2\delta - \Theta})\text{”}, \end{aligned} \tag{33}$$

for some $\Theta > 0$. (We reiterate that the error in (33) is heuristic only; a statement of this strength is not currently known.[3] That said, the true statement serves the same purpose in our application.) This is the

[3] Added in print: A power savings error now is known, and even for all $\mathfrak{q}$ (not just square-free) by work of Magee-Oh-Winter/Bourgain-Kontorovich-Magee [MOW16, BKM15]. For our purposes, the weaker result in [BGS11] suffices, and in fact none of our estimates would improve (though the exposition would be slightly simpler) if we used [MOW16, BKM15] instead.

"spectral gap" or "expander" property of $\Gamma_{\mathcal{A}}$, and follows from a resonance-free region for the resolvent of a certain "congruence" transfer operator, see §2.3.

Inserting the expander property (33) into $|\mathfrak{A}_{\mathfrak{q}}|$ in (32) gives the desired decomposition (26), with local density

$$\beta(\mathfrak{q}) = \frac{1}{|\mathrm{SL}_2(\mathfrak{q})|} \sum_{\gamma_0 \in \mathrm{SL}_2(\mathfrak{q})} \mathbf{1}_{\{\mathrm{tr}\,\gamma_0 \equiv 0(q)\}},$$

and error

$$|r(\mathfrak{q})| \ll \mathfrak{q}^C N^{2\delta-\Theta}. \tag{34}$$

Then the local density condition (27) follows classically from primitivity (25), and, in light of (31), the average error condition (28) requires (a condition weaker than)

$$\sum_{\mathfrak{q}<\mathcal{Q}} |r(\mathfrak{q})| \ll \mathcal{Q}^C N^{2\delta-\Theta} < N^{2\delta-\varepsilon},$$

or

$$\mathcal{Q} = N^{\alpha} < N^{\Theta/C-\varepsilon}. \tag{35}$$

In this way, one can prove *some* exponent of distribution $\alpha > 0$, cf. Remark 16. If one were to compute the numerical values of the constants C and Θ from the proof of (33), which would be a feat in itself, one would obtain a numeric but astronomically small α. Our goal here is to do better.

Remark 36. The best one may hope to be true is a Ramanujan-type "square-root cancellation" error, where $\Theta = \delta$ and $C = 0$ in (33), which leads to $C = 2$ in (34) and $C = 3$ in (35). (Note that one cannot obtain an improvement here along the lines of Hong-Kontorovich [HK15] by a better modular decomposition in (32), as it is easy to see that the trace is only stabilized mod $\mathfrak{q}$ by the full congruence group and not some subgroup.) The "Ramanujan-quality" exponent would thus be $\alpha = \Theta/C = \delta/3$ in (35), which approaches $1/3$ as δ approaches 1; this explains the claim in Remark 16.

The novel technique employed here, used in some form already in [BK10, BK14a, BK14b, BK15, BK16, BK17], is to take inspiration from Vinogradov's method, developing a "bilinear forms" approach, as follows. Instead of (30), let X and Y be two more parameters, each a power of N, with $XY = N$, and set (roughly)

$$a_N(n) \text{ ":=" } \sum_{\substack{\gamma \in \Gamma \\ \|\gamma\|<X}} \sum_{\substack{\xi \in \Gamma \\ \|\xi\|<Y}} \mathbf{1}_{\{\mathrm{tr}(\gamma\xi)=n\}}. \tag{37}$$

This sum better encapsulates the group structure of $\Gamma_{\mathcal{A}}$, while still only being supported on the traces $\mathcal{T}_{\mathcal{A}}$ of $\Gamma_{\mathcal{A}}$. Again, this is still an oversimplification; see §3 for the actual construction of $\mathfrak{A}$.

Instead of directly appealing to expansion as in (32), we first invoke finite abelian harmonic analysis, writing

$$|\mathfrak{A}_{\mathfrak{q}}| = \sum_{n \equiv 0(\mathfrak{q})} a_N(n) = \sum_n \left[\frac{1}{\mathfrak{q}} \sum_{r(\mathfrak{q})} e_{\mathfrak{q}}(rn) \right] a_N(n). \tag{38}$$

After some manipulations, we decompose our treatment according to whether $\mathfrak{q}$ is "small" or "large". For $\mathfrak{q}$ small, we apply expansion as before. For $\mathfrak{q}$ large, the corresponding exponential sum already has sufficient cancellation (on average over $\mathfrak{q}$ up to the level $\mathcal{Q}$) that it can be treated as an error term in its entirety. It is in this range of large $\mathfrak{q}$ that we exploit the bilinear structure of (37).

2.3 Expansion

Here is a formal statement of "expansion," as needed in our context. Let $\mathcal{A} \subset \mathbb{N}$ be our finite alphabet with dimension $\delta_{\mathcal{A}}$ sufficiently near 1. As such, it must contain the sub-alphabet $\mathcal{A}_0 := \{1,2\} \subset \mathcal{A}$. This has the consequence that for all $q \geq 1$,

$$\Gamma(\mathrm{mod}\, q) \cong \mathrm{SL}_2(q), \tag{39}$$

cf. Remark 10. Furthermore, we will only require expansion for the fixed alphabet $\mathcal{A}_0$, so as to make the expansion constants absolute, and not dependent on $\mathcal{A}$; see footnote 4 on page 17.

To this end, let $\Gamma_0 \subset \mathrm{SL}_2(\mathbb{Z})$ be the semigroup as in (9) corresponding to $\mathcal{A}_0$. The following proposition is proved in [BK17, Prop. 2.9].

Proposition 40. *Given any $Y \gg 1$, there is a non-empty subset $\mathfrak{K} = \mathfrak{K}(Y) \subset \Gamma_0$ so that*

1. *for all $\mathfrak{a} \in \mathfrak{K}$, $\|\mathfrak{a}\| < Y$, and*
2. *for all square-free q and $\mathfrak{a}_0 \in \mathrm{SL}_2(q)$,*

$$\left| \frac{\#\{\mathfrak{a} \in \mathfrak{K} : \mathfrak{a} \equiv \mathfrak{a}_0 (q)\}}{|\mathfrak{K}|} - \frac{1}{|\mathrm{SL}_2(q)|} \right| \ll \mathfrak{E}(Y;q), \tag{41}$$

where

$$\mathfrak{E}(Y;q) := \begin{cases} e^{-c\sqrt{\log Y}}, & \text{if } q \leq C \log Y, \\ q^C Y^{-\Theta}, & \text{if } q > C \log Y. \end{cases} \tag{42}$$

3 The Sifting Set and Initial Manipulations

3.1 Construction of $\mathfrak{A}$

The first goal in this subsection is to construct the appropriate sifting sequence $\mathfrak{A} = \{a_N(n)\}$. Let $\mathcal{A} \subset \mathbb{N}$ be our fixed alphabet with corresponding dimension $\delta_{\mathcal{A}}$ near 1, and let $\Gamma_{\mathcal{A}}$ be the semigroup in (9). Since $\mathcal{A}$ is fixed, we drop the subscripts, writing $\Gamma = \Gamma_{\mathcal{A}}$ and $\delta = \delta_{\mathcal{A}}$.

Let N be the main growing parameter, and let

$$X = N^x, \quad Y = N^y, \quad Z = N^z, \quad x,y,z > 0, \quad x+y+z = 1, \tag{43}$$

be some parameters to be chosen later; in particular,

$$N = XYZ. \tag{44}$$

We think of X as large, $X > N^{1/2}$, and Y as tiny, of size N^{ε}.

Let $\mathfrak{K} = \mathfrak{K}(Y) \subset \Gamma_0 \subset \Gamma$ be the set constructed in Proposition 40. We also create certain subsets

$$\Xi \subset \{\xi \in \Gamma : \|\xi\| < X\}, \qquad \Omega \subset \{\omega \in \Gamma : \|\omega\| < Z\},$$

as follows. Applying Theorem 22 with $N = X$ and

$$\kappa \;=\; 2(1-\delta)+\varepsilon \tag{45}$$

(here ε is fixed, sufficiently small, and δ is sufficiently close to 1), gives a subset $\mathcal{S}'_X$ of $\{\xi \in \mathrm{SL}_2(\mathbb{Z}) : \|\xi\| < X\}$ of size

$$|\mathcal{S}_X \setminus \mathcal{S}'_X| \;<\; X^{2-\kappa} \;=\; X^{2\delta-\varepsilon},$$

cf. (23), and having additive energy controlled as in (24). Note that Hensley's estimate (31) gives

$$\{\xi \in \Gamma : \|\xi\| < X\} \;\asymp\; X^{2\delta},$$

which is too big to be contained in the complement $\mathcal{S}_X \setminus \mathcal{S}'_X$. So defining

$$\Xi \;:=\; \mathcal{S}'_X \cap \{\xi \in \Gamma : \|\xi\| < X\} \tag{46}$$

gives a subset of Γ of proportional size,

$$|\Xi| \;\asymp\; X^{2\delta}, \tag{47}$$

and controlled additive energy,

$$E(\Xi) \;\le\; E(\mathcal{S}'_X) \;\ll\; X^{4+4(1-\delta)+3\varepsilon}. \tag{48}$$

We construct the set Ω in the same fashion, obtaining

$$|\Omega| \;\asymp\; Z^{2\delta}, \tag{49}$$

and

$$E(\Omega) \;\ll\; Z^{4+4(1-\delta)+3\varepsilon}. \tag{50}$$

Note that, since δ will be taken close to 1, (48), (50) provide a nearly optimal additive energy control.

Then we can finally define the sifting sequence $\mathfrak{A} = \{a_N(n)\}$ by:

$$a_N(n) := \sum_{\xi\in\Xi} \sum_{\mathfrak{a}\in\mathfrak{K}} \sum_{\omega\in\Omega} \mathbf{1}_{\{n=\mathrm{tr}(\xi\mathfrak{a}\omega)\}}. \tag{51}$$

Note that $a_N(n)$ is supported on $n \ll N$ by (44). We record from the above that

$$|\mathfrak{A}| = |\Xi|\cdot|\mathfrak{K}|\cdot|\Omega| \gg |\mathfrak{K}|(XZ)^{2\delta}. \tag{52}$$

3.2 Initial Manipulation

Next for parameters $1 \ll Q_0 < \mathcal{Q}$ and any square-free $\mathfrak{q} < \mathcal{Q}$, we decompose

$$\begin{aligned} |\mathfrak{A}_{\mathfrak{q}}| \;&=\; \sum_{n\equiv 0(\mathfrak{q})} a_N(n) = \sum_n \frac{1}{\mathfrak{q}} \sum_{q|\mathfrak{q}} \sideset{}{'}\sum_{r(q)} e_q(rn) a_N(n) \\ &=\; \mathcal{M}_{\mathfrak{q}} + r(\mathfrak{q}), \end{aligned} \tag{53}$$

say, according to whether or not $q < Q_0$. Here

$$\mathcal{M}_{\mathfrak{q}} \;:=\; \sum_n \frac{1}{\mathfrak{q}} \sum_{\substack{q|\mathfrak{q}\\ q<Q_0}} \sideset{}{'}\sum_{r(q)} e_q(rn) a_N(n) \tag{54}$$

will be treated as a "main" term, the remainder $r(\mathfrak{q})$ being an error.

4 Main Term Analysis

In this section, we analyze the main term, $\mathcal{M}_{\mathfrak{q}}$, proving the following

Proposition 55. *Let β be the multiplicative function given at primes by*

$$\beta(p) := \frac{1}{p}\left(1+\frac{\chi_4(p)}{p}\right)\left(1-\frac{1}{p^2}\right)^{-1}, \tag{56}$$

where χ_4 is the Dirichlet character mod 4. There is a decomposition

$$\mathcal{M}_{\mathfrak{q}} = \beta(\mathfrak{q})\,|\mathfrak{A}| + r^{(1)}(\mathfrak{q}) + r^{(2)}(\mathfrak{q}), \tag{57}$$

where

$$\sum_{\mathfrak{q}<\mathcal{Q}} |r^{(1)}(\mathfrak{q})| \ll |\mathfrak{A}| \log \mathcal{Q}\left(\frac{1}{e^{c\sqrt{\log Y}}} + \mathcal{Q}_0^C Y^{-\Theta}\right), \tag{58}$$

and

$$\sum_{\mathfrak{q}<\mathcal{Q}} |r^{(2)}(\mathfrak{q})| \ll |\mathfrak{A}| \frac{\mathcal{Q}^{\varepsilon}}{\mathcal{Q}_0}. \tag{59}$$

Proof. Inserting the definition (51) of a_N into (54) gives

$$\begin{aligned}\mathcal{M}_{\mathfrak{q}} &= \sum_{\xi\in\Xi}\sum_{\mathfrak{a}\in\mathfrak{K}}\sum_{\omega\in\Omega}\frac{1}{\mathfrak{q}}\sum_{\substack{q|\mathfrak{q}\\ q<\mathcal{Q}_0}}\sum_{r(q)}{}' e_q(r\,\mathrm{tr}(\xi\mathfrak{a}\omega)) \\ &= \sum_{\xi\in\Xi}\sum_{\omega\in\Omega}\frac{1}{\mathfrak{q}}\sum_{\substack{q|\mathfrak{q}\\ q<\mathcal{Q}_0}}\sum_{r(q)}{}'\sum_{\mathfrak{a}_0\in \mathrm{SL}_2(q)} e_q(r\,\mathrm{tr}(\xi\mathfrak{a}_0\omega))\left[\sum_{\substack{\mathfrak{a}\in\mathfrak{K}\\ \mathfrak{a}\equiv\mathfrak{a}_0(q)}} 1\right].\end{aligned}$$

Apply (41) to the innermost sum, giving

$$\mathcal{M}_{\mathfrak{q}} = \mathcal{M}_{\mathfrak{q}}^{(1)} + r^{(1)}(\mathfrak{q}),$$

say, where

$$\mathcal{M}_{\mathfrak{q}}^{(1)} := |\mathfrak{A}|\,\frac{1}{\mathfrak{q}}\sum_{\substack{q|\mathfrak{q}\\ q<\mathcal{Q}_0}}\sum_{r(q)}{}'\frac{1}{|\mathrm{SL}_2(q)|}\sum_{\gamma\in\mathrm{SL}_2(q)} e_q(r\,\mathrm{tr}(\gamma)),$$

and

$$|r^{(1)}(\mathfrak{q})| \ll |\mathfrak{A}|\,\frac{1}{\mathfrak{q}}\sum_{\substack{q|\mathfrak{q}\\ q<\mathcal{Q}_0}} q^4\,\mathfrak{E}(Y;q).$$

The error $\mathfrak{E}$ is as given in (42). We estimate

$$\begin{aligned}\sum_{\mathfrak{q}<\mathcal{Q}}|r^{(1)}(\mathfrak{q})| &\ll |\mathfrak{A}|\sum_{q<\mathcal{Q}_0} q^4\,\mathfrak{E}(Y;q)\sum_{\substack{\mathfrak{q}<\mathcal{Q}\\ \mathfrak{q}\equiv 0(q)}}\frac{1}{\mathfrak{q}} \\ &\ll |\mathfrak{A}|\log\mathcal{Q}\left[(\log Y)^C e^{-c\sqrt{\log Y}} + \mathcal{Q}_0^C Y^{-\Theta}\right],\end{aligned}$$

thus proving (58).

Returning to $\mathcal{M}_{\mathfrak{q}}^{(1)}$, we add back in the large divisors $q \mid \mathfrak{q}$, writing

$$\mathcal{M}_{\mathfrak{q}}^{(1)} \;=\; \mathcal{M}_{\mathfrak{q}}^{(2)} + r^{(2)}(\mathfrak{q}),$$

say, where

$$\mathcal{M}_{\mathfrak{q}}^{(2)} \;:=\; |\mathfrak{A}|\,\frac{1}{\mathfrak{q}}\sum_{q|\mathfrak{q}}\sideset{}{'}\sum_{r(q)}\frac{1}{|\mathrm{SL}_2(q)|}\sum_{\gamma\in\mathrm{SL}_2(q)} e_q(r\,\mathrm{tr}(\gamma)).$$

Let $\rho(q)$ be the multiplicative function given at primes by

$$\rho(p) \;:=\; \frac{1}{|\mathrm{SL}_2(p)|}\sum_{\gamma\in\mathrm{SL}_2(p)}\sideset{}{'}\sum_{r(p)} e_p(r\,\mathrm{tr}(\gamma)),$$

so that

$$\mathcal{M}_{\mathfrak{q}}^{(2)} \;=\; |\mathfrak{A}|\,\frac{1}{\mathfrak{q}}\prod_{p|\mathfrak{q}}\Big(1+\rho(p)\Big).$$

By an elementary computation, we evaluate explicitly that

$$\rho(p) \;=\; \frac{p(p+\chi_4(p))}{p^2-1} - 1,$$

and hence

$$\mathcal{M}_{\mathfrak{q}}^{(2)} \;=\; |\mathfrak{A}|\cdot\beta(\mathfrak{q}),$$

with β as given in (56).

Lastly, we deal with $r^{(2)}$. It is easy to see from the above that $|\rho(p)| \ll 1/p$, so $|\rho(q)| \ll q^{\varepsilon}/q$, giving the bound

$$|r^{(2)}(\mathfrak{q})| \;\ll\; |\mathfrak{A}|\,\frac{1}{\mathfrak{q}}\sum_{\substack{q|\mathfrak{q}\\ q\geq Q_0}}\frac{q^{\varepsilon}}{q} \;\ll\; |\mathfrak{A}|\,\frac{\mathfrak{q}^{\varepsilon}}{\mathfrak{q}}\frac{1}{Q_0}.$$

The estimate (59) follows immediately, completing the proof. □

Remark 60. Since Y in (43) is a small power of N, the first error term in (58) saves an arbitrary power of $\log N$, as required in (28). For the rest of the paper, all other error terms will be power savings. In particular, setting

$$Q_0 \;=\; N^{\alpha_0}, \qquad \alpha_0 > 0, \tag{61}$$

the error in (59) is already a power savings, while the second term in (58) requires that

$$\alpha_0 \;<\; \frac{y\Theta}{C}. \tag{62}$$

It is here that we crucially use the expander property for Γ, but the final level of distribution will be independent of Θ.

5 Proof of Theorem 17

5.1 Initial Manipulations

Returning to (53), it remains to control the average error term

$$\mathcal{E} := \sum_{\mathfrak{q}<\mathcal{Q}} |r(\mathfrak{q})| = \sum_{\mathfrak{q}<\mathcal{Q}} \left| \sum_{\xi\in\Xi} \sum_{\mathfrak{a}\in\mathfrak{K}} \sum_{\omega\in\Omega} \frac{1}{\mathfrak{q}} \sum_{\substack{q|\mathfrak{q}\\ q\geq Q_0}} \sum_{r(q)}{}' e_q(r\,\mathrm{tr}(\xi\mathfrak{a}\omega)) \right|, \tag{63}$$

the goal being to verify (28). We first massage $\mathcal{E}$ into a more convenient form.

Let $\zeta(\mathfrak{q}) := |r(\mathfrak{q})|/r(\mathfrak{q})$ be the complex unit corresponding to the absolute value in (63), and rearrange terms as:

$$\mathcal{E} = \sum_{Q_0\leq q<\mathcal{Q}} \frac{\zeta_1(q)}{q} \sum_{\xi\in\Xi} \sum_{\mathfrak{a}\in\mathfrak{K}} \sum_{\omega\in\Omega} \sum_{r(q)}{}' e_q(r\,\mathrm{tr}(\xi\mathfrak{a}\omega)),$$

where we have set

$$\zeta_1(q) := \sum_{\mathfrak{q}<\mathcal{Q}/q} \frac{\zeta(q\mathfrak{q})}{\mathfrak{q}}.$$

Note for future reference that

$$|\zeta_1(q)| \ll \log \mathcal{Q}. \tag{64}$$

Leaving the special set $\mathfrak{K}$ alone, we break the q sum into dyadic pieces

$$\mathcal{E} \ll \sum_{\mathfrak{a}\in\mathfrak{K}} \sum_{\substack{Q_0\leq Q<\mathcal{Q}\\ \text{dyadic}}} |\mathcal{E}_1(Q;\mathfrak{a})|, \tag{65}$$

where we have defined

$$\mathcal{E}_1(Q;\mathfrak{a}) := \sum_{q\asymp Q} \frac{\zeta_1(q)}{q} \sum_{\xi\in\Xi} \sum_{\omega\in\Omega} \sum_{r(q)}{}' e_q(r\,\mathrm{tr}(\xi\mathfrak{a}\omega)). \tag{66}$$

It remains to estimate $\mathcal{E}_1(Q;\mathfrak{a})$.

5.2 Bounding $\mathcal{E}_1$

We claim the following estimate.

Theorem 67. *For any $\varepsilon > 0$, and any $1 \ll Q_0 < Q < \mathcal{Q} < N \to \infty$, with*

$$Q < Z, \qquad Q^2 = o(X), \tag{68}$$

we have

$$|\mathcal{E}_1(Q;\mathfrak{a})| \ll N^{1-\delta+\varepsilon} Q |\Omega|^{1/2} X^2 Z \left[\frac{Q^{1/2}}{Z^{1/2}} + \frac{1}{Q^{1/8}} \right]. \tag{69}$$

Proof. Start by applying Cauchy-Schwarz in q, r, and the "short" variable ω to (66). This opens the "long" variable ξ into a pair of such, as follows.

$$\begin{aligned}|\mathcal{E}_1(Q;\mathfrak{a})|^2 &\ll \left(\sum_{q\asymp Q}\sum_{\omega\in\Omega}\sum_{r(q)}{}' \frac{|\zeta_1(q)|^2}{q^2}\right)\left(\sum_{q\asymp Q}\sum_{\substack{\omega\in \mathrm{SL}_2(\mathbb{Z})\\ \|\omega\|<Z}}\sum_{r(q)}{}'\left|\sum_{\xi\in\Xi} e_q(r\,\mathrm{tr}(\xi\mathfrak{a}\omega))\right|^2\right)\\ &\ll |\Omega|\log^2 Q\left(\sum_{\xi,\xi'\in\Xi}\left|\sum_{q\asymp Q}\sum_{r(q)}{}'\sum_{\omega\in\Omega} e_q(r\,\mathrm{tr}((\xi-\xi')\mathfrak{a}\omega))\right|\right).\end{aligned}$$

Collect the difference of ξ and ξ' into a single variable, writing

$$\xi-\xi' = M \in M_{2\times 2}(\mathbb{Z}) \cong \mathbb{Z}^4,$$

and setting

$$\mathcal{N}_M^{\Xi}(X) := \sum_{\xi,\xi'\in\Xi} \mathbf{1}_{\{M=\xi-\xi'\}}. \tag{70}$$

In view of the additive energy bound (48), we have

$$\sum_{M\in\mathbb{Z}^4}\mathcal{N}_M^{\Xi}(X)^2 \ll X^{4+\tau},$$

where we have set (cf. (45))

$$\tau = 4(1-\delta)+3\varepsilon.$$

So writing

$$|\mathcal{E}_1(Q;\mathfrak{a})|^2 \ll N^{\varepsilon}|\Omega|\sum_{\substack{M\in\mathbb{Z}^4\\ \|M\|\ll X}}\mathcal{N}_M^{\Xi}(X)\left|\sum_{q\asymp Q}\sum_{r(q)}{}'\sum_{\omega\in\Omega} e_q(r\,\mathrm{tr}(M\mathfrak{a}\omega))\right|,$$

we apply Cauchy-Schwarz in the M variable, giving

$$\begin{aligned}|\mathcal{E}_1(Q;\mathfrak{a})|^4 &\ll N^{\varepsilon}|\Omega|^2X^{4+\tau}\sum_{M\in\mathbb{Z}^4}\Psi\left(\frac{M}{X}\right)\left|\sum_{q\asymp Q}\sum_{r(q)}{}'\sum_{\omega\in\Omega} e_q(r\,\mathrm{tr}(M\mathfrak{a}\omega))\right|^2\\ &\ll N^{\varepsilon}X^{\tau}|\Omega|^2X^4\sum_{q,q'\asymp Q}\sum_{r(q)}{}'\sum_{r'(q')}{}'\sum_{\omega,\omega'\in\Omega}\\ &\qquad\sum_{M\in\mathbb{Z}^4}\Psi\left(\frac{M}{X}\right)e\left(M\cdot\left(\frac{r}{q}\mathfrak{a}\omega-\frac{r'}{q'}\mathfrak{a}\omega'\right)\right)\\ &\ll X^{\tau}Q^4|\Omega|^2X^8\sum_{q,q'\asymp Q}\sum_{r(q)}{}'\sum_{r'(q')}{}'\sum_{\omega,\omega'\in\Omega}\mathbf{1}_{\{\|\frac{q'r\mathfrak{a}\omega-r'q\mathfrak{a}\omega'}{qq'}\|<\frac{1}{X}\}}.\end{aligned}$$

Here we have inserted a suitable bump function Ψ and applied Poisson summation to the sum on $M\in\mathbb{Z}^4$. Assuming $qq'\ll Q^2=o(X)$ as in (68), the innermost condition implies

$$q'r\omega \equiv qr'\omega' \pmod{qq'}.$$

Taking determinants gives

$$(q'r)^2 \equiv (r'q)^2 (\mathrm{mod}\, qq'),$$

whence reducing mod q gives

$$(q'r)^2 \equiv 0 (\mathrm{mod}\, q).$$

But this implies $(q')^2 \equiv 0 (\mathrm{mod}\, q)$, since $(r,q) = 1$. Because q is square-free, we have thus forced $q' \equiv 0 (\mathrm{mod}\, q)$. By symmetry, we also have $q \equiv 0 (\mathrm{mod}\, q')$, and hence

$$q = q', \qquad r \equiv ur' (\mathrm{mod}\, q), \qquad \text{and} \qquad \omega \equiv u\omega' (\mathrm{mod}\, q),$$

where $u^2 \equiv 1(q)$; note that there are at most $2^{\nu(q)} \ll N^\varepsilon$ such u's. We then have

$$|\mathcal{E}_1(Q;\mathfrak{a})|^4 \ll N^\varepsilon X^\tau |\Omega|^2 X^8 \sum_{q \asymp Q} \sum_{u^2 \equiv 1(q)} \sideset{}{'}\sum_{\substack{r, r' (q) \\ r \equiv ur'(q)}} \sum_{\omega, \omega' \in \Omega} \mathbf{1}_{\{\omega \equiv u\omega' (\mathrm{mod}\, q)\}}.$$

We dispose of u in the last summation via Cauchy-Schwarz:

$$\begin{aligned}
\sum_{\omega,\omega' \in \Omega} \mathbf{1}_{\{\omega \equiv u\omega' (\mathrm{mod}\, q)\}} &= \sum_{\gamma \in \mathrm{SL}_2(q)} \left[\sum_{\omega \in \Omega} \mathbf{1}_{\{\omega \equiv \gamma(q)\}} \right] \left[\sum_{\omega' \in \Omega} \mathbf{1}_{\{u\omega' \equiv \gamma(q)\}} \right] \\
&\leq \left(\sum_{\gamma \in \mathrm{SL}_2(q)} \left[\sum_{\omega \in \Omega} \mathbf{1}_{\{\omega \equiv \gamma(q)\}} \right]^2 \right)^{1/2} \\
&\quad \times \left(\sum_{\gamma \in \mathrm{SL}_2(q)} \left[\sum_{\omega' \in \Omega} \mathbf{1}_{\{u\omega' \equiv \gamma(q)\}} \right]^2 \right)^{1/2} \\
&= \sum_{\omega,\omega' \in \Omega} \mathbf{1}_{\{\omega \equiv \omega' (\mathrm{mod}\, q)\}},
\end{aligned}$$

since $(u,q) = 1$. Applying this estimate gives

$$\begin{aligned}
|\mathcal{E}_1(Q;\mathfrak{a})|^4 &\ll N^\varepsilon X^\tau Q\, |\Omega|^2 X^8 \sum_{q \asymp Q} \sum_{\omega,\omega' \in \Omega} \mathbf{1}_{\{\omega \equiv \omega' (\mathrm{mod}\, q)\}} \\
&= N^\varepsilon X^\tau Q\, |\Omega|^2 X^8 \sum_{q \asymp Q} \sum_{\substack{M \in \mathbb{Z}^4 \\ M \equiv 0(q)}} \mathcal{N}_M^\Omega(Z),
\end{aligned}$$

where we have now set

$$\mathcal{N}_M^\Omega(Z) := \sum_{\omega,\omega' \in \Omega} \mathbf{1}_{\{\omega - \omega' = M\}}.$$

We first isolate the $M = 0$ term, writing

$$|\mathcal{E}_1(Q;\mathfrak{a})|^4 \ll N^\varepsilon X^\tau Q\, |\Omega|^2 X^8 \left(QZ^2 + \mathcal{E}_2 \right), \tag{71}$$

say, where

$$\mathcal{E}_2 := \sum_{q \asymp Q} \sum_{\substack{M \in \mathbb{Z}^4 \\ M \equiv 0(q), M \neq 0}} \mathcal{N}_M^\Omega(Z).$$

Applying the Cauchy-Schwarz inequality in the variables q and M and recalling (68), i.e. $Q < Z$ gives

$$\begin{aligned}\mathcal{E}_2^2 &\ll Q\Big(\frac{Z}{Q}\Big)^4 \sum_{q\asymp Q} \sum_{\substack{M\in\mathbb{Z}^4, M\neq 0\\ M\equiv 0(q)}} \mathcal{N}_M^{\Omega}(Z)^2 \\ &\ll \frac{Z^4}{Q^3} \sum_{M\in\mathbb{Z}^4, M\neq 0} \mathcal{N}_M^{\Omega}(Z)^2 \sum_{q|M} 1 \ll \frac{Z^4}{Q^3} N^{\varepsilon} \sum_M \mathcal{N}_M^{\Omega}(Z)^2 \\ &\ll \frac{Z^{8+\tau}}{Q^3} N^{\varepsilon}\end{aligned} \tag{72}$$

where this time the additive energy bound (50) was used.

