AN IMPROVEMENT ON ZAREMBA’S CONJECTURE

SHINNYIH HUANG

Department of Mathematics, Yale University

Abstract. We prove there exists a density one subset \( D \subset \mathbb{N} \) such that each \( n \in D \) is the denominator of a finite continued fraction with partial quotients bounded by 5.

CONTENTS

1. Introduction 1
2. Preliminaries 5
3. Construction of Ensemble 8
4. Major Arcs Analysis 18
5. Setup for Minor Arcs Analysis 25
6. Minor Arcs Analysis I 26
7. Minor Arc Analysis II 32
8. Proof of Theorem 1.6 35
Appendix A. Proof of Proposition 3.4 38
References 44

1. Introduction

1.1. History of Zaremba’s Conjecture. Zaremba’s conjecture has been closely related to numerical integration and pseudorandom number generation, see [Nie78] and [Kon13]. Several new assertions were made since Zaremba’s conjecture was proposed in 1972. To better understand this conjecture, we first introduce some notations.

For \( x \in (0, 1) \), the integers \( a_i \) in the continued fraction expansion of \( x \),

\[
x = [a_1, a_2, \ldots, a_k, \ldots] = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_k + \ddots}}}},
\]

are called partial quotients of \( x \).

We now borrow some notations from the paper [BK13]. For a fixed finite set \( \mathcal{A} \subset \mathbb{N} \), which we call an alphabet, let \( \mathcal{C}_\mathcal{A} \) denote the collection of all \( x \in (0, 1) \) with partial quotients \( a_j \) belonging to the alphabet \( \mathcal{A} \). Moreover, let

\[
A := \max \mathcal{A}.
\]

---

E-mail address: shinnyih.huang@yale.edu.
Date: January 24, 2014.
For some fixed $A$, we say a reduced fraction $x$ is **absolutely Diophantine** if there exists a fraction expansion $x = [a_1, a_2, \ldots, a_k]$ with $a_j$ bounded by $A$ for $\forall 1 \leq j \leq k$.

Let $\mathbb{R}_A$ denote the set of rationals whose partial quotients belong to $A$,

$$\mathbb{R}_A := \left\{ \frac{b}{d} = [a_1, a_2, \ldots, a_k] : 0 < b < d, (b, d) = 1, \text{ and for } \forall j, a_j \in A \right\},$$

and let $D_A \subset \mathbb{N}$ be the set of denominators of fractions in $\mathbb{R}_A$,

$$D_A := \left\{ d : \exists (b, d) = 1 \text{ with } \frac{b}{d} \in \mathbb{R}_A \right\}.$$

We now state the Zaremba’s conjecture.

**Conjecture 1.1.** (Zaremba [Zar72]) Every positive integer is the denominator of a reduced absolutely Diophantine fraction.

Bourgain and Kontorovich later proposed an alternative conjecture. In particular, we call an integer $d$ admissible (for $A$) if it passes all finite local obstructions:

$$\forall q > 1, d \in D_A \pmod{q}.$$

Let $\mathbb{A}_A$ denote the set of all admissible numbers,

$$\mathbb{A}_A := \{ d \in \mathbb{Z} : (1.1) \text{ holds} \}.$$

We say $d$ is represented (by $A$) if $d \in D_A$. The multiplicity of a denominator is the number of coprime numerators $0 < b < d$ with $b/d \in \mathbb{R}_A$. Clearly, $d$ is represented if and only if its multiplicity is positive.

**Conjecture 1.2.** ([BK13, p. 3]) If the dimension $\delta_A$ exceeds $1/2$, then the set of denominators $D_A$ contains every sufficiently large admissible integer.

Specifically, they call such phenomenon as a local-global principle, where the dimension condition and “sufficiently large” are local obstructions at infinity. They further showed the following theorem as an approximation to Conjecture 1.2.

**Theorem 1.3.** ([BK13, p. 3]) For dimension $\delta_A > \delta_0 = 307/312 \approx 0.984$, the set of denominators $D_A$ contains almost every admissible integer. More precisely, there is a constant $c = c(A) > 0$ so that

$$\text{#}(D_A \cap [N/2, N]) \gg N^{2\delta_A - \frac{1001}{312}},$$

as $N \to \infty$. Furthermore, each $d$ produced above appears with multiplicity

$$\gg N^{2(\delta_A - \frac{1001}{312})}.$$  

The constants $c$ are effectively computable, and the implied constants above depend only on $A$.

**Remark 1.4.** Hensley [Hen92] gives the following asymptotic expansion

$$\delta_{[1, 2, \ldots, A]} = 1 - \frac{6}{\pi^2 A} - \frac{72 \log A}{\pi^4 A^2} + O\left(\frac{1}{A^2}\right).$$

Hence, there exists $A$ with $\delta_{[1, 2, \ldots, A]}$ arbitrarily close to 1. In fact, Bourgain and Kontorovich showed that $A = 50$ is large enough for $\delta_A > \delta_0 \approx 0.984$.

Recently, Frolenkov and Kan [FK13] gave a refinement to the constant $\delta_0$ at the cost of a weaker result. In particular, they proved the following positive density statement.

**Theorem 1.5.** ([FK13]) For dimension $\delta_A > \delta_0 = 5/6$, a positive proportion of integers satisfy Zaremba’s conjecture. That is,

$$\text{#}(D_A \cap [N]) \gg N.$$
In this paper, we again refine the methods in Frolenkov and Kan’s paper to its full strength, and show the following effective density one statement with an improved $\delta_0$ compared to Theorem 1.3.

**Theorem 1.6.** For dimension $\delta_{\mathcal{A}} > \delta_0 = 5/6 \approx 0.83333$, the set of denominators $\mathcal{D}_{\mathcal{A}}$ contains almost every admissible integer. Specifically, there is a constant $c = c(\mathcal{A}) > 0$ so that

$$\frac{\#(\mathcal{D}_{\mathcal{A}} \cap [N/2, N])}{\#(\mathcal{D}_{\mathcal{A}} \cap [N/2, N])} = 1 + O\left(N^{-c/\log \log N}\right),$$

as $N \to \infty$. Furthermore, for any fixed constant $\tau$ small enough, each $d$ produced above appears with multiplicity

$$\gg N^{2\delta_{\mathcal{A}}-1-\tau},$$

as $N \to \infty$, and the implied constants above depend only on $\mathcal{A}$.

**Remark 1.7.** Jenkinson [Jen04] showed that $\delta_{\mathcal{A}} = 0.8368 > 0.8333$, when $\mathcal{A} = \{1, 2, 3, 4, 5\}$. Hence Theorem 1.6 is true with this alphabet.

**Remark 1.8.** Bourgain and Kontorovich [BK13] pointed out in Remark 1.20 that to present the density one statement, they made no effort to optimize the constant $\delta_0$. This paper combines their work with the work of Frolenkov and Kan [FK13] to prove the same statement as in Theorem 1.3 with smaller $\delta_0$.

1.2. **Overview of Ideas.** First of all, we reformulate Conjecture 1.2. Recall a well-known observation that

$$\frac{b}{d} = [a_1, a_2, \ldots, a_k]$$

is equivalent to

$$\begin{pmatrix} * & b \\ * & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_k \end{pmatrix}.$$

Hence it is natural to look at the semigroup $\mathcal{G}_{\mathcal{A}} \subset \text{GL}(2, \mathbb{Z})$ generated by matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix},$$

for $a \in \mathcal{A}$. Then the orbit

$$O_{\mathcal{A}} := \mathcal{G}_{\mathcal{A}} \cdot e_2$$

of $e_2 = (0, 1)^t$ under $\mathcal{G}_{\mathcal{A}}$ corresponds to $\mathcal{R}_{\mathcal{A}}$, that is, if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\gamma \cdot e_2 = (b, d)^t$. To obtain the number $d$, we use the inner product of this orbit with $e_2$ that is $\langle \gamma \cdot e_2, e_2 \rangle = d$. Therefore, we have

$$\mathcal{D}_{\mathcal{A}} = \langle O_{\mathcal{A}}, e_2 \rangle = \langle \mathcal{G}_{\mathcal{A}} \cdot e_2, e_2 \rangle.$$

Zaramba’s conjecture can now be reformulated as: For some finite alphabet $\mathcal{A}$,

$$\mathbb{N} \subset \langle \mathcal{G}_{\mathcal{A}} \cdot e_2, e_2 \rangle.$$

For convenience, we pass from $\mathcal{G}$ to its determinant one subsemigroup

$$\Gamma_{\mathcal{A}} = \mathcal{G}_{\mathcal{A}} \cap \text{SL}(2, \mathbb{Z}),$$

which is (freely and finitely) generated by the matrix products

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & a' \end{pmatrix},$$

for $a, a' \in \mathcal{A}$. The Orbit $O$ is recovered as a finite union of “coset” orbits

$$O_{\mathcal{A}} = \Gamma_{\mathcal{A}} \cdot e_2 \bigcup_{a \in \mathcal{A}} \Gamma_{\mathcal{A}} \cdot \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} e_2.$$
Now, one can see that each $\gamma \in \Gamma_{A}$ produces a fraction with $\langle \gamma e_2, e_2 \rangle$ as its denominator. Hence, a natural procedure is to consider the following exponential sum:

$$S_N(\theta) := \sum_{\gamma \in \Gamma_{\mathbb{A}}, \parallel \gamma \parallel < N} e(\langle \gamma e_2, e_2 \rangle),$$

where $\Gamma = \Gamma_{\mathbb{A}}$, $\theta \in [0, 1]$, and $\parallel \gamma \parallel = \sqrt{a^2 + b^2 + c^2 + d^2}$ is the Frobenius matrix norm. In fact, instead of taking the summation of $\gamma$ over the whole ball $\parallel \gamma \parallel < N$, we define a set $\Omega_N \subset \Gamma$ called ensemble, see (3.50). The exponential sum which we will work on is defined as follows.

$$S_N(\theta) := \sum_{\gamma \in \Omega_N} e(\langle \gamma e_2, e_2 \rangle).$$

Then we have

$$R_N(d) := \widehat{S}_N(d) = \int_0^1 S_N(\theta)e(-d\theta)d\theta = 1_{\langle \gamma e_2, e_2 \rangle = d}.$$

Next, we decompose the integral into “major arcs” and “minor arcs”, where the former represents those $\theta$ near rational with small denominators and the latter is the rest. Specifically, we write

$$R_N(d) = \int_{\mathbb{R}} S_N(\theta)e(-d\theta)d\theta + \int_{[0,1]\backslash \mathbb{R}} S_N(\theta)e(-d\theta)d\theta = M_N(d) + \mathcal{E}_N(d).$$

Our goal is to show that $M_N(d)$ is bounded below by $\frac{1}{\log \log N} \frac{|\Omega_N|}{N}$ while we bound above the $L^2$-norm of the minor arcs by roughly $\frac{|\Omega_N|^2}{N^{1 + c}/\log \log N}$. On the other hand, $R_N(d)$ is small only when $\mathcal{E}(d) \gg M(d)$. Hence, by Parseval’s theorem, the number of $d \leq N$ with $\mathcal{E}(d) \gg M(d)$ is $\ll \frac{N^2 (\log \log N)^2}{|\Omega_N|^2} \cdot \frac{|\Omega_N|^2}{N^{1 + c}/\log \log N} \ll N^{1 - c'/\log \log N}$.

In §2, we present several tools for the construction of $\Omega_N$ and arguments in major and minor arcs analysis. We use §3 to construct the main ensemble $\Omega_N$, assuming the existence of some special set with nice modular and archimedean distribution properties. We carry out the major arcs analysis in §4, and set up the exponential sum in §5. In §6 and §7, we bound the exponential sum in minor arcs by $L^2$ norm. Finally, we prove Theorem 1.6 in §7.

Acknowledgement. We thank Alex Kontorovich for introducing this problem, continuous support, and insightful comments. Moreover, the author acknowledges support from Kontorovich’s NSF grants DMS-1209373, DMS-1064214, DMS-1001252, and Kontorovich’s NSF CAREER grant DMS-1254788.
2. Preliminaries

2.1. Large Matrix Products. In this section, we review the large matrix products in [BK13]. Recall that \( \Gamma = \Gamma_A \) is the semigroup generated by the matrix products

\[
\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & a' \end{pmatrix},
\]

for \( a, a' \in \mathcal{A} \). By induction, we can show the following inequality is true for \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \), \( \gamma \neq I \).

\[
1 \leq a \leq \min(b, c) \leq \max(b, c) < d.
\]

That is to say, every non-identity matrix \( \gamma \in \Gamma \) is hyperbolic. On the other hand, since \( d \) is always the largest element in each \( \gamma \), we have that the trace and the Frobenius norm, \( \|\gamma\| = \sqrt{a^2 + b^2 + c^2 + d^2} \), are comparable:

\[
(2.1) \quad \|\gamma\| \leq 2\text{tr}(\gamma) \leq 2\sqrt{2}\|\gamma\|,
\]

and so are the norm, sup-norm, and second column norm:

\[
(2.2) \quad \|\gamma\|_{\infty} = d < |\gamma e_2| = \sqrt{b^2 + d^2} < \|\gamma\| < \sqrt{2}|\gamma e_2| < 2\|\gamma\|_{\infty}.
\]

We now use the notation for eigenvalues and eigenvectors in [BK13]. For \( \gamma \in \Gamma \), let the expanding and contracting eigenvalues of \( \gamma \) be \( \lambda_+(\gamma) \) and \( \lambda_-(\gamma) = 1/\lambda_+(\gamma) \), with corresponding normalized eigenvectors \( v_+(\gamma) \) and \( v_-(\gamma) \). Simple linear algebra and (2.1) show that

\[
(2.3) \quad \lambda_+(\gamma) = \text{tr}(\gamma) + O\left(\frac{1}{\|\gamma\|}\right),
\]

where the implied constant is absolute. Write \( \lambda = \lambda_+ \) for the expanding eigenvalue.

Note that for all \( \gamma \in \Gamma \), the eigenvalues are real, and \( \lambda > 1 \) for \( \gamma \neq I \). We have the following useful results regarding the multiplicity of eigenvalues.

**Proposition 2.1.** ([BK13, p: 10]) For every \( \gamma \in \Gamma \) sufficiently large, we have

\[
(2.4) \quad \left| \langle v_+(\gamma), v_-(\gamma) \rangle \right| \geq \frac{1}{2}.
\]

In addition, the eigenvalue of any two large norm matrices \( \gamma, \gamma' \in \Gamma \) with large norms behave essentially multiplicatively, subject to the directions of their expanding eigenvectors being near to each other. Specifically,

\[
(2.5) \quad \lambda(\gamma\gamma') = \lambda(\gamma)\lambda(\gamma') \left[ 1 + O\left( \left| v_+(\gamma) - v_+(\gamma') \right| + \frac{1}{\|\gamma\|^2} + \frac{1}{\|\gamma'\|^2} \right) \right].
\]

Moreover, the expanding vector of the product \( \gamma\gamma' \) faces a nearby direction to that of the first \( \gamma \), (and the same in reverse),

\[
(2.6) \quad \left| v_+(\gamma\gamma') - v_+(\gamma) \right| \ll \frac{1}{\|\gamma\|^2} \quad \text{and} \quad \left| v_-(\gamma\gamma') - v_-(\gamma') \right| \ll \frac{1}{\|\gamma'\|^2}.
\]

All the implied constants above are absolute.
2.2. **Distributional Properties.** In this section, we restate another important result regarding sector counting in the paper [BK13].

Once and for all, we fix \( x = [A, A, \ldots, A, \ldots] \in \mathbb{C} \). Since \( A = \max \mathcal{A} > 1 \), we have

\[
x = \frac{-A + \sqrt{A^2 + 4}}{2} < \sqrt{2} - 1.
\]

Let

\[
v = v_x := \frac{(x, 1)}{\sqrt{1 + x^2}}
\]

be the corresponding unit vector. One can easily check by (2.7) that

\[
\langle v, e_2 \rangle = \frac{1}{\sqrt{1 + x^2}} > \sqrt{\frac{3}{4}}.
\]

The following estimate follows from Lalley’s methods [Lal89].

**Proposition 2.2.** ([BK13, p. 13]) There is a constant \( c = c(\mathcal{A}) > 0 \) so that as long as \( H < T^{c/\log \log T} \), we have

\[
\# \left\{ \gamma \in \Gamma : \|\gamma\| < T \text{ and } |v_\gamma(\gamma) - v| < \frac{1}{H} \right\} \gg \frac{T^{2\delta}}{H},
\]

as \( T \to \infty \). The implied constants depend at most on \( \mathcal{A} \).

Bourgain-Gamburd-Sarnak [BGS11] later extended the work of Lalley’s to a congruence setting, and proved the following theorem.

**Theorem 2.3.** ([BGS11]) There exists an integer

\[
B = B(\mathcal{A}) \geq 1.
\]

and a constant

\[
c = c(\mathcal{A}) > 0
\]

so that the following holds. For any \( (q, \mathfrak{B}) = 1 \), any \( \omega \in \mathrm{SL}_2(q) \), and any \( \gamma_0 \in \Gamma \), there is a constant \( C(\gamma_0) > 0 \) so that

\[
\# \left\{ \gamma \in \Gamma : \gamma \equiv \omega \pmod{q}, |v_\gamma(\gamma) - v| < \frac{1}{H}, \text{ and } \frac{\|\gamma_0\|}{\|\gamma\|} \leq T \right\} = C(\gamma_0) \cdot T^{2\delta} \cdot \frac{\mu(I)}{|\mathrm{SL}_2(q)|} + O\left(T^{2\delta - c/\log \log T}\right), \quad \text{as } T \to \infty.
\]

With the same setting for \( \mathfrak{B} \) and \( c \), we have, for any \( q \) with \( \mathfrak{B} \mid q \),

\[
\# \left\{ \gamma \in \Gamma : \gamma \equiv \omega \pmod{q}, |v_\gamma(\gamma) - v| < \frac{1}{H}, \text{ and } \frac{\|\gamma_0\|}{\|\gamma\|} \leq T \right\} = \frac{|\mathrm{SL}_2(\mathfrak{B})|}{|\mathrm{SL}_2(q)|} \cdot \# \left\{ \gamma \in \Gamma : \gamma \equiv \omega \pmod{q}, |v_\gamma(\gamma) - v| < \frac{1}{H}, \text{ and } \frac{\|\gamma_0\|}{\|\gamma\|} \leq T \right\} + O\left(T^{2\delta - c/\log \log T}\right)
\]

We will use Theorem 2.3 to construct a special set which has good modular distribution. In addition, each element of this special set has its expanding eigenvector close to \( v \), and its expanding eigenvalue close to some parameter \( T \).
2.3. **Test Functions with Compactly Supported Fourier Transform.**

For later purposes, we define a smooth test Function $\Upsilon \in L^1(\mathbb{R})$ such that its fourier transform $\widehat{\Upsilon}$ is compactly supported.

