Dynamics of continued fractions and distribution of modular inverses (in progress)

Hae-Sang Sun (UNIST)
Joint with Jungwon Lee

2021 Dec. 10,

PANT-Kyoto 2021 (RIMS, Online)

Contents

A classical problem

Conjecture (folklore)

Let $\varepsilon > 0$. For a prime $p \gg 1$ and any integer a, there exist integers x, y such that $|x|, |y| < p^{\frac{1}{2}+\varepsilon}$ and $xy \equiv a \pmod{p}$.

- It is known (Garaev for prime p, Khan-Shparlinski for composite p) that such x, y exist with $|x|, |y| \ll p^{\frac{3}{4}}$.
- The results are based mainly on the Weil bound of Kloosterman sums.
- It is an open problem to improve the exponent $3/4$.

A classical problem : Special Case

- Let $(n, m) = 1$ and $\overline{m}$ the modular inverse of m modulo n.
- For an integer $n \geq 1$ and a real number $0 < x < n$, set

$$R(n, x) := \#\{1 \leq m \leq n \,|\, (m, n) = 1,\ 1 \leq \overline{m} \leq x\}.$$

Conjecture (folklore)

For a prime p, the number $R(p, p^{1/2+\epsilon}) > 0$ for any $\epsilon > 0$.

- It is well-known that

$$R(p, p^{3/4+\epsilon}) \gg p^{1/2+\epsilon}.$$

- It is an open problem to improve the exponent $3/4$.

Main result

For $0 < \beta < 1$, we want to study an average sum of the form

$$\sum_{Q<n<M} R(n, n^{\beta}).$$

Theorem

There is a β such that

$$\sum_{M(1-M^{-\epsilon})<n<M} R(n, n^{\beta+\epsilon}) \gg M^{1+\beta}$$

- Hence, we can say on average that

$$\text{``}R(n, n^{\beta+\epsilon}) \gg n^{\beta+\epsilon}\text{''}.$$

Research in progress

Question

How much is β close to $\frac{1}{2}$?

- We introduce a dynamical approach to study the problem.
- Investigate spectral properties of generalized Perron-Frobenius transfer operator $\mathcal{L}_s$.
- The exponent β is related to the spectral gap and eigenvalue of $\mathcal{L}_s$.

Reformulation of problem

- Set $\Sigma_n := \left\{ \frac{m}{n} \,\middle|\, 1 \leq m < n, (m,n) = 1 \right\}$.
- For $r = \frac{m}{n} \in \Sigma_n$, set

$$r^* = \frac{\overline{m}}{n} \in \Sigma_n.$$

For $n \leq M$,

$$R(n, n^\beta) \geq R(n, \frac{n}{M^{1-\beta}}) = \sum_{r \in \Sigma_n} \mathbb{I}_{(0, \frac{1}{M^{1-\beta}})}(r^*).$$

Hence, we have

$$\sum_{Q<n<M} R(n, n^\beta) \geq \sum_{Q<n<M} \sum_{r \in \Sigma_n} \mathbb{I}_{(0, \frac{1}{M^{1-\beta}})}(r^*).$$

Smooth approximation of interval

Let Ψ_M be an inner smooth approximation of $\mathbb{I}_{(0,\frac{1}{M^{1-\beta}})}$ with

- $\Psi_M \leq \mathbb{I}_{(0,\frac{1}{M^{1-\beta}})}$,
- $\|\Psi_M\|_{L^1} \asymp \frac{1}{M^{1-\beta}}$, and
- $\|\Psi_M'\|_\infty \ll M^{1-\beta}$.

Generating functions

Then,

$$\sum_{Q<n<M} R(n, n^{\beta}) \geq \sum_{Q<n<M} \sum_{r\in\Sigma_n} \Psi_M(r^*).$$

- For a function Ψ on the interval, consider a Dirichlet series

$$L_{\Psi}(s) := \sum_{n\geq 1} \frac{\sum_{r\in\Sigma_n} \Psi(r^*)}{n^s}$$

- Need to study the behavior of this generating function.
- Apply Tauberian argument.

‘

Contents

Truncated Perron's Formula

- Let $F(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$.
- σ_a: the abscissa of absolute convergence of $F(s)$.

Theorem

For all $D > \sigma_a$, one has

$$\sum_{n\leq M} a_n = \frac{1}{2\pi i}\int_{D-iT}^{D+iT} F(s)\frac{M^s}{s}ds + O\left(\frac{M^D|F|(D)}{T} + \frac{A(M)M\log M}{T} + A(M)\right)$$

where

$$|F|(\sigma) = \sum_{n\geq 1}\frac{|a_n|}{n^\sigma}$$

for $\sigma > \sigma_a$ and $a_n = O(A(n))$ with $A(n)$ being non-decreasing.