Combining (72) with (71) gives (69), as claimed. □

5.3 Proof of Theorem 17

We give a sketch, as the details are very similar to [BK17, §6]. Inserting (69) in (65) and recalling (49) and (52) gives

$$\mathcal{E} \ll N^{3(1-\delta)+\varepsilon} |\mathfrak{A}| \left(\frac{\mathcal{Q}^{1/2}}{Z^{1/2}} + \frac{1}{Q_0^{1/8}} \right). \tag{73}$$

With δ very near 1, the second term in (73) is a power saving as long as Q_0 is some tiny power.[4] Recalling (61), (62), this requires $Y = N^y$ with $y > 0$ an arbitrary small fixed exponent (taking δ accordingly close to 1). Writing $\mathcal{Q} = N^{\alpha}$, $X = N^x$, $Z = N^z$ with

$$1 = x + y + z \approx x + z$$

the first term in (73) gives a power savings provided $z > \alpha + 6(1-\delta+\varepsilon)$, while (68) is satisfied for $x > 2\alpha$. Hence, taking $\delta = \delta(\eta)$ close enough to 1, we reach exponent of distribution $\alpha > \frac{1}{3} - \eta$. This proves Theorem 17.

6 Proof of Theorem 22

Recall our notation

$$\mathcal{S}_N = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \|\gamma\| < N\},$$

and for an integer matrix $M \in M_{2\times 2}(\mathbb{Z}) = \mathbb{Z}^4$, set

$$\mathcal{N}_N(M) := \sum_{\gamma,\gamma'\in\mathcal{S}_N} \mathbf{1}_{\{\gamma+\gamma'=M\}}.$$

This is the number of representations of M as a sum of two elements of $\mathcal{S}_N$. The additive energy of $\mathcal{S}_N$ is the square of the L^2 norm of $\mathcal{N}_N$:

$$E(\mathcal{S}_N) := \#\{\gamma_1,\gamma_2,\gamma_3,\gamma_4 \in \mathcal{S}_N : \gamma_1+\gamma_2 = \gamma_3+\gamma_4\} = \sum_{M\in\mathbb{Z}^4} \mathcal{N}_N(M)^2.$$

[4] It is here that we crucially need expansion to a *fixed* alphabet, so we can move δ near 1 without affecting Q_0; cf. §2.3.

Remark 74.

- When $M = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, we clearly have
$$\mathcal{N}_N(M) = |\mathcal{S}_N| \asymp N^2,$$
so this one term already contributes N^4 to the energy.
- If $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, then the number of representations, $\mathcal{N}_N(M)$, is of order N, since for all $n \ll N$,
$$\begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} - \begin{pmatrix} n-1 & 1 \\ -1 & 0 \end{pmatrix} = M. \tag{75}$$
Such M's have determinant zero, and we show below that this is the key feature allowing (75). There are about N^2 such $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ (since once we fix $|a|, |d| \le N$, there are only N^ε values for b, c satisfying $ad = bc$), and each contributes $\mathcal{N}_N(M)^2 \asymp N^2$ to the energy, for a net contribution of around N^4.
- Generically, we expect $\mathcal{N}_N(M)$ to be of size N^ε, which again would contribute N^4 to the energy, since there are this many generic M.

It is thus reasonable to make the following

Conjecture 76. *The additive energy of* $\mathrm{SL}_2(\mathbb{Z})$ *is as small as possible,*
$$E(\mathcal{S}_N) \ll N^{4+\varepsilon}.$$

While we are not able to prove this full conjecture, Theorem 22 will be a sufficiently strong substitute in our applications.

Our first goal is to understand straight lines in $G := \mathrm{SL}_2(\mathbb{R})$; these are responsible for the behavior in (75).

Lemma 77. *Two matrices $A, B \in G$ lie on a line in G; that is, for all $t \in \mathbb{R}$,*
$$tA + (1-t)B \in G, \tag{78}$$
if and only if
$$\det(A - B) = 0.$$

Proof. We use the elementary formula:
$$\det(X+Y) = \det(X) + \det(Y) + \det(X)\,\mathrm{tr}(X^{-1} \cdot Y). \tag{79}$$
By (78), we have
$$1 = \det(tA + (1-t)B) = t^2 + (1-t)^2 + t^2\,\mathrm{tr}(t^{-1}A^{-1} \cdot (1-t)B),$$
which simplifies to
$$(\mathrm{tr}(A^{-1}B) - 2)t(t-1) = 0.$$
This equation holds for all t if and only if $\mathrm{tr}(A^{-1}B) = 2$. Now using (79) again gives
$$\det(A - B) = 2 - \mathrm{tr}(A^{-1} \cdot B),$$
from which the claim follows. □

Remark 80. This explains the phenomenon observed in (75). Indeed, let $\gamma_t = B + t(A-B) = tA + (1-t)B$ as in (78). So if A, B and t are all integral, and hence $\gamma_t \in \mathrm{SL}_2(\mathbb{Z})$, then $M = A - B$ has many representations as $\gamma_t - \gamma_{t-1} = M$.

Next recall the Cartan decomposition $G = KAK$, that is, any $g \in G$ can be expressed as

$$g = k_\theta a_t k_\varphi,$$

where

$$k_\theta \ = \ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \qquad \text{and} \qquad a_t \ = \ \begin{pmatrix} e^t & \\ & e^{-t} \end{pmatrix}, \ t \geq 0.$$

Lemma 81. *There is a small absolute constant $c > 0$ with the following property. Let $A_1, A_2 \in \mathcal{S}_N$, and write*

$$A_j \ = \ k_{\theta_j} a_{t_j} k_{\varphi_j}.$$

Assume that

$$|\theta_1 - \theta_2| < \frac{c}{N}, \quad |t_1 - t_2| < c, \quad \text{and} \quad |\varphi_1 - \varphi_2| < \frac{c}{N}.$$

Then

$$\det(A_1 - A_2) = 0.$$

Proof. Using (79) yet again gives

$$\det(A_1 - A_2) \ = \ 2 - \mathrm{tr}(A_1^{-1} \cdot A_2) \ = \ 2 - \mathrm{tr}(k_{\theta_2 - \theta_1} a_{t_2} k_{\varphi_2 - \varphi_1} a_{-t_1}).$$

Write $\theta' = \theta_2 - \theta_1$ and $\varphi' = \varphi_2 - \varphi_1$. One then computes:

$$\begin{aligned} \mathrm{tr}(k_{\theta'} a_{t_2} k_{\varphi'} a_{-t_1}) \ &= \ \cos(\theta')\cos(\varphi')(e^{t_1 - t_2} + e^{t_2 - t_1}) \\ &\qquad - \sin(\theta')\sin(\varphi')(e^{t_1 + t_2} + e^{-t_1 - t_2}) \\ &= \ (1 + O(c^2 N^{-2}))(2 + O(c)) \\ &\qquad - O(c^2 N^{-2}) O(N^2) \\ &= \ 2 + O(c), \end{aligned}$$

since $c < 1$. Thus we have $\det(A_1 - A_2) = O(c)$, but since this is an integer, we can take c small enough (independent of N) to force the desired conclusion. □

In light of this lemma, we restrict our attention to "sub-slabs" of $\mathcal{S}_N$ in which the θ and φ parameters are restricted to intervals of length c/N, and t to an interval of length $c \asymp 1$. That is, for each such triplet $\Theta_\alpha, T_\alpha, \Phi_\alpha$ of intervals of length $|\Theta_\alpha| = |\Phi_\alpha| = c/N$, $|T_\alpha| = c$, set

$$\mathcal{S}_{N,\alpha} \ := \ \{A = k_\theta a_t k_\varphi \in \mathcal{S}_N : (\theta, t, \varphi) \in \Theta_\alpha \times T_\alpha \times \Phi_\alpha\}.$$

We will require $O(N^2)$ such to cover $\mathcal{S}_N$:

$$\mathcal{S}_N = \bigsqcup_\alpha \mathcal{S}_{N,\alpha}.$$

The previous lemma tells us that the elements of a slab $\mathcal{S}_{N,\alpha}$, if any, snap to a single affine line in $\mathrm{SL}_2(\mathbb{R}) \subset \mathbb{R}^4$. If we can make the "slope" of this line large, then the points will be far-spaced, implying that there can be only very few of them in a single slab. Let us make this precise.

