ETH COLLOQUIUM

DIOPHANTINE APPLICATIONS OF THE THEORY OF GROUP EXPANSION

OVERVIEW

- **Expansion in $SL_2(q)$- Cayley Graphs and generalization of Selberg Theorem**

- **Hyperbolic lattice point counting**

- **Diophantine properties of integral Apollonian circle packings**

- **Zaremba's conjecture on continued fractions**

GRAPH EXPANSION

$\mathcal{G} = k$-regular graph on vertex set $V, |V| = n$

$$(k \text{ fixed}, \ n \to \infty)$$

CHEEGER CONSTANT

$$h(\mathcal{G}) = \min_{|S| \leq \frac{n}{2}} \frac{|\partial S|}{|S|}$$

∂S = edges from S to $V \backslash S$

EXPANDER FAMILIES

k fixed

$\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \ldots$ k regular graphs $(|V_i| \to \infty)$

is expander families provided

$$h(\mathcal{G}_i) > c \text{ for all } \mathcal{G}_i$$

where $c > 0$ is some constant

SPECTRAL INTERPRETATION

$A(\mathcal{G})$ = adjacency matrix of $\mathcal{G}$ (k- regular)

$$A_{ij} = \begin{cases} 1 & \text{if } (i,j) \in \mathcal{G} \\ 0 & \text{otherwise} \end{cases}$$

EIGENVALUES: $k = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$

SPECTRAL GAP: $k - \lambda_1$

$$\frac{1}{2}(k - \lambda_1) \leq h(\mathcal{G}) \leq \sqrt{2k(k - \lambda_1)}$$

DO EXPANDER GRAPHS EXIST?

M. Pinsker (73)

'Given $k \geq 3$, a random (= typical)

k-regular graph on n vertices

$(n \to \infty)$ is an expander graph'

(Implicit in earlier work of Kolmogorov and Barzdin on networks)

A. Kolmogorov **B. Barzdin**

'On the realization of networks in $3D$-space

(PROBLEMY KIBERNETIKI, 1967)

What is the minimal amount of space needed to realize a k regular graph on n vertices using a wiring with wires of thickness 1?'

$$(k \text{ fixed}, \ n \to \infty)$$

HOW TO PRODUCE EXPLICITLY EXPANDER GRAPHS?

USE OF ALGEBRAIC METHODS

First construction: **G. Margulis** (73)

Expansion of **CAYLEY GRAPHS** on groups

SELBERG'S THEOREM

$\langle S \rangle$ finite index subgroup in $SL_2(\mathbb{Z})$

$\pi_q : SL_2(\mathbb{Z}) \to SL_2(q)$ (mod q reduction)

Cayley graphs

$$\mathcal{G}\big(SL_2(q), \pi_q(S)\big) \quad q \in \mathbb{Z}, (q, q_0) = 1$$

is expander family

EXAMPLE

$$p = 5$$

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad S = \{A, A^{-1}, B\}$$

C_{60} = Cayley Graph $X(PSL_2(5), S_5)$

A. LUBOTZKY's 1-2-3 problem

$$S_1 = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\} \qquad \text{OK}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\} \qquad \text{OK}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\} \qquad ?$$

THEOREM

Assume $\langle S \rangle$ non-elementary subgroup of $SL_2(\mathbb{Z})$

There is $q_0 \in \mathbb{Z}$ such that

$$\mathcal{G}(SL_2(q), \pi_q(S)) \qquad (q, q_0) = 1$$

is expander family

q	prime	**B-Gamburd**, based on work of **H. Helfgott**
q	square-free	**B-Gamburd-Sarnak**
q	arbitrary	**B-Varju**

GENERALIZATION OF SELBERG'S SPECTRAL GAP THEOREM TO INFINITE VOLUME CASE

$\Lambda = \langle S \rangle \subset SL_2(\mathbb{Z})$ $\qquad$ $\delta(\Lambda) > \frac{1}{2}$

$\Lambda_q = \Lambda \cap \Gamma(q)$

spectrum of $\mathbb{H}/\Lambda_q$? $\qquad$ $\lambda_0(\Lambda_q) = \lambda_0(\Lambda)$

THEOREM

There is $\varepsilon = \varepsilon(\Lambda) > 0$ *such that* $\lambda_1(\Lambda_q) > \lambda_0 + \varepsilon$ *for all* $q \in \mathbb{Z}_+$

Proof of spectral gap based on expander family $\mathcal{G}\big(SL_2(q), \pi_q(S)\big)$

Combinatorial spectral gap $\Rightarrow$ geometric spectral gap (**Burgers, Brooks**)

DISTRIBUTION IN THIN GROUPS

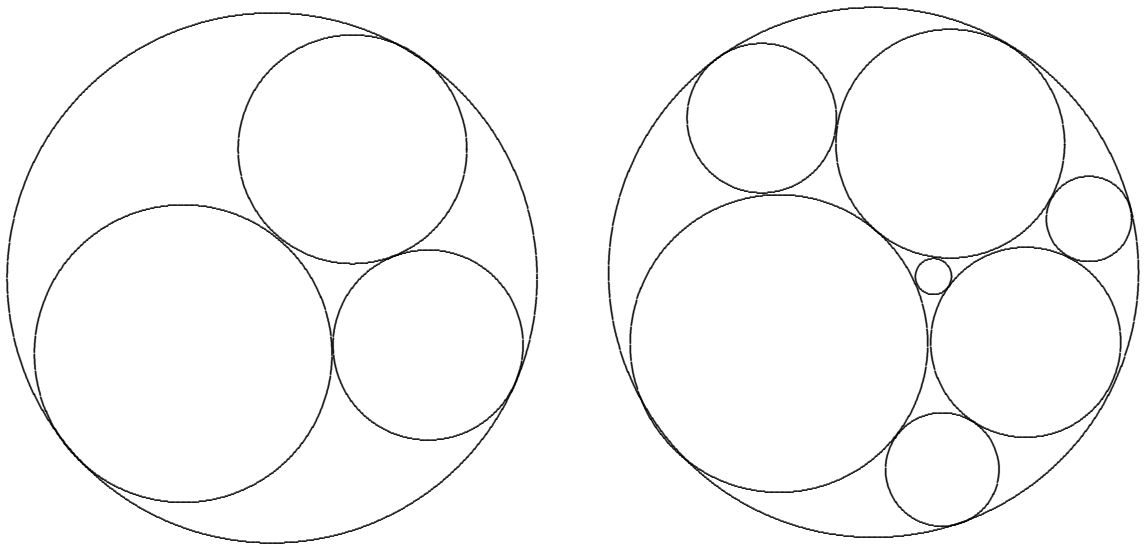
$$\Lambda = \langle S \rangle \subset SL_2(\mathbb{Z}) \qquad \delta(\Lambda) > \frac{1}{2}$$

There is $q_0 = q_0(\Lambda) \in \mathbb{Z}_+$ such that if $(q, q_0) = 1$ and $g \in SL_2(q)$

$$\left|\left\{\gamma \in \Lambda |\ \|\gamma\| \leq N \text{ and } \pi_q(\gamma) = g\right\}\right| \sim \frac{N^{2\delta}}{|SL_2(q)|} + 0(q^C N^{2\delta - \varepsilon})$$