In particular, let $\widehat{F}(x) = \text{rect}(x) = 1_{[-\frac{1}{2}, \frac{1}{2}]}$ be the indicator function of the interval $[-\frac{1}{2}, \frac{1}{2}]$. One can easily check that $F(x) = \text{sinc}(x) = \frac{\sin \pi x}{\pi x}$. If we take the convolution of $\widehat{F}(x)$ with itself, then we get the triangle function $\psi(x)$ as follows.

\[
(2.15) \quad \psi(x) := \begin{cases} 
1 + x & \text{if } -1 < x < 0, \\
1 - x & \text{if } 0 \leq x < 1, \\
0 & \text{otherwise}
\end{cases}
\]

Also, we define the function $\Upsilon(x)$ as

\[
(2.16) \quad \Upsilon(x) = \widehat{\psi}(x) = \text{sinc}(x)^2.
\]

This shows that $\widehat{\Upsilon}(x) = \psi(x)$ is compactly supported and $\Upsilon(x) \in L^1(\mathbb{R})$. In fact, we can control the support of $\Upsilon(x)$ by changing $\psi(x)$ to $\text{sinc}(ax)^2$.

Similarly, the following separable function

\[
\Upsilon(x, y) = \text{sinc}(ax)^2 \text{sinc}(ay)^2,
\]

is a two-dimensional smooth function with compactly supported Fourier transform.
3. Construction of Ensemble

3.1. Auxiliary Parameters $N_j$. In this section, we define a sequence of parameters $N_j$ for the construction of $\Omega_N$. In contrast to decomposing $N$ dyadically in [BK13], the difference $N_{j+1}/N_j$ between two consecutively terms $N_j$ and $N_{j+1}$ is not larger than $N_j^{\varphi}$, where $\varphi$ is an arbitrarily small fixed constant. We now define $\varphi$ as follows.

For $N$ large and $\delta$ exceeding $\delta_0 = 5/6$, let

$$\varphi = r \cdot (\delta - \delta_0),$$

where $r \leq 1/1000$ is the fixed constant given in Theorem 1.6. Thus, there exists some positive integer $J_1$ such that

$$J = (1 - \varphi)^{J_1} \leq \varphi < (1 - \varphi)^{J_1-1}.$$ 

Notice $J_1$ is of constant size and only depends on $\varphi$.

We define another large parameter $J_2$ as follows.

$$J_2 = \left\lceil \log \log N - C_{A, \mathcal{A}} \log(1 - \varphi) \right\rceil,$$

where the constant $C_{A, \mathcal{A}}$ depends only on $\mathcal{A}$, and is chosen to dominate the implied constants in (3.65) and (3.66), and that (3.21) is true. Note that we have $J_2 > 2J_1 + 2$ for $N$ sufficiently large. Since $\mathcal{A}$ is fixed throughout, we denote $C_{A, \mathcal{A}}$ by $C_A$. Also, let

$$J = J_1 + J_2.$$

We now construct the auxiliary parameters as

$$N_{-J}, \ldots, N_{-J_1}, \ldots, N_0, N_1, \ldots, N_{J_1}, \ldots, N_J, N_{J+1},$$

where $N_{J+1} = N$, and

$$N_j = \begin{cases} 
N_j^{1/(1-\varphi)^{-J_1}} & \text{when } -J \leq j \leq -J_1, \\
N_j^{1/2(1-\varphi)^{-J}} & \text{when } -J_1 < j \leq 0, \\
N_j^{1/2(1-\varphi)^{J_1}} & \text{when } 0 \leq j < J_1, \\
N_j^{1/2(1-\varphi)^{-J_1}} & \text{when } J_1 \leq j \leq J.
\end{cases}$$

It is elementary to show that the cases coincide when $j = 0$, with $N_0 = \sqrt{N}$. We also have $N_{-J_1} = N^{1/4}$, and $N_{J_1} = N^{1/4}$. The following Lemma lists some important properties of these parameters $N_j$.

**Lemma 3.1.**

1. For $-J \leq m \leq J$, we have

$$N_m N_{-m} = N.$$  

2. For $-J \leq m \leq J - 1$, we have

$$\frac{N_{m+1}}{N_m} = \begin{cases} 
N_m^{(1-\varphi)^{J_1-1}} & \text{when } -J_1 + 1 \leq m \leq J_1 - 2, \\
N_m^{1/2(1-\varphi)^{-1}} & \text{when } m = -J_1 \text{ or } J_1 - 1, \\
N_m^{1/2(1-\varphi)^{-J_1-1}} & \text{when } m \leq -J_1 - 1 \text{ or } m \geq J_1,
\end{cases}$$

and

$$N_m \geq N_m^{1-\varphi}.$$  

3. For $-J \leq m \leq J - 1$, we have

$$\frac{N_{m+1}}{N_m} \geq 2^{2^2\varphi^{-2}},$$

$$N_m \geq N_m^{1-\varphi}.$$  

and

$$N_m \geq N_m^{1-\varphi}.$$
(3.11) \[ 2^{(1-\varrho)2^{j-2}} \leq \frac{N}{N_{J+1}} \leq 2^{2^{j-2}}. \]

**Proof.** (3.7), (3.8), (3.10), and (3.11) follow directly from (3.3), definition of \( N_j \), and that \( J_2 > J_1 \). To prove (3.9), we consider the following cases.

1. Case \( j \leq -J_1 - 1 \) or \(-J_1 + 1 \leq j \leq -1 \). This case is elementary from (3.6).
2. Case \( j = -J_1, J_1 - 1 \). Straightforward computation shows that we need \( \varrho \geq (1 - \varrho)^{J_1} \), and \( 3\varrho \geq (1 - \varrho)^{J_1 - 1} \) which both follow directly from (3.2).
3. Case \( 0 \leq j \leq J_1 - 2 \) or \( J_1 \leq j \). For \( \forall m \geq 0 \in \mathbb{Z} \), we have the following inequality.

\[
\frac{3\varrho}{(1-\varrho)^m} + (1-\varrho)^2 \geq 3\varrho + (1-\varrho)^2 \geq 1.
\]

This implies that
\[
\frac{3}{4} - \frac{1}{4}(1-\varrho)^j \geq \frac{3}{4}(1-\varrho) - \frac{1}{4}(1-\varrho)^{j+2},
\]
and hence also implies (3.9).

The next lemma shows that for any number \( M \) sufficiently large, we can bound \( M \) above and below by \( N_j \) and \( N_{j-1} \) respectively for some \( j \). Through (3.8), one can see the upper bound \( N_j \) and lower bound \( N_{j-1} \) of \( M \) are close.

**Lemma 3.2.** For any \( M \) with

(3.12) \[ N_{j-1} \leq M \leq N_{j}, \]

there exist indices \( j \) and \( h \), such that

(3.13) \[ -J + 1 \leq j \leq J - 1, \quad h = -j, \]

and for which we have

(3.14) \[ N_{j-1} \leq M \leq N_{j}, \quad \text{and} \quad \frac{N}{N_h} \leq M \leq \frac{N}{N_{h-1}}. \]

Moreover, the above inequalities imply that

(3.15) \[ N_j^{1-\varrho} \leq M \leq N_j, \quad \text{and} \quad \left( \frac{N}{N_{h-1}} \right)^{1-\varrho} \leq M \leq \frac{N}{N_{h-1}}. \]

**Proof.** Since the sequence \( \{N_j\} \) is increasing, there exists an index \( j \), with \(-J + 1 \leq j \leq J - 1 \), such that

\[ N_{j-1} \leq M \leq N_j. \]

By (3.9), we then have

\[ N_j^{1-\varrho} \leq N_{j-1} \leq M \leq N_j. \]

On the other hand, since \( N_m N_{-m} = N \), the second inequalities in (3.14) and (3.15) hold.

The next corollary follows directly from Lemma (3.2).
Corollary 3.3. For any $M$ with
\begin{equation}
2^{-\frac{\varrho^2}{1-\varrho}} \leq M < N_{J-1},
\end{equation}
there exist indices $j$ and $h$, such that
\begin{equation}
-J + 1 \leq j \leq J - 1, \quad h = -j,
\end{equation}
and for which the following inequalities hold.
\begin{equation}
N_j^{1-\varrho} \leq M \leq N_j, \quad \left(\frac{N}{N_{h-1}}\right)^{1-\varrho} \leq M \leq \frac{N}{N_{h-1}}.
\end{equation}
Moreover, we have
\begin{equation}
M \leq N_j \leq M^{1+2\varrho}, \quad M \leq \frac{N}{N_{h-1}} \leq M^{1+2\varrho}.
\end{equation}
For later exposition, we set
\begin{equation}
\overline{C} = \left\lceil \frac{x_{\varrho^2}}{1-\varrho} \right\rceil.
\end{equation}
Moreover, we let the constant $C_{\varrho}$ to be large enough so that
\begin{equation}
\overline{C} \geq 2^{12}.
\end{equation}

3.2. The Special Set $\mathbb{N}$. First, we point out a special parameter $N_\mathcal{I}$ among $N_j$’s which is closely related the special set $\mathbb{N}$. Set $M$ to be $N^{2/3}$ in Corollary 3.3, and thus we obtain an index $\mathcal{J}$ such that
\begin{equation}
N_j^{\frac{2}{3}} \leq N_\mathcal{I} \leq N_j^{\frac{2}{3}(1+2\varrho)}.
\end{equation}
Notice the index $\mathcal{J}$ is independent of $N$ since its only condition is
\begin{equation}
\frac{3}{4} - \frac{1}{4}(1-\varrho)^{2-1} \leq \frac{2}{3} \leq \frac{3}{4} - \frac{1}{4}(1-\varrho)^{2}.
\end{equation}
We follow the construction of $\mathbb{N}$ in [BK13]. Notice that to show such a set exists, we need the Theorem 2.3 and the random extraction argument in §8.2 in [BGS11].

Recall the fixed density point $x \in \mathbb{C}$ with
\begin{equation}
v = v_x := \frac{(x, 1)}{\sqrt{1+x^2}}.
\end{equation}
For ease of presentation, we assume that for all $q \geq 1$, the reduction of $\Gamma$ is full,
\begin{equation}
\Gamma \pmod{q} \equiv \text{SL}_2(q),
\end{equation}
which is the case for any alphabet $\mathcal{A}$ containing 1 and 2. Minor changes are needed in general case, see Remark 3.5.

Let
\begin{equation}
b := \frac{\varrho^2}{4}(1-\varrho)^{2-1},
\end{equation}
and with $R = |\text{SL}_2(\mathbb{F})|$, let $a_0 = \frac{bc}{x_{\varrho^2} R}$ be a constant depending only on $\mathcal{A}$ since the parameters $b$ in (3.25), $\mathbb{F}$ in (2.11), and $c$ in (2.12) all depend only on $\mathcal{A}$. Then we set
\begin{equation}
B := N^b,
\end{equation}
and
\begin{equation}
Q := N^{a_0/\log \log N}.
\end{equation}
Let $\mathcal{U} \subset \left[ \frac{1}{400} B, \frac{399}{400} B \right]$ be an arithmetic progression of real numbers starting with $\mu_0 = \frac{1}{400} B$ having common difference

(3.28) $|u - u'| = \frac{2B}{Q^5}$,

for $u, u'$ consecutive terms in $\mathcal{U}$, and ending with $u > \left(\frac{399}{400} - \frac{2}{Q^5}\right) B$. Hence the cardinality of $\mathcal{U}$ is

(3.29) $|\mathcal{U}| \approx Q^5$.

We recall the Proposition 3.9 in [BK13]. See Appendix A for a detailed proof.

**Proposition 3.4.** ([BK13, p. 12]) For each $u \in \mathcal{U}$, there are non-empty sets $\mathcal{N}_u \subset \Gamma$, all of the same cardinality

(3.30) $|\mathcal{N}_u| = |\mathcal{N}_{u'}|$, 

so that the following holds. For every $a \in \mathcal{N}_u$, its expanding eigenvector is restricted by

(3.31) $|v(a) - v| < \frac{B}{Q^5}$,

and its expanding eigenvalue $\lambda(a)$ is restricted by

(3.32) $|\lambda(a) - u| < \frac{B}{Q^5}$.

In particular,

(3.33) $\frac{1}{500} B < \lambda(a) < B,$

for $N$ sufficiently large. Moreover, for any $q < Q$, any $\omega \in SL_2(q)$, and any $u \in \mathcal{U}$, we have

(3.34) $\# \{a \in \mathcal{N}_u : a \equiv \omega \pmod{q}\} = \frac{|\mathcal{N}_u|}{|SL_2(q)|} (1 + O(Q^{-4}))$,

where the implied constant does not depends on $q$, $\omega$, or $u$.

**Remark 3.5.** When we have local obstruction, for any $q$, let set $\mathcal{S}_q$ be the set of admissible $\omega \in SL_2(q)$. That is to say,

$\mathcal{S}_q = \{\omega \in SL_2(q) : \exists \gamma \in \Gamma \text{ s.t. } \gamma \equiv \omega \pmod{q}\}.$

Then instead of (3.34), we have that for any $q < Q$, any $\omega \in \mathcal{S}_q$, and any $u \in \mathcal{U}$, we have

$\# \{a \in \mathcal{N}_u : a \equiv \omega \pmod{q}\} = \frac{|\mathcal{N}_u|}{|\mathcal{S}_q|} (1 + O(Q^{-4})).$

With the sets $\mathcal{N}_u$ as above, we define the special set $\mathcal{N}$ to be the union of the sets $\mathcal{N}_u$.

(3.35) $\mathcal{N} := \bigsqcup_{u \in \mathcal{U}} \mathcal{N}_u$.

Note that the sets $\mathcal{N}_u$ are disjoint by (3.28) and (3.32).
3.3. **The set** $\Xi(M, H; L, k)$. The next Proposition follows directly from Proposition 2.2 equipped pigeonhole argument.

**Proposition 3.6.** ([BK13, p. 14]) Given $M \gg 1$ and $H < M^{c \log \log M}$ (the constant $c$ is given in Proposition 2.2), there exists some $L$ in the range

$$\frac{1}{4} M \leq L \leq 4M,$$

an integer $k \approx \log M$, and a set $\Xi = \Xi(M, H; L, k) \subset \Gamma$ having the following properties. For $\gamma \in \Xi$, the expanding eigenvalues are controlled to within $1/\log L$:

$$L \left(1 - \frac{1}{\log L}\right) < \lambda(\gamma) < L,$$

the expanding eigenvectors are controlled to within $1/H$:

$$|v_+(\gamma) - v| < \frac{1}{H},$$

and the wordlength metric $\ell$ (in the generators (1.11) of $\Gamma$) is controlled exactly:

$$\ell(\gamma) = k.$$

Moreover, the cardinality of $\Xi$ is controlled by

$$\frac{L^{2\delta}}{H(\log L)^2} \ll \#\Xi \ll L^{2\delta}.$$

3.4. **Decomposing $N$ and the Ensemble $\Omega_N$.** We construct the set $\Omega_N$ using the auxiliary parameters $N_j$ in §3.1 as follows.

**Setup:** We start by taking

$$M_{-J} = N_{-J} \geq 2^{c_{\psi_{-1}}}, \quad H = \log M_{-J},$$

and use Proposition 3.6 to generate a set $\Xi(M_{-J}, H; L_{-J}, k)$. We use $\Xi_{-J}$ to represent $\Xi(M_{-J}, H; L, k)$. Notice that we have

$$L_{-J} = \alpha_{-J} N_{-J},$$

where $\alpha_{-J} \in (1/4, 4)$. We also have

$$|\Xi_{-J}| \gg \frac{L_{-J}^{2\delta}}{(\log L_{-J})^3}.$$  

**Step 1:** Next we set

$$M_{-J+1} = \frac{N_{-J+1}}{L_{-J}} = \frac{N_{-J+1}}{\alpha_{-J} N_{-J}}, \quad H = \log M_{-J+1},$$

and generate another set $\Xi(M_{-J+1}, H; L_{-J+1}, k)$, denoted by $\Xi_{-J+1}$. Again, we have $L_{-J+1} = \alpha_{-J+1} M_{-J+1}$, with $\alpha_{-J+1} \in (1/4, 4)$, and

$$|\Xi_{-J+1}| \gg \frac{L_{-J+1}^{2\delta}}{(\log L_{-J+1})^3}.$$  

**Iterate:** Start with $j = 2 - J$ and iterate up to $j = \frac{j}{2} - 1$, as defined in (3.22). For each such $j$, set

$$M_j := \frac{N_j}{L_j} = \frac{N_j}{\alpha_{j-1} N_{j-1}}, \quad H = \log M_j,$$
and generate a set \( \Xi(M_j, H; L_j, k) \), denoted by \( \Xi_j \). Note that \( L_j = \alpha_j M_j \), with \( \alpha_j \in (1/4, 4) \), and

\[
|\Xi_j| \gg \frac{L_j^{2\delta}}{(\log L_j)^{3/2}}.
\]

**Special Set** \( \mathbb{N} \): Recall that we have presupposed the existence of a set \( \mathbb{N} \) in (3.35), all of whose expanding eigenvectors are within \( Q^{-5} \) (\( Q \) is defined in (3.27)) of \( \nu \), and with eigenvalues of size \( B \), see (3.33). From (3.25) and (2.11), we have \( B = N^b = N_j / N_{j-1} \). For the sake of convenience, the symbol \( L_j \) also represents \( B \) in the later context.