Assume that $A, B \in \mathcal{S}_{N,\alpha}$; then $\det(A-B) = 0$ by Lemma 81. Set $M = B - A$; this is the "slope." Since $\det M = 0$, we can write M as:

$$M = \begin{pmatrix} rv_1 & sv_1 \\ rv_2 & sv_2 \end{pmatrix}, \tag{82}$$

in which $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ is a primitive vector in $\mathbb{Z}^2$, and $r, s \in \mathbb{Z}$. Observe moreover that

$$\det B \;=\; \det(A+M) \;=\; \det A + \det M + \det A \cdot \mathrm{tr}(A^{-1} \cdot M),$$

where we again used (79). Hence

$$\mathrm{tr}(A^{-1} \cdot M) = 0, \tag{83}$$

which, on writing $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, gives

$$drv_1 - brv_2 - csv_1 + asv_2 = 0. \tag{84}$$

Multiplying (84) by a and using $ad = 1 - bc$ gives

$$rv_1 = bcrv_1 + abrv_2 + acsv_1 - a^2 sv_2 = (cv_1 + av_2)(br - as),$$

which implies that

$$|cv_1 + av_2| \; |br - as| \le |rv_1| \le \|M\|. \tag{85}$$

This equation gives our requisite lower bound on the slope. We can finally define the desired subset $\mathcal{S}'_N$ of $\mathcal{S}_N$.

Definition 86. Given small parameters $\kappa > 0$ and $\varepsilon > 0$, set

$$\kappa_1 = \kappa + \varepsilon,$$

and define

$$\begin{aligned} \mathcal{S}'_N \;=\; \Bigg\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \|A\| \le N \text{ and } \\ \min_{\substack{k \in \mathbb{Z}^2 \\ 0 < |k| < N^{1-\kappa_1}}} |k| \cdot \min\left(|k_1 a + k_2 b|, |k_1 a + k_2 c|\right) > N^{1-\kappa_1} \Bigg\}. \end{aligned} \tag{87}$$

Lemma 88. *We have*

$$|\mathcal{S}_N \setminus \mathcal{S}'_N| \;\ll\; N^{2-\kappa_1+\varepsilon}. \tag{89}$$

Thus (23) holds, since $\kappa < \kappa_1$. (Recall that ε is arbitrary while ε here is fixed.)

Proof. We will bound the number of $A \in \mathrm{SL}_2(\mathbb{Z})$ with $\|A\| < N$ and for which there exists some $0 < |k| < N^{1-\kappa_1}$ so that

$$|k_1 a + k_2 b| \ \le \ N^{1-\kappa_1}/|k|.$$

Break $|k|$ dyadically into $|k| \asymp K$, with $K < N^{1-\kappa_1}$. We may assume $|a| \ge |b| > 0$ (since $b = 0$ gives only parabolic elements), so $(a,b) = 1$, and break $|a|$ dyadically into $|a| \asymp M$, with $M \le N$. Write

$$y \ = \ k_1 a + k_2 b,$$

so that

$$|y| \ \ll \ \frac{N^{1-\kappa_1}}{K}.$$

Thus we have

$$|\mathcal{S}_N \setminus \mathcal{S}'_N| \ \ll \sum_{\substack{K < N^{1-\kappa_1} \\ \text{dyadic}}} \sum_{\substack{M \le N \\ \text{dyadic}}} \sum_{\substack{k \in \mathbb{Z}^2 \\ |k| \asymp K}} \sum_{\substack{y \in \mathbb{Z} \\ |y| \ll \frac{N^{1-\kappa_1}}{K}}} \sum_{\substack{(a,b)=1, |b| \le |a| \asymp M \\ y = k_1 a + k_2 b}} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ |(c,d)| < N}} \mathbf{1}_{\{ad-bc=1\}}. \tag{90}$$

We will estimate this expression from the inside out.

Once (a,b) is determined, the equation $ad - bc = 1$ has a unique solution (c_0, d_0) with $0 \le d_0 < |a|$ and $0 \le c_0 < |b|$, and all other solutions (c,d) satisfy $c \equiv c_0 (\mathrm{mod}\, a)$. Of course, once c is determined, so is d, and hence the last summation of (90) contributes

$$\ll \ 1 + \frac{N}{M}.$$

To determine (a,b), we handle separately the cases $y = 0$ or not. If the former, that is, $k_1 a = -k_2 b$, we first choose k_1 and a (for which there are KM choices), and then there are N^{ε} choices for k_2 and b. This gives a net contribution to (90) of

$$\ll \sum_{\substack{K < N^{1-\kappa_1} \\ \text{dyadic}}} \sum_{\substack{M \le N \\ \text{dyadic}}} KMN^{\varepsilon} \left(1 + \frac{N}{M}\right) \ \ll \ N^{2-\kappa_1+\varepsilon}.$$

Now we assume $y \neq 0$. We want to exploit $k_2 b = y - k_1 a$, so we must handle separately whether $y - k_1 a = 0$ or not. In the case $y = k_1 a$, we choose y first (with at most $N^{1-\kappa_1}/K$ possible values), whence there are N^{ε} choices for k_1 and a (recall $y \neq 0$). Since $b \neq 0$, the condition $k_2 b = y - k_1 a = 0$ implies that $k_2 = 0$; then we are free to choose b (in M choices). In total, the contribution of this case to (90) is

$$\ll \sum_{\substack{K < N^{1-\kappa_1} \\ \text{dyadic}}} \sum_{\substack{M \le N \\ \text{dyadic}}} \frac{N^{1-\kappa_1}}{K} N^{\varepsilon} M \left(1 + \frac{N}{M}\right) \ \ll \ N^{2-\kappa_1+\varepsilon}.$$

Lastly we consider the case $y \neq 0$ and $y \neq k_1 a$. We fix y, k_1, and a, with $N^{1-\kappa-1}/K \cdot K \cdot M$ choices. Then there are N^{ε} choices for k_2 and b satisfying $k_2 b = y - k_1 a$, giving a final contribution of

$$\ll \sum_{\substack{K < N^{1-\kappa_1} \\ \text{dyadic}}} \sum_{\substack{M \le N \\ \text{dyadic}}} \frac{N^{1-\kappa_1}}{K} KMN^{\varepsilon} \left(1 + \frac{N}{M}\right) \ \ll \ N^{2-\kappa_1+\varepsilon}$$

to (90). This completes the proof. □

Now suppose $A,B \in \mathcal{S}_{N,\alpha} \cap \mathcal{S}'_N$ and $M = B - A \neq 0$. We claim that $\|M\| \geq N^{1-\kappa_1}$. Assume by contradiction that $\|M\| < N^{1-\kappa_1}$. Then M is of the form (82) satisfying also (83), and moreover the vectors $(v_2, v_1), (-s, r)$ are of size at most $N^{1-\kappa_1}$, so enter in the definition of $\mathcal{S}'_N$ in (87). By this definition, we have that

$$\|M\| \;\geq\; |cv_1 + av_2|\,|br - as| \;>\; \frac{N^{1-\kappa_1}}{|v|}\frac{N^{1-\kappa_1}}{|(r,s)|} \;\gg\; \frac{N^{2-2\kappa_1}}{\|M\|},$$

so

$$\|A - B\| \;=\; \|M\| \;\gg\; N^{1-\kappa_1} \;=\; N^{1-\kappa-\varepsilon}.$$

That is, any such A and B, while all lying on a single line, are also very much spaced apart. This immediately gives the following

Corollary 91.

$$|\mathcal{S}_{N,\alpha} \cap \mathcal{S}'_N| \;\ll\; N^{\kappa+\varepsilon},$$

and hence the additive energy of each such slab is

$$E(\mathcal{S}_{N,\alpha} \cap \mathcal{S}'_N) \;\ll\; N^{2\kappa+\varepsilon}|\mathcal{S}_{N,\alpha} \cap \mathcal{S}'_N|. \tag{92}$$

To put the various slabs and their energies together, we appeal to the recent resolution [BD15] of the L^2-decoupling conjecture; more precisely, we require the version for "generalized cones" proved in [Oh16, Theorem 1.1], in the following form.

