

Arithmetic progressions in primes

Alex Gorodnik
CalTech

Lake Arrowhead, September 2006

Introduction

Theorem (Green, Tao)

Let $A \subset \mathcal{P} := \{\text{primes}\}$ such that

$$\limsup_{N \rightarrow \infty} \frac{|A \cap [1, N]|}{|\mathcal{P} \cap [1, N]|} > 0.$$

Then for any $k \in \mathbb{N}$,

$$\{a, a + d, \dots, a + (k - 1)d\} \subset A$$

for some $a, d \in \mathbb{N}$.

Previous results

Van der Corput showed in $(k = 3)$ -case that

$$\#\{a, d \in [1, N] : a, a + d, a + 2d \in \mathcal{P}\} \sim \gamma_3 \cdot \frac{N^2}{(\log N)^3}$$

Conjecture (Hardy, Littlewood)

$$\#\{a, d \in [1, N] : a, a + d, \dots, a + (k - 1)d \in \mathcal{P}\} \sim \gamma_k \cdot \frac{N^2}{(\log N)^k}$$

for explicit $\gamma_k > 0$.

Compare with a random subset of $[1, N]$ of density $\frac{1}{\log N}$.

Green-Tao proof gives a lower estimate $\gamma'_k \cdot \frac{N^2}{(\log N)^k}$
for small $\gamma'_k > 0$.

Conjecture (Erdős, Turán)

Every set $A \subset \mathbb{N}$ such that

$$\sum_{a \in A} \frac{1}{a} = \infty$$

contains arbitrary long arithmetic progressions.

Szemerédi Theorem

Theorem (Szemerédi)

Let $A \subset \mathbb{N}$ such that

$$\limsup_{N \rightarrow \infty} \frac{1}{N} |A \cap [1, N]| > 0.$$

Then for any $k \in \mathbb{N}$,

$$\{a, a + d, \dots, a + (k - 1)d\} \subset A$$

for some $a, d \in \mathbb{N}$.

Note that

$$|\mathcal{P} \cap [1, N]| \sim \frac{N}{\log N} \quad \text{as } N \rightarrow \infty.$$

Almost primes

$$\mathcal{P}_R := \{\text{numbers with all prime factors } \geq R\}.$$

Then for $R = N^\alpha$ with small $\alpha > 0$,

▶ $\mathcal{P}_R \cap [1, N]$ contains arbitrary long AP as $N \rightarrow \infty$.

▶

$$\limsup_{N \rightarrow \infty} \frac{|\mathcal{P} \cap [1, N]|}{|\mathcal{P}_R \cap [1, N]|} > 0.$$

Naive Strategy: Prove an analog of Szemerédi theorem for subsets of almost primes (**relative Szemerédi theorem**).

Effective Szemerédi theorem

Theorem

Given $k \geq 3$ and $\delta > 0$, there exists $N_0 = N_0(k, \delta) > 0$ such that for every $N > N_0$ and every $A \subset [1, N]$ with $|A| > \delta N$, the set A contains an arithmetic progression of length k .

- ▶ Upper estimate (Bourgain): $N_0(3, \delta) \leq \exp(\delta^{-2} \log(1/\delta))$.
- ▶ Upper estimate (Gowers): $N_0(k, \delta) \leq \exp(e^{\delta^{-c_k}})$.
- ▶ Lower estimate (Rankin): $N_0(k, \delta) \geq \exp(\log(1/\delta)^{d_k})$.
- ▶ Expected: $N_0(k, \delta) \leq \exp(c'_k \delta^{-1}) \Rightarrow$ AP in primes.

Szemerédi Theorem (other formulation)

\mathbb{Z}_N = the field of residues mod N ,

$$\mathbb{E}(f(x) | x \in A) = \frac{1}{|A|} \sum_{x \in A} f(x)$$

Theorem (Szemerédi)

Given $k \geq 3$ and $\delta > 0$, there exists $c = c(k, \delta) > 0$ such that for a function $f : \mathbb{Z}_N \rightarrow \mathbb{R}$ satisfying

$$0 \leq f \leq 1 \text{ and } \mathbb{E}(f) \geq \delta,$$

we have

$$\mathbb{E}(f(x)f(x+r) \cdots f(x+(k-1)r) | x, r \in \mathbb{Z}_N) \geq c$$

for sufficiently large N .

Relative Szemerédi Theorem

Theorem (Green, Tao)

Fix $k \geq 3$ and $\delta > 0$,

$\nu : \mathbb{Z}_N \rightarrow \mathbb{R}^+$ be a **k -pseudorandom** function with $\mathbb{E}(\nu) = 1 + o(1)$.

Then for any function $f : \mathbb{Z}_N \rightarrow \mathbb{R}^+$ satisfying

$$0 \leq f \leq \nu \text{ and } \mathbb{E}(f) \geq \delta,$$

we have

$$\mathbb{E}(f(x)f(x+r) \cdots f(x+(k-1)r) | x, r \in \mathbb{Z}_N) \geq c(k, \delta) - o_{k, \delta}(1)$$

as $N \rightarrow \infty$.

Pseudorandom function is defined to satisfy

- ▶ linear form condition,
- ▶ correlation condition.

Linear form condition

A function $\nu : \mathbb{Z}_N \rightarrow \mathbb{R}^+$ is called a **measure** if

$$\mathbb{E}(\nu) = 1 + o(1).$$

A measure ν satisfies **(m_0, t_0, L_0) -linear form condition** if for any $m \leq m_0$, $t \leq t_0$, and linear forms

$$\psi_i(x) = \sum_{j=1}^t L_{ij}x_j + b_i, \quad i = 1, \dots, m,$$

where L_{ij} are rationals (assume N is prime) with the numerator/denominator bounded by L_0 and the t -tuples $(L_{ij}; j = 1, \dots, t)$ are not zero and not rational multiples of each other and $b \in \mathbb{Z}_N$, we have

$$\mathbb{E}(\nu(\psi_1(x)) \cdots \nu(\psi_m(x)) | x \in \mathbb{Z}_N^t) = 1 + o_{m_0, t_0, L_0}(1).$$

Hardy-Littlewood conjecture

Linear form condition roughly says that the events

“ $\psi_j(x)$ is almost prime”

are essentially independent. This is the Hardy-Littlewood prime tuples conjecture. Define

$$\Lambda(n) = \begin{cases} \log p & \text{for } n = p^k, \\ 0 & \text{otherwise,} \end{cases}$$

Note that $\mathbb{E}(\Lambda) = 1 + o(1)$.

Conjecture (Hardy-Littlewood)

Assuming that L_{ij} and b_i are positive,

$$\mathbb{E}(\Lambda(\psi_1(x)) \cdots \Lambda(\psi_m(x)) | x \in \mathbb{Z}_N^t) = \alpha + o_{m_0, t_0, L_0}(1)$$

for explicit $\alpha = \alpha(\psi_1, \dots, \psi_m) > 0$.

Correlation condition

A measure ν satisfies **m_0 -correlation condition**

if for every $m = 2, \dots, m_0$,

there exists a function $\tau = \tau_m : \mathbb{Z}_N \rightarrow \mathbb{R}^+$ such that

$$\mathbb{E}(\tau^q) = O_{m,q}(1) \quad \text{for all } q \geq 1$$

and

$$\mathbb{E}(\nu(x + h_1) \cdots \nu(x + h_m) | x \in \mathbb{Z}_N) \leq \sum_{1 \leq i < j \leq m} \tau(h_i - h_j)$$

for all $h_1, \dots, h_m \in \mathbb{Z}_N$.

A measure ν is called **k -pseudorandom** if it satisfies $(k2^{k-1}, 3k - 4, k)$ -linear form condition and 2^{k-1} -correlation condition.

Relative Szemerédi Theorem

Theorem (Green, Tao)

Fix $k \geq 3$ and $\delta > 0$, and let ν be a k -pseudorandom measure. Then for any function $f : \mathbb{Z}_N \rightarrow \mathbb{R}^+$ satisfying

$$0 \leq f \leq \nu \text{ and } \mathbb{E}(f) \geq \delta,$$

we have

$$\mathbb{E}(f(x)f(x+r) \cdots f(x+(k-1)r) | x, r \in \mathbb{Z}_N) \geq c(k, \delta) - o_{k, \delta}(1)$$

as $N \rightarrow \infty$.

Finitary ergodic theory

$$(X, \mu, T) \iff (\mathbb{Z}_N, \text{uniform measure}, x \mapsto x + 1).$$

We are interested in averages

$$\mathbb{E}(f_0(x) T^i f_1(x) \cdots T^{(k-1)i} f_{k-1}(x) | x, i \in \mathbb{Z}_N)$$

as $N \rightarrow \infty$.

For a probability measure preserving system (X, μ, T) , the **Koopman–von-Neumann decomposition** is

$$L^2(X) = \{\text{weakly mixing}\} \oplus \{\text{compact (almost periodic)}\}.$$

is used in the proof of Furstenberg's multiple recurrence.

A finitary analog of Koopman–von-Neumann decomposition is crucial in the proof of relative Szemerédi theorem.

Sketch of the proof (step 1)

The crucial step is to show:

“Koopman–von-Neumann decomposition” : $f = f_U + f_{U^\perp} + E$

with the **error term** E satisfying $\mathbb{E}(E) = o(1)$, and

$$E \geq 0, \quad f_U + f_{U^\perp} \geq 0.$$

Then

$$\begin{aligned} & \mathbb{E}(f(x) \cdots f(x + (k-1)r) | x, r \in \mathbb{Z}_N) \\ & \geq \mathbb{E}((f_U + f_{U^\perp})(x) \cdots (f_U + f_{U^\perp})(x + (k-1)r) | x, r \in \mathbb{Z}_N). \end{aligned}$$

The function f_U is **uniform (weakly mixing)** component of f :

$$\begin{aligned} & \mathbb{E}(f_U) = o(1), \\ & \mathbb{E}(f_0(x) f_1(x+r) \cdots f_{k-1}(x+(k-1)r) | x, r \in \mathbb{Z}_N) \text{ is small,} \end{aligned}$$

where each f_i is either f_U or f_{U^\perp} , and $f_i \neq f_{U^\perp}$ for some i .

Sketch of the proof (step 2)

It suffices to prove a lower estimate for

$$\mathbb{E}(f_{U^\perp}(x) f_{U^\perp}(x+r) \cdots f_{U^\perp}(x+(k-1)r) | x, r \in \mathbb{Z}_N) \geq ?.$$

The **antiuniform (almost periodic)** component f_{U^\perp} satisfies

$$0 \leq f_{U^\perp} \leq 1 + o(1).$$

Hence, the lower estimate follows from the classical Szemerédi theorem.

Gowers uniformity norms

These norms are used to control multiple averages.

Lemma (Van der Corput)

For $f : \mathbb{Z}_N \rightarrow \mathbb{R}$,

$$|\mathbb{E}(f)|^2 = \mathbb{E}(\mathbb{E}(f \cdot T^h f) | h \in \mathbb{Z}_N).$$

Gowers uniformity norms are defined inductively:

$$\|f\|_{U^1} = |\mathbb{E}(f)|,$$

$$\|f\|_{U^k} = \mathbb{E}(\|f \cdot T^h f\|_{U^{k-1}}^{2^{k-1}} | h \in \mathbb{Z}_N)^{1/2^k}.$$

or equivalently,

$$\|f\|_{U^d} = \mathbb{E} \left(\prod_{\omega \in \{0,1\}^d} f(x + \omega h) \mid x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^d \right)^{1/2^d}.$$

Gowers uniformity norms

For a family of functions f_ω , $\omega \in \{0,1\}^d$, we define **d -dimensional Gowers inner product**:

$$\langle (f_\omega)_{\omega \in \{0,1\}^d} \rangle_{U^d} = \mathbb{E} \left(\prod_{\omega \in \{0,1\}^d} f_\omega(x + \omega h) \mid x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^d \right).$$

Then we have **Gowers Cauchy-Schwartz inequality**:

$$|\langle (f_\omega)_{\omega \in \{0,1\}^d} \rangle_{U^d}| \leq \prod_{\omega \in \{0,1\}^d} \|f_\omega\|_{U^d}.$$

Generalized von Neumann theorem

Theorem

For a k -pseudorandom measure $\nu : \mathbb{Z}_N \rightarrow \mathbb{R}^+$,

$\lambda_0, \dots, \lambda_{k-1} \in \mathbb{Z}$, $\lambda_i \neq \lambda_j$,

functions $f_0, \dots, f_{k-1} : \mathbb{Z}_N \rightarrow \mathbb{R}$ such that $|f_i| \leq \nu + 1$, we have

$$\mathbb{E} \left(\prod_{i=0}^{k-1} f_i(x + \lambda_i h) \mid x, h \in \mathbb{Z}_N \right) = O \left(\min_{0 \leq i \leq k-1} \|f_i\|_{U^{k-1}} \right) + o(1).$$