On some problems of Additive Combinatorics and Dynamical Systems

I. D. Shkredov

Steklov Mathematical Institute

Introduction

Let $G = (G, +)$ be an (abelian) group.
Additive Combinatorics studies any combinatorial questions involving the group operation.

The *sumset* and the *difference set* of A and B

$$A + B = \{a + b \ : \ a \in A,\ b \in B\}.$$

$$A - B = \{a - b \ : \ a \in A,\ b \in B\}.$$

If $\mathcal{R} = (\mathcal{R}, +, *)$ is a ring, then the *product* set of A, B is

$$A * B = \{a * b \ : \ a \in A,\ b \in B\}.$$

Arithmetic combinatorics (we study both operations simultaneously).

Examples

Theorem (Lagrange, 1770)

Let $\mathcal{S} = \{0^2, 1^2, 2^2, \dots, \}$ be the set of squares. Then

$$4\mathcal{S} = \mathbb{N}\,.$$

Theorem (Vinogradov 1937, Helfgott 2013)

Let $\mathcal{P}$ be the primes numbers with zero and one. Then

$$3\mathcal{P} \supset \{2n+1 \ : \ n \in \mathbb{N}\}\,.$$

Previously Shnirel'man (1930): $\exists k$ s.t. $k\mathcal{P} = \mathbb{N}$, his method was (almost) additive–combinatorial.

Szemerédi's theorem, I

Theorem (Schur, 1916)

Let $h \in \mathbb{N}$. Then for any colouring of $\mathbb{N}$ in h colors $C_1, \ldots, C_h$ there is C_j and $x, y, z \in C_j$ s.t.

$$x + y = z\,.$$

Theorem (Van der Waerden, 1927)

Let $h, k \in \mathbb{N}$. Any colouring of $\mathbb{N}$ in h colors a monochromatic possess an arithmetic progression of length k.

AP3 (progressions of length three): $x + y = 2z$.

Szemerédi's theorem, II

Theorem (Szemerédi's, 1969)

Let $A \subseteq \{1, 2, \dots, N\}$ be a set having no APk. Then

$$|A| = o(N), \qquad N \to \infty .$$

Szemerédi's theorem implies van der Waerden's theorem.

Graphs: Ajtai, Szemerédi, Ruzsa.
Hypergraphs: Rödl, Tao, Gowers.
Ergodic approach: Furstenberg, Ornstein, Bergelson, Leibman, Tao, Austin.
Analytic: Gowers, Green, Tao.

Szemerédi's theorem, III

Theorem (Ajtai–Szemerédi, 1974, Furstenberg–Katznelson, 1978)

Let $A \subseteq \{1, 2, \dots, N\}^2$ has no configurations

$$\{(x, y), (x + d, y), (x, y + d)\}, \quad d \neq 0.$$

Then

$$|A| = o(N^2), \qquad N \to \infty.$$

This result is equivalent to simultaneous recurrence under the action of two commutative measure–preserving operators.

$\{(0, 1), (1, 0)\}$ can be replaced to any finite configuration.

Dynamical reformulation

Let $(X, \mathcal{B}, T, \mu)$ be a dynamical system, $\mu(X) < \infty$.

Theorem (Furstenberg, 1977)

Let $k \geq 2$. Then for any measurable E, $\mu(E) > 0$ there is $n \in \mathbb{N}$ s.t.

$$\mu(E \cap T^{-n}E \cap T^{-2n}E \cap \cdots \cap T^{-(k-1)n}E) > 0\,.$$

This result is *equivalent* the Szemerédi theorem.

Furstenberg correspondence principle

Let $A \subset \mathbb{Z}$, $D^*(A) > 0$. Then there is $(X, \mathcal{B}, \mu, T)$ and a set E, $\mu E = D^*(A)$ s.t. for all $k \geq 3$ and $m_1, m_2, \ldots, m_{k-1}$ one has

$$D^*(A \cap (A+m_1) \cap \cdots \cap (A+m_{k-1})) \geq \mu(E \cap T^{-m_1}E \cap \cdots \cap T^{-m_{k-1}}E)\,.$$

Any set of integers is coded by a dynamical system.