**After the Special Set:** Set \( \alpha_2 = \alpha_{2-1} \), where \( \alpha_{2-1} \) is obtained by (3.42). We take

\[
M_{j+1} := \frac{N_{j+1}}{\alpha_2 N_j^2} = \frac{\varphi}{4\alpha_2} (1 - \varphi)^2, \quad H = Q^2,
\]

and generate a set \( \Xi(M, H; L, k) \), denoted by \( \Xi_{j+1} \). Note that \( L_{j+1} = \alpha_{j+1} M_{j+1} \), with \( \alpha_{j+1} \in (1/4, 4) \), and

\[
|\Xi_{j+1}| \gg \frac{L_{j+1}^{2\delta}}{(\log L_{j+1})^{3/2}}.
\]

**Iterate Again:** Start with \( j = j + 2 \) and iterate up to \( j = J \), as defined in (3.22). For each such \( j \), set

\[
M_j := \frac{N_j}{L_{j-1}^2} = \frac{N_j}{\alpha_j N_{j-1}}, \quad H = \log M_j,
\]

and generate a set \( \Xi(M_j, H; L_j, k) \), denoted by \( \Xi_j \). Note that \( L_j = \alpha_j M_j \), with \( \alpha_j \in (1/4, 4) \), and

\[
|\Xi_j| \gg \frac{L_j^{2\delta}}{(\log L_j)^3}.
\]

**End:** For the last step, \( j = J + 1 \). We set

\[
M_{J+1} = \frac{N}{L_{J}} = \frac{N}{\alpha J L_{J}}, \quad H = \log M_{J+1},
\]

and generate the last set \( \Xi_{J+1} = \Xi(M_{J+1}, H; L_{J+1}, k) \). We have the last parameter \( L_{J+1} = \alpha_{J+1} M_{J+1} \), with \( \alpha_{J+1} \in (1/4, 4) \), and

\[
|\Xi_{J+1}| \gg \frac{L_{J+1}^{2\delta}}{(\log L_{J+1})^{3/2}}.
\]

We now define the ensemble \( \Omega_N \) by concatenating the sets \( \Xi_j \) developed above.

\[
\Omega_N := \Xi_{-J} \cdot \Xi_{-J+1} \cdot \cdots \Xi_{-2} \cdot \mathbb{N} \cdot \Xi_{-1} \cdot \Xi_{-2} \cdot \cdots \Xi_{J} \cdot \Xi_{J+1}.
\]

Once setting up the ensemble \( \Omega_N \), we may give the formal definition of exponential sum \( S_N(\theta) \) as follows.

For \( \theta \in [0, 1] \), let

\[
S_N(\theta) = \sum_{\gamma \in \Omega_N} e(\langle \gamma e_2, e_2 \rangle).
\]
3.5. **Properties of $\Omega_N$.** For $\gamma \in \Omega_N$, write
\[
\gamma = \xi_{-J} \xi_{-J+1} \cdots \xi_{J+1}
\]
according to the decomposition (3.49), where $a \in S$, and for $\forall j, \xi_j \in \Xi_j$. Note that by the fixed wordlength restriction, the decomposition is unique. (Start from both tails, and gradually determine all the $\xi_j$.) First of all, we have the following observation.

**Lemma 3.7.** With $J_2 > J_1$, by choosing the constant $C_0$ and $N$ sufficiently large, we have
\[
(3.51) \quad \frac{2}{Q^2} + \sum_{j=J_2+1}^{J_1} \frac{1}{\log L_j} < \frac{1}{C'}
\]
where $C$ is a large constant depending only on $C_0$.

**Remark 3.8.** We will specify the bound $C$ should satisfy later, and thus also give a lower bound of $C_0$.

**Proof.** From the construction of $\Omega_N$, we have
\[
(3.52) \quad L_{-J} = \alpha_{-J} M_{-J},
\]
and for $j \neq 2, 3 + 1$, we have
\[
(3.53) \quad L_j = \frac{\alpha_j N_j}{\alpha_{j-1} N_{j-1}} = \frac{\alpha_j}{\alpha_{j-1}} \begin{cases} 
N^{3(1-\varphi)} |\varphi|^{j-1} & \text{when } -J + 1 \leq j \leq -J_1 \text{ or } J_1 + 1 \leq j \leq J, \\
N^{3(1-\varphi)} |\varphi|^{-j+1} & \text{when } j = -J + 1 \text{ or } j = J_1, \\
N^{3(1-\varphi)} |\varphi|^{-j+\frac{1}{2}} & \text{when } 2 - J_1 \leq j \leq J_1 - 1,
\end{cases}
\]
By the fact that $\frac{N_{n+1}}{N_n} \geq 2^{2^C n^{-2}}$ and $J_2 > J_1$, for $C_0$ sufficiently large, the following bound is true.
\[
(3.54) \quad \sum_{j=J_2+1}^{J_1} \frac{1}{\log L_j} \leq 4 \cdot \frac{2}{\varphi} \cdot \frac{1}{\log N} \cdot \left( \frac{1}{(1-\varphi)^{J_2}} + \frac{1}{(1-\varphi)^{J_1-1}} + \cdots + \frac{1}{(1-\varphi) + 1} \right)
\]
\[
\leq \frac{32}{\log N} \cdot \frac{1}{\varphi (1-\varphi)^{J_2}} \cdot (1 + (1-\varphi) + (1-\varphi)^2 + \cdots)
\]
\[
\leq \frac{32}{\log N} \cdot \frac{1}{\varphi^2 (1-\varphi)^{J_2}}
\]
\[
\leq \frac{32}{\varphi^2 (1-\varphi)^{2C_0}}.
\]
Therefore, as long as $C_0$ and $N$ are large enough, we can make the constant $C$ arbitrarily small. \(\square\)

The next Lemma gives an upper and lower bound to products of $L_j$’s.

**Lemma 3.9.** For any $-J \leq j \leq h \leq J + 1$, we have
\[
(3.55) \quad \frac{1}{4} < \frac{L_{-J} L_{-J+1} \cdots L_h}{N_h} < 4
\]
and
\[
(3.56) \quad \frac{1}{16} < \frac{L_{J_1} L_{J_1+1} \cdots L_h}{N_h/N_{J_1-1}} < 16
\]

**Proof.** This follows directly from the definition of $L_j$ in §3.4. \(\square\)

We can now use Lemma 3.7 to show we have control on the eigenvalues and eigenvectors of products of $\Xi_j$’s.
Lemma 3.10. For any \(-J \leq j \leq h \leq J + 1\), and \(a \in \mathbb{N}\), \(\xi_j \in \Xi_j, \ldots, \xi_h \in \Xi_h\), we have the following control on the eigenvalues of large products:

\begin{align}
(3.57) & \quad \frac{1}{2} < \frac{\lambda(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h)}{L_j L_{j+1} \cdots L_{h-1} L_h} < 2, \\
(3.58) & \quad \frac{1}{1000} < \frac{\lambda(\xi_j \xi_{j+1} \cdots a \cdots \xi_{h-1} \xi_h)}{L_j L_{j+1} \cdots B \cdots L_{h-1} L_h} < 2, \\
(3.59) & \quad \frac{1}{2} < \frac{\lambda(\xi_j \xi_{j+1} \cdots \xi_{2j-1} \xi_{2j+1} \cdots \xi_{h-1} \xi_h)}{L_j L_{j+1} \cdots L_{2j-1} L_{2j+1} \cdots L_{h-1} L_h} < 2,
\end{align}

In addition, the eigenvectors of large products are close to \(v\). That is, for \(j \neq 2 + 1\),

\begin{align}
(3.60) & \quad |v_+(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h) - v| \ll \frac{1}{\log L_j}, \\
(3.61) & \quad |v_+(\xi_{2j+1} \cdots \xi_{h-1} \xi_h) - v| \ll \frac{1}{B^5},
\end{align}

where the implied constant depends only on \(A\).

In fact, since

\[
L_j L_{j+1} \cdots L_{h-1} L_h = \begin{cases} \alpha_h N_h & \text{if } j = -J, \\ \alpha_j N_{j-1} & \text{if } j > -J, \end{cases}
\]

we have

\begin{equation}
(3.62) \quad \frac{1}{8} < \frac{\lambda(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h)}{N/B} < 8,
\end{equation}

and for any \(j > -J\) and any \(h \geq j\), we have

\begin{equation}
(3.63) \quad \frac{1}{1600} < \frac{\lambda(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h)}{N_h/N_{j-1}} < 32.
\end{equation}

Proof. We mimick the proof of Lemma 3.38 in [BK13]. First of all, (3.60) and (3.61) follows directly from (2.6), (3.44), and the construction of \(\Omega_N\) in §3.4. Take \(v_+(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h) - v\) as an example, we have

\begin{equation}
(3.64) \quad |v_+(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h) - v| \leq \left|v_+(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h) - v_+(\xi_j)\right| + |v_+(\xi_j) - v|
\end{equation}

\[
\ll \frac{1}{\|\xi_j\|^2} + \frac{1}{\log L_j}.
\]

For (3.57), we are able to prove by the finite bound in (3.7) and downward induction on \(j\) that

\[
\lambda(\xi_j \xi_{j+1} \cdots \xi_{h-1} \xi_h) = L_j L_{j+1} \cdots L_{h-1} L_h
\]

\[
\times \left[1 + O\left(\frac{1}{\log L_j} + \frac{1}{\log L_{j+1}} + \cdots + \frac{1}{\log L_h}\right)\right]
\]

\[
= L_j L_{j+1} \cdots L_{h-1} L_h \left[1 + O\left(\frac{1}{C}\right)\right],
\]

where the implied constant only depends on \(A\), and the constant \(C\) is from Lemma (3.7). Hence we need the constant \(C\) to be large enough to beat the implied constant so that (3.57) is true.
Similarly, for (3.58), we have the following equation
\[ \lambda(\xi_j^{\xi_{j+1} \cdots \xi_{h-1} \xi_h}) = L_j L_{j+1} \cdots L_{h-1} L_h \]
(3.66)
\[ \times \left[ 1 + O\left( \frac{2}{Q^5} + \frac{1}{\log L_j} + \frac{1}{\log L_{j+1}} + \cdots + \frac{1}{\log L_h} \right) \right] \]
\[ = L_j L_{j+1} \cdots L_{h-1} L_h \left[ 1 + O\left( \frac{1}{Q^5} \right) \right]. \]

Thus, again we want the constant \( C \) in Lemma (3.7) large enough so that (3.58) follows from (3.33). We can prove the last equation (3.59) using similar arguments as above.

Finally, combining (3.57), (3.58), and (3.59) with (3.55) and (3.56), we prove (3.62) and (3.63).

□

Next, we need the following observation to control the size of products of \( \Xi_j \)'s.

**Lemma 3.11.** For any \( -J \leq j \leq J + 1 \), and \( N \) sufficiently large, we have
\[ \log L_{-J} \log L_{-J+1} \cdots \log L_j \leq 2 \frac{12(\log \log N_j)^2}{(\log(1 - \varrho))^2}. \]
(3.67)
Similarly, for any \( -J \leq h \leq J, \) we have
\[ \log L_{h+1} \log L_{h+2} \cdots \log L_{J+1} \leq 2 \frac{12(\log(\log N/j)^2}{(\log(1 - \varrho))^2}. \]
(3.68)

**Proof.** Here we give the proof of (3.67). Notice that since the magnitude of \( L_j \) and \( L_{-J+1} \) are the same (off by bounded constants \( \alpha_j \)'s only), the proof of (3.68) is the same as the one of (3.67). Let us consider the following two cases.

Case (1). When \( j \leq -J_1 \). From (3.52) and (3.53), we have that for \( -J \leq i \leq -J_1 \)
\[ \log \log L_j \leq \log \log N + (-j - J_1) \log(1 - \varrho). \]

This implies that
\[ \log \log L_{-J} + \log \log L_{-J+1} + \cdots + \log \log L_j \leq (j + J + 1) \left[ \log \log N + (-j - J_1) \log(1 - \varrho) \right]. \]
(3.69)
On the other hand, by (3.6), we have for \( N \) large enough,
\[ \log \log \mathcal{N}_j \geq \frac{1}{2} \left[ \log \log N + (-j - J_1) \log(1 - \varrho) \right]. \]
(3.70)
Moreover, (3.70) implies that
\[ \frac{\log \log \mathcal{N}_j}{-\log(1 - \varrho)} \geq \frac{1}{2} \left( \frac{\log \log N}{-\log(1 - \varrho)} + j + J_1 \right) \geq \frac{1}{2} (J_2 + 1 + j + J_1) = \frac{1}{2} (j + J + 1), \]
(3.71)
where the second inequality comes from (3.3).

Therefore, when \( j \leq -J_1 \), equations (3.69), (3.70), and (3.71) imply (3.67).

Case (2). When \( j > -J_1 \). Then we have \( \mathcal{N}_j \geq N^{1/4} \). That is to say, for \( N \) large enough,
\[ \log \log \mathcal{N}_j \geq \frac{1}{2} \log \log N. \]
(3.72)

Similar to (3.69), the following inequality is true.
\[ \log \log L_{-J} + \log \log L_{-J+1} + \cdots + \log \log L_j \leq (j + J + 1) \log \log N. \]
(3.73)
Also we have,
\[ j + J + 1 \leq 2J + 2 \leq 3J_2 \leq \frac{3 \log \log N}{-\log(1 - \varrho)}, \]
(3.74)
where the last inequality comes from (3.3).

Combining (3.72), (3.73), and (3.74), we then prove (3.67).
Finally, the size of $\Omega_N$ is bounded below as follows.

**Lemma 3.12.** We have

$$\# \Omega_N \gg rN^{2\delta - \varrho},$$

where the implied constant depends only on $A$ and $r$.

**Proof.** We recall from (3.49) that

$$\Omega_N := \Xi_{-J} \cdot \Xi_{-J+1} \cdots \Xi_{-1} \cdot N \cdot \Xi_{2+1} \cdot \Xi_{3+2} \cdots \Xi_{J} \cdot \Xi_{J+1}.$$ 

From the construction of $\Xi_j$ in § 3.4, we have that (crudely using $|N| \geq 1$)

$$\Omega_N \geq \frac{N^{2\delta}}{L^2_\delta} \cdot \frac{1}{(\log L \log L_{-J} \cdots \log L_{J+1})^4}.$$ 

Apply Lemma 3.11, and then we get

$$\Omega_N \geq \frac{N^{2\delta}}{L^2_\delta} \cdot \frac{2^{4s(\log \log N)^2}}{\log(1 - \varrho)} \geq \frac{N^{2\delta}}{N^{\delta \varrho/6}} \cdot \frac{2^{4s(\log \log N)^2}}{2^{s(\log(1 - \varrho))}}.$$ 

The second inequality is true because $\frac{1}{4}(1 - \varrho)^2 \leq \frac{1}{12}$, see (3.23). Finally, observe that

$$N^{-\delta \varrho/6} \cdot \frac{2^{4s(\log \log N)^2}}{\log(1 - \varrho)} \gg N^{-\varrho},$$

where the implied constant depends on $\varrho$, and hence on $r$. Therefore, we have (3.75). □
4. Major Arcs Analysis

In this section, we estimate the major arcs contribution. We follow the similar approach as the major arcs analysis in [BK13]. First of all, the special set $\mathbb{S}$ we constructed in §3.2 allows us to split the exponential sum $S_N$ as a product of modular and archimedean components in the major arcs. Secondly, we show that the major arcs contribution is of the correct magnitude.

4.1. Splitting into Modular and Archimedean Components.

Let $Q$ be as in (3.27), and $B$ as in (2.11). We define the usual major arcs of level $Q$ as follows.

(4.1) $M_Q = \bigsqcup_{q < Q \atop (a,q) = 1} \left\{ \frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N} \right\}.$

Let $\nu_q : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ record the mod $q$ distribution of $\mathcal{D}$. That is, for $a \in \mathbb{Z}/q\mathbb{Z}$, set

(4.2) $\nu_q(a) := \frac{1}{|\text{SL}_2(q)|} \sum_{\omega \in \text{SL}_2(q)} e\left(\frac{a}{q} \langle \omega \epsilon_2, \epsilon_2 \rangle\right)$.

We first introduce the following Lemma which is crucial to the major arcs analysis.

**Lemma 4.1.** Recall the existence of $\Omega_N$ in (3.48). We write the ensemble $\Omega_N$ as follows.

(4.3) $\Omega_N = \Omega^{(1)} \cdot \mathbb{S} \cdot \Omega^{(2)},$

where $\Omega^{(1)} = \Xi_1 \Xi_2 \cdots \Xi_{J-1}$ and $\Omega^{(2)} = \Xi_1 \Xi_2 \cdots \Xi_{J+1}$.

Then, for any $\gamma_2 \in \Omega^{(2)}$, we have

$\langle e_2, v_-(\gamma_2) \rangle \gg 1$.

The implied constant does not depend on $\gamma_2$.

**Proof.** First of all, we have

$\langle e_2, v_-(\gamma_2) \rangle = \langle e_2, v_+(\gamma_2) \rangle \langle v_+(\gamma_2), v_-(\gamma_2) \rangle$

$+ \langle e_2, v_+(\gamma_2) \rangle \langle v_+(\gamma_2), v_-(\gamma_2) \rangle$.

Denote $\langle e_2, v_+(\gamma_2) \rangle$ by $m_1$ and $\langle v_+(\gamma_2), v_-(\gamma_2) \rangle$ by $m_2$. We already have $m_2 \geq \frac{1}{2}$ from (2.4). On the other hand, from (3.44) and (2.6), we obtain

(4.4) $m_1 = \langle v, e_2 \rangle \left[ 1 + O\left(\frac{1}{Q^2}\right) \right]$, and $m_2 \geq \frac{1}{2}$.

Combining (4.4) with the inequality

$\langle e_2, v_-(\gamma_2) \rangle \geq m_1 m_2 - \sqrt{1 - m_1^2} \sqrt{1 - m_2^2}$

completes the proof. 

The following theorem is similar to Theorem 4.2 in [BK13], but we need to alter the proof since our the ensemble $\Omega_N$ is different from the one in the original paper.

**Theorem 4.2.** ([BK13, p. 19]) There exists a function $\sigma_N : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$, given explicitly in (4.21), satisfying the following conditions.

1. The Fourier transform

$\hat{\sigma}_N : \mathbb{Z} \to \mathbb{C} : n \mapsto \int_0^1 \sigma_N(\theta)e(-n\theta)d\theta$

is real-valued and non-negative, with

(4.5) $\sigma_N(0) = \sum_n \sigma_N(n) \ll |\Omega_N|$. 