Based on Lax-Phillips theory

APOLLONIAN CIRCLE PACKINGS



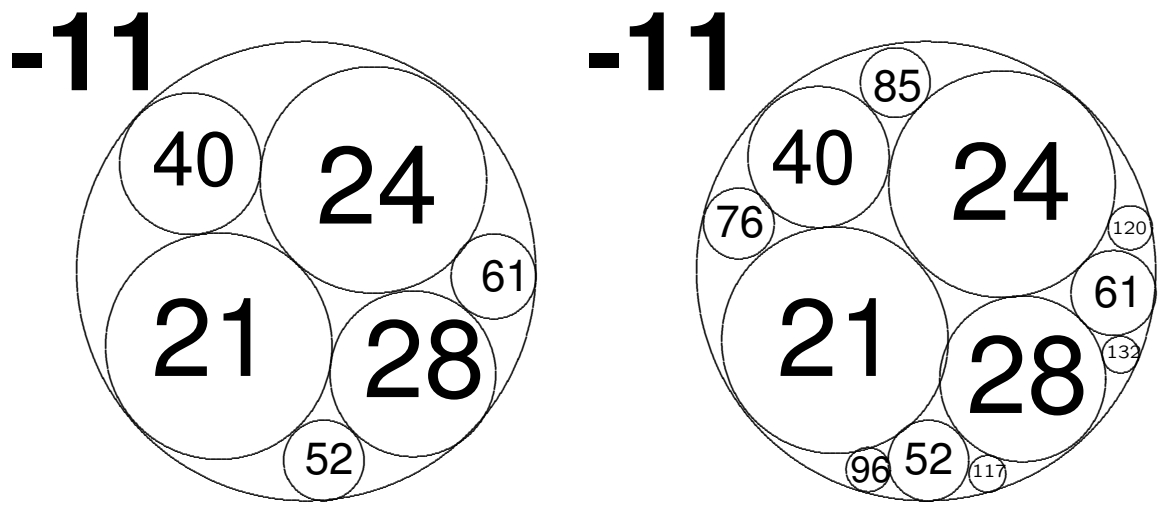
APOLLONIUS' THEOREM

Given 3 mutually tangent circles, there are exactly two circles tangent to all three

INTEGRAL APOLLONIAN CIRCLE PACKINGS AND SODDY'S THEOREM

EXAMPLE

$\mathcal{P}_0$= packing corresponding to quadruple (-11, 21, 24, 28)



ALL CURVATURES IN THE PACKING ARE INTEGRAL

(**F. Soddy**, 1937)

WHICH INTEGERS ARE PRODUCED IN A GIVEN INTEGRAL ACP?

(Graham, Lagarias, Mallow, Wilks, Yan - Sarnak)

CONJECTURE 1 (Positive density conjecture)

Set of curvatures is a subset of $\mathbb{Z}$ of positive density

CONJECTURE 2 (Local to global principle)

All integers are produced, up to finite congruence condition

DESCARTE FORM AND THE APOLLONIAN GROUP

$$F(x_1, x_2, x_3, x_4) = 2(x_1^2+x_2^2+x_3^2+x_4^2)-(x_1+x_2+x_3+x_4)^2$$

$$O_F = \textbf{Orthogonal group}$$

$$A = \langle S_1, S_2, S_3, S_4 \rangle \textbf{ Apollonian packing group}$$

$$S_1 = \begin{bmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad S_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad S_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{bmatrix}$$

$\mathcal{P}_0$ = orbit of root quadruple $a = (-11, 21, 24, 28)$ under group A

MAIN FEATURES OF APOLLONIAN GROUP

• Under spin double cover, A is obtained as a finitely generated subgroup Γ of $SL_2(\mathbb{Z}+i\mathbb{Z})$ of dimension

$$\delta = 1,30568\ldots \qquad \textbf{(D. Boyd)}$$

to which spectral methods apply

• The subgroups
$\langle A_1, A_2, A_3\rangle, \langle A_2, A_3, A_4\rangle, \langle A_3, A_4, A_1\rangle, \langle A_4, A_1, A_2\rangle$
are arithmetic and their orbits may be described by binary quadratic forms

DIOPHANTINE ANALYSIS

THEOREM 1 (**Fuchs**) *Determination of* $\pi_q(A) \subset GL_4(\mathbb{Z}/q\mathbb{Z})$
for every q*. Ramified set consists only of 2 and 3*

THEOREM 2 (**B-Fuchs**) *Positive density conjecture holds*

THEOREM 3 (**B-Kontorovich**) *Local/global principle holds*
up to exceptional set of size at most $T^{1-\varepsilon}$*, for some* $\varepsilon > 0$

EXAMPLE (**packing** $\mathcal{P}_0$) **Only congruence restriction**

$a(C) \in \{0, 4, 12, 13, 16, 21\} \pmod{24}$

$\#\{a < T; \pi_{24}(a) \in \{0, 4, 12, 13, 16, 21\}, a \text{ not a } \mathcal{P}_0\text{-curvature}\} < T^{1-\varepsilon}$

