

2. LINEAR SURJECTIONS ONTO  $\mathbb{Z}/p\mathbb{Z}$ 

We are still working toward the proof of the BKT result from [1]. Today we will use the results from last week—namely, Theorem 1.1 and Lemma 1.2—to find a polynomial  $P$  that depends only on  $\delta$  such that  $P(A, A, \dots, A) = F$ . On the one hand, this is rather incredible: for any fixed  $\delta$ , the same polynomial  $P$  works for  $p = 101$  and primes  $> 10^{10^{10}}$ ! On the other hand, this result may not be too surprising, given the restrictions on  $|A|$ . In any event, the fact that  $P$  is independent of everything (except  $\delta$ ) is what allows us to prove the BKT theorem.

The first step towards finding  $P$  is the following:

**Lemma 2.1.** *Let  $\delta > 0$  be given. Suppose  $A \subset F := \mathbb{Z}/p\mathbb{Z}$  for some prime  $p$  such that  $p^\delta < |A| < p^{1-\delta}$ . Then there is a  $k = k(\delta)$  and there are  $\xi_1, \dots, \xi_k \in F^*$  such that*

$$A \cdot \xi_1 + A \cdot \xi_2 + \dots + A \cdot \xi_k = F$$

*Proof.* First, I claim that there are  $k = k(\delta)$  and  $\xi_i \in F^*$  such that  $|A \cdot \xi_1 + \dots + A \cdot \xi_k| \geq |F|/10$ . To that end, choose  $k$  to be some big number, bigger than  $2/\delta$ . Then by Lemma 1.2, there are  $\xi_i \in F^*$  such that

$$|A \cdot \xi_1 + \dots + A \cdot \xi_k| \geq \frac{|A|^k}{2^{k-1}} > \frac{p^{\delta k}}{2^{k-1}} > \frac{p^2}{2^{k-1}}$$

by the assumption on  $|A|$ . But, for any fixed  $k$ ,  $\lim_{p \rightarrow \infty} \frac{10p}{2^{k-1}} \rightarrow \infty$ , so there is a  $N \in \mathbb{N}$  such that  $10p/2^{k-1} \geq 1$  for all  $p \geq N$ . Therefore,

$$|A \cdot \xi_1 + \dots + A \cdot \xi_k| > \frac{p^2}{2^{k-1}} > \frac{p}{10}$$

for all  $p \geq N$ .

For the primes  $p < N$ , clearly some  $k' = O(N)$  applications of Theorem 1.1 will do the trick, and this proves the claim since  $N$  depends only on  $k$  and  $k$  depends only on  $\delta$ .

Now, by Exercise 1.1, