Graph Theory and Additive Combinatorics

Lecturer: Prof. Yufei Zhao

1
Introduction

1.1 Schur's theorem

In the 1910's, Schur attempted to prove Fermat's Last Theorem by reducing the equation $X^n + Y^n = Z^n$ modulo a prime p. However, he was unsuccessful. It turns out that, for every positive integer n, the equation has nontrivial solutions mod p for all sufficiently large primes p, which Schur established by proving the following classic result.

Schur (1916)

Theorem 1.1 (Schur's theorem)**.** *If the positive integers are colored with finitely many colors, then there is always a monochromatic solution to $x + y = z$ (i.e., x, y, z all have the same color).*

We will prove Schur's theorem shortly. But first, let us show how to deduce the existence of solutions to $X^n + Y^n \equiv Z^n \pmod{p}$ using Schur's theorem.

Schur's theorem is stated above in its "infinitary" (or qualitative) form. It is equivalent to a "finitary" (or quantitative) formulation below.

We write $[N] := \{1, 2, \ldots, N\}$.

Theorem 1.2 (Schur's theorem, finitary version)**.** *For every positive integer r, there exists a positive integer $N = N(r)$ such that if the elements of $[N]$ are colored with r colors, then there is a monochromatic solution to $x + y = z$ with $x, y, z \in [N]$.*

With the finitary version, we can also ask quantitative questions such as how big does $N(r)$ have to be as a function of r. For most questions of this type, we do not know the answer, even approximately.

Let us show that the two formulations, Theorem 1.1 and Theorem 1.2, are equivalent. It is clear that the finitary version of Schur's theorem implies the infinitary version. To see that the infinitary version implies the finitary version, fix r, and suppose that for every

N there is some coloring $\phi_N\colon [N] \to [r]$ that avoids monochromatic solutions to $x + y = z$. We can take an infinite subsequence of (ϕ_N) such that, for every $k \in \mathbb{N}$, the value of $\phi_N(k)$ stabilizes as N increases along this subsequence. Then the ϕ_N's, along this subsequence, converges pointwise to some coloring $\phi\colon \mathbb{N} \to [r]$ avoiding monochromatic solutions to $x + y = z$, but this contradicts the infinitary statement.

Let us now deduce Schur's claim about $X^n + Y^n \equiv Z^n \pmod p$.

Theorem 1.3. *Let n be a positive integer. For all sufficiently large primes p, there are $X, Y, Z \in \{1, \dots, p-1\}$ such that $X^n + Y^n \equiv Z^n \pmod p$.*

Schur (1916)

Proof of Theorem 1.3 assuming Schur's theorem (Theorem 1.2). We write $(\mathbb{Z}/p\mathbb{Z})^\times$ for the group of nonzero residues mod p under multiplication. Let H be the subgroup of n-th powers in $(\mathbb{Z}/p\mathbb{Z})^\times$. The index of H in $(\mathbb{Z}/p\mathbb{Z})^\times$ is at most n. So the cosets of H partition $\{1, 2, \dots, p-1\}$ into at most n sets. By the finitary statement of Schur's theorem (Theorem 1.2), for p large enough, there is a solution to

$$x + y = z \quad \text{in } \mathbb{Z}$$

in one of the cosets of H, say aH for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Since H consists of n-th powers, we have $x = aX^n$, $y = aY^n$, and $z = aZ^n$ for some $X, Y, Z \in (\mathbb{Z}/p\mathbb{Z})^\times$. Thus

$$aX^n + aY^n \equiv aZ^n \pmod p.$$

Hence

$$X^n + Y^n \equiv Z^n \pmod p$$

as desired. □

Now let us prove Theorem 1.2 by deducing it from a similar sounding result about coloring the edges of a complete graph. The next result is a special case of Ramsey's theorem.