Theorem 93. *The energy of $\mathcal{S}'_N$ is controlled by that of its slabs by:*

$$E(\mathcal{S}'_N) \;\ll\; N^{2+\varepsilon}\left\{\sum_\alpha E(\mathcal{S}'_N \cap \mathcal{S}_{N,\alpha})\right\}. \tag{94}$$

Before explaining how (94) follows from [Oh16], let us first observe that we now have proved (24) and hence Theorem 22.

Proof of Theorem 22 assuming Theorem 93. Indeed, combining (94) with (92) gives

$$E(\mathcal{S}'_N) \;\ll\; N^{2+\varepsilon}\sum_\alpha N^{2\kappa}|\mathcal{S}_{N,\alpha} \cap \mathcal{S}'_N| \;=\; N^{2+2\kappa+\varepsilon+\varepsilon}|\mathcal{S}'_N| \;\ll\; N^{4+2\kappa+\varepsilon}.$$

□

Remark 95. While we believe Conjecture 76 for the full set $\mathcal{S}_N$, our use of L^2-decoupling makes it absolutely essential to excise certain regions of $\mathcal{S}_N$, leaving only $\mathcal{S}'_N$. Indeed, the region responsible for (75), that is, having $\theta \approx 0,\ \varphi \approx 0$, already contributes N^3 to the energy of its slabs; together with an extra loss of size N^2 on the right side of (94), this would give an unacceptable net contribution of N^5 to the energy.

It remains to establish Theorem 93.

Proof. The linear map

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\frac{a+d}{2}, \frac{a-d}{2}, \frac{b-c}{2}, \frac{b+c}{2}\right)$$

identifies $SL_2(\mathbb{R})$ and the hyperboloid

$$\tilde{C} : x^2 - y^2 + z^2 - w^2 = 1.$$

Thus

$$\frac{1}{N}(\tilde{C} \cap \{\xi \in \mathbb{R}^4 : \|\xi\| \leq N\})$$

is the set

$$\{\xi = (x,y,z,w) : \|\xi\| \leq 1 \text{ and } x^2 - y^2 + z^2 - w^2 = \frac{1}{N^2}\}.$$

This lies within a $\frac{1}{N^2}$-neighborhood of

$$\{\xi \in C : \|\xi\| \leq 1\},$$

where C is the cone

$$C : x^2 - y^2 + z^2 - w^2 = 0.$$

We will use the decoupling theorem obtained in [Oh16] (see Therem 1.1) to the conical surface taking $p = 4$, $\delta \asymp \frac{1}{N^2}$. Denote C_δ a δ-neighborhood of C. In the parametrization

$$x = r\cos\theta, y = r\cos\psi, z = r\sin\theta, w = r\sin\psi \tag{96}$$

the slab-decomposition of C_δ is obtained by restricting $(\theta,\psi) \in I_\alpha \times J_\alpha$, I_α, J_α intervals of size $\delta^{\frac{1}{2}} \asymp \frac{1}{N}$. Denoting $\{\tau_\alpha\}$ the corresponding slabs, we obtain therefore (denoting by $\widehat{f}$ the Fourier transform of f on $\mathbb{R}^4$).

Lemma 97. *Let supp $\widehat{f} \subset C_\delta \cap [\|\xi\| \asymp 1]$ and $f_\alpha = (\widehat{f}|_{\tau_\alpha})^\vee$ the Fourier restriction of f to τ_α. Then*

$$\|f\|_{L^4(B_{N^2})} \ll N^{\frac{1}{2}+\varepsilon} \left(\sum_\alpha \|f_\alpha\|^4_{L^4(B_{N^2})}\right)^{1/4}. \tag{98}$$

Here we have denoted

$$\|f\|_{L^p(B_K)} = \left(\int_{\mathbb{R}^4} |f(x)|^p \left(1 + \frac{|x|}{K}\right)^{-100} dx\right)^{\frac{1}{p}}$$

(i.e. the L^p-norm of f on an appropriately 'smoothed' ball $\{x \in \mathbb{R}^4 : |x| < K\}$).

According to the previous discussion,

$$\tilde{C} \cap [\|\xi\| \asymp N] \subset C_{\frac{1}{N}} \cap [\|\xi\| \asymp N].$$

Rescaling (98) implies therefore

Lemma 99. *Let supp* $\widehat{f} \subset \tilde{C}_{\frac{1}{N}} \cap [\|\xi\| \asymp N]$ *and* $f_\alpha = (\widehat{f}|_{N\tau_\alpha})^\vee$. *Then*

$$\|f\|_{L^4(B_N)} \ll N^{\frac{1}{2}+\varepsilon} \left(\sum_\alpha \|f_\alpha\|^4_{L^4(B_N)} \right)^{\frac{1}{4}}. \tag{100}$$

To prove Theorem 93, we apply Lemma 99 in the discretized setting, taking

$$f(x) = \sum_{\xi \in \mathcal{S}'_N} e(x.\xi). \tag{101}$$

Note that (101) is a 1-periodic function in x and hence

$$N^{-4}\|f\|^4_{L^4(B_N)} \asymp \int_{[0,1]^4} |f(x)|^4 dx = E(\mathcal{S}'_N).$$

Thus (100) allows us to bound the additive energy of $\mathcal{S}'_N$ in terms of the additive energies of its subsets $\mathcal{S}'_N \cap N\tau_\alpha$; it remains to reinterpret intervals of the form $N\tau_\alpha$ as $S_{N,\alpha}$.

As discussed previously, we identify $G = \mathrm{SL}_2(\mathbb{R})$ and $\tilde{C}$, so that $\mathcal{S}'_N$ may be thought of as a subset of $\tilde{C}$. Writing $A \in G$ as

$$A = k_u a_t k_v \tag{102}$$

we have

$$A = e^t \begin{pmatrix} \cos u \cos v & \cos u \sin v \\ -\sin u \cos v & -\sin u \sin v \end{pmatrix} + O\left(\frac{1}{N}\right)$$

and hence, by (96)

$$\begin{cases} r\cos\theta = \frac{1}{2}e^t \cos(u+v) + O(\frac{1}{N}) \\ r\cos\psi = \frac{1}{2}e^t \cos(u-v) + O(\frac{1}{N}) \\ r\sin\theta = \frac{1}{2}e^t \sin(u+v) + O(\frac{1}{N}) \\ r\sin\psi = \frac{1}{2}e^t \sin(v-u) + O(\frac{1}{N}). \end{cases}$$

Thus

$$\begin{cases} e^t = 2r + O(\frac{1}{N}) \\ \cos\theta = \cos(u+v) + O(\frac{1}{N^2}) \\ \cos\psi = \cos(u-v) + O(\frac{1}{N^2}) \\ \sin\theta = \sin(u+v) + O(\frac{1}{N^2}) \\ \sin\psi = \sin(v-u) + O(\frac{1}{N^2}). \end{cases}$$

Restriction of $(\theta,\psi) \in I_\alpha \times J_\alpha$ corresponds therefore to a restriction of $(u,v) \in I'_\alpha \times J'_\alpha$, with I'_α, J'_α size $\frac{1}{N}$ intervals. Hence $\mathcal{S}'_N \cap N\tau_\alpha$ corresponds to $\mathcal{S}'_N \cap \mathcal{S}_{N,\alpha}$, as needed. □

7 Proof of Theorem 21

Recall from (20) that $\mathscr{D}_{\mathcal{A}}$ is the set of discriminants which arise from the alphabet $\mathcal{A}$. Set $\mathcal{A} = \{1,\dots,A\}$ with $A = 50$. In his thesis, Mercat connects the Arithmetic Chaos Conjecture with Zaremba's, by proving the following

Theorem 103 ([Mer12])**.** *If the reduced rational m/n has all partial quotients bounded by A, and if the denominator n arises as a solution to the Pellian equation $n^2 - \Delta r^2 = \pm 1$, then $\mathbb{Q}[\sqrt{\Delta}] \cap \mathfrak{C}_{\mathcal{A}}$ is non-empty.*

In fact, he exhibits a periodic continued fraction in $\mathbb{Q}[\sqrt{\Delta}]$ via an explicit construction involving the partial quotients of m/n.