Further results

Theorem (Katznelson–Furstenberg, 1978–1980)

Let $T_1, \dots, T_k$ be commutative maps, preserving a finite measure μ. Then for any E with $\mu E > 0$ $\exists n > 0$ s.t.

$$\mu(E \cap T_1^{-n} E \cap T_2^{-n} E \cap \dots \cap T_k^{-n} E) > 0\,.$$

Theorem (Bergelson–Leibman)

Let $T_1, \dots, T_k$ be commutative maps, preserving a finite measure μ. Also, let $p_1(n), \dots, p_k(n) \in \mathbb{Z}[x]$ with $p_i(0) = 0$. Then for any E with $\mu E > 0$ one has

$$\liminf_{n\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu(T_1^{-p_1(n)} E \cap T_2^{-p_2(n)} E \cap \dots \cap T_k^{-p_k(n)} E) > 0\,.$$

On recurrence time

For any $A, B \in \mathcal{B}$, $\mu(A), \mu(B) > 0$ put

$$R_{A,B} = \{n \in \mathbb{Z} \ : \ \mu(A \cap T^{-n}B) > 0\}, \qquad R_A = R_{A,A}.$$

From Ergodic theorem it follows that $D^*(R_A) \geq \mu(A)$. What if

$$C\mu(A) \geq D^*(R_A) \geq \mu(A) \ ?$$

Theorem (Björklund–Fish–Shkredov, 2021)

Let T be an ergodic map. Then

1) If $D^*(R_A) < \frac{3}{2}\mu(A)$, then $R_A = r\mathbb{Z}$, $r \leq 1/\mu(A)$.
2) If T is totally ergodic, then $D^*(R_{A,B}) \geq \min\{1, \mu(A) + \mu(B)\}$.
3) If $D^*(R_A) \leq C\mu(A)$ for small A, then $C \leq 2$.

Actually, we have full description of $R_{A,B}$ in 2) and 3).
The proof uses Kneser's theorem from AC.

Szemerédi's theorem, IV

Theorem (Roth, 1953)

Let $A \subseteq \{1, 2, \dots, N\}$ be a set having no AP3. Then

$$|A| = O\left(\frac{N}{\log\log N}\right).$$

Heath–Brown (1987) , Szemerédi (1990), Bourgain (1999, 2008), Sanders (2011, 2012), Bloom (2014), Schoen (2020), Bloom–Sisask (2020).

Theorem (Gowers, 1998)

Let $A \subseteq \{1, 2, \dots, N\}$ be a set having no APk. Then

$$|A| = O\left(\frac{N}{(\log\log N)^{c_k}}\right), \qquad c_k > 0\,.$$

Szemerédi's theorem, V

Theorem (Shkredov, 2006–2009)

Let $A \subseteq \{1, 2, \dots, N\}^2$ has no "corners"

$$\{(x, y), (x + d, y), (x, y + d)\}, \quad d \neq 0.$$

Then

$$|A| = O\left(\frac{N^2}{(\log\log N)^C}\right), \qquad C > 0.$$

This is two–dimensional analogue of Roth/Szemerédi theorem.

Corollary (Shkredov)

Let $(X, \mathcal{B}, T, S, \mu, d)$ be a measure–preserving system with metric d (μ and d are agreed) and T_1, T_2 commute. Then for a.e. $x \in X$

$$\liminf (\log\log n)^C \cdot \max\{d(T_1^n x, x), d(T_2^n x, x)\} \leq 1.$$

Applications: Number Theory

Theorem (Chudakov, Van der Corput, Chowla, 1938–1944)

The primes contains infinitely many arithmetic progressions of length three.

Vinogradov's method: $x + y + z = N$ и $x + y = 2z$.

Theorem (Green–Tao, 2008)

The primes contain infinitely many arbitrary long arithmetic progressions.

Reducing to a *relative* Szemerédi theorem.

Green–Tao–Ziegler, 2012: general linear forms.

Applications: Number Theory

APk in primes.

Theorem (Green–Tao–Ziegler, 2012)

The number of AP4 of primes numbers $p_1 < p_2 < p_3 < p_4 \leq N$ is

$$(1 + o(1))\mathfrak{S}_1 \frac{N^2}{\log^4 N},$$

where

$$\mathfrak{S}_1 = \frac{3}{4} \prod_{p \geq 5} \left(1 - \frac{3p-1}{(p-1)^3}\right).$$

The proof uses the high–order Fourier analysis, dynamical systems and *nilsequences*.

Linear equations, I

Van der Waerden theorem:

$$x + y = 2z\,, \qquad x, y, z \in A\,.$$

Schur's theorem:

$$x + y = z\,, \qquad x, y, z \in A\,.$$

General affine linear equation:

$$c_1 x_1 + \cdots + c_k x_k = 0\,,$$

where $c_1 + \cdots + c_k = 0$ и $x_j \in A$.

Theorem (Mashulam, 1995, Bloom, 2014)

Supppose $A \subseteq \{1, 2, \dots, N\}$ has no solutions to the equation

$$c_1 x_1 + \cdots + c_k x_k = 0\,,$$

where $c_1 + \cdots + c_k = 0$ and $x_j \in A$. Then for any $\varepsilon > 0$

$$|A| = O\left(\frac{N}{(\log N)^{k-2+\varepsilon}}\right)\,.$$

Theorem (Behrend, 1946)

Let $k \geq 2$. Then there is $A \subseteq \{1, 2, \dots, N\}$ s.t.

$$|A| \gg N \cdot \exp(-C\sqrt{\log N})$$

and A has no solutions to the affine equation

$$a_1 x_1 + \cdots + a_k x_k = (a_1 + \cdots + a_k) y\,.$$

Linear equations, II

Theorem (Schoen–Shkredov, 2014)

Let $N, k \in \mathbb{N}$, $k \geq 6$, and $c_1, \dots, c_k \in \mathbb{Z}$ with $c_1 + \dots + c_k = 0$. Then any $A \subseteq \{1, 2, \dots, N\}$ having no solutions of

$$c_1 x_1 + \dots + c_k x_k = 0$$

satisfies

$$|A| \ll \exp(-\log^{1/7} N) N \,,$$

where $c = c(c_1, \dots, c_k) > 0$.

Lower bound (Behrend, 1947): $|A| \gg N \exp(-C \log^{1/2} N)$.

Linear equations: ideas of the proof

$A+B$ must be structured.
The convolution (we have $\operatorname{supp}(1_A * 1_B)(x) = A+B$):

$$(1_A * 1_B)(x) := \sum_y 1_A(y) 1_B(-y+x)\,.$$

Theorem on almost periodicity of the convolution (Croot–Sisask, 2010)

Let $\epsilon \in (0,1)$, $K \geq 1$, $p \geq 2$ be parameters, $A, B \subseteq \mathrm{G}$ be some sets, $|A+B| \leq K|A|$ and $f : \mathrm{G} \to \mathbb{C}$ be a function. Then there is $b \in B$ and a sets $T \subseteq B$, $|T| \geq |B|(2K)^{-O(\epsilon^{-2}p)}$ such that for all $t \in T - b$ one has

$$\|(f * 1_A)(x+t) - (f * 1_A)(x)\|_{L_p} \leq \epsilon |A|^{1/p} \|f\|_{L_p}\,.$$

Kahane's conjecture, I

Let $\mathbb{T} = \mathbb{R}/(2\pi\mathbb{Z})$ and $W(\mathbb{T})$ be the Banach algebra of continuous complex functions f equipped with the Wiener norm

$$\|f\|_{W(\mathbb{T})} := \sum_{k\in\mathbb{Z}} |\hat{f}(k)| < \infty\,.$$

Here

$$\hat{f}(k) = (2\pi)^{-1} \int_{\mathbb{T}} f(t) e^{-ikt}\, dt\,, \quad k \in \mathbb{Z}\,.$$

Theorem (Beurling–Helson, 1953)

Any endomorphism of $AW(\mathbb{T})$ is trivial i.e. has the form

$$f(t) \to f(\nu t + t_0)\,,$$

where $\nu \in \mathbb{Z}$.

Kahane's conjecture, II

Theorem (Beurling–Helson, equivalent form)

Let $\varphi : \mathbb{T} \to \mathbb{T}$ be a continuous map. Suppose that

$$\|e^{in\varphi}\|_{W(\mathbb{T})} = O(1)\,, \quad n \in \mathbb{Z}, \quad |n| \to \infty\,.$$

Then $\varphi(t) = \nu t + \varphi(0)$, $\nu \in \mathbb{Z}$.

Conjecture (Kahane, 1962)

Let $\varphi : \mathbb{T} \to \mathbb{T}$ be a continuous map. Suppose that

$$\|e^{in\varphi}\|_{W(\mathbb{T})} = o(\log|n|)\,, \quad |n| \to \infty\,.$$

Then φ is a linear function.

Kahane's conjecture, III

Theorem (Lebedev, 2012)

Let $\varphi : \mathbb{T} \to \mathbb{T}$ be a continuous map. Suppose that

$$\|e^{in\varphi}\|_{W(\mathbb{T})} = o\left(\left(\frac{\log\log|n|}{(\log\log\log|n|)}\right)^{1/12}\right), \quad |n| \to \infty .$$

Then φ is a linear function.