Theorem 1.4. *For every positive integer r, there is some integer $N = N(r)$ such that if the edges of K_N, the complete graph on N vertices, are colored with r colors, then there is always a monochromatic triangle.*

Ramsey (1929)

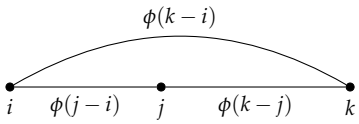
FRANK RAMSEY (1903–1930) had made major contributions to mathematical logic, philosophy, and economics, before his untimely death at age 26 after suffering from chronic liver problems.

Proof. We use induction on r. Clearly $N(1) = 3$ works for $r = 1$. Let $r \geq 2$ and suppose that the claim holds for $r - 1$ colors with $N = N'$. We will prove that taking $N = r(N' - 1) + 2$ works for r colors..

Suppose we color the edges of a complete graph on $r(N' - 1) + 2$ vertices using r colors. Pick an arbitrary vertex v. Of the $r(N' - 1) + 1$ edges incident to v, by the pigeonhole principle, at least N' edges incident to v have the same color, say red. Let V_0 be the vertices joined to v by a red edge. If there is a red edge inside V_0, we obtain a red

triangle. Otherwise, there are at most $r-1$ colors appearing among $|V_0| \geq N'$ vertices, and we have a monochromatic triangle by induction. □

We are now ready to prove Schur's theorem by setting up a graph whose triangles correspond to solutions to $x+y=z$, thereby allowing us to "transfer" the above result to the integers.



Proof of Schur's theorem (Theorem 1.2). Let $\phi\colon [N] \to [r]$ be a coloring. Color the edges of a complete graph with vertices $\{1, \dots, N+1\}$ by giving the edge $\{i,j\}$ with $i<j$ the color $\phi(j-i)$. By Theorem 1.4, if N is large enough, then there is a monochromatic triangle, say on vertices $i<j<k$. So $\phi(j-i) = \phi(k-j) = \phi(k-i)$. Take $x=j-i$, $y=k-j$, and $z=k-i$. Then $\phi(x)=\phi(y)=\phi(z)$ and $x+y=z$, as desired. □

Notice how we solved a number theory problem by moving over to a graph theoretic setup. The Ramsey theorem argument in Theorem 1.4 is difficult to do directly inside the integers. Thus we gained greater flexibility by considering graphs. Later on we will see other more sophisticated examples of this idea, where taking a number theoretic problem to the land of graph theory gives us a new perspective.

1.2 *Highlights from additive combinatorics*

Schur's theorem above is one of the earliest examples of an area now known as ***additive combinatorics***, which is a term coined by Terry Tao in the early 2000's to describe a rapidly growing body of mathematics motivated by simple-to-state questions about addition and multiplication of integers. The problems and methods in additive combinatorics are deep and far-reaching, connecting many different areas of mathematics such as graph theory, harmonic analysis, ergodic theory, discrete geometry, and model theory. The rest of this section highlights some important developments in additive combinatorics in the past century.

Green (2009)

In the 1920's, van der Waerden proved the following result about monochromatic arithmetic progressions in the integers.

Theorem 1.5 (van der Waerden's theorem)**.** *If the integers are colored with finitely many colors, then one of the color classes must contain arbitrarily long arithmetic progressions.*

B. L. van der Waerden, Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk.* **15**, 212–216, 1927.

Remark 1.6. Having arbitrarily long arithmetic progressions is very different from having infinitely long arithmetic progressions. As an exercise, show that one can color the integers using just two colors so

that there are no infinitely long monochromatic arithmetic progressions.

In the 1930's, Erdős and Turán conjectured a stronger statement, that any subset of the integers with positive density contains arbitrarily long arithmetic progressions. To be precise, we say that $A \subseteq \mathbb{Z}$ has ***positive upper density*** if

$$\limsup_{N\to\infty} \frac{|A \cap \{-N, \dots, N\}|}{2N+1} > 0.$$

(There are several variations of this definition—the exact formulation is not crucial.)

Erdős and Turán (1936)

In the 1950's, Roth proved the conjecture for 3-term arithmetic progression using Fourier analytic methods. In the 1970's, Szemerédi fully settled the conjecture using combinatorial techniques. These are landmark theorems in the field. Much of what we will discuss are motivated by these results and the developments around them.

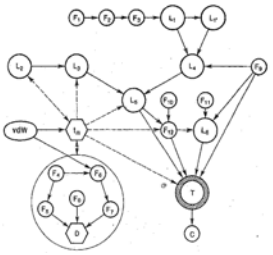
ENDRE SZEMERÉDI (1940–) received the prestigious Abel Prize in 2012 "for his fundamental contributions to discrete mathematics and theoretical computer science, and in recognition of the profound and lasting impact of these contributions on additive number theory and ergodic theory."

Theorem 1.7 (Roth's theorem)**.** *Every subset of the integers with positive upper density contains a 3-term arithmetic progression.*

Roth (1953)

Theorem 1.8 (Szemerédi's theorem)**.** *Every subset of the integers with positive upper density contains arbitrarily long arithmetic progressions.*

Szemerédi (1975)



Szemerédi's proof was a combinatorial tour de force. This figures is taken from the introduction of his paper showing the logical dependencies of his argument.

Szemerédi's theorem is deep and intricate. This important work led to many subsequent developments in additive combinatorics. Several different proofs of Szemerédi's theorem have since been discovered, and some of them have blossomed into rich areas of mathematical research. Here are some the most influential modern proofs of Szemerédi's theorem (in historical order):

- The ergodic theoretic approach (Furstenberg)
- Higher-order Fourier analysis (Gowers)
- Hypergraph regularity lemma (Rödl et al./Gowers)

Furstenberg (1977)

Gowers (2001)

Rödl et al. (2005)

Gowers (2007)

Another modern proof of Szemerédi's theorem results from the *density Hales–Jewett theorem*, which was originally proved by Furstenberg and Katznelson using ergodic theory, and subsequently a new combinatorial proof was found in the first successful Polymath Project, an online collaborative project initiated by Gowers.

Furstenberg and Katznelson (1991)

Polymath (2012)

All subsequent Polymath Project papers are written under the pseudonym D. H. J. Polymath, whose initials stand for "density Hales–Jewett."

The relationships between these disparate approaches are not yet completely understood, and there are many open problems, especially regarding quantitative bounds. A unifying theme underlying all known approaches to Szemerédi's theorem is the ***dichotomy between structure and pseudorandomness***. We will later see different

Tao (2007)

facets of this dichotomy both in the context of graph theory as well as in number theory.

Here are a few other important subsequent developments to Szemerédi's theorem.

Instead of working over subsets of integers, let us consider subsets of a higher dimensional lattice $\mathbb{Z}^d$. We say that $A \subset \mathbb{Z}^d$ has positive upper density if

$$\limsup_{N\to\infty} \frac{|A \cap [-N, N]^d|}{(2N+1)^d} > 0$$

(as before, other similar definitions are possible). We say that A ***contains arbitrary constellations*** if for every finite set $F \subset \mathbb{Z}^d$, there is some $a \in \mathbb{Z}^d$ and $t \in \mathbb{Z}_{>0}$ such that $a + t \cdot F = \{a + tx : x \in F\}$ is contained in A. In other words, A contains every finite pattern, each consisting of some finite subset of the integer grid allowing dilation and translation. The following multidimensional generalization of Szemerédi's theorem was proved by Furstenberg and Katznelson initially using ergodic theory, though a combinatorial proof was later discovered as a consequence of the hypergraph regularity method mentioned earlier.

Theorem 1.9 (Multidimensional Szemerédi theorem)**.** *Every subset of $\mathbb{Z}^d$ of positive upper density contains arbitrary constellations.*

Furstenberg and Katznelson (1978)

For example, the theorem implies that every subset of $\mathbb{Z}^d$ of positive upper density contains a 10×10 set of points that form an axis-aligned square grid.

There is also a polynomial extension of Szemerédi's theorem. Let us first state a special case, originally conjectured by Lovász and proved independently by Furstenberg and Sárkőzy.

Theorem 1.10. *Any subset of the integers with positive upper density contains two numbers differing by a square.*

Furstenberg (1977)
Sárközy (1978)

In other words, the set always contains $\{x, x + y^2\}$ for some $x \in \mathbb{Z}$ and $y \in \mathbb{Z}_{>0}$. What about other polynomial patterns? The following polynomial generalization was proved by Bergelson and Leibman.

Theorem 1.11 (Polynomial Szemerédi theorem)**.** *Suppose $A \subset \mathbb{Z}$ has positive upper density. If $P_1, \dots, P_k \in \mathbb{Z}[X]$ are polynomials with $P_1(0) = \cdots = P_k(0) = 0$, then there exist $x \in \mathbb{Z}$ and $y \in \mathbb{Z}_{>0}$ such that $x + P_1(y), \dots, x + P_k(y) \in A$.*

Bergelson and Leibman (1996)

We leave it as an exercise to formulate a common extension of the above two theorems (i.e., a multidimensional polynomial Szemerédi theorem). Such a theorem was also proved by Bergelson and Leibman.

We will not cover the proof of Theorems 1.9 and 1.11. In fact, currently the only known general proof of the polynomial Szemerédi theorem uses ergodic theory, though for special cases there are some recent exciting developments. Peluse (2019+)

Building on Szemerédi's theorem as well as other important developments in number theory, Green and Tao proved their famous theorem that settled an old folklore conjecture about prime numbers. Their theorem is considered one of the most celebrated mathematical results this century.

Theorem 1.12 (Green–Tao theorem)**.** *The primes contain arbitrarily long arithmetic progressions.* Green and Tao (2008)

We will discuss many central ideas behind the proof of the Green–Tao theorem. See the reference on the right for a modern exposition of the Green–Tao theorem emphasizing the graph theoretic perspective, and incorporating some simplifications of the proof that have been found since the original work. Conlon, Fox, and Zhao (2014)

1.3 What's next?

One of our goals is to understand two different proofs of Roth's theorem, which can be rephrased as:

Theorem 1.13 (Roth's theorem)**.** *Every subset of $[N]$ that does not contain 3-term arithmetic progressions has size $o(N)$.*

Roth originally proved his result using Fourier analytic techniques, which we will see in the second half of this book. In the 1970's, leading up to Szemerédi's proof of his landmark result, Szemerédi developed an important tool known as the ***graph regularity lemma***. Szemerédi (1978)

Ruzsa and Szemerédi used the graph regularity lemma to give a new graph theoretic proof of Roth's theorem. One of our first goals is to understand this graph theoretic proof. Ruzsa and Szemerédi (1978)

As in the proof of Schur's theorem, we will formulate a graph theoretic problem whose solution implies Roth's theorem. This topic fits nicely in an area of combinatorics called ***extremal graph theory***. A starting point (historically and also pedagogically) in extremal graph theory is the following question:

Question 1.14. What is the maximum number of edges in a triangle-free graph on n vertices?

This question is relatively easy, and it was answered by Mantel in the early 1900's (and subsequently rediscovered and generalized by Turán). It will be the first result that we shall prove next. However, even though it sounds similar to Roth's theorem, it cannot be used to

deduce Roth's theorem. Later on, we will construct a graph that corresponds to Roth's theorem, and it turns out that the right question to ask is:

Question 1.15. What is the maximum number of edges in an n-vertex graph where every edge is contained in a unique triangle?

This innocent looking question turns out to be incredible mysterious. We are still far from knowing the truth. We will later prove, using Szemerédi's regularity lemma, that any such graph must have $o(n^2)$ edges, and we will then deduce Roth's theorem from this graph theoretic claim.

18.217 Graph Theory and Additive Combinatorics

Fall 2019