A NEW FORM OF THE HARDY-LITTLEWOOD CIRCLE METHOD

Major arcs analysis: Based on spectral theory

Minor arcs estimates: Exploits binary quadratic forms produced by arithmetic subgroups

ZAREMBA'S CONJECTURE

Continued fraction expansion

$$\frac{b}{d} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \; + \frac{1}{a_k}}} = [a_1, \ldots, a_k]$$

$$\mathcal{R}_A = \left\{ \frac{b}{d} = [a_1, \ldots, a_k];\ 1 \leq a_j \leq A \text{ for all } j = 1, \ldots, k \right\}$$

$$\mathcal{D}_A = \left\{ d \in \mathbb{N};\ \text{there is } (b, d) = 1 \text{ with } \frac{b}{d} \in \mathcal{R}_A \right\}$$

CONJECTURE 1 (**Z**, 1971) *For some sufficiently large* A*, we have*

$$\mathcal{D}_A = \mathbb{N}$$

In fact, $A = 5$ *should suffice* $(54 \notin \mathcal{D}_4)$

CONJECTURE 2 (**N**, 1978) $\mathcal{D}_3$ *contains every sufficiently large integer*

CONJECTURE 3 (**H**, 1996) *Same statement for* $\mathcal{D}_2$

Note that $\mathcal{R}_1 = \{f_n/f_{n+1}\}, \mathcal{D}_1 = \{f_n\} =$ Fibonacci numbers

Niederreiter (86) showed that $\{2^j\} \subset \mathcal{D}_3$

MOTIVATION

Numerical integration, Monte-Carlo methods,

Pseudo-random numbers

DISCREPANCY

$$X = \{x_j\}_{j \le N} \subset Q = [0,1]^s$$

$$D(X) = \max_{\substack{I \subset Q \\ \text{box}}} \left| |I| - \frac{1}{N}(\#\{j \le N; x_j \in I\}) \right|$$

Zaremba (1966) $(s = 2)$

Take $(b, d) = 1$ with $\frac{b}{d} \in \mathcal{R}_A$. Let

$$X = \left\{ x_j = \left(\frac{j}{d}, \frac{bj}{d} \right) ;\ 1 \leq j \leq d \right\}$$

where $\frac{bj}{d}$ is reduced $(\mathrm{mod}\, 1)$. Then

$$D(X) < \left(\frac{4A}{\log(A+1)} + \frac{4A+1}{\log d} \right) \frac{\log d}{d}$$

$\Rightarrow$ role of diophantine properties

OPTIMALITY

W. Schmidt Irregularities of distribution VII (1972)

Theorem Any sequence $X = \{x_j\}_{j \leq N}$ in $[0,1]^2$ satisfies

$$D(X) > c\,\frac{\log N}{N}$$

Pseudo-randomness of modular multiplication

$$x \mapsto bx \pmod{d}$$

Special case of liner congruential PRNG $x \mapsto bx + c \pmod{d}$

Take d prime and b primitive $\pmod{d}$

Statistical properties of

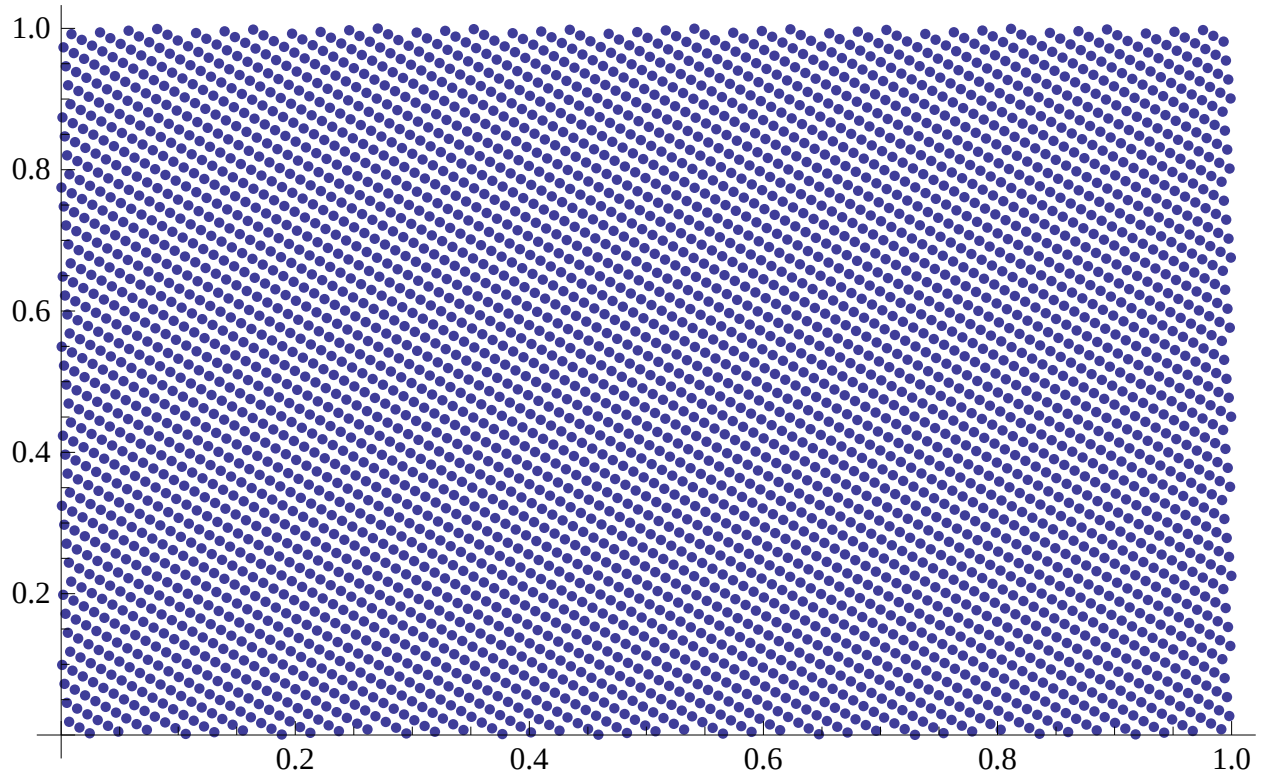
$$X_1 = \left\{ \frac{b^j}{d} \pmod{1}; 1 \leq j < d \right\}$$

and

$$X_2 = \left\{ \left(\frac{b^j}{d}, \frac{b^{j+1}}{d} \right); 1 \leq 1 < d \right\}$$

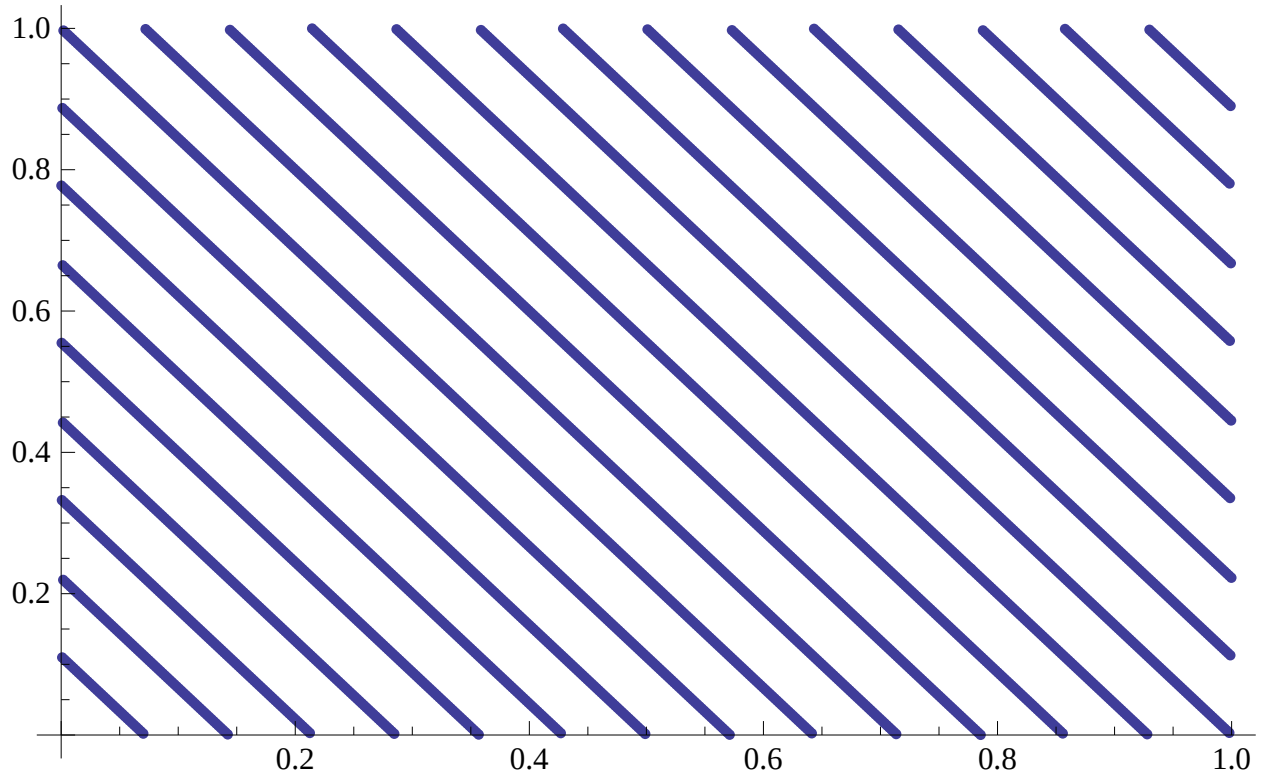
(serial correlation of pairs)