With his theorem, we can now sketch a

Proof of Theorem 21. Iwaniec's theorem [Iwa78] states that the number of n up to N with $\Delta = n^2 + 1$ having at most 2 prime factors is at least $CN/\log N$. Taking the alphabet $\mathcal{A} = \{1,\dots,50\}$ in [BK14a], the exceptional set is of order much smaller than $N/\log N$, and hence 100% of such denominators n have a coprime numerator m with m/n having all partial quotients bounded by $A = 50$. Clearly setting $r = 1$ gives a solution to $n^2 - \Delta r^2 = -1$, whence $\Delta \in \mathscr{D}_{\mathcal{A}}$ by Mercat's theorem. □

Acknowledgments

It is our pleasure to thank Curt McMullen for many detailed comments and suggestions on an earlier version of this paper, and Tim Browning, Zeev Rudnick, and Peter Sarnak for illuminating conversations. Thanks also to Michael Rubinstein for numerics related to Conjecture 76. The second-named author would like to thank the hospitality of the IAS, where much of this work was carried out.

References

[Art24] Emil Artin. Ein mechanisches system mit quasiergodischen bahnen. *Abh. Math. Sem. Univ. Hamburg*, 3(1):170–175, 1924. 2

[BD15] Jean Bourgain and Ciprian Demeter. The proof of the l^2 decoupling conjecture. *Ann. of Math. (2)*, 182(1):351–389, 2015. 22

[BGS06] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Sieving and expanders. *C. R. Math. Acad. Sci. Paris*, 343(3):155–159, 2006. 5

[BGS10] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Affine linear sieve, expanders, and sum-product. *Invent. Math.*, 179(3):559–644, 2010. 5

[BGS11] J. Bourgain, A. Gamburd, and P. Sarnak. Generalization of Selberg's 3/16th theorem and affine sieve. *Acta Math*, 207:255–290, 2011. 5, 8

[BK10] J. Bourgain and A. Kontorovich. On representations of integers in thin subgroups of $\mathrm{SL}(2,\mathbf{Z})$. *GAFA*, 20(5):1144–1174, 2010. 9

[BK14a] J. Bourgain and A. Kontorovich. On Zaremba's conjecture. *Annals Math.*, 180(1):137–196, 2014. 6, 9, 25

[BK14b] Jean Bourgain and Alex Kontorovich. On the local-global conjecture for integral Apollonian gaskets. *Invent. Math.*, 196(3):589–650, 2014. 9

[BK15] Jean Bourgain and Alex Kontorovich. The Affine Sieve Beyond Expansion I: Thin Hypotenuses. *Int. Math. Res. Not. IMRN*, (19):9175–9205, 2015. 5, 9

[BK16] J. Bourgain and A. Kontorovich. Beyond Expansion III: Reciprocal Geodesics, 2016. `arXiv:1610.07260`. 9

[BK17] J. Bourgain and A. Kontorovich. Beyond expansion II: Low-lying fundamental geodesics. *J. Eur. Math. Soc. (JEMS)*, 19(5):1331–1359, 2017. 9, 10, 17

[BKM15] J. Bourgain, A. Kontorovich, and M. Magee. Thermodynamic expansion to arbitrary moduli, 2015. To appear, *Crelle's Journal* `arXiv:1507.07993`. 8

[FK14] Dmitrii A. Frolenkov and Igor D. Kan. A strengthening of a theorem of Bourgain-Kontorovich II. *Mosc. J. Comb. Number Theory*, 4(1):78–117, 2014.

[Goo41] I. J. Good. The fractional dimensional theory of continued fractions. *Proc. Cambridge Philos. Soc.*, 37:199–228, 1941.

[Gre86] G. Greaves. The weighted linear sieve and Selberg's λ^2-method. *Acta Arith.*, 47(1):71–96, 1986. 6

[Hen89] Doug Hensley. The distribution of badly approximable numbers and continuants with bounded digits. In *Théorie des nombres (Quebec, PQ, 1987)*, pages 371–385. de Gruyter, Berlin, 1989. 8

[Hen92] Doug Hensley. Continued fraction Cantor sets, Hausdorff dimension, and functional analysis. *J. Number Theory*, 40(3):336–358, 1992. 3

[Hen96] Douglas Hensley. A polynomial time algorithm for the Hausdorff dimension of continued fraction Cantor sets. *J. Number Theory*, 58(1):9–45, 1996.

[HK15] Jiuzu Hong and Alex Kontorovich. Almost prime coordinates for anisotropic and thin pythagorean orbits. *Israel J. Math.*, 209(1):397–420, 2015. 9

[Hua15] ShinnYih Huang. An improvement to Zaremba's conjecture. *Geom. Funct. Anal.*, 25(3):860–914, 2015.

[Hum16] G. Humbert. Sur les fractions continues ordinaires et les formes quadratiques binaires indéfinies. *Journal de mathématiques pures et appliquées 7e série*, 2:104–154, 1916. 2

[Iwa78] Henryk Iwaniec. Almost-primes represented by quadratic polynomials. *Invent. Math.*, 47:171–188, 1978. 6, 25

[Jen04] Oliver Jenkinson. On the density of Hausdorff dimensions of bounded type continued fraction sets: the Texan conjecture. *Stoch. Dyn.*, 4(1):63–76, 2004.

[McM09] Curtis T. McMullen. Uniformly Diophantine numbers in a fixed real quadratic field. *Compos. Math.*, 145(4):827–844, 2009. 2, 3

[McM12] C. McMullen. Dynamics of units and packing constants of ideals, 2012. Online lecture notes, http://www.math.harvard.edu/~ctm/expositions/home/text/papers/cf/slides/slides.pdf. 2, 3

[Mer12] P. Mercat. Construction de fractions continues périodiques uniformément bornées, 2012. To appear, *J. Théor. Nombres Bordeaux*. 3, 6, 25

[MOW16] M. Magee, H. Oh, and D. Winter. Uniform congruence counting for Schottky semigroups in $\mathrm{SL}(2,Z)$, 2016. arXiv:1601.03705. 8

[MVW84] C. Matthews, L. Vaserstein, and B. Weisfeiler. Congruence properties of Zariski-dense subgroups. *Proc. London Math. Soc*, 48:514–532, 1984. 4

[Oh16] Changkeun Oh. Remarks on Wolff's inequality for hypersurfaces, 2016. arXiv:1602.05861v2. 22, 23

[Ser85] Caroline Series. The modular surface and continued fractions. *J. London Math. Soc. (2)*, 31(1):69–80, 1985. 2

[Wil80] S. M. J. Wilson. Limit points in the Lagrange spectrum of a quadratic field. *Bull. Soc. Math. France*, 108:137–141, 1980. 3

[Woo78] A. C. Woods. The Markoff spectrum of an algebraic number field. *J. Austral. Math. Soc. Ser. A*, 25(4):486–488, 1978. 3

AUTHORS

Jean Bourgain
School of Mathematics
Institute for Advanced Study
Princeton, NJ
bourgain [at] ias [dot] edu
https://www.math.ias.edu/people/faculty/bourgain

Alex Kontorovich
Department of Mathematics
Rutgers University
New Brunswick, NJ
alex.kontorovich [at] rutgers [dot] edu
http://sites.math.rutgers.edu/~alexk/