Lebedev's proof based on some methods of Additive Combinatorics.

Kahane's conjecture, IV

Theorem (Konyagin–Shkredov, 2014)

Let $\varphi : \mathbb{T} \to \mathbb{T}$ be a continuous map. Suppose that

$$\|e^{in\varphi}\|_{W(\mathbb{T})} = o\left(\frac{\log^{1/22}|n|}{(\log\log|n|)^{3/11}}\right), \quad |n| \to \infty .$$

Then φ is a linear function.

Thus our result differs from Kahane's conjecture

$$\|e^{in\varphi}\|_{W(\mathbb{T})} = o(\log|n|), \qquad |n| \to \infty$$

by the constant $1/22$.

Kahane's conjecture: ideas of the proof

Let $A \subseteq \mathsf{G}$, $|\mathsf{G}| < \infty$

$$A + A = \{a_1 + a_2 \ : \ a_1, a_2 \in A\}\,.$$

It is easy to see (in particular, small $|A+A|$ implies large energy):

$$|A|^4 \leq \mathrm{E}(A)|A+A|\,.$$

$$\mathrm{E}(A) := |\{a_1+a_2 = a_3+a_4 \ : \ a_1,a_2,a_3,a_4 \in A\}| = |\mathsf{G}|^{-1}\sum_r |\hat{1}_A(r)|^4$$

Conversely: large $\mathrm{E}(A)$ implies that the sumset of a certain set is small (Balog–Szemerédi–Gowers theorem, 1998).
Combinatorics (=growth of sets) is equiavalent to estimation of $\hat{A}$ $(\mathrm{E}(A))$.
It is easy to see (Hölder) (plus a converse result):

$$|A|^3 \leq \|1_A\|^2_{W(\mathsf{G})} \cdot \mathrm{E}(A)\,.$$

Sum–product, I

General principle

If A belongs to a ring $\mathcal{R}(+,*)$ and

$$|A+A|, |A*A| \ll |A|^{1+\varepsilon},$$

then A has "large" intersection with a subring.

Erdős, Szemerédi, Ford, Elekes (Incidence Geometry), Bourgain, Katz, Tao, Konyagin, Garaev, Solymosi, Chang, Rudnev, ...

Applications: Number Theory, Additive Combinatorics, Dynamical Systems, Cryptography, Computer Science and so on.

Sum–product, II

Theorem (Erdős–Szemerédi, 1983)

Let $A \subset \mathbb{Z}$, $|A| < \infty$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{1+c}.$$

where $c > 0$ is an absolute constant.

Bourgain–Katz–Tao, 2004 / Bourgain–Glibichuk–Konyagin, 2006

Let $A \subseteq \mathbb{F}_p$, $|A| < p^{1-\varepsilon}$. Then there is $\delta = \delta(\varepsilon) > 0$ s.t.

$$\max\{|A \cdot A|, |A+A|\} \gg_\varepsilon |A|^{1+\delta}.$$

Sum–product, III

Theorem (Konyagin–Shkredov, 2016, ..., Rudnev–Stevens, 2020)

Let $A \subset \mathbb{R}$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{4/3+c}\,, \qquad |A| \to \infty\,,$$

where $c > 0$ is an absolute constant.

Theorem (Rudnev–Shakan–Shkredov, 2019)

Let $A \subset \mathbb{F}_p$, $|A| < p^{5/8}$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{1+2/9}\,.$$

Applications: new exponential sums, distribution of mulplicative subgroups, additive decomposition and so on.

Applications: exponential sums

Theorem (Bourgain–Glibichuk–Konyagin, 2006)

Let $\delta \in (0,1]$, p be a prime number and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \geq p^\delta$. Then there is $\varepsilon = \varepsilon(\delta) > 0$ such that $\xi \neq 0$ one has

$$|\sum_{x \in \Gamma} e^{2\pi i x\xi/p}| \ll |\Gamma| p^{-\varepsilon} \,.$$

Thus any mulplicative subgroup Γ, $|\Gamma| \geq p^\delta$ is uniformly distributed, i.e., $\forall a, b \in \{1, 2, \ldots, p\}$ one has

$$|\Gamma \cap [a,b]| = \frac{|\Gamma|}{p} \cdot (b-a) + O(|\Gamma|^{1-\varepsilon'}) \,.$$

Applications: Dynamical systems

Let $a, b > 1$ be integers $\log a / \log b \notin \mathbb{Q}$ (exm. $a = 2$, $b = 3$).

Theorem (Furstenberg, 1967)

The sequence

$$\{2^n 3^m \alpha\}_{n,m \in \mathbb{N}}$$

is dense in $[0, 1]$, provided α is irrational.

How dense are sets

$$\{a^n b^m \alpha \ : \ n, m \leq N\}, \quad \text{and}$$

$$\{a^n b^m \ : \ s \in S\}, \qquad S \subseteq \mathbb{Z}/N\mathbb{Z} \ ?$$

If the subgroup $\langle a, b \rangle$ in $\mathbb{Z}/N\mathbb{Z}$ has size N^{ε} and S is a, b invariant, then just S itself has no gaps of size N^{-c}.

Theorem (Bourgain, Lindenstrauss, Michel, Venkatesh, 2009)

Let $\alpha \in \mathbb{R}/\mathbb{Z}$ such that for some k one has $\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^k}$, $\forall q \geq 2$. Then the set

$$\{a^n b^m \alpha \ : \ n, m \leq N\}$$

is $(\log\log N)^{-\kappa\varepsilon/100}$–dense in $\mathbb{R}/\mathbb{Z}$ with $\kappa = \kappa(a, b, k) > 0$.

Theorem (Bourgain, Lindenstrauss, Michel, Venkatesh, 2009)

Let $S \subseteq \mathbb{Z}/N\mathbb{Z}$, $|S| > N^{\varepsilon}$. Then the set

$$\{k \cdot s \ : \ k = a^n b^m < N\,, s \in S\}$$

is $(\log\log N)^{-\kappa\varepsilon/100}$–dense.

Another consequence is the uniform distribution of Diffie–Hellman sequence (Bourgain, 2004)

$$(g^x, g^y, g^{xy}) \in \mathbb{F}_p^3 \,,$$

where $1 \le x, y \le p^\delta$.

Bourgain's *expander* map. If

$$x * y := x^2 + xy \,, \qquad x, y \in \mathbb{F}_p \,,$$

then for any $A, B \subseteq \mathbb{F}_p$, $|A| = |B|$

$$|A * B| = |\{a * b \ : \ a \in A,\, b \in B\}| \gg \min\{|A|^{1+\varepsilon}, p\} \,.$$

Bourgain (2005), Shkredov (2010).

Non–abelian problems

Addition and multiplication in $\mathrm{Aff}(\mathbb{F})$ (similarly in $\mathrm{SL}_2(\mathbb{F})$):

$$\begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 \\ 0 & 1 \end{pmatrix} = \mathbb{F}\,.$$

$$\begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} st & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{F}^* \setminus \{0\}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} aA + bC & aB + bD \\ cA + dC & cB + dD \end{pmatrix}\,.$$

The operation include both $+$ and $*$.

Growth in groups: given $A \subseteq \mathrm{G}$ what can we say about $f(n) = |A^n|$?

Growth in finite simple groups

Conjecture (Babai, 1992)

Let G be a finite simple group, $A \subseteq \mathrm{G}$ be a set and $\langle A \rangle = \mathrm{G}$. Then there is $n \ll (\log |\mathrm{G}| / \log |A|)^C$ such that $A^n = \mathrm{G}$.

Theorem (Helfgott, Breuillard–Green–Tao, Pyber–Szabó, 2008–2016)

Let G be a finite simple group of Lie type of rank r, $A \subseteq \mathrm{G}$ be a set and $\langle A \rangle = \mathrm{G}$. Then either $A^3 = \mathrm{G}$ or

$$\left|A^3\right| > |A|^{1+c(r)}.$$

In particular, $A^n = \mathrm{G}$ for

$$n \ll (\log |\mathrm{G}| / \log |A|)^{C(r)}.$$

An application of sum–product and growth in groups: Zaremba's conjecture

Let $\alpha \in [0,1]$. The continued fraction expansion for α is

$$\alpha = \cfrac{1}{c_1 + \cfrac{1}{c_2 + \dots}} = [c_1, c_2, \dots], \qquad c_j \in \mathbb{N}.$$

Conjecture (Zaremba, 1972)

Let q be a positive integer. Then there exists a, $(a,q) = 1$ such that

$$\frac{a}{q} = [c_1, c_2, \dots, c_s]$$

has all $c_j \leq \mathcal{M} = 5$.

It is known (Korobov, 1963) for $\mathcal{M} = O(\log q)$.

Motivation–I

Theorem (Koksma–Hlawka, 1961)

Let $f : [0,1]^d \to \mathbb{R}$ be a function of bounded variation $\mathrm{V}(f)$ and $X \subseteq [0,1]^d$ be a finite set. Then

$$\left| \int_{[0,1]^d} f(u)\, du - \frac{1}{|X|} \sum_{x \in X} f(x) \right| \le \mathrm{V}(f) \cdot \mathrm{Disc}(X)\,,$$

where

$$\mathrm{Disc}(X) := \sup_{R = \prod_{i=1}^{d} [a_i, b_i]} \left| \frac{|X \cap R|}{|X|} - \mu(R) \right| .$$

Theorem (Schmidt, 1972)

For any finite X one has $\mathrm{Disc}(X) \gg \frac{\log |X|}{|X|}$.

Motivation–II

Monte–Carlo gives $\mathrm{Disc}(X) \sim \frac{1}{|X|^{1/2}}$.

Now take winding of our two–dimensional torus

$$X = X(a,q) = \left\{ \left(\frac{j}{q}, \frac{aj}{q} \right) \right\}_{j=1}^{q} \subseteq [0,1]^2 .$$

Theorem (Zaremba, 1966)

Let $\frac{a}{q} = [c_1, \ldots, c_s]$ and $M = \max_{j \le s} c_j$. Then

$$\mathrm{Disc}(X(a,q)) \le \left(\frac{4M}{\log(M+1)} + \frac{4M+1}{\log q} \right) \frac{\log q}{q} .$$

For the constant M this bound is essentially best possible.

Theorem (Moshchevitin–Murphy–Shkredov, 2019)

For any prime p and $\varepsilon > 0$ there is $M = M(\varepsilon)$ and $1 \le a < p$ s.t.

$$\frac{a}{p} = [c_1, \dots, c_s], \quad c_j \le M, \quad \forall j \notin \left(\frac{1}{2} - \varepsilon, \frac{1}{2} + \varepsilon\right) \cdot s\,.$$

Theorem: modular form of Zaremba's conjecture (Shkredov, 2020)

Let $\epsilon \in (0, 1]$. There exists $M = M(\epsilon)$ s.t. for any prime p there is

$$q = O(p^{1+\epsilon}), \qquad q \equiv 0 \pmod{p}$$

with a, $(a, q) = 1$ s.t.

$$\frac{a}{q} = [c_1, \dots, c_s], \quad c_j \le M\,.$$

Zaremba's conjecture: ideas of the proof

Let $\frac{a}{p} = [c_1, c_2, \ldots, c_s]$ and $\frac{p_n}{q_n} = [c_1, c_2, \ldots, c_n]$, $c_j \leq M$. Then

$$aq_{s-1} - p_{s-1}p = p_s q_{s-1} - p_{s-1}q_s = \pm 1$$

that is $\pm q_{s-1} \equiv a^{-1} \pmod{p}$.

Kloosterman sums is an analytical instrument to find inverse in $\mathbb{F}_p$.

Our combinatorial instrument: *growth in* $\mathrm{SL}_2(\mathbb{F}_p)$

$$\begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} \ldots \begin{pmatrix} 0 & 1 \\ 1 & c_s \end{pmatrix} = \begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix} \in \pm A \subset \mathrm{SL}_2(\mathbb{F}_p)$$

under the assumptions

$$c_j \leq M \qquad \text{and} \qquad q_s < p\,.$$

By Hensley's lemma we know size of A

$$|A| \sim p^{2w_M} = p^{2-O(1/M)}\,.$$

Growth of $A^n \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ corresponds to the Zaremba question.

Pre–result on the limit set of Fuchsian groups.

Theorem (Hensley, 1989–1992)

For any M

$$w_M := \mathcal{HD}\left(\{\alpha = [c_1, c_2, \dots] \in [0,1] \ : \ \forall c_j \le M\}\right) =$$

$$= 1 - \frac{6}{\pi^2 M} - \frac{72 \log M}{\pi^4 M^2} + O\left(\frac{1}{M^2}\right), \qquad M \to \infty .$$

$$w_2 = 0.531280506277205141624468 6\ldots > \frac{1}{2}$$

Thus $w_M = 1 - O(1/M)$, $M \to \infty$ (Khinchin).

Thank you for your attention!