$\Rightarrow D(X_2)$ is essentially $D(X)$



$$\left\{ \left(\frac{b^n}{d}, \frac{b^{n+1}}{d} \right) \bmod 1 \right\}_{n=1}^{d}$$

$$\frac{b}{d} = \frac{3523}{4547} = [1, 3, 2, 3, 1, 2, 3, 2, 1, 3]$$



$$\left\{ \left(\frac{b^n}{d}, \frac{b^{n+1}}{d} \right) \bmod 1 \right\}_{n=1}^{d}$$

$$\frac{b}{d} = \frac{3535}{4547} = [1, 3, 2, 35, 1, 1, 1, 4]$$

Theorem (**B-Kontorovich**, 2011)

For $A = 50$, $\mathcal{D}_A$ is of density one

Quantitatively, if

$$\mathcal{D}_A(N) = \mathcal{D}_A \cap [1, N]$$

we have

$$\#\mathcal{D}_A(N) = N + 0\Big(N^{1-\frac{1}{\log\log N}}\Big)$$

Corollary *(linear congruential map)*

$\mathcal{R}_{51}$ contains infinitely many fractions $\frac{b}{d}$ with d prime so that the multiplier b is a primitive root mod d

CONTINUED FRACTION CANTOR SETS AND DIMENSION

$$\mathcal{C}_A = \{[a_1, \ldots, a_j, \ldots]; a_j \leq A \text{ for all } j \geq 1\} \subset [0, 1]$$

δ_A = Hausdorff dimension of $\mathcal{C}_A$

$$\mathcal{C}_1 = \left\{\frac{1}{\varphi}\right\} \quad \varphi = \frac{1+\sqrt{5}}{2}$$

$\mathcal{C}_2$ is Cantor set, $\delta_2 = 0,5312805\ldots$ (**Jenkinson–Pollicott**)

For large A

$$\delta_A = 1 - \frac{6}{\pi^2}\frac{1}{A} - \frac{72}{\pi^4}\frac{\log A}{A^2} + 0\left(\frac{1}{A^2}\right) \qquad \text{(**Hensley**)}$$

SEMI-GROUP ORBITS

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

equivalent to

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

$\mathcal{G}_A \subset GL_2(\mathbb{Z})$ semi-group generated by matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \qquad 1 \leq a \in A$$

Orbit $\mathcal{O}_A = \mathcal{G}_A.e_2$ in one-to-one correspondence with $\mathcal{G}_A$

$$\mathcal{D}_A = \langle \mathcal{G}_A.e_2, e_2 \rangle$$