Properties of L_Ψ

- Set $I = (0,1)$.
- For $t > 0$ and $\Psi \in C^1(I)$, set

$$\|\Psi\|_{(t)} := \|\Psi\|_\infty + \frac{\|\Psi'\|_\infty}{t}.$$

Proposition

For any $0 < \xi < \frac{1}{5}$, we can find $0 < \alpha_0 = \alpha_0(\xi) \le \frac{1}{2}$ with the following properties: for any $\Psi \in C^1(I)$,

1. *$L_\Psi(2s)$ has only a simple pole at $s = 1$ in the strip $|\Re s - 1| \le \alpha_0$.*
2. *In the strip $|\Re s - 1| \le \alpha_0$,*

$$|L_\Psi(2s)| \ll \max(1, |t|^\xi)\|\Psi\|_{(t)}$$

   with $t = \Im s$ and $\Psi \in C^1(I)$.

- The exponent ξ and constant α_0 are related to the spectral gap and eigenvalue of a generalized Perron-Frobenius transfer operator.

Main result

Applying Tauberian argument, we obtain:

Proposition

There exist constants $0 < \delta < 2$, $\kappa > 0$ *such that for all* $\Psi \in C^1(I)$, *we have*

$$\sum_{n \leq M} \sum_{r \in \Sigma_n} \Psi(r^*) = \|\Psi\|_{L^1} M^2 + O\left(M^\delta \|\Psi\|_{(M^\kappa)} \right).$$

The implicit constant, δ*, and* κ *are independent of* Ψ.

- Two constants δ and κ are related to the spectral gap and eigenvalue.

The proof: Cont'd

We have shown that

$$\sum_{n<M}\sum_{r\in\Sigma_n}\Psi_M(r^*) = \|\Psi_M\|_{L^1}M^2 + O(M^\delta\|\Psi_M\|_{(M^\kappa)}).$$

and

$$\sum_{n<Q}\sum_{r\in\Sigma_n}\Psi_M(r^*) = \|\Psi_M\|_{L^1}Q^2 + O(Q^\delta\|\Psi_M\|_{(Q^\kappa)}).$$

Setting $Q = M(1-M^{-\epsilon})$, we have

$$M^2 - Q^2 \asymp M^{2-\epsilon}.$$

Hence

$$\sum_{Q<n<M}\sum_{r\in\Sigma_n}\Psi_M(r^*) \gg M^{\beta-1}M^{2-\epsilon} + O(M^\delta M^{1-\beta-\kappa}).$$

Setting $\beta = \frac{\delta-\kappa}{2}+\epsilon$, we get the statement.

Contents

Setting

- For $r \in \mathbb{Q} \cap I$, set
$$r = [0; m_1, m_2, \cdots, m_\ell]$$
with $\ell = \ell(r)$, the length of the expansion.
- Set
$$\frac{P_i}{Q_i} := [0; m_1, m_2, \ldots, m_i]$$
- Recall the Gauss map
$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor .$$
- Then, $T(r) = [0; m_2, \cdots, m_\ell]$.

Perron-Frobenius Transfer operator

- (T, I) is an ergodic system with the invariant measure $\dfrac{dx}{\log 2(1+x)}$.
- The Perron-Frobenius transfer operator for T is

$$\mathcal{L}\Psi(x) = \sum_{n\geq 1} \frac{1}{(n+x)^2}\Psi(\frac{1}{n+x})$$

  where $\Psi \in L^\infty(I)$.
- On $C^1(I)$, the operator $\mathcal{L}$ has the simple dominant eigenvalue 1, of which the eigenfunction is $\Psi_0(x) = \dfrac{1}{1+x}$.
- There is a spectral gap for $\mathcal{L}$.

Generalized Perron-Frobenius Transfer operator

- Let $s = \sigma + it$.
- For $x \in I$, $\Re(s) > \frac{1}{2}$, and $\Psi \in L^\infty(I)$, define a transfer operator

$$\mathcal{L}_s \Psi(x) = \sum_{m \geq 1} \frac{1}{(m+x)^{2s}} \Psi\left(\frac{1}{m+x}\right).$$

- And set

$$\mathcal{F}_s \Psi(x) = \sum_{m \geq 2} \frac{1}{(m+x)^{2s}} \Psi\left(\frac{1}{m+x}\right).$$

- When $\sigma \sim 1$, the spectral properties of $\mathcal{L}_\sigma$ is same as $\mathcal{L} = \mathcal{L}_1$.
- By Perturbation theory, one can obtain the spectral properties of $\mathcal{L}_s$ when σ is near 1.