From (3.33), (3.31), (2.6), and (3.44), we see that for any For any

Using the decomposition (4.3), we rewrite the exponential sum

Consequently, when

\[ \theta \]

\[ \sum \]

\[ \langle \gamma_1 a \gamma_2 e_2, e_2 \rangle \]

\[ \lambda(a) \]

\[ (3.32) \]

\[ \text{Note that we have the good archimedean property (3.32). But to use this property, we must convert the expression } \langle \gamma_1 a \gamma_2 e_2, e_2 \rangle \text{ into one involving } \lambda(a). \text{ Before giving the argument, we need the following lemma to show that the contracting vector } v_-(\gamma_2) \text{ is close to } e_1. \]

Write \( v_\pm \) for \( v_\pm(\gamma_2) \), and observe that \( \langle \gamma_2 e_2, \gamma_1 e_2 \rangle = \langle \gamma_1 a \gamma_2 e_2, e_2 \rangle \). We can express \( a \gamma_2 e_2 \) as a linear combination of \( v_\pm \), and obtain the following equation

where we used the construction of \( \Omega_N \), Lemma 4.1, (2.6), and that

\[ v_- = v_-(\gamma_2) = v_-(\gamma_2)(1 + O(N^{-1})). \]

Similarly, we have

\[ \langle \gamma_2 e_2, \gamma_1 e_2 \rangle = \lambda(\gamma_2) \frac{\langle e_2, v_-(\gamma_2) \rangle}{\langle v_+, v_-(\gamma_2) \rangle} \langle e_1, \gamma_1 e_2 \rangle \left[ 1 + O\left( \frac{1}{Q^5} \right) \right]. \]

Combining (4.10) and (4.11), we get

\[ \langle a \gamma_2 e_2, \gamma_1 e_2 \rangle = \lambda(a) \langle \gamma_2 e_2, \gamma_1 e_2 \rangle \left[ 1 + O\left( \frac{1}{Q^5} \right) \right], \]

\[ = \lambda(a) \langle \gamma_2 e_2, \gamma_1 e_2 \rangle + O\left( N/Q^3 \right). \]

Consequently, when \( \theta \) is in the major arcs \( \mathcal{M}_Q \), the following equations hold.

\[ S_N \left( \frac{a}{q} + \beta \right) = \sum_{\gamma \in \mathcal{O}_Q} \sum_{\gamma_1 \in (\mathcal{O}_Q)^2} e\left( \frac{a}{q} \langle \gamma_1 a \gamma_2 e_2, \gamma_1 e_2 \rangle \right) e\left( \beta \langle \gamma_2 e_2, \gamma_1 e_2 \rangle \right) \]

\[ = \sum_{\gamma \in \mathcal{O}_Q} \sum_{\gamma_1 \in (\mathcal{O}_Q)^2} e\left( \frac{a}{q} \langle \gamma_1 a \gamma_2 e_2, \gamma_1 e_2 \rangle \right) e\left( \beta \lambda(a) \langle \gamma_2 e_2, \gamma_1 e_2 \rangle \right) + O\left( Q^{-4} |\Omega_N| \right) \]

\[ = \sum_{\gamma \in \mathcal{O}_Q} \sum_{\omega \in \text{SL}_2(q)} e\left( \frac{a}{q} \langle \omega \gamma_2 e_2, \gamma_1 e_2 \rangle \right) \sum_{\alpha \equiv a \pmod{q}} e\left( \beta \lambda(a) \langle \gamma_2 e_2, \gamma_1 e_2 \rangle \right) + O\left( Q^{-4} |\Omega_N| \right), \]

where \( \sum_{\gamma \in \mathcal{O}_Q} \) is a double sum over \( i = 1, 2 \), and the second equation comes from Taylor expansion and (4.12).
Since $\mathcal{N}$ is the disjoint union of $\mathcal{N}_u$, again by (3.32) and Taylor expansion, the innermost sum becomes

$$(4.14) \quad \sum_{a \in \mathcal{N} \atop a \equiv \omega (\mod q)} e(\beta u(a \langle \gamma e, \gamma_1 e \rangle)) = [1 + O(Q^{-4})] \sum_{u \in \mathcal{U}} \left( \sum_{a \in \mathcal{N}_u \atop a \equiv \omega (\mod q)} 1 \right) e(\beta u(\langle \gamma e, \gamma_1 e \rangle)).$$

One can see that what we need is a good distribution property for the set $\mathcal{N}$ to estimate $\sum_{a \in \mathcal{N}_u \atop a \equiv \omega (\mod q)} 1$. Hence, by (3.30) and (3.34), we have

$$(4.15) \quad \sum_{a \in \mathcal{N}_u \atop a \equiv \omega (\mod q)} 1 = \frac{|\mathcal{N}_u| (1 + O(Q^{-4}))}{|\mathcal{U}|} = \frac{|\mathcal{N}| (1 + O(Q^{-4}))}{|\mathcal{U}| \cdot |\mathcal{SL}_2(q)|},$$

where the implied constant is independent of $u$, $\omega$, or $q$. Inserting (4.15) and (4.14) into (4.13), we get

$$(4.16) \quad S_N \left( \frac{a}{q} + \beta \right) = \frac{1}{|\mathcal{SL}_2(q)|} \sum_{\gamma \in \Omega \atop \omega \in \mathcal{SL}_2(q)} e\left( \frac{a}{q} \langle \omega \gamma e, \gamma_1 e \rangle \right)$$

$$\times \frac{|\mathcal{N}|}{|\mathcal{U}|} \sum_{u \in \mathcal{U}} e\left( \beta u(\langle \gamma e, \gamma_1 e \rangle) \right) \times (1 + O(Q^{-4}))$$

$$= \frac{1}{|\mathcal{SL}_2(q)|} \sum_{\omega \in \mathcal{SL}_2(q)} \sum_{\gamma \in \Omega \atop \gamma \equiv \omega (\mod q)} e\left( \beta u(\langle \gamma e, \gamma_1 e \rangle) \right) \times (1 + O(Q^{-4})),$$

where the second equation comes from the fact that for each fixed $\gamma_1$, $\gamma_2$, the $\omega$ sum runs over all of $\mathcal{SL}_2(q)$. One can see that what we already acquired the first term $v_q(a)$ in the above expression.

Next, we want to know the distribution of frequencies for $\sum_{\gamma \in \Omega \atop \omega \in \mathcal{U}} e(\beta u(\langle \gamma e, \gamma_1 e \rangle))$, where use the following observation.

Fix $\gamma_1 \in \Omega^{(1)}$, $\gamma_2 \in \Omega^{(2)}$, and $u \in \mathcal{U}$. For any integer $m$ close to $u(\langle \gamma e, \gamma_1 e \rangle)$,

$$(4.17) \quad |m - u(\langle \gamma e, \gamma_1 e \rangle)| \leq B(\langle \gamma e, \gamma_1 e \rangle)/Q^5,$$

we have

$$(4.18) \quad e(\beta u(\langle \gamma e, \gamma_1 e \rangle)) = e(\beta m) (1 + O(Q^{-4})),$$

and the number of integers $m$ in (4.17) is $2B(\langle \gamma e, \gamma_1 e \rangle)/Q^5 + O(1) = (1 + O(Q^{-4}))2B(\langle \gamma e, \gamma_1 e \rangle)/Q^5$. Hence, we have

$$(4.19) \quad e(\beta u(\langle \gamma e, \gamma_1 e \rangle)) = \frac{Q^5 (1 + O(Q^{-4}))}{2B(\langle \gamma e, \gamma_1 e \rangle)} \sum_{m \in \mathbb{Z}, \min \{|m - u(\langle \gamma e, \gamma_1 e \rangle)| \leq \frac{Q}{Q^5}\} e(\beta m),$$

for $N$ large enough.

Rearranging the sum over $u$ and $m$, and inserting (4.19) into (4.16) leads to

$$(4.20) \quad S_N \left( \frac{a}{q} + \beta \right) = v_q(a) \mathcal{N}(\beta) (1 + O(Q^{-4})), $$

where

$$(4.21) \quad \mathcal{N}(\beta) := \frac{|\mathcal{U}|}{|\mathcal{U}|} \sum_{\gamma \in \Omega \atop \gamma \equiv \omega (\mod q)} \frac{Q^5}{2B(\langle \gamma e, \gamma_1 e \rangle)} \sum_{m \in \mathbb{Z}, \min \{|m - u(\langle \gamma e, \gamma_1 e \rangle)| \leq \frac{Q}{Q^5}\} e(\beta m)} \sum_{u \in \mathcal{U}} 1.$$
and thus proves (4.7). Moreover, one can easily check that

$$\bar{\omega}_N(n) = \frac{|\Omega|}{|\mathcal{U}|} \sum_{\gamma \in \Omega^0} Q^5 \left| \frac{n}{\langle \gamma_2 e_2, \gamma_1 e_2 \rangle} \sum_{u \in \mathcal{U}} 1_{|\frac{n}{\langle \gamma_2 e_2, \gamma_1 e_2 \rangle} - \frac{u}{Q^2}| \leq \frac{n}{Q}} \right|$$

is real and non-negative.

We need to show that \(n/\langle \gamma_2 e_2, \gamma_1 e_2 \rangle\) is comparable to \(N/B\). First of all, using (2.1), (2.2), and Lemma 3.10, we get

$$\frac{1}{16} \frac{N}{B} < \langle \gamma_2 e_2, \gamma_1 e_2 \rangle = \langle \gamma_1 \gamma_2 e_2, e_2 \rangle < \frac{8N}{B}.$$ Combining with the fact that \(\frac{1}{50} N < n < \frac{1}{20} N\), we obtain the following estimate for \(n/\langle \gamma_2 e_2, \gamma_1 e_2 \rangle\).

$$\frac{1}{400} B \leq \frac{n}{\langle \gamma_2 e_2, \gamma_1 e_2 \rangle} < \frac{399}{400} B.$$ Finally, by the definition (3.28) of \(u \in \mathcal{U}\) in this range, we have the innermost sum

$$\sum_{u \in \mathcal{U}} 1_{|\frac{n}{\langle \gamma_2 e_2, \gamma_1 e_2 \rangle} - \frac{u}{Q^2}| \leq \frac{n}{Q^2}} \geq 1.$$ This leads us to (4.6) as follows.

$$\bar{\omega}_N(n) \gg \frac{|\Omega|}{|\mathcal{U}|} \sum_{\gamma \in \Omega^0} Q^5 \left| \frac{n}{\langle \gamma_2 e_2, \gamma_1 e_2 \rangle} \right| \frac{|\Omega_1|}{N} \frac{|\Omega_2|}{N} = \frac{|\Omega_N|}{N}. \quad \square$$

4.2. The Major Arcs Contribution. The argument of this section goes exactly the same as the one in §4.2 in [BK13]. The idea is to contruct such test function that is periodic and has mass centered around each major arc. Consider the triangle function \(\psi(x)\) as in (2.15). We adjust the support around the origin, and obtain \(\psi_N\) as follows.

$$\phi_N(x) := \psi \left( \frac{N}{Q} x \right).$$

Periodize \(\psi_N\) on \(\mathbb{R}/\mathbb{Z}\):

$$\Psi_N(\theta) := \sum_{m \in \mathbb{Z}} \phi_N(\theta + m),$$

and put each such spike at a major arc:

$$\Psi_{Q,N}(\theta) = \sum_{q < Q} \sum_{(\alpha,q) = 1} \Psi_N \left( \theta - \frac{\alpha}{q} \right)$$

Note that the support of \(\Psi_{Q,N}\) is \(\mathfrak{M}_Q\).

Recall that

$$R_N(n) := \tilde{S}_N(n) = \int_0^1 S_N(\theta) e(-n\theta) d\theta,$$

and decompose it into a (smoothed) major arcs contribution and an error

$$R_N(n) = M_N(n) + E_N(n),$$

where

$$M_N(n) = \int_0^1 \Psi_{Q,N}(\theta) S_N(\theta) e(-n\theta) d\theta,$$
Lemma 4.3. Assume that \( q \) is a prime power \( p^r \). Let \( c_q(m) \) be the Ramanujan’s sum defined as follows.

\[
c_q(m) = \sum_{(a,q)=1} e\left(\frac{a}{q}m\right).
\]

Moreover, we defined a function \( C_q(n) \) which averages \( c_q(m) \) over the group \( SL_2(q) \) as follows.

\[
C_q(n) = \frac{1}{|SL_2(q)|} \sum_{\omega \in SL_2(q)} c_q(d - n),
\]

where \( \omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). Then, we have

\[
C_q(n) = \begin{cases} 
\frac{-1}{p+1}, & \text{when } t = 1 \text{ and } p \mid n. \\
\frac{1}{p^2+1}, & \text{when } t = 1 \text{ and } p \nmid n. \\
0, & \text{when } t \geq 2.
\end{cases}
\]

Proof. First of all, by the Mobius inversion formula, we have

\[
c_q(m) = \sum_{d\mid (q,m)} d\mu\left(\frac{q}{d}\right), \mu \text{ is the Mobius function.}
\]

Using (4.34) and the fact that \( C_q(n) = p^{3r-2}(p^2-1) \), we can easily prove the two cases when \( t = 1 \). For \( t \geq 2 \), by (4.34), we rewrite \( C_q(n) \) as

\[
C_q(n) = \frac{1}{|SL_2(q)|} \sum_{\omega \in SL_2(q)} \sum_{d\mid (q,m)} d\mu\left(\frac{q}{d}\right), \text{ where } m = \langle \omega e_2, e_2 \rangle - n,
\]

\[
= (p^r - p^{r-1}) \sum_{\omega \in SL_2(q)} \mathbf{1}_{\{d\mid n(p^{r-1})\}} - p^{r-1} \sum_{\omega \in SL_2(q)} \mathbf{1}_{\{d
ot\mid n(p^{r-1})\}}.
\]

We will show that

\[
(p-1) \sum_{\omega \in SL_2(q)} \mathbf{1}_{\{d\mid n(p^{r-1})\}} = \sum_{\omega \in SL_2(q)} \mathbf{1}_{\{d
ot\mid n(p^{r-1})\}}.
\]

In fact, (4.36) is true if we can show that for any \( \gamma \equiv \begin{pmatrix} * & * \\ * & n \end{pmatrix} \pmod{p^{r-1}} \), we have

\[
(p-1) \sum_{\omega \in SL_2(q)} \mathbf{1}_{\{d\mid n(p^{r-1})\}} = \sum_{\omega \in SL_2(q)} \mathbf{1}_{\{d
ot\mid n(p^{r-1})\}}.
\]

Indeed, for any \( \omega \equiv \begin{pmatrix} a_1 & b_1 \\ c_1 & n \end{pmatrix} \pmod{p^{r-1}} \), the general expression for \( \omega \) is

\[
\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_1 + p^{r-1}k_1 & b_1 + p^{r-1}k_2 \\ c_1 + p^{r-1}k_3 & n + p^{r-1}k_4 \end{pmatrix}
\]
where \( 0 \leq k_i < p_i \) and satisfy
\[
(4.39) \quad p \mid k_1 n + k_4 a - k_3 b_1 - k_2 c + \frac{a_1 n - b_1 c_1}{p^{i-1}}.
\]

Now, one can see that no matter what choice of \( k_4 \) we fix, there are always \( p^2 \) choices for the tuple \((k_1, k_2, k_3)\). Consequently, we must have (4.37) which thus concludes (4.33). \( \square \)

Equipped with (4.2), we obtain the following theorem as in [BK13] with a different range of \( n \).

**Theorem 4.4.** ([BK13, p. 23]) For \( \frac{1}{50} N \leq n < \frac{1}{25} N \),
\[
(4.40) \quad \mathcal{M}_N(n) \gg \frac{1}{\log \log N} \frac{\#\Omega_N}{N}.
\]

**Proof:** We continue to work on (4.30). For \( \Psi_{Q,N}(\theta) \), we use (4.27), and for \( S_N(\theta) \), we use (4.20). Consequently, we obtain
\[
(4.41) \quad \mathcal{M}_N(n) = \int_0^1 \sum_{q < Q} \sum_{(a,q)=1} \Psi_N \left( \theta - \frac{a}{q} \right) v_q(a) \sigma_N(\beta) (1 + O(Q^{-1})e(-n\theta)) d\theta.
\]
Replacing \( \theta \) by \( \frac{\nu}{q} + \beta \), we get
\[
(4.42) \quad \mathcal{M}_N(n) = \sum_{q < Q} \sum_{(a,q)=1} v_q(a) e\left(-\frac{a}{q} \right) \int_0^1 \Psi_N (\beta) \sigma_N(\beta) e(-n\beta) (1 + O(Q^{-1})) d\beta.
\]
From (4.21), the possible range of \( m \) is of size \( 2B(\gamma_2 e_2, \gamma_1 e_2) \). Therefore, the size of \( \sigma_N(\beta) \) is at most
\[
(4.43) \quad |\sigma_N(\beta)| \ll \frac{\#\Omega(1)\#\Omega(2)Q^2}{\#\Omega_N},
\]
where the implied constant is absolute. This implies that
\[
(4.44) \quad \mathcal{M}_N(n) = \sum_{q < Q} \sum_{(a,q)=1} v_q(a) e\left(-\frac{a}{q} \right) \int_0^1 \Psi_N (\beta) \sigma_N(\beta) e(-n\beta) d\theta + O \left( Q^2 \cdot Q^{-4} \cdot \frac{Q}{N} \cdot \#\Omega_N \right),
\]
where
\[
(4.45) \quad \mathcal{M}_N(n) = \int_0^1 \Psi_N (\beta) \sigma_N(\beta) e(-n\beta) d\beta.
\]

Our first task is to estimate the singular series \( \mathcal{M}_N(n) \). We write the singular series as follows.
\[
(4.46) \quad \mathcal{M}_N(n) = \sum_{q < Q} \frac{1}{|SL_2(q)|} \sum_{\omega \in SL_2(q)} \sum_{(a,q)=1} e \left( \frac{a}{q} (\omega e_2, e_2) - n \right) = \sum_{q < Q} \frac{1}{|SL_2(q)|} \sum_{\omega \in SL_2(q)} c_q ((\omega e_2, e_2) - n),
\]
where \( c_q(m) \) is the Ramanujan sum, see Lemma 4.3.

Recall the average function \( C_q(n) \) in Lemma 4.3. Since the Ramanujan’s sum is multiplicative, by Chinese remainder theorem again, we have \( C_q(n) \) is also multiplicative. Consider the following indicator
\[
\nu_q(q) = \begin{cases} 1, & \text{if } q = p_1 \cdots p_{2k}, \text{for distinct primes } p_i, \text{ and for all } i, \ p_i \mid n. \\ 0, & \text{otherwise.} \end{cases}
\]

Then the contribution of \( \sum_{q < Q} C_q(n) \) is at most
\[
(4.47) \quad \sum_{q < Q} C_q(n) \leq \left( \sum_{q < Q} \frac{1}{q} \nu_q(q) \right) \prod_{p \mid n} \left( 1 + \frac{1}{p^{i-1}} \right) \leq \frac{2}{\phi} \sum_{q < Q} v_q(q) = o \left( \frac{1}{\log \log n} \right),
\]
where the last equality comes from the definition of $Q$ and the assumption that $\frac{1}{40}N \leq n < \frac{1}{25}N$.

