

OVERVIEW AND OUTLINE

Arithmetic combinatorics is the study of finite subsets of abelian groups and rings. For example, let $A, B \subseteq \mathbb{Z}$ be finite, non-empty subsets of the integers. What can we say about the following sets?

$$\begin{aligned} A + B &= \{a + b \mid a \in A, b \in B\} \\ A - B &= \{a - b \mid a \in A, b \in B\} \\ A \cdot B &= \{ab \mid a \in A, b \in B\} \end{aligned}$$

Our main goal is to prove from first principles a recent theorem of Jean Bourgain, Nets Katz, and Terry Tao on the growth of subsets in finite fields of prime order (see [1]):

Theorem 0.1 (BKT). *Let $\delta > 0$ be given. Then there exist constants $c = c(\delta) > 0$ and $\varepsilon = \varepsilon(\delta) > 0$ (depending only on δ) such that for any prime p and any subset $A \subseteq F := \mathbb{Z}/p\mathbb{Z}$ with $|F|^\delta < |A| < |F|^{1-\delta}$, we have*

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{1+\varepsilon}$$

Since a subring S of a ring R has the property that $|S + S| = |S|$ and $|S \cdot S| = |S|$, we can restate the conclusion of the theorem in the following way. In general, if $A, B \subseteq Z$ are subsets of some abelian group, then we will let $|A| \lesssim |B|$ denote $|A| = O(|B|)$, i.e. there is a constant C (independent of A and B) such that $|A| \leq C|B|$. Now, if Z is a ring—so both addition and multiplication are defined—we can call $A \subseteq Z$ an **approximate subring** if $|A + A| \lesssim |A|$ and $|A \cdot A| \lesssim |A|$. The theorem says that finite fields of prime order contain no approximate subrings.

As a warm-up, let's think a little bit about subsets of \mathbb{Z} . From now on, A and B will always denote finite, non-empty subsets of the group or ring under consideration (unless stated otherwise). It may be helpful to observe that translating given sets A and B does not affect $|A + B|, |A - B|$, etc. For example, the sum of the translated sets has the same size as the sum itself:

$$|(A + x) + (B + y)| = |A + B + (x + y)| = |A + B|$$

Exercise 0.1. *Let $Z = \mathbb{Z}$, the ring of integers.*

- (a) *Let $A, B \subseteq Z$. Show $|A| + |B| - 1 \leq |A + B| \leq |A||B|$.*
- (b) *Given $m, n \geq 1$ and $m + n - 1 \leq s \leq mn$, construct $A, B \subseteq Z$ such that $|A| = m, |B| = n$, and $|A + B| = s$.*

A statement similar to (a) for $Z = \mathbb{Z}/p\mathbb{Z}$ where p is prime is called the Cauchy-Davenport inequality. This and a similar lower bound (in terms of a multiplicative factor rather than an additive one) will play a crucial role in the proof of Theorem 0.1, and we will prove both inequalities next time.

One can often think of arithmetic combinatorics as “approximate group theory”. If $H \leq Z$ is a finite subgroup¹ of an abelian group Z , then H is closed under addition and subtraction: $H + H = H - H = H$. In particular, $|H + H| = |H|$ as we noted above in the case that Z is a ring. On the other hand, given a subset $A \subseteq Z$ such that $|A + A| \lesssim |A|$, what can we say about $|A - A|, |A + A - A|$, etc.?

¹We will always use the $H \leq G$ notation to distinguish H as a subgroup rather than just a subset of G .

Exercise 0.2. Let $A, B \subseteq Z$ be finite, non-empty subsets of an abelian group Z . Show that $|A + B| = |A|$ if and only if there is a finite subgroup $H \leq Z$ such that A is the union of cosets of H and B is contained in some coset of H .

In particular, if $A = B$, this exercise says that $|A + A| = |A|$ if and only if A is the coset of some finite subgroup. It turns out that if A is **essentially closed under addition**, in the sense that $|A + A| \lesssim |A|$, then we can say something interesting about the size of sets of the form $A \pm A \pm \dots \pm A$. More generally, if A is **essentially B invariant**, i.e. $|A + B| \lesssim |A|$, then $|mB - nB| \lesssim |A|$ (where $mB = B + B + \dots + B$, m times).² This is known as sumset estimates, and it will follow from a more general theorem called Plünnecke’s theorem.

Since the BKT theorem deals with sizes of subsets, we will focus on results from arithmetic combinatorics on cardinality, not structure. However, one can often find non-trivial information about the *structure* of, say, $A + B$, given information on A and B . For example, a very deep theorem called Frieman’s theorem says that if a subset is essentially closed under addition, then it is very close to being a (generalized) arithmetic progression! We will not require these sorts of results, so, in order to save time, we will not cover them. For more on Frieman’s theorem, see Lecture 2 of [3].

Our strategy for proving the BKT theorem is this: after proving the Cauchy-Davenport inequality and its refinement, we will be able to show that

$$(1) \quad F = A \cdot \xi_1 + A \cdot \xi_2 + \dots + A \cdot \xi_k$$

for k relatively small, depending only on δ . We need a bit more notation. Let $P \in \mathbb{Z}[X_1, X_2, \dots, X_n]$ be a polynomial with integral coefficients in n variables, and let $P(A, A, \dots, A)$ be its evaluation at the subset A with respect to our notation above. For example, if $P(X, Y) = X - Y$, then $P(A, A) = A - A$. Now, given the “linear surjection” result as in equation 1, we will deduce the existence of a polynomial P such that $P(A, A, \dots, A) = F$. However, assuming that the conclusion of the theorem is false, we will find—using standard results such as sumset estimates and the Gowers-Balog-Szemerédi theorem—that for our polynomial P , we have $|P(A, A, \dots, A)| \lesssim |A|^{1+C\varepsilon}$ for some constant C and any $\varepsilon > 0$. Thus we will arrive at a contradiction by choosing a sufficiently small ε since $|A| < |F|^{1-\delta} < |F|$.

Although the BKT result is only for finite fields of prime order, similar results may be obtained for arbitrary finite fields. The difference is, of course, that there are nontrivial subfields $1 < K < \mathbb{F}_q$ when q is not prime, so in particular $|K + K| = |K \cdot K| = |K|$, contradicting the conclusion of Theorem 0.1. However, this is essentially all that can happen. For more on this, see Theorem 4.3 in [1] as well as Theorem 2.4 in [2].

Our primary resources for this seminar are Tao’s notes on arithmetic combinatorics [3] and the BKT paper [1]; in particular, with the exception of the proof of Gowers’ result that we will encounter in Week 5, all the results and proofs are from these two sources. My sole contributions are reorganization, exposition, and the occasional correction of a typo. I also add some details to Tao’s proofs in order to aid my understanding of the arguments, and I hope these are illuminating rather than distracting.

Here is my proposed outline for the rest of the course:

²I admit that I’m being rather loose with the \lesssim notation. For now, just think of it as meaning “small relative to”. In the next few lectures, I hope to be a bit more careful.

- Week 1** Bounds on $|A + B|$
- Lower bounds on $|A + B|$ and $|A + \xi B|$: Cauchy-Davenport, Cauchy-Davenport refinement;
 - Upper bounds on $|A + B|$: Ruzsa lemmata
- Week 2** Linear surjections onto F
- $F = A\xi_1 + \dots + A\xi_k$, $k = O(1/\delta)$;
 - if there is a linear map $B^k \rightarrow F$, then there is a linear map $\tilde{B}^{k-1} \rightarrow F$ for a related \tilde{B}
- Week 3** Sumset estimates
- Plünnecke's theorem: roughly, $|A + B| \lesssim |A| \implies |A' + B + B| \lesssim |A'|$ for some $A' \subseteq A$
 - Cartesian product trick: transfer a problem in Z to one in $Z \times Z$
- Week 4** $|AA - AA| \lesssim |A|$ implies $|P(A, A, \dots, A)| \lesssim |A|$ for all polynomials P
- notion of “essentially contained”
 - notion of “good elements” and properties of good elements
 - finish proof of BKT
- Week 5** No approximate subrings implies $|A \cdot A - A \cdot A| \lesssim |A|$
- Cauchy-Schwartz inequality
 - Popularity argument
 - the Gowers-Balog-Szemerédi theorem
- Weeks 6–8** Applications of BKT
- incidence problem
 - Erdős distance problem
 - Kakeya problem
 - $SL_2(p)$ has small diameter (Helfgott)
 - constructions of extractors
 - ...?

References.

- [1] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.
- [2] H. A. Helfgott. Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, 2005.
- [3] Terry Tao. Math 254a: Some highlights of arithmetic combinatorics, 2003.