Iteration of $\mathcal{L}_s$

It can be proved that

- $\mathcal{L}_s^n \mathcal{F}_s \Psi(0) = \sum_{\substack{\ell(r)=n+1 \\ r \in \mathbb{Q} \cap I}} \Psi\left(\frac{Q_{\ell-1}}{Q_\ell}\right) \frac{1}{Q_\ell(r)^{2s}}.$

- Note: $r^* = \begin{cases} \frac{Q_{\ell-1}}{Q_\ell} & \text{if } \ell = \ell(r) \text{ is odd} \\ 1 - \frac{Q_{\ell-1}}{Q_\ell} & \text{if } \ell \text{ is even} \end{cases}.$

- Define
$$\mathcal{J}\Psi(x) := \Psi(1-x).$$

Key relation for L_Ψ

Note that

$$L_\Psi(s) = \sum_{n\geq 1} \frac{\sum_{r\in\Sigma_n} \Psi(r^*)}{n^s}$$
$$= \sum_{r\in\mathbb{Q}\cap I} \frac{\Psi(r^*)}{Q(r)^s}.$$

Theorem

For $\Psi \in L^1(I)$ and $\Re(s) > \frac{1}{2}$, we obtain

$$L_\Psi(2s) = (\mathcal{I} - \mathcal{L}_s^2)^{-1}\mathcal{F}_s\Psi(0) + (\mathcal{I} - \mathcal{L}_s^2)^{-1}\mathcal{L}_s\mathcal{F}_s\mathcal{J}\Psi(0)$$
$$= (\mathcal{I} - \mathcal{L}_s^2)^{-1}\mathcal{M}_s\Psi(0).$$

where $\mathcal{M}_s := \mathcal{F}_s + \mathcal{F}_s\mathcal{J}$.

Contents

Spectral Properties of $\mathcal{L}_s$

A (incomplete) list of the spectral properties of $\mathcal{L}_s$ is:

- $\mathcal{L}_\sigma$ has a unique dominant eigenvalue $\lambda(\sigma)$ of maximal modulus, which is real and simple.
- There is a spectral gap for $\mathcal{L}_\sigma$.
- The eigenvalue $\lambda(s)$ of $\mathcal{L}_s$ is analytic for s with $\sigma \sim 1$
- $\lambda(1) = 1$.

Restrict the operators on the space $C^1(I)$.

Theorem (Characteristic of a dominant eigenvalue)

$(\mathcal{I} - \mathcal{L}_s)^{-1}$ *has a unique simple pole at* $s = 1$ *in a fixed critical strip.*

Behavior of the quasi-inverse

Theorem (Dolgopyat)

For each $0 < \xi < \frac{1}{5}$, there exists $\alpha_0 > 0$ such that if $|\sigma - 1| \leq \alpha_0$, then for all $|t| \gg 1$ and all n, one has

$$\|\mathcal{L}_s^n\|_{(t)} \ll |t|^\xi \gamma^n$$

for some $0 < \gamma < 1$.

- ξ is related to the spectral gap of $\mathcal{L} = \mathcal{L}_1$.
- α_0 is determined by an explicit behavior of $\lambda(s)$ near $s = 1$.

Research Goal

1. Determine explicitly the spectral gap of $\mathcal{L}$.
2. Investigate the explicit behavior of $\lambda(s)$ near 1.

Contents

Elements in an interval

Consider a variant of the problem: For an interval $J \subseteq I$, estimate

$$R_J(n,x) := \#\left\{1 \leq m \leq n \,\middle|\, \frac{m}{n} \in J,\ m \in R(n,x)\right\}.$$

One possible approach is to study:

$$L_{\Psi,J} := \sum_{r \in J \cap \mathbb{Q}} \frac{\Psi(r^*)}{Q(r)^{2s}}.$$

Basic idea:

- When $r \in J$, the first few digits of continued fraction expansions of r are completely determined and there is no restriction on the remaining digits.

Open fundamental intervals

For integers $m_1, \cdots, m_n \geq 1$, denote an open fundamental interval of depth n by

$$K(m_1, \cdots, m_n) := \{[0; m_1, \cdots, m_n + x] \,|\, 0 < x < 1\}.$$

- The end points of $K = K(m_1, \cdots, m_n)$ are $\dfrac{P_n}{Q_n}$ and $\dfrac{P_n + P_{n-1}}{Q_n + Q_{n-1}}$.
- The length is $|K| = \dfrac{1}{Q_n(Q_n + Q_{n-1})} \asymp \dfrac{1}{Q_n^2}$.
- $r \in K$ if and only if the first n digits of r are $m_1, \cdots, m_n$ (with no restriction on the remaining digits).