Therefore, we can extend the sum $\sum_{q<Q}6_q(n)$ to $\sum_{q<\infty}$ which leads us to the following new series

\[(4.48)\quad G(n) = \sum_{q<\infty} C_q(n).\]

Moreover, by the multiplicativity of $C_q(n)$ and Lemma 4.3, we have

\[(4.49)\quad G(n) = \prod_{p|n} \left(1 + \frac{1}{p} \right) \cdot \prod_{p|n} \left(1 - \frac{1}{p + 1}\right) = \prod_{p|n} \left(1 - \frac{1}{p + 1}\right) \cdot \prod_{p|n} \left(1 + \frac{1}{p}\right) \leq \frac{1}{n} \sigma_1(n) \ll \log \log n,
\]

where $\sigma_1(n) = \sum_{d|n} d$, and the last inequality comes from Robin’s inequality [Rob82]. Thus, we get

\[6(n) \gg \frac{1}{\log \log n},\]

and by (4.47), we obtain

\[(4.51)\quad G_Q(n) \gg \frac{1}{\log \log n}.
\]

Let us move on to the singular integral $\mathfrak{I}_N(n)$. By elementary Fourier analysis, we have

\[(4.52)\quad \mathfrak{I}_N(n) = \sum_{m \in \mathbb{Z}} \phi_N(n-m) \tilde{\sigma}_N(m) = \frac{Q}{N} \sum_{m \in \mathbb{Z}} \psi \left( \frac{Q}{N} (n-m) \right) \tilde{\sigma}_N(m).
\]

Moreover, by the definition of $\psi$ in (2.15), $\tilde{\psi}(x) > 2/5$ when $|x| < 1/2$. Consequently,

\[(4.53)\quad \mathfrak{I}_N(n) \gg \frac{Q}{N} \sum_{|m-n| < N/(2Q)} \tilde{\sigma}_N(m).
\]

Since $\frac{1}{40}N \leq n < \frac{1}{25}N$, we can ensure that for $N$ large enough, the following inequality is true for any $m$ with $|m-n| < N/(2Q)$.

\[
\frac{1}{50}N < m < \frac{1}{20}N.
\]

Therefore, we may apply Theorem 4.2 and get

\[(4.54)\quad \mathfrak{I}_N(n) \gg \frac{Q}{N} \cdot \frac{N}{2Q} \cdot \frac{\#\Omega_N}{N} \gg \frac{\#\Omega_N}{N}.
\]

Combining (4.54) with (4.51), we obtain

\[(4.55)\quad M_N(n) \gg \frac{1}{\log \log N} \cdot \frac{\#\Omega_N}{N},
\]

where we also use the fact that $Q^{-1} = o \left( \frac{1}{\log \log N} \right)$.

\[\Box\]
5. Setup for Minor Arcs Analysis

Our task is to estimate the integral of exponential sum as in (4.31).

\[ E_N(n) := \int_0^1 (1 - \Psi_{Q,N})S_N(\theta)e(-n\theta)d\theta. \]

Specifically, we hope to bound the \( L^2 \)-norm of \((1 - \Psi_{Q,N})S_N(\theta)e(-n\theta)\). To do so, we decompose \([0, 1]\) into dyadic regions. First of all, by Dirichlet approximation, for every number \( \theta \in [0, 1] \), there exists a fraction \( a/q \) with \( 1 \leq q \leq \sqrt{N} \) such that

\[ |\theta - a/q| < \frac{1}{q \sqrt{N}}. \]

Consequently, we have

\[ \int_0^1 |S_N(\theta)|^2 d\theta \ll \sum_{1 \leq Q < N^{1/2}} \sum_{\substack{\ell \leq K \leq N^{1/2} \theta}} |W_{Q,K}|^2 d\theta. \]

where we define \( W_{Q,K} \) as follows.

Recall the constant \( \tilde{C} \) defined in (3.20). For \( K \geq 2\tilde{C} \), we set

\[ W_{Q,K} = \left\{ \theta = a/q + \frac{\ell}{TN} + t : \frac{1}{2}Q \leq q < Q, (a,q) = 1, \frac{KT}{2} \leq |\ell| < K, |t| < \frac{1}{T.N} \right\}, \]

where \( q, a, \ell \in \mathbb{Z} \) and \( T = T(Q, K) \) is some parameter we will set later. When \( K \) is at constant level as \( \tilde{C} \leq K < 2\tilde{C} \), we set

\[ W_{Q,K} = \left\{ \theta = a/q + \beta : \frac{1}{2}Q \leq q < Q, (a,q) = 1, |\beta| < \frac{K}{N} \right\}. \]

We shift our focus back to the case when \( K \geq 2\tilde{C} \). For any \( \theta \in W_{Q,K} \) and \( \gamma \in \Omega_N \), we have by Taylor expansion and Lemma 3.10 that

\[ \left| e(\langle \gamma e_2, e_2 \rangle \theta) - e(\langle \gamma e_2, e_2 \rangle \left( a/q + \frac{\ell}{TN} \right) ) \right| \leq \frac{1}{T}. \]

This implies

\[ |S_N(\theta) - S_N \left( \frac{a}{q} + \frac{\ell}{TN} \right)| \leq \frac{\#\Omega_N}{T}. \]

By triangle inequality, we get

\[ |S_N(\theta)|^2 \leq 2 \left\{ |S_N \left( \frac{a}{q} + \frac{\ell}{TN} \right) |^2 + \frac{\left( \#\Omega_N \right)^2}{T^2} \right\}. \]

Finally, integrating \( |S_N(\theta)|^2 \) over \( W_{Q,K} \), we obtain

\[ \int_{W_{Q,K}} |S_N(\theta)|^2 \ll \frac{1}{TN} \sum_{\frac{1}{2}Q < Q} \sum_{(a,q)=1} \sum_{\frac{KT}{2} \leq |\ell| < KT} \left| S_N \left( \frac{a}{q} + \frac{\ell}{TN} \right) \right|^2 + \frac{KQ^2}{T^2N}(\#\Omega_N)^2, \]

where the implied constant is absolute. Now, we set

\[ T = KQ^2. \]
Then the last inequality becomes

\[(5.8) \quad \int_{W_{Q,K}} |S_N(\theta)|^2 \ll \frac{1}{T N} \sum_{P_{Q,K}} \left| S_N \left( \frac{a}{q} + \frac{\ell}{T N} \right) \right|^2 + \frac{1}{KQ} \frac{(\#\Omega_N)^2}{N}, \]

where

\[P_{Q,K} = \left\{ \frac{a}{q} + \frac{\ell}{T N} : \frac{1}{2} \leq q < Q, q \geq a, (q,a) = 1, \frac{1}{2} K T \leq \ell < K T \right\}.\]

**Remark 5.1.** The inequality (5.7) can be think of as approximating the integral with Riemann sum. The larger \(T\) we pick, the closer the triple sum in the right hand side of (5.7) is to the integral \(\int_{W_{Q,K}} |S_N(\theta)|^2\). We specifically choose \(T = KQ^2\) so that we have a \(KQ\) saving in the error term \(\frac{KQ^2}{T^2N} (\#\Omega_N)^2\). This concept can also be found in [FK13].

On the other hand, when \(\widetilde{C} \leq K < 2\widetilde{C}\), we use the following inequality instead.

\[(5.9) \quad \int_{W_{Q,K}} |S_N(\theta)|^2 \ll \frac{K}{N \sup_{|\beta| < K/N} \sum_{P_{Q,\beta}} \left| S_N \left( \frac{a}{q} + \beta \right) \right|^2, \]

where

\[P_{Q,\beta} = \left\{ \frac{a}{q} + \beta : \frac{1}{2} \leq q < Q, q \geq a, (q,a) = 1 \right\}.\]

In §6 and §7, we will derive bounds for \(\sum_{P_{Q,K}} |S_N \left( \frac{a}{q} + \frac{\ell}{T N} \right)\|^2\) for different magnitudes of \(K\) and \(Q\). When \(K\) is of constant magnitude \(\widetilde{C}\), one can slightly altered the proof in §6 and §7 to bound the sum \(\sum_{P_{Q,\beta}} \left| S_N \left( \frac{a}{q} + \beta \right) \right|^2\).

Moreover, for some technical reasons, we replace \(N\) in (5.2) by \(N' = 2^{26}N\). Thus, \(Q\) and \(K\) must satisfy \(Q < 2^{13} \sqrt[3]{N}\) and \(KQ < 2^{13} \sqrt[3]{N}\).

6. **MINOR ARCS ANALYSIS I**

We recall that our task is to estimate the exponential sum

\[(6.1) \quad \sum_{P_{Q,K}} |S_N(\theta)|^2, \]

where \(P_{Q,K} = \left\{ \frac{a}{q} + \frac{\ell}{T N} : \frac{1}{2} \leq q < Q, q \geq a, (q,a) = 1, \frac{1}{2} K T \leq \ell < K T \right\}, N' = 2^{26}N\), and \(T = KQ^2\).

Hence, the size of \(P_{Q,K}\) is \(KQ^2T\).

Our goal is to have a bound slightly better than \(\frac{(\#\Omega_N)^2}{N}\). Specifically, we want some extra saving of \(K\) or \(Q\) as follows.

\[\sum_{P_{Q,K}} |S_N(\theta)|^2 \ll \frac{(\#\Omega_N)^2}{N} \frac{1}{K^\alpha Q \ell^\beta}. \]

In this section, we use a “triple” Kloosterman refinement to give a bound for \(\sum_{P_{Q,K}} |S_N(\theta)|^2\). This bound will suffice as long as \(Q\) or \(K\) is large.

**Remark 6.1.** The reason we call the method we use in this section a “triple” Kloosterman refinement is that \(P_{Q,K}\) takes summation over \(a, q, \) and \(\ell\). Bringing in a new sum allows us to gain extra cancellations in the exponential sum. An interesting project would be to generalize this idea to other problems involving circle method. The concept of “triple” Kloosterman refinement originated in [Kor92].

First of all, we recall an observation in [FK13]. A similar statement can also be found in [Kon02].
Lemma 6.2. ([FK13, p. 33]) Let $W$ be a finite subset of $[0, 1]$ such that $|W| > 3$. Suppose that $f : W \rightarrow \mathbb{R}_+ \cup \{0\}$ is a non-negative function such that for any subset $Z \subset W$, we have

\[(6.2) \quad \sum_{\theta \in Z} f(\theta) \leq C_1 |Z|^\frac{1}{2},\]

where $C_1$ is independent of the choice of $Z$. Then we have

\[(6.3) \quad \sum_{\theta \in W} f^2(\theta) \leq 2C_1^2 \log |W|.
\]

Proof. We order $f(\theta)$ in the following way

\[f_1 \geq f_2 \geq \cdots \geq f_{|W|} \geq 0.\]

Therefore, for any $k$ with $1 \leq k \leq |W|$, we have

\[k f_k \leq \sum_{n=1}^{k} f_n \leq C_1 k^\frac{1}{2}.\]

This implies that $f_k \leq C_1 k^{-\frac{1}{2}}$, and thus $f_k^2 \leq C_1^2 k^{-1}$. Therefore

\[(6.4) \quad \sum_{\theta \in W} f^2(\theta) \leq C_1^2 (\log |W| + 1) \leq 2C_1^2 \log |W|.
\]

Remark 6.3. This is not a hard proof. However, it does contribute more saving than the following approach given that our $L^\infty$ bound saves only $KQ$.

\[
\sum_{\theta \in W} f^2(\theta) \leq \left( \sup_{\theta \in W} f \right) \sum_{\theta \in W} f(\theta).
\]

Hence, by Lemma (6.2), it is natural to look for a universal bound for $\sum_{\theta \in Z} |S_N(\theta)|$, where $Z$ is an arbitrary subset of $P_{Q,K}$. Specifically, the following theorem holds for any subset $Z \subset P_{Q,K}$.

Theorem 6.4. For any subset $Z \subset P_{Q,K}$, we have

\[(6.5) \quad \sum_{\theta \in Z} |S_N(\theta)| \ll \#\Omega_N \cdot \frac{N^{1-\delta} 2^{(\log \log N)^2}}{\sqrt{KQ}} \cdot |Z|^\frac{1}{2} \cdot \tau^{-\frac{1}{2}}.
\]

Remark 6.5. Throughout the rest of the paper, the implied constants for inequalities with symbol $\ll$ depend only on $\mathcal{A}$ and $\varrho$. Notice that $\mathcal{A}$ and $\varrho$ are fixed in the beginning.

Remark 6.6. When $K$ is at constant level $\tilde{C}$, Theorem 6.4 read as follows instead. For any subset $Z \subset P_{Q,\beta}$, we have

\[
\sum_{\theta \in Z} |S_N(\theta)| \ll \#\Omega_N \cdot \frac{N^{1-\delta} 2^{(\log \log N)^2}}{\sqrt{\mathcal{Q}}} \cdot |Z|^\frac{1}{2}.
\]

Proof. We decompose ensemble $\Omega_N$ as follows.

\[(6.6) \quad \Omega_N = (\Xi_{-J} \Xi_{-J+1} \cdots \Xi_{J_1}) (\Xi_{J_1+1} \cdots \Xi_{J+1}) = \Omega^{(1)} \Omega^{(2)},
\]

where $\Omega^{(1)} = \Xi_{-J} \Xi_{-J+1} \cdots \Xi_{J_1}$ and $\Omega^{(2)} = \Xi_{J_1+1} \cdots \Xi_{J+1}$. By Lemma 3.10, for any $g_1 \in \Omega^{(1)}$, and $g_2 \in \Omega^{(2)}$, we have

\[(6.7) \quad \frac{1}{16000} < \frac{\lambda(g_1)}{H_1} < 32, \quad \frac{1}{16000} < \frac{\lambda(g_2)}{H_2} < 32.
\]
Denote $N^{3/4}$ by $H_1$ and $N^{1/4}$ by $H_2$. Now we define the measure $\mu$ and $\nu$ on $\mathbb{Z}^2$ by
\[
\mu(x) := \sum_{y_1 \in \mathcal{Y}} 1_{x = y_1 e_1},
\]
\[
\nu(y) := \sum_{y_2 \in \mathcal{Y}} 1_{y = y_2 e_2},
\]
with $\mu, \nu \leq 1$. Writing
\[
S_N(\theta) = \sum_x \mu(x) \nu(y) e(\theta(x, y)),
\]
we proceed to bound
\[
\sum_{\theta \in \mathbb{Z}} |S_N(\theta)| = \sum_{\theta \in \mathbb{Z}} \zeta(\theta) S_N(\theta)
\]
\[
= \sum_{\theta = \frac{a}{q} + \frac{\ell}{T N'}} \zeta(\theta) \sum_x \sum_y \mu(x) \nu(y) e(\theta(x, y)),
\]
which $\zeta$ has modulus 1. Consider a non-negative bump function $\Upsilon$, see §2.3, which is at least one on $[-1, 1]^2$, and has Fourier transformation supported in a ball of radius $1/2^{28}$ about the origin. Apply Cauchy-Schwarz in the sum $x$, insert the function $\Upsilon$, reverse orders, and apply Poisson summation:
\[
(6.8) \quad \sum_{\theta \in \mathbb{Z}} |S_N(\theta)| \ll N^{3/4} \left( \sum_x \Upsilon \left( \frac{x}{32H_1} \right) \right) \sum_{\theta \in \mathbb{Z}} \left| \zeta(\theta) \sum_y \nu(y) e(\theta(x, y)) \right|^2 \ll N^{3(\delta+1)/4} \chi^{1/2},
\]
where
\[
(6.9) \quad \chi = \chi_{\theta, K := \sum_{\theta' \in \mathbb{Z}} \sum_{y' \in \mathbb{Z}} \nu(y') 1_{\{||\theta - \theta'|| < \frac{1}{2^{28} H_1} \}}.
\]
Here $\theta' = \frac{a'}{q'} + \frac{\ell'}{T N'}$. Also, we write $y = (y_1, y_2)$, and the same with $y'$. Recall that $y = g_2 e_2$ for some (non-identity) $g_2 \in \Gamma$, and the same of $y'$; hence we have
\[
y_1 y'_1 y_2 y'_2 \neq 0.
\]
On the other hand, besides the innermost condition in (6.9), we have
\[
(6.10) \quad \left| y_1 \frac{\ell}{T N'} - y'_1 \frac{\ell'}{T N'} \right| \leq \left| y_1 \frac{\ell}{T N'} \right| + \left| y'_1 \frac{\ell'}{T N'} \right| \leq \frac{64H_2 K}{N'},
\]
and the same with $|y_2 \frac{\ell}{T N'} - y'_2 \frac{\ell'}{T N'}|$. Thus, we have the following inequality:
\[
(6.11) \quad \left| y_1 \frac{a}{q} - y'_1 \frac{a'}{q'} \right| \leq \left| y_1 \theta - y'_1 \theta' \right| + \left| y_1 \frac{\ell}{T N'} - y'_1 \frac{\ell'}{T N'} \right| \leq \frac{1}{2^{28} H_1} + \frac{64H_2 K}{N'},
\]
and similarly with $y_2, y'_2$.

Let $Y := \begin{pmatrix} y_1 & y'_1 \\ y_2 & y'_2 \end{pmatrix}$, so that
\[
(6.12) \quad \mathcal{Y} := \det(Y) = y_1 y'_2 - y_2 y'_1.
\]
Observe then by (6.11), (6.7), \( Q < \left( \frac{2^{26} N}{1} \right)^{1/2} \), and \( KQ < \left( \frac{2^{26} N}{1} \right)^{1/2} \) that

\[
\| y_1 a - y_2 a' \| \leq \| y'_1 \left( y_1 a - y_1 a' \right) \| + \| y'_2 \left( y_2 a' - y_2 a \right) \|
\]

\[
\leq 32H_2 \left( \frac{1}{2^{28} H_1} + \frac{64H_2 K}{N'} \right) \times 2 < \frac{1}{Q}.
\]

This forces \( Y \equiv 0 \pmod{q} \). The same arguments gives \( Y \equiv 0 \pmod{q'} \), and hence we have

\( Y \equiv 0 \pmod{q} \),

where \( \frac{1}{2} Q \leq q < Q \) is the least common multiple of \( q \) and \( q' \).

Decompose \( \chi \) in (6.9) as \( \chi = \chi_1 + \chi_2 \) according to whether \( Y = 0 \) or not; we handle the two contributions separately.

### 6.1. Bounding \( \chi_1 \): the case \( Y = 0 \).

The condition \( Y = 0 \) implies that \( y_1/y_2 = y'_1/y'_2 \). Recall that rationals have unique continued fraction expansions (of even length), and thus \( y_1 = y'_1 \). Now, set

\[
\tilde{r} = \frac{1}{2^{28} H_1} + \frac{64H_2 K}{N'},
\]

and

\[
\alpha = \left| \frac{a}{q} - \frac{a'}{q'} \right|.
\]

The equation (6.11) now becomes

\( ||y_1 a|| \leq \tilde{r} \).

Furthermore, the above equation can be rewritten as

\( y_1 \alpha = n_1 + t_1 \tilde{r}, \) and \( y_2 \alpha = n_2 + t_2 \tilde{r}, \)

where \( |t_1|, |t_2| \leq 1 \). Fix \( \theta = \frac{a}{q} + \frac{t}{T N'}, \) we will show that \( \theta' \) has \( \ll T \) choices. To prove this, we consider two cases - \( \alpha = 0 \), or \( \alpha \neq 0 \).

1. \( \alpha = 0 \). This implies that

\[
\left| y \left( \frac{\ell - \ell'}{T N'} \right) \right| = \left| y \left( \theta - \theta' \right) \right| \leq \frac{1}{2^{28} H_1}.
\]

Consequently, we have \( \ll T \) choices for \( \ell' \).

2. \( \alpha \neq 0 \). Straightforward computation shows that

\( (y_1 n_2 - y_2 n_1) = (t_1 y_2 - t_2 y_1) \tilde{r}. \)

Hence,

\[
|y_1 n_2 - y_2 n_1| = (y_1 + y_2) \tilde{r} \leq 32H_2 \left( \frac{1}{2^{28} H_1} + \frac{64H_2 K}{N'} \right) \times 2 < \frac{1}{Q} < 1.
\]

Thus, \( y_1 n_2 - y_2 n_1 = 0 \), and by the fact that \( (y_1, y_2) = 1 \), we obtain \( n_1 = y_1 t \), and \( n_2 = y_2 t \). However, since \( t < 1 \), the only choices for \( t \) are 0 or 1.

1. \( t = 0 \). We have

\[
y_2 \alpha = t_2 \tilde{r},
\]

which implies

\[
\alpha < \frac{32}{H_2} \tilde{r}.
\]
(2) \( t = 1 \). We have
\[
y_2 \alpha = y_2 + t_2 \hat{r} \Rightarrow y_2(1 - \alpha) = -t_2 \hat{r},
\]
which implies
\[
1 - \alpha < \frac{32}{H_2} \hat{r}.
\]
Since \( K \geq \bar{C} > 2^{12} \), we have \( \frac{32}{H_2} \hat{r} < \frac{1}{Q} \), and thus both case (1) and case (2) have no solution with \( \alpha \neq 0 \).

From the above discussion, we conclude that
\[
|\chi_1| \ll |\Omega^{(2)}| |Z| T,
\]
where \( |\Omega^{(2)}| \) is the number of choices for \( g_2 \), \( |Z| \) is the number of choices for \( \theta \), and \( T \) is the number of choices for \( \theta' \).

\textbf{Remark 6.7.} Minor modification is needed when \( K \) is at constant level. The case \( \alpha = 0 \) directly implies that \( \theta' \) is fixed. The proof for the case \( \alpha \neq 0 \) remain unchanged. Then, we have
\[
|\chi_1| \ll |\Omega^{(2)}| |Z|.
\]

6.2. \textbf{Bounding} \( \chi_2 \): the case \( \mathcal{Y} \neq 0 \).
Note that \( |\mathcal{Y}| \leq 64H_2^2 \). Since \( q|\mathcal{Y} \), and \( \mathcal{Y} \neq 0 \), we have
\[
a \leq Q^2, a \leq 64H_2^2 \Rightarrow q \leq 8H_2 Q \Rightarrow \frac{1}{q} \geq \frac{1}{8H_2 Q}.
\]
Moreover, from the definition of \( H_1 \) and \( H_2 \), one can easily show that
\[
\frac{1}{2^{28}H_1} < \frac{1}{16H_2 Q'} \quad \frac{64H_2 K}{N'} < \frac{1}{16H_2 Q'}
\]
Hence, (6.11) implies that
\[
\left\| y_1 \frac{a}{q} - y_1' \frac{a'}{q'} \right\| < \frac{1}{8H_2 Q} \leq \frac{1}{a}.
\]
This forces
\[
y_1 \frac{a}{q} - y_1' \frac{a'}{q'} \equiv 0 \pmod{1}, \quad \text{and} \quad \left| y_1 \frac{\ell'}{TN'} - y_1' \frac{\ell'}{TN'} \right| \leq \frac{1}{2^{28}H_1}
\]
and the same holds for \( y_2, y_2' \). Let \( \bar{q} := (q, q') \) and \( q = q_1 \bar{q}, q' = q_1' \bar{q} \) so that \( q = q_1 q_1' \bar{q} \). Then (6.18) becomes
\[
y_1 a q_1' \equiv y_1' a' q_1 \pmod{q},
\]
and the same for \( y_2, y_2' \). Recall \( a \) and \( q \) are coprime, as are \( a' \) and \( q' \). It then follows that \( q_1 |y_1 \), and similarly, \( q_1 |y_2 \). But since \( y \) is a visual vector, we need \( q_1 = 1 \). The same argument applies to \( q_1' \), so we have \( q = q' = q \). Then (6.18) now reads
\[
y_1 a \equiv y_1' a' \pmod{q},
\]
and similarly for \( y_2, y_2' \).

We start by fixing \( q_2' \) for which there are \( |\Omega^{(2)}| \) choices. Now the vector \( y' \) is fixed. Next, we fix \( \theta \in \mathbb{Z} \) for which there are \( |Z| \) choices. Now the parameters \( a, q \), and \( \ell \) are fixed. Notice that from (6.18), we have
\[
\frac{\mathcal{Y} \ell}{T} = \frac{|y_1 y_2 - y_2 y_1'| \ell}{T} \leq y_1' \left| y_2 \ell - y_2' \ell' \right| T + y_2' \left| y_1 \ell' - y_1' \ell \right| T < \left| y_1 \ell - y_1' \ell' \right| T \leq \frac{N'}{2^{28}H_1} \cdot 64H_2 \ll H_2^2.
\]
This implies that
\[
|y_1 y_2 - y_2 y_1'| \ll \frac{H_2^2}{K}.
\]
Since \( q|\mathcal{Y} \), there are \( \ll \frac{H^2}{KQ} \) choices for \( t' \) (note that \( KQ \ll H^2 \)), where

\[
(6.21) \quad y_1 y_2' - y_2 y_1' = t' q.
\]

Now, we fix \( t' \). Again, with \( y \) and \( y' \) being visual vectors, all solutions to (6.21) are of the following form

\[
(6.22) \quad y_1 = y_1' + s y_1', \quad y_2 = y_2' + s y_2',
\]

where \( s \in \mathbb{Z} \) and \((y_1', y_2')\) is a solution to (6.21). (Note that \( y' \) is already fixed.)

In addition, we have

\[
\left| \frac{y_1 \ell - y_2 \ell'}{y_2} \right| \leq \frac{N'}{28 H_1}.
\]

Dividing both side by \( y_2' \), we get

\[
\left| \ell' - \frac{y_2}{y_2'} \ell \right| \leq \frac{\ell' - y_2}{y_2'} \frac{N'}{28 H_1} \leq 8000 \ell'.
\]

After we take away the absolute sign and use (6.22), the above equation becomes

\[
(6.23) \quad \frac{y_2}{y_2'} \ell + s \ell - 8000 \ell' \leq \frac{y_2}{y_2'} \ell + s \ell + 8000 \ell'.
\]

Since \( \ell, \ell' \approx K \ell \), there are only \( \ll 1 \) choices for \( s \). Fix \( s \), and so \( y \) is fixed by (6.22).

Finally, with \( s \) fixed, there are \( \ll T \) choices for \( \ell' \). The above discussion implies that

\[
(6.24) \quad |\chi_2| \ll \Omega(2) |Z| \frac{H^2}{KQ} T.
\]

Remark 6.8. When \( K \) is at constant level, we stop at (6.19). That is, for fixed \( y' \), there are \( \ll \frac{H^2}{Q} \) choices for \( y \). Then, from (6.19), \( a' \) is uniquely determined by \( a \). Consequently, we have

\[
|\chi_2| \ll \Omega(2) |Z| \frac{H^2}{Q}.
\]

6.3. Combining \( \chi_1 \) and \( \chi_2 \). First of all, from the previous subsections, the upper bound of \( |\chi_2| \) dominates the one of \( |\chi_1| \) since \( KQ \ll H^2 \). Therefore, (6.8) becomes

\[
(6.25) \quad \sum_{\theta \in \mathcal{Z}} |S_N(\theta)| \ll \frac{N^{\delta+1}}{\sqrt{KQ}} |Z| \frac{1}{T} \frac{1}{T}, \tag{6.25}
\]

which implies (6.5).

Once we have the universal bound for any subset \( Z \subset P_{Q,K} \), Lemma 6.2 and Lemma 3.12 imply the following theorem.

**Theorem 6.9.** Assume that \( Q < (2^{26} N)^{1/2} \) and \( KQ < (2^{26} N)^{1/2} \). Then for any \( \epsilon > 0 \),

\[
(6.26) \quad \frac{1}{T N'} \sum_{\theta \in P_{Q,K}} |S_N(\theta)|^2 \ll \epsilon \frac{(\Omega_N)^2 N^{2(1-\delta)+2\epsilon+\epsilon}}{KQ}.
\]

That is to say, we have

\[
(6.27) \quad \int_{W_{Q,K}} |S_N(\theta)|^2 d\theta \ll \epsilon \frac{(\Omega_N)^2 N^{2(1-\delta)+2\epsilon+\epsilon}}{KQ}.
\]

Remark 6.10. It is not hard to show that we still have (6.27) for the case \( \bar{C} \leq K < 2\bar{C} \).
7. MINOR ARC ANALYSIS II

In this section, we push the method of previous section down to the level of \( Q \) and \( K \) being of constant size. However, instead of using a “triple” Kloosterman refinement, we use only a double refinement. That is to say, we will leave \( a \) fixed and estimate the sum over \( q \) and \( \ell \).

Specifically, define a set \( P_{Q,K,a} \) as follows.

\[
P_{Q,K,a} = \left\{ \frac{a}{q} + \frac{\ell}{T N'} : \frac{1}{2} Q \leq q < Q, q \geq a, \frac{1}{2} K T \leq \ell < K T \right\}.
\]

Hence the size of \( P_{Q,K,a} \) is \( KQ \). We now bound \( \sum_{\theta \in P_{Q,K,a}} |S_N(\theta)|^2 \) by \( Q \) times \( \sum_{\theta \in P_{Q,K,a}} |S_N(\theta)|^2 \). Again, we are looking for a universal bound over \( \sum_{\theta \in Z} |S_N(\theta)|^2 \) for any subset \( Z \subset P_{Q,K,a} \).

**Remark 7.1.** Here, the double Kloosterman refinement is not in the usual setting since we take summations over \( q \) and \( \ell \) instead.

**Theorem 7.2.** Assume that

\[
KQ \leq N^{2(1-\delta)+3\rho}.
\]

Then for any subset \( Z \subset P_{Q,K,a} \) and any \( \epsilon > 0 \), we have

\[
\sum_{\theta \in Z} |S_N(\theta)| \ll \#\Omega_N \cdot \frac{(KQ^2)^{1-\delta}(K^{3/2}Q^3)^{4\rho+\epsilon}}{\sqrt{KQ^2}} \cdot |Z|^{1/2} \cdot T^{1/2}.
\]

**Remark 7.3.** When \( K \) is at constant level, we have instead

\[
\sum_{\theta \in Z} |S_N(\theta)| \ll \#\Omega_N \cdot \frac{(KQ^3)^{1-\delta}(K^{3/2}Q^3)^{4\rho+\epsilon}}{Q} \cdot |Z|^{1/2}.
\]

**Proof.** Our goal is to decompose the ensemble \( \Omega_N \) as follows.

\[
\Omega_N = \Omega^{(1)} \Omega^{(2)} = \Omega^{(1)} [\Omega^{(3)} \Omega^{(4)} \Omega^{(5)}],
\]

where

\[
\Omega^{(1)} = \Xi_{-j} \Xi_{-j+1} \cdots \Xi_{j_1},
\]

\[
\Omega^{(2)} = \Xi_{j_1+1} \Xi_{j_1+2} \cdots \Xi_{j_2},
\]

\[
\Omega^{(3)} = \Xi_{j_1+1} \Xi_{j_1+2} \cdots \Xi_{j_3},
\]

\[
\Omega^{(4)} = \Xi_{j_2+1} \Xi_{j_2+2} \cdots \Xi_{j_4},
\]

\[
\Omega^{(5)} = \Xi_{j_3+1} \Xi_{j_3+2} \cdots \Xi_{j_5}.
\]

The parameters \( j_1, j_2 \) and \( h \) will be determined later.

First of all, it is easy to verify that

\[
\left( KQ^2 (KQ^2)^{2\rho} \sqrt{K} \right)^{1+2\rho} < K^{3/2} Q^2 (K^6 Q^{12})^\rho.
\]

Thus, by (3.1) and (7.2), we have

\[
(7.5) \quad \left( KQ^2 (KQ^2)^{2\rho} \sqrt{K} \right)^{1+2\rho} < N^{2/3}
\]

which implies that

\[
(7.6) \quad KQ^2 (KQ^2)^{2\rho} \sqrt{K} < N^{1-\rho}.
\]
Hence, by Corollary 3.3, we can find parameters \(-J + 1 \leq j_1, j_2, h \leq J - 1\) such that

\[
KQ^2 \leq Nj_1 \leq (KQ^2)^{1+2\vartheta},
\]

(7.7)

\[
KQ^2 (KQ^2)^{2\vartheta} \sqrt{K} \leq Nj_2 \leq (KQ^2 (KQ^2)^{2\vartheta} \sqrt{K})^{1+2\vartheta},
\]

\[
Q \leq \frac{N}{N_{h-1}} \leq Q^{1+2\vartheta}.
\]

Let us denote \(N_{j_1}\) by \(H_1\), \(N_{j_2}/N_{j_1}\) by \(H_2\), \(N_{h-1}/N_{j_1}\) by \(H_3\), \(N/\Omega_{h-1}\) by \(H_4\), \(N/\Omega_{j_1}\) by \(H_5\), and \(N/\Omega_{j_1}\) by \(H_2\). It is elementary to show that

\[
H_3 = \frac{N_{j_2}}{N_{j_1}} \geq \sqrt{K}.
\]

To decompose \(\Omega_N\) properly, we need to show that \(h \geq j_2 + 2\) and \(j_2 > j_1\).

1. To show that \(h \geq j_2 + 2\), we prove \(j_2 < j < h\) instead. The first inequality follows from (3.22) and (7.5) that

\[
N_1 \geq N^{2/3} \geq \left( KQ^2 (KQ^2)^{2\vartheta} \sqrt{K} \right)^{1+2\vartheta} \geq N_{j_2}.
\]

The second inequality comes from

\[
\frac{N}{N_1} \geq N^{\frac{1-\vartheta}{2}} > Q^{1+2\vartheta} \geq \frac{N}{N_{h-1}}.
\]

2. To show that \(j_1 < j_2\), one can see from (7.7) that the index \(j_1\) we choose satisfies

\[
N_{j_1-1} \leq KQ^2 \leq N_{j_1}.
\]

Hence we have,

\[
KQ^2 (KQ^2)^{2\vartheta} \sqrt{K} > (KQ^2)^{1+2\vartheta} \geq N_{j_1-1} \geq N_{j_1},
\]

where the last inequality comes from the fact that \(N_{j_1-1} \geq N_{j_1}^{1-\vartheta}\). The above inequality then implies \(j_1 < j_2\).

The above arguments show that (7.4) is legitimate. Moreover, since we have \(j_2 < j < h\), the special set \(\Omega\) belongs to \(\Omega^{(3)}\). This plays a crucial role in later estimation.

We now follow the similar argument in Theorem 6.4 and obtain

\[
\sum_{\theta \in \mathbb{Z}} |S_N(\theta)| \ll \sqrt{#\Omega^{(1)}H_1 \sqrt{K}},
\]

where

\[
\chi = \# \left\{ g_2, g_2' \in \Omega^{(2)}, \theta, \theta' \in \mathbb{Z} : \left\| \left( g_2\theta - g_2'\theta' \right) e_2 \right\| \leq \frac{1}{2^{28}H_1} \right\}
\]

(7.10)

Besides the innermost condition in (7.10), we also have

\[
\left\| \left( g_2 - g_2' \right) e_2 \right\| \leq 2 \cdot \frac{32H_2K_T}{T'N'} \leq \frac{K}{10H_1} < \frac{1}{2Q^2}.
\]

Consequently,

\[
\left\| \left( g_2 - g_2' \right) e_2 \right\| \leq \left\| \left( g_2 - g_2' \right) e_2 \right\| + \left\| \left( g_2 - g_2' \right) e_2 \right\| < \frac{1}{Q^2}.
\]

This implies that

\[
\left( g_2 - g_2' \right) e_2 \equiv 0 \pmod{1}
\]

(7.12)
Again, we can conclude that

\[(7.13) \quad q = q', \quad g_2 e_2 \equiv g'_2 e_2 \pmod{q},\]

and

\[(7.14) \quad \left| \frac{g_2 e_2 - g'_2 e_2}{\mathcal{T} N'} \right| = \left| (g_2 \theta - g'_2 \theta) e_2 \right| \leq \frac{1}{2^{28} H_1}.\]

We start by fixing $g'_2$ for which there are $\#\Omega^{(2)}$ choices. Denote $g'_2 e_2$ by $v'_2 = (x'_1, x'_2)$ and $g_2 e_2$ by $v_2 = (x_1, x_2)$. Notice that $v'_2$ is now fixed. Next, we fix $\theta \in \mathbb{Z}$ for which there are $|\mathbb{Z}|$ choices. Hence, (7.13) and (7.14) now read

\[(7.15) \quad v_2 \equiv v'_2 \pmod{q}, \quad \left| \frac{x_1 \ell - x'_1 \ell'}{\mathcal{T} N'} \right|, \left| \frac{x_2 \ell - x'_2 \ell'}{\mathcal{T} N'} \right| \leq \frac{1}{2^{28} H_1}.

