M 392C: Dynamical Systems - The Green-Tao Theorem

Aaron Benda

April 2026

1 The Main Statement

The purpose of this talk is to outline the approach to Ben Green and Terrence Tao's proof of arithmetic progressions in the primes. In particular, we wish to emphasize the inspiration from ergodic theory, and generally the manner in which their work interacts with the field.

First, the main statement:

Theorem 1.1: Green-Tao

The prime numbers contain infinitely many arithmetic progressions of length k for all $k \in \mathbb{N}$.

In fact, the conclusion holds for any subset of primes of positive relative upper density.

2 Szemerédi's Theorem and Multiple Recurrence

The starting point for the approach of Green-Tao is Szemerédi's Theorem.

Theorem 2.1: Szemerédi's Theorem

Suppose $A \subseteq \mathbb{N}$ has positive upper density, i.e.

$$d^*(A) = \limsup_{N\to\infty} \frac{1}{N} |A \cap [1, N]| > 0.$$

Then for any $k \in \mathbb{N}$, A contains an arithmetic progression of length k (in fact, infinitely many such progressions).

The connection to ergodic theory comes through Furstenberg's multiple recurrence theorem:

Theorem 2.2: Multiple Recurrence

Suppose (X, μ, T) is a pmp system, and $k \in \mathbb{N}$. For any measurable $E \subseteq X$ with $\mu(E) > 0$, we have

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu(E \cap T^{-n}E \cap ... \cap T^{-(k-1)n}E) > 0.$$

This is because of the following correspondence principle:

Theorem 2.3: Correspondence Principle

Suppose $A \subseteq \mathbb{N}$ has positive upper density. There is a pmp system (X, μ, T) and measurable $E \subseteq X$ with $\mu(E) = d^*(A)$ such that for any $k \in \mathbb{N}$ and integers $m_1, ...m_{k-1} \geq 1$,

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

3 Reformulated and Relative Szemerédi Theorem

Another forumlation in $\mathbb{Z}/N\mathbb{Z}$:

Theorem 3.1: Finite Szemerédi

Let $N \in \mathbb{N}$, $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$. Fix $\delta > 0$, and $k \geq 3$. There is some minimal $N_0(\delta, k) < \infty$ such that: If $N \geq N_0(\delta, k)$ and $A \subseteq \mathbb{Z}_N$ with $|A| \geq \delta N$, then A contains an arithmetic progression of length k.
Another way to say this: if $0 \leq f \leq 1$ (imagine an indicator function), then whenever

$$\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N) \geq \delta,$$

we must have

$$(\star) \quad \mathbb{E}(f(x)f(x+r)\dots f(x+(k-1)r) \mid x, r \in \mathbb{Z}_N) \geq c(k, \delta) - o_{k,\delta}(1).$$

Importantly, the constant at the end does not depend on f or N. This is actually true for any function with expectation at least δ which remains bounded.

The key is to study the equation $(\star)$ for the indicator function of the primes. This is too hard to do directly, so Green-Tao use some more analytically convenient functions that enable them to draw the same conclusion.

The kind of functions they have to work with:

Definition 3.2: Pseudorandom measures

A function $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ is called a **measure** if $\mathbb{E}(\nu) = 1 + o(1)$. (Note: it is not a measure in the traditional sense, and Green-Tao comment a more appropriate name might be *normalized probability density*.)
A measure is called **pseudorandom** if it satisfies the *linear forms condition* and the *correlation condition*.

They then construct a pseudorandom measure which majorizes (a modified version of) the von Mangoldt function:

$$\Lambda(p^k) = \log(p), \quad \text{otherwise} \quad \Lambda(n) = 0.$$

Linear forms and correlation conditions for the measure ν:

1. Linear forms condition: pick at most m_0 linear forms $\psi_i : \mathbb{Z}_N^t \to \mathbb{Z}_n$ with rational coefficients (denominators bounded by L_0) and $t \leq t_0$. Then

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

2. Correlation condition: let $m_0 \in \mathbb{N}$, and that there exist $\tau_m : \mathbb{Z}_N \to \mathbb{R}^+$ satisfying $\mathbb{E}(\tau^q) = O_{m,q}(1)$ for which

$$\mathbb{E}(\nu(x+h_1) \dots \nu(x+h_m)) \leq \sum_{1 \leq i < j \leq m} \tau(h_i - h_j).$$

These conditions are designed to be inspired by the ergodic-theoretic notion of weak mixing.

4 Gowers Norms

The following are called *Gowers uniformity norms* in combinators and ergodic theory.

Definition 4.1: Two approaches

Let $f : \mathbb{Z}_N \to \mathbb{C}$ be given. Define $\|f\|_{U^1} = |\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N)|$. Then, inductively, set

$$\|f\|_{U^d} = \mathbb{E}(\|\overline{f(x)} f(x+h)\|_{U^{d-1}}^{2^{d-1}} \mid h \in \mathbb{Z}_N)^{1/2^d}.$$

Instead now, suppose (X, μ, T) is a pmp system, and for $f \in L^\infty(\mu)$ define $\|f\|_{U^1} = |\int f d\mu|$. Then, inductively, set

$$\|f\|_{U^d}^{2^d} = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \|f \overline{T^n f}\|_{U^{d-1}}^{2^{d-1}}.$$

Gowers norms are supposed to be a measure of randomness, and there is a so-called *anti-uniform/dual* norm which is designed to measure structure. For general f, the resulting decompositon looks something like

Weakly mixing part: $f - \mathbb{E}(f \mid \mathcal{B})$ and almost periodic part: $\mathbb{E}(f \mid \mathcal{B})$.

An important component of the Green-Tao approach is to decompose functions according to this randomness versus structure. In particular, a lack of Gowers uniformity implies correlation.

Now, from the point of view of Gowers norms, pseudorandom functions are those close to 1.

Lemma 4.2

Suppose that ν is k-pseudorandom, then

$$\|\nu - 1\|_{U^d} = o(1)$$

for all $1 \leq d \leq k-1$.

5 Their Approach

The main theorem that Green-Tao actually establish to enable the proof:

Theorem 5.1: Relative Szemerédi

Fix $k \geq 3$ and $0 < \delta \leq 1$. Suppose $\nu : \mathbb{Z}_N \to \mathbb{R}^+$ is k-pseudorandom. Suppose $f : \mathbb{Z}_N \to \mathbb{R}^+$ is any nonnegative function obeying $0 \leq f(x) \leq \nu(x)$ and $\mathbb{E}(f) \geq \delta$. Then

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

Their work proceeds by constructing a pseudorandom measure which majorizes their modified von Mangoldt function, which in turn enables them to conclude the desired result.

One other way to phrase a general relative Szemeredi theorem:

Theorem 5.2: Conlon-Fox-Zhao

For every natural number $k \geq 3$ and every $\delta > 0$, if $S \subseteq \mathbb{Z}_N$ satisfies the k-linear forms condition and N is sufficiently large, then any subset of S of relative density at least δ contains an arithmetic progression of length k.