Decomposing an interval J

Let $\mathfrak{A}_n$ be the collection of open fundamental intervals defined inductively as follows:

- Let $\mathfrak{A}_1$ be the collection of (consecutive) open fundamental intervals of depth 1 that are included in J.
- Let $\mathfrak{A}_j$ be defined for $1 \leq j \leq n$. Then, $\mathfrak{A}_{n+1}$ is the collection of open fundamental intervals of depth $n+1$ that are included in

$$J \setminus \bigcup_{j=1}^{n} \bigcup_{K \in \mathfrak{A}_j} K.$$

Structure of $\mathfrak{A}_n$

- Let $a < b$ be the end points of J.
- Let $[0; u_1, u_2, \cdots]$ and $[0; v_1, v_2, \cdots]$ be the (possibly finite) continued fraction expansions of a and b, respectively.

Proposition

When n is even and sufficiently large,

$$\mathfrak{A}_n = \{K(u_1, \cdots, u_{n-1}, k) \mid k \geq u_n + 1\} \cup \{K(v_1, \cdots, v_{n-1}, k) \mid 1 \leq k \leq v_n\}$$

and when n is odd and sufficiently large,

$$\mathfrak{A}_n = \{K(u_1, \cdots, u_{n-1}, k) \mid 1 \leq k \leq u_n\} \cup \{K(v_1, \cdots, v_{n-1}, k) \mid k \geq v_n + 1\}.$$

- Set

$$\mathfrak{A}^{\pm} = \bigcup_{(-1)^n = \pm 1} \mathfrak{A}_n.$$

An operator for K

Definition

For $K = K(m_1, \cdots, m_n)$, define

$$\mathcal{D}_s^K \Psi(x) := \frac{1}{Q_n(m_1, \cdots, m_n + x)^{2s}} \Psi\left(\frac{P_n(m_n, \cdots, m_1 + x)}{Q_n(m_n, \cdots, m_1 + x)}\right)$$

Obvious but crucial observations are:

- When $K \in \mathfrak{A}^+$,

$$\mathcal{D}_s^K (\mathcal{I} - \mathcal{L}_s^2)^{-1} \mathcal{M}_s \Psi(0) = \sum_{r \in \mathbb{Q} \cap K} \frac{\Psi(r^*)}{Q(r)^{2s}}.$$

- When $K \in \mathfrak{A}^-$,

$$\mathcal{D}_s^K (\mathcal{I} - \mathcal{L}_s^2)^{-1} \mathcal{M}_s \mathcal{J} \Psi(0) = \sum_{r \in \mathbb{Q} \cap K} \frac{\Psi(r^*)}{Q(r)^{2s}}.$$

Definition of interval operators

Definition

Define

$$\mathcal{D}_s^{J,\pm} = \sum_{K\in\mathfrak{A}^\pm} \mathcal{D}_s^K$$
$$\mathcal{D}_s^J = \mathcal{D}_s^{J,+} + \mathcal{D}_s^{J,-}$$

Proposition

Let $\frac{p_n}{q_n}$ and $\frac{P_n}{Q_n}$ be the n-th convergents of the end points of J, respectively. Then

$$\|\mathcal{D}_s^{J,\pm}\|_\infty \ll \sum_{K\in\mathfrak{A}^\pm} |K|^\sigma \ll \frac{1}{2\sigma-1}\sum_{n\geq 1} \frac{1}{q_n^{2\sigma}} + \frac{1}{Q_n^{2\sigma}}.$$

- For $\Psi \in L^\infty(I)$, the series $\mathcal{D}_s^{J,\pm}\Psi(x)$ is absolutely convergent for $\Re s > \frac{1}{2}$.

Expression for Dirichlet series

Theorem

$$L_{\Psi,J}(2s) = \mathcal{D}_s^J \Psi(0) + \mathcal{D}_s^{J,+}(\mathcal{I} - \mathcal{L}_s^2)^{-1}\mathcal{M}_s \Psi(0) \\ + \mathcal{D}_s^{J,-}(\mathcal{I} - \mathcal{L}_s^2)^{-1}\mathcal{M}_s \mathcal{J}\Psi(0).$$

Properties of Dirichlet series

Proposition

With the same data as before,

1. *The series $L_{\Psi,J}(2s)$ has only a simple pole at $s = 1$ in the strip $|\Re s - 1| \leq \alpha_0$ and its residue $E_{\Psi,J}$ satisfying*

$$E_{\Psi,J} = |J| \cdot \|\Psi\|_{L^1}.$$

2. *In the strip $|\Re s - 1| \leq \alpha_0$, we have*

$$|L_{\Psi,J}(2s)| \ll \left(\|\mathcal{D}_s^{J,+}\|_\infty + \|\mathcal{D}_s^{J,-}\|_\infty\right) \max(1, |t|^\xi)\|\Psi\|_{(t)}$$

   with $t = \Im s$.

The implicit constants are independent of J and Ψ.

Thanks for your attention!