We write $g_2 = g_3 g_4 g_5$, where $g_3 \in \Omega^{(3)}$, $g_4 \in \Omega^{(4)}$, and $g_5 \in \Omega^{(5)}$. Also, let $g_3$ be \(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\), and $g_4 g_5 e_2$ be $(y_1, y_2)$. Then we naturally have

\[x_1 = ay_1 + by_2, \quad x_2 = cy_1 + dy_2.\]

This implies that $x_1 / x_2$ and $b / d$ are close:

\[(7.16) \quad \frac{x_1}{x_2} = \frac{ay_1 + by_2}{cy_1 + dy_2} = \frac{b}{d} + \frac{y_1}{(cy_1 + dy_2)d} \Rightarrow \left| \frac{x_1}{x_2} - \frac{b}{d} \right| \leq \frac{1}{d^2}.\]

On the other hand, we have

\[(7.17) \quad \left| \frac{x'_1}{x'_2} - \frac{x_1}{x_2} \right| = \left| \frac{x'_1}{x'_2} - \frac{x_1 \ell}{x_2 \ell} \right| = \left| \frac{x'_2 \ell (x_1 \ell - x'_1 \ell') + x'_1 \ell' (x'_2 \ell' - x_2 \ell)}{x'_2 x'_2 \ell' - x_2 x_2 \ell'} \right| \leq \frac{\mathcal{T} N}{2^{28} H_1} \cdot \frac{4}{H_2 K \mathcal{T}} \ll \frac{1}{K}.\]

Combine (7.16) and (7.17), we get

\[(7.18) \quad \left| b - x'_1 \right| \ll \frac{1}{H_2^2} + \frac{1}{K}.\]

Finally, by the fact that the fraction $\frac{b}{d}$ uniquely determines $g_3$ and each two distinct fractions $\frac{b}{d}$ and $\frac{b'}{d'}$ have difference at least $\frac{1}{d d'} \gg \frac{1}{H_3^2}$, we conclude that there are $\ll \frac{H_3^2}{K}$ choices for $\frac{b}{d}$, and thus for $g_3$. (Here we use the fact that $H_3 \geq \sqrt{K}$.)

Now, we fix the element $g_3$, and fix the next element $g_4$ for which there are $\#\Omega^{(4)}$ choices. We denote $g_3 g_4$ as \(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\), and $g_5 e_2 = z = (z_1, z_2)$. Since $g_3 g_4 \in \text{SL}(2, \mathbb{Z})$, we have the following equations

\[z_1 \equiv d_1 x'_1 - b_1 x'_2 \pmod{q}, \quad z_2 \equiv c_1 x'_1 + a_1 x'_2 \pmod{q}.

Again we have $H_5 \geq Q$ and $\lambda(g_5) \approx H_5$, thus there are $\ll \frac{H_5^2}{Q}$ choices for $g_5$. Finally, from (7.14), there are $\ll \mathcal{T}$ choices for $\ell'$. 

34
Combining all the estimates for \( g_2, g_2', \theta, \theta' \), we get

\[
\sum_{\theta \in \mathbb{Z}} |S_N(\theta)| \ll \#\Omega_N \cdot \frac{(H_1H_3H_5)^{1-\delta} 2^c (\log \log(H_1H_3H_5))^2}{\sqrt{KQ}} \cdot T^{\frac{1}{2}} \cdot |Z|^\frac{1}{2},
\]

(7.19)

\[
\ll \#\Omega_N \cdot \frac{(K^{3/2}Q^3)^{1-\delta} (K^{3/2}Q^3)^{4c + \epsilon}}{\sqrt{KQ^2}} \cdot |Z|^\frac{1}{2} \cdot T^{\frac{1}{2}}
\]

Remark 7.4. Even when \( K \) is at constant level, we still have (7.13). After fixing \( g_2' \), we then directly fix \( g_3 \) and \( g_4 \) so that we do not gain a \( K \) saving from \( g_3 \). The rest argument stays the same. Hence, (7.19) becomes

\[
\sum_{\theta \in \mathbb{Z}} |S_N(\theta)| \ll \#\Omega_N \cdot \frac{(H_1H_3H_5)^{1-\delta} 2^c (\log \log(H_1H_3H_5))^2}{Q} \cdot |Z|^\frac{1}{2}.
\]

Same as the case when \( K \) or \( Q \) is large, we now have a general bound for \( \sum_{\theta \in \mathbb{Z}} |S_N(\theta)| \), then Lemma 6.2 implies the following theorem

**Theorem 7.5.** Assume that

\[
KQ \leq N^{2(1-\delta)+3\delta_0}.
\]

Then for any \( \epsilon > 0 \),

\[
\frac{1}{T^N} \sum_{P(\theta, K)} |S_N(\theta)|^2 \ll \epsilon \frac{(\#\Omega_N)^2 (K^{3/2}Q^3)^{2(1-\delta)} (KQ)^{e}}{N Q}
\]

(7.20)

Hence, we have

\[
\int_{W_{Q,K}} |S_N(\theta)|^2 d\theta \ll \epsilon \frac{(\#\Omega_N)^2 (K^{3/2}Q^3)^{2(1-\delta)} (KQ)^{e}}{N Q}
\]

(7.21)

Remark 7.6. Again, (7.21) remains the same when \( K \) is at constant level.

8. **Proof of Theorem 1.6**

As we have the estimate for major arcs, we combine the results in previous two sections to estimate the minor arcs.

**Theorem 8.1.** Assume

\[
\delta > \delta_0 = \frac{5}{6}.
\]

Then for some \( c > 0 \),

\[
\sum_{n \in \mathbb{Z}} |E_N(n)|^2 \ll \left( \frac{|\Omega_N|^2}{N} Q^{-c} \right).
\]

(8.2)

**Proof.** By Parseval, we have

\[
\sum_{n \in \mathbb{Z}} |E_N(n)|^2 = \int_0^1 |1 - \Psi_{Q,N}(\theta)|^2 |S_N(\theta)|^2 d\theta = \int_{\mathbb{M}_Q} + \int_m,
\]

where we broke the integral into the major arcs \( \mathbb{M}_Q \) and the complementary minor arcs \( m = [0, 1] \setminus \mathbb{M}_Q \).
On the major arcs, note from (2.15) that $1 - \psi(x) = |x|$ on $[-1, 1]$. Then using (8.2) and dyadically decomposing $K < Q$ gives

$$
\int_{\mathfrak{M}_Q} \ll \sum_{q < Q} \sum_{(a,q) = 1} \int_{|\beta| < Q/N} \left| N \theta \right|^2 \left| S_{N}(\theta) \right|^2 d\theta 
\ll \sum_{Q < Q} \sum_{i = 0}^{\log Q} 2^{-2i} I_{Q,K}
$$

(8.4)

$$
\ll \sum_{Q < Q} \sum_{i = 0}^{\log Q} 2^{-2i} \frac{\left(\#\Omega_N\right)^2}{N} \frac{1}{K^{c_1} Q^{c_2}}
\ll \sum_{Q < Q} \sum_{i = 0}^{\log Q} \frac{\left(\#\Omega_N\right)^2}{Q^{c_2}} \frac{1}{N} \frac{1}{K^{c_1}} \ll \frac{\left(\#\Omega_N\right)^2}{Q^{c_2}}.
$$

where for each $i$, we have $K = Q/2^i$,

$$
I_{Q,K} = \int_{W_{Q,K}} \left| S_{N}(\theta) \right|^2 d\theta,
$$

and also $0 < c_1 < 1 - 3(1 - \delta)$ and $0 < c_2 < 1 - 6(1 - \delta)$. Note that since $0 < c_1 < 1$, the term $\sum_{i = 0}^{\log Q} 2^{-2i} \frac{\left(\#\Omega_N\right)^2}{N} \frac{1}{K^{c_1} Q^{c_2}}$ contributes at most $\frac{\left(\#\Omega_N\right)^2}{NQ^{c_1}}$.

On the other hand, we decompose the minor arcs $m$ into dyadic regions

$$
\int_{m} \ll \sum_{Q < Q^{1/2}} \sum_{K < Q^{1/2}} I_{Q,K},
$$

where at least one of $Q$ or $K$ exceeds $Q$, and $I_{Q,K}$ is defined above.

Write $Q = N^\alpha$, $K = N^\kappa$, with the parameters $(\alpha, \kappa)$ ranging in

(8.5) $0 \leq \alpha < 1/2$ and $0 \leq \kappa < 1/2 - \alpha$.

We break the summation into the following two ranges:

$$
R_1 : = \{ (\alpha, \kappa) : \alpha + \kappa > 2(1 - \delta) + 3Q \}
R_2 : = \{ (\alpha, \kappa) : \alpha + \kappa \leq 2(1 - \delta) + 3Q \}.
$$

Clearly, $R_1$ and $R_2$ cover the whole region (8.5). Moreover, from (6.27) and (7.21), we have the following bound in both regions.

(8.6) $\int_{W_{Q,K}} \left| S_{N}(\theta) \right|^2 d\theta \ll \frac{\left(\#\Omega_N\right)^2}{N} \frac{1}{K^{c_1} Q^{c_2}}.$

Thus, dyadically summing over $Q$ and $K$, we obtain

(8.7) $\int_{m} \ll \frac{\left(\#\Omega_N\right)^2}{N} \frac{1}{Q^{c_2}}$.

Finally, combining the above result with (8.4) completes the proof of (8.2).

We are now in the position to derive Theorem 1.6.

Proof of Theorem 1.6.
Let \( g(N) \) denote the set of \( n \simeq N \) which have a small representation number \( R_n(n) \),
\[
\mathcal{G}(N) := \left\{ \frac{1}{40} N \leq n \leq \frac{1}{25} N : R_N(n) < \frac{1}{2} \mathcal{M}_N(n) \right\}.
\]
(8.8)
Therefore, the error function must have large value at those fibers by Theorem 4.4.
\[
|E_N(n)| = |R_N(n) - \mathcal{M}_N(n)| \gg \frac{1}{\log \log N} \frac{\# \Omega_N}{N}.
\]
(8.9)
With Theorem 8.1, we have
\[
\# \mathcal{G}(N) \ll \sum_{\frac{1}{40} N \leq n \leq \frac{1}{25} N} \frac{1}{\log \log N} \sum_n |E_N(n)|^2
\ll \frac{N^2 (\log \log N)^2}{(\# \Omega_N)^2} \sum_n |E_N(n)|^2
\ll \frac{N^2 (\log \log N)^2 (\# \Omega_N)^2}{(\# \Omega_N)^2} \frac{1}{N} \frac{\# \Omega_N}{Q^c}
\ll N^{1-c/\log \log N},
\]
which implies (1.6).

Moreover, for \( n \in \left[ \frac{1}{40} N, \frac{1}{25} N \right] \setminus \mathcal{G}(N) \), the representation number \( R_N(n) \) is large. That is,
\[
|R_N(n)| \geq \frac{1}{2} \mathcal{M}_N(n) \gg \frac{1}{\log \log N} \frac{\# \Omega_N}{N}.
\]
Finally, by Lemma 3.12, we conclude that
\[
|R_N(n)| \gg N^{2\delta - 1 - r},
\]
as \( N \to \infty \).
For the sake of completeness, we include two important appendices at the end of Bourgain and Kontrovich’s paper [BK13]. Combining these two arguments, we are able to construct a special set with nice distribution of eigenvalues and congruence property.

### A.1. Random Extraction Argument.

**Lemma A.1.** Let $\mu = \mu_S$ be the probability measure of a finite set $S \subset SL(2, \mathbb{Z})$. That is,

\begin{equation}
\mu(\gamma) = \frac{1}{|S|} \sum_{s \in S} I_{s - \gamma},
\end{equation}

and fix $\eta > 0$. Let $q_0 < Q$ be a fixed modulus, let $\omega_0 \in SL_2(q_0)$ be a fixed element, and let $D = D_{q_0} \subset [1, Q]$ be the set of moduli $q < Q$ with $q_0 | q$. Assume that for all $q \in D$ and all $\omega \in SL_2(q)$ with $\omega \equiv \omega_0$ (mod $q_0$), the projection

\begin{equation}
\pi_q[\mu](\omega) = \sum_{\gamma \equiv \omega \pmod{q}} \mu(\gamma)
\end{equation}

is near the uniform measure on $SL_2(q)$ conditioned on being $\equiv \omega_0$ (mod $q_0$).

\begin{equation}
\left\| \pi_q[\mu] - \frac{|SL_2(q_0)|}{|SL_2(q)|} \right\|_{L^\infty(\equiv \omega_0 \pmod{q_0})} < \eta.
\end{equation}

That is to say, we have

\begin{equation}
\max_{q \in D} \max_{\omega \in SL_2(q) \pmod{q_0}} \left| \pi_q[\mu] - \frac{|SL_2(q_0)|}{|SL_2(q)|} \right| < \eta.
\end{equation}

Then for any

\begin{equation}
\eta^{-2} \log Q \ll T \ll \eta^{1/2} S^{1/2}.
\end{equation}

there exists $T$ distincts points $\gamma_1, \ldots, \gamma_T \in S = \text{supp} \mu$ that the probability measure $v = v_{T, \gamma_1, \ldots, \gamma_T}$ defined by

\begin{equation}
v = \frac{1}{T} (I_{\gamma_1} + \cdots + I_{\gamma_T})
\end{equation}

has the same property. That is to say, we have

\begin{equation}
\max_{q \in D} \max_{\omega \in SL_2(q) \pmod{q_0}} \left| \pi_q[\mu] - \frac{|SL_2(q_0)|}{|SL_2(q)|} \right| \ll \eta,
\end{equation}

where the implied constant is absolute.

**Proof.** We define $S^T$ to be the set of all $T$-tuple of elements (not neccessary distinct) in $S$. That is to say,

\begin{equation}
S^T = \{ (\gamma_1, \gamma_2, \ldots, \gamma_T) : \gamma_i \in S \}.
\end{equation}

For any element $s = (s_1, \ldots, s_T) \in S^T$, we define $D_s$ as

\begin{equation}
D_s = \max_{q \in D} \max_{\omega \in SL_2(q) \pmod{q_0}} \left| \pi_q[\mu_s] - \frac{|SL_2(q_0)|}{|SL_2(q)|} \right|,
\end{equation}

where as in (A.6), we have

\begin{equation}
v_s = \frac{1}{T} (I_{s_1} + \cdots + I_{s_T}).
\end{equation}
Now, we uniformly randomly choose an element $s$ from $S^T$. Our goal is to show that

$$\mathbb{E}(D_s) \ll \eta.$$  

On the other hand, by definition of expectation, we have

$$\mathbb{E}(D_s) = \mathbb{E}
\left(
\max_{q \in D} \max_{\omega \equiv \omega_0 \pmod{q_0}} \left| \pi_q[v_s] - \frac{|\text{SL}_2(q_0)|}{|\text{SL}_2(q)|} \right|
\right)
$$

(A.11)

$$= \sum_{s \in S^T} \max_{q \in D} \max_{\omega \equiv \omega_0 \pmod{q_0}} \left| \pi_q[v_s] - \frac{|\text{SL}_2(q_0)|}{|\text{SL}_2(q)|} \right| \mu^{(T)}(s),$$

where $\mu^{(T)}(s) = \frac{1}{|S|^T}$ is the probability measure on $S^T$.

To employ the given uniform distribution property (A.4), we notice the following elementary observation.

$$\pi_q[\mu](\omega) = \sum_{\gamma \equiv \omega \pmod{q}} \frac{1}{|S|} \sum_{s \in S} 1_{s = \gamma}$$

(A.12)

$$\pi_q[\mu](\omega) = \frac{1}{|S|^T} \sum_{\gamma \equiv \omega \pmod{q}} |S|^{T-1} \sum_{s \in S} 1_{s = \gamma}$$

$$= \mu^{(T)}(s') \sum_{\gamma \equiv \omega \pmod{q}} \sum_{s' \in S^T} v_{s'}(\gamma)$$

$$= \mathbb{E}\left( \pi_q[v_{s'}](\omega) \right),$$

where $s'$ is also chosen uniformly and randomly from $S^T$. We remind ourselves that the expectation $\mathbb{E}$ here is over the probability space $S^T$. That is to say, we have $q$ and $\omega$ fixed in (A.12). From (A.4) and (A.12), we get

$$\max_{q \in D} \max_{\omega \equiv \omega_0 \pmod{q_0}} \left| \mathbb{E}\left( \pi_q[v_s](\omega) \right) - \frac{|\text{SL}_2(q_0)|}{|\text{SL}_2(q)|} \right| < \eta.$$  

(A.13)

Now, we use triangle inequality as follows.

$$\max_{q \in D} \max_{\omega \equiv \omega_0 \pmod{q_0}} \left| \pi_q[v_s] - \frac{|\text{SL}_2(q_0)|}{|\text{SL}_2(q)|} \right|$$

(A.14)

$$\leq \max_{q \in D} \max_{\omega \equiv \omega_0 \pmod{q_0}} \left| \pi_q[v_s] - \mathbb{E}\left( \pi_q[v_{s'}](\omega) \right) \right| + \eta$$
Consequently, (A.11) becomes

\[
\mathbb{E}_s(D_s) < \eta + \mathbb{E}_s \left( \max_{q \in D} \max_{\omega \in \text{SL}_2(q) \bmod q_0} \left| \pi_q[v_s] - \mathbb{E}_{\pi'_q} \left( \pi_q[v_{s'}](\omega) \right) \right| \right)
\]

\[
\leq \eta + \mathbb{E}_s \left( \max_{q \in D} \max_{\omega \in \text{SL}_2(q) \bmod q_0} \mathbb{E}_{\pi'_q} \left( \left| \pi_q[v_s] - \pi_q[v_{s'}] \right| \right) \right)
\]

\[
\leq \eta + \mathbb{E}_s \left( \mathbb{E}_{\pi'_q} \left( \max_{q \in D} \max_{\omega \in \text{SL}_2(q) \bmod q_0} \left| \pi_q[v_s] - \pi_q[v_{s'}] \right| \right) \right)
\]

\[
\leq \eta + \mathbb{E}_s \left( \mathbb{E}_{\pi'_q} \left( \max_{q \in D} \max_{\omega \in \text{SL}_2(q) \bmod q_0} \left| \pi_q[v_s] - \pi_q[v_{s'}] \right| \right) \right.
\]

\[
\left. \leq \eta + \mathbb{E}_s \left( \mathbb{E}_{\pi'_q} \left( \max_{q \in D} \max_{\omega \in \text{SL}_2(q) \bmod q_0} \left| \pi_q[v_s] - \pi_q[v_{s'}] \right| \right) \right) \right)
\]

(A.15)

where \( \mathbb{E}_s \) and \( \mathbb{E}_{s'} \) represent the expectation over random variables \( s \) and \( s' \) respectively. For each \( j \), we denote the random variable \( 1_{\{s_j \equiv \omega(q)\}} - 1_{\{s'_j \equiv \omega(q)\}} \) by \( f_{q,\omega}(s_j, s'_j) \). Clearly, for any fixed \( q \) and \( \omega \), \( f_{q,\omega}(s_j, s'_j) \) are i.i.d. symmetric random variables with mean 0 and bounded by 1.

Now, replacing the \( L^\infty \)-norm by \( L^p \)-norm (we determine \( p \) later) of \( \frac{1}{T} \sum_{j=1}^{T} 1_{\{s_j \equiv \omega(q)\}} - 1_{\{s'_j \equiv \omega(q)\}} \), we get

(A.16)

\[
\mathbb{E}_s(D_s) \leq \eta + \frac{1}{T} \mathbb{E}_s \mathbb{E}_{\pi'_q} \left( \left\| \sum_{j=1}^{T} f_{q,\omega}(s_j, s'_j) \right\|_{L^p} \right),
\]

where

\[
\left\| \sum_{j=1}^{T} f_{q,\omega}(s_j, s'_j) \right\|_{L^p} = \left( \sum_{q \in D} \sum_{\omega \in \text{SL}_2(q) \bmod q_0} \left| \sum_{j=1}^{T} f_{q,\omega}(s_j, s'_j) \right|^p \right)^{\frac{1}{p}}.
\]
By the concavity of $x^{1/p}$, the symmetric property of $f_{q,\omega}(s, s')$, and Kahane contraction principle with Khintchine’s inequality [Haa81], (A.16) becomes

\[
\mathbb{E}_s(D_s) \leq \eta + \frac{1}{T} \mathbb{E}_s \mathbb{E}_{s'} \left( \left| \sum_{q \in \mathbb{D}} \sum_{\omega \in \text{SL}_2(q)} \left| \frac{T}{1} \sum_{j=1}^T f_{q,\omega}(s_j, s'_j) \right|^p \right)^{\frac{1}{p}} \right)
\leq \eta + \frac{1}{T} \left( \mathbb{E}_s \mathbb{E}_{s'} \left( \left| \sum_{j=1}^T f_{q,\omega}(s_j, s'_j) \right|^p \right)^{\frac{1}{p}} \right)
\leq \eta + \frac{1}{T} \sum_{q \in \mathbb{D}} \sum_{\omega \in \text{SL}_2(q)} \mathbb{E}_s \mathbb{E}_{s'} \left( \left| \sum_{j=1}^T f_{q,\omega}(s_j, s'_j) \right|^p \right)^{\frac{1}{p}}
= \eta + \frac{1}{T} \left( \mathbb{E}_s \mathbb{E}_{s'} \left( \left| \sum_{j=1}^T \epsilon_j f_{q,\omega}(s_j, s'_j) \right|^p \right)^{\frac{1}{p}} \right)
= \eta + \frac{1}{T} \left( Q^4 p^\varepsilon T^\frac{p}{2} \right)^{\frac{1}{p}} \ll \eta + Q^\frac{1}{2} T^{-\frac{1}{2}}.
\]

To obtain the best bound for $\mathbb{E}_s(D_s)$, we take $p = \log Q$. Then the above inequality becomes

(A.17) \quad $\mathbb{E}_s(D_s) \ll (\log Q)^{\frac{1}{2}} T^{-\frac{1}{2}} + \eta.$

That is to say, when $T \gg \eta^{-2} \log Q$, we have

(A.18) \quad $\mathbb{E}_s(D_s) \ll \eta.$

Nonetheless, we need to exclude the contribution of $s$, with non-distinct elements, in $\mathbb{E}_s(D_s)$. We call such $s$ with non-distinct elements bad tuple. Notice crudely, the number of bad tuples is at most $\sum_{D \subseteq \mathbb{N}} |D|^{T-1}$. Consequently, under the assumption that $T \leq \eta^{1/2} S^{1/2}$, the contribution of $D_s$, with bad tuple, in $\mathbb{E}_s(D_s)$ is at most $\frac{1}{T} \cdot \frac{T}{\lambda} \cdot |S|^T - 1 \leq \frac{T^2}{|S|} \leq \eta$. Together with (A.18), we conclude Lemma A.1.

\[\square\]

A.2. Construction of $N$ using Theorem 2.3.

To utilize Theorem 2.3, we need a similar statement but about eigenvalue instead of norm in (2.13) and (2.13). We use similar method in (4.10) to achieve this goal. Assume both expanding eigenvectors $\gamma$ and $\gamma_0$ are within $1/H$ about $v$, and their norms are large enough (at least $> H$). One can see that for $i, j \in \{1, 2\}$

\[
\langle \gamma \gamma_0 e_i, e_j \rangle = \mathcal{A}(\gamma) \mathcal{A}(\gamma_0) \langle e_i, v_-(\gamma_0)^2 \rangle \cdot \langle e_j, v \rangle \left( 1 + O \left( \frac{1}{H} + \frac{1}{\|\gamma\|^2} + \frac{1}{\|\gamma_0\|^2} \right) \right)
\]

(A.19) \quad $\mathcal{A}(\gamma_0) \left( \frac{e_i, v_-(\gamma_0)^2}{\langle v, v_-(\gamma_0)^2 \rangle} \cdot \langle e_j, v \rangle \right) \left( 1 + O \left( \frac{1}{H} \right) \right),$
and
\[ \langle \gamma_0 e_i, e_j \rangle = \lambda(\gamma_0) \frac{\langle e_i, v_{\gamma_0}(\gamma_0)^{\frac{1}{2}} \rangle \cdot \langle e_j, v_{\gamma_0}(\gamma_0)^{\frac{1}{2}} \rangle}{\langle v, v_{\gamma_0}(\gamma_0)^{\frac{1}{2}} \rangle} \left( 1 + O\left( \frac{1}{H} \right) \right). \]  

Consequently, combining (A.19) and (A.20), we get
\[ \frac{\|\gamma_0\|}{\|\gamma_0\|} = \lambda(\gamma) \left( 1 + O\left( \frac{1}{H} \right) \right). \]

This allows us to derive the following corollary.

**Corollary A.2.** With \( \mathcal{B} \) and \( c \) as given in Theorem 2.3. Given two parameters \( H, H_1 = o(T) \), for any modulus \( q \) with \( \mathcal{B} \equiv 1 \), we have
\[ \# \left\{ \gamma \in \Gamma : \gamma \equiv \omega \quad \text{(mod } q), \ |v_+(\gamma) - v| < \frac{1}{H}, \text{ and } \lambda(\gamma) = T \left( 1 + O\left( \frac{1}{H_1} \right) \right) \right\} \]
\[ \leq C(\gamma_0) \cdot \frac{T^{2\delta}}{H_1} \cdot \frac{\mu(T)}{|\text{SL}_2(q)|} \cdot \left( 1 + O\left( \frac{1}{H_1} \right) \right) + O\left( T^{2\delta - c/\log \log T} \right). \]

On the other hand, for any \( q \) with \( \mathcal{B} \mid q \), we have
\[ \frac{|\text{SL}_2(\mathcal{B})|}{|\text{SL}_2(q)|} \cdot \# \left\{ \gamma \in \Gamma : \gamma \equiv \omega \quad \text{(mod } q), \ |v_+(\gamma) - v| < \frac{1}{H}, \text{ and } \lambda(\gamma) = T \left( 1 + O\left( \frac{1}{H_1} \right) \right) \right\} \]
\[ \leq \frac{|\text{SL}_2(\mathcal{B})|}{|\text{SL}_2(q)|} \cdot \left( 1 + O\left( \frac{1}{H_1} \right) \right) + O\left( T^{2\delta - c/\log \log T} \right). \]

**Proof of Proposition 3.4:**
Assuming the parameters \( b \) in (3.25), \( \mathcal{B} \) and \( c \) in Theorem 2.3, we recall the parameter \( Q \) to be
\[ Q := N^{a_0/\log \log N}, \]
where \( R = |\text{SL}_2(\mathcal{B})| \) and
\[ a_0 = \frac{bc}{40R}. \]

Also, note that elements in the special set \( \mathcal{N} \) are roughly of size \( B \), where as in (3.26)
\[ B = N^b. \]

We now set the parameters \( H \) and \( H_1 \) in Corollary A.2 to be
\[ H = Q^{12}, \text{ and } H_1 = Q^6. \]

For an alphabet \( \mathcal{A} \) containing 1 and 2, the reduction of \( \Gamma \) (mod \( \mathcal{B} \)) is full. That is to say, for each \( \gamma_i \in \text{SL}_2(\mathcal{B}) \), we can find an element \( g_i \in \Gamma \) such that
\[ g_i \equiv \gamma_i \quad \text{(mod } \mathcal{B}). \]

(We have \( g_i \) depends on \( \mathcal{B} \), thus only on \( \mathcal{A} \).)

Since \( B = N^b \) and \( b \) is a constant, for \( N \) large enough, we can find some element \( g_0 \) such that
\[ \frac{1}{2} B^{1/200} \leq \lambda(g_0) < B^{1/200}, \text{ and } |v_+(g_0) - v| < Q^{-6}. \]

Thus the products \( g_0 g_i \), with \( i = 1, 2, \ldots, R \), still form a complete residue system mod \( \mathcal{B} \). Moreover, by (2.6), we have control on the expanding vector \( v_+(g_0 g_i) \)
\[ |v_+(g_0 g_i) - v| \ll O(Q^{-6}). \]
where we used the fact that \( Q = o(B) \). The expanding eigenvalues \( \lambda(g_0 \gamma_i) \) are also controlled as follows.

\[
\lambda(g_0 \gamma_i) \asymp B^{1/200}.
\]

Now, for each \( u \in \mathcal{U} \), \( \frac{1}{400} B \leq u < B \), and each \( i = 1, 2, \ldots, R \), we choose a parameter \( T_{u,i} \) such that

\[
T_{u,i} \lambda(g_0 \gamma_i) = u.
\]

One can see from (A.27) that no matter what choice of \( u \) and \( i \), we always have \( T_{u,i} \asymp B^{199/(200R)} = N^{1/200R} \). Then for each \( u \) and \( i \), by (2.13) with \( q = 1 \), we have

\[
\#M_{u,i} := \# \left\{ \gamma \in \Gamma : |v_+ - v| < \frac{1}{H}, |\lambda(\gamma) - T_{u,i}| < \frac{T_{u,i}}{HH_1} \right\} \gg \frac{T_{u,i}^{2\delta}}{HH_1} + O \left( T_{u,i}^{2\delta - \epsilon} \log \log T_{u,i} \right)
\]

(A.29)

By \( T_{u,i} \asymp N^{1/200} \), we have

\[
T_{u,i}^{1/\log \log T_{u,i}} \gg N^{199/(200R)} \gg Q^{18}.
\]

Hence, \( Q^{18} = o \left( T_{u,i}^{1/\log \log T_{u,i}} \right) \) and the major term in (A.29) dominates the error term.

Moreover, since we have \( \#M_{u,i} \), by pigeonhole principle, there exists some \( \gamma_0 \in M_{u,i} \) such that the set

\[
\#M'_{u,i} := \# \{ \gamma \in M_{u,i} : \gamma \equiv \gamma_0 \ (\text{mod } \mathfrak{B}) \}
\]

(A.30)

satisfies

\[
\#M'_{u,i} \geq \#M_{u,i} \gg \frac{T_{u,i}^{2\delta}}{Q^{18}} \gg N^c.
\]

The last inequality is trye since \( \mathfrak{B} \) only depends on \( \mathcal{A} \), and \( c \) can be any constant less than \( 199/200R \).

Now, for each \( u \) and \( i \), let us consider sets

\[
\tilde{M}_{u,i} := \gamma_0^{R - 1} \cdot g_0 \cdot \mathcal{G}_i \subset \Gamma.
\]

(A.31)

Hence, by (2.5) and (2.6), for any \( \gamma \in \tilde{M}_{u,i} \), we have

\[
|v_+(\gamma) - v| \leq Q^{-12}, \quad \text{and} \quad \lambda(\gamma) = u \left( 1 + O \left( Q^{-6} \right) \right)
\]

which we can derive \( |\lambda(\gamma) - u| < B/Q^4 \) by sacrifising one \( Q \) in \( O \left( Q^{-6} \right) \) in (A.32).

Also, for all \( q < Q \) with \( \mathfrak{B} | q \), and all \( \omega \in SL_2(q) \) with \( \omega \equiv g_0 \gamma_i \ (\text{mod } \mathfrak{B}) \), we have from Corollary A.2, (A.30), and (A.31) that

\[
\# \{ \gamma \in \tilde{M}_{u,i} : \gamma \equiv \omega \ (\text{mod } q) \} = \frac{|SL_2(\mathfrak{B})|}{|SL_2(q)|} \cdot \#\tilde{M}_{u,i} \cdot \left( 1 + O \left( \frac{1}{Q^3} \right) \right) + O \left( \frac{T_{u,i}^{2\delta}}{Q^{18}} \right)
\]

(A.32)

\[
= \frac{|SL_2(\mathfrak{B})|}{|SL_2(q)|} \cdot \#\tilde{M}_{u,i} \cdot \left( 1 + O \left( \frac{1}{Q^3} \right) \right),
\]

where \( O \left( \frac{T_{u,i}^{2\delta}}{Q^{18}} \right) \) is absorbed into \( O \left( \frac{1}{Q^6 |SL_2(q)|} \right) \#\tilde{M}_{u,i} \). Note that (A.33) is also equivalent to a statement of uniform distribution.

\[
\frac{\# \{ \gamma \in \tilde{M}_{u,i} : \gamma \equiv \omega \ (\text{mod } q) \}}{\#\tilde{M}_{u,i}} - \frac{|SL_2(\mathfrak{B})|}{|SL_2(q)|} \ll \frac{1}{Q^3},
\]

(A.34)

where this is true for any \( u \) and \( i \).
Hence, we can utilize the random extraction argument Lemma A.1 with $q_0 = \mathfrak{B}$ and $\eta = 1/Q^5$. That is to say, for every fixed $u$, there exists some large enough constant $c'_u < \frac{5}{2}$ such that for any $i = 1, \ldots, R$, we can find a subset $\mathcal{S}_{u,i} \subset \mathcal{M}_{u,i}$ for which
\[
\# \mathcal{S}_{u,i} = N^{c'_u},
\]
and
\[
(A.35) \quad \# \{ g \in \mathcal{S}_{u,i} : g \equiv \omega \pmod{q} \} = \frac{|\text{SL}_2(\mathfrak{B})|}{|\text{SL}_2(q)|} \cdot \# \mathcal{S}_{u,i} \cdot \left( 1 + O\left( \frac{1}{Q^5} \right) \right),
\]
Take the union of all $\mathcal{S}_{u,i}$, we obtain
\[
\tilde{\mathcal{S}}_u = \bigcup_i \mathcal{S}_{u,i}.
\]
Since for every $\mathcal{S}_{u,i}$, we have $\# \mathcal{S}_{u,i} = \# \tilde{\mathcal{S}}_u/|\text{SL}_2(\mathfrak{B})|$, Equation (A.35) implies that for any $q < Q$ with $\mathfrak{B} | q$, and any $\omega \in \text{SL}_2(q)$,
\[
(A.36) \quad \# \{ g \in \tilde{\mathcal{S}}_u : g \equiv \omega \pmod{q} \} = \frac{\# \tilde{\mathcal{S}}_u}{|\text{SL}_2(q)|} \cdot \left( 1 + O\left( \frac{1}{Q^5} \right) \right),
\]
Furthermore, observe that
\[
\# \{ g \in \tilde{\mathcal{S}}_u : g \equiv \omega \pmod{q} \} = \sum_{\omega' \in \text{SL}_2(q')} \# \{ g \in \tilde{\mathcal{S}}_u : g \equiv \omega' \pmod{q} \},
\]
where $q' = [q, \mathfrak{B}]$. One can thus remedy the condition $\mathfrak{B} | q$ while preserving (A.36).

Again, we use Lemma A.1 with with $q_0 = 1$ and $\eta = 1/Q^5$ for the set $\tilde{\mathcal{S}}_u$. Consequently, there exists some constant $c' < \frac{c'}{2}$ such that for each $u$, there exists a subset $\mathcal{S}_u \subset \tilde{\mathcal{S}}_u$ where
\[
\# \mathcal{S}_u = N^{c'},
\]
and (A.36) holds with $\tilde{\mathcal{S}}_u$ replaced by $\mathcal{S}_u$. Take the union
\[
\mathcal{S} = \bigcup_u \mathcal{S}_u.
\]
One can now easily conclude (3.34) from (A.36), and hence construct the special set $\mathcal{S}$.

References

[BGS11] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Generalization of selberg’s 3/16 theorem and affine sieve. Acta Mathematica, 207(2):255–290, 2011. 6, 10

[BK13] Jean Bourgain and Alex Kontorovich. On zaremba’s conjecture. Annals Math, 2013. 1, 2, 3, 5, 6, 8, 10, 11, 12, 15, 18, 21, 23, 38

[FK13] D.A. Frolenkov and I.D. Kan. A reinforcement of the bourgain-kontorovich’s theorem by elementary methods ii, 2013. 1, 2, 3, 26, 27

[Haa81] Uffe Haagerup. The best constants in the khintchine inequality. Studia Mathematica, 70(3):231–283, 1981. 41

[Hen92] Doug Hensley. Continued fraction cantor sets, hausdorff dimension, and functional analysis. Journal of Number Theory, 40(3):336 – 358, 1992. 2

[Jen04] Oliver Jenkinson. On the density of hausdorff dimensions of bounded type continued fraction sets: The texan conjecture. Stochastics and Dynamics, 04(01):63–76, 2004. 3

[Kon02] S.V. Konyagin. Estimates for trigonometric sums over subgroups and for Gauss sums. In IV International conference “Modern problems of number theory and its applications”. Current Problems, Part III. Dedicated to the 180th anniversary of the birth of P. L. Chebyshev and the 110th anniversary of the birth of I. M. Vinogradov. Proceedings of the conference held in Tula, Russia, September 10–15, 2001., pages 86–114. Moscow: Moskovskij Gosudarstvennyj Universitet im. M. V. Lomonosova, Mehaniko-Matematicheskij Fakul'tet, 2002. 26

[Kon13] Alex Kontorovich. From apollonius to zaremba: Local-global phenomena in thin orbits. Bull. Amer. Math. Soc. (N.S.), 50(2):187–228, 2013. 1

[Kor92] N. M. Korobov. Exponential Sums and their Applications. Kluwer Academic, Dordrecht, Netherlands, 1992. 26
[Lal89] Steven P. Lalley. Renewal theorems in symbolic dynamics, with applications to geodesic flows, noneuclidean tessellations and their fractal limits. *Acta Mathematica*, 163(1):1–55, 1989. 6

[Nie78] Harald Niederreiter. Quasi Monte-Carlo methods and pseudo-random numbers. *Bull. Amer. Math. Soc.*, 84(6):957–1041, 1978. 1

[Rob82] G. Robin. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl.*, 9(63):187–213, 1982. 24

[Zar72] S. K. Zaremba. La méthode des "bons treillis" pour le calcul des intégrales multiples. (French) Applications of number theory to numerical analysis (Proc. Sympos., Univ. Montreal, Montreal, Que., 1971). Academic Press, New York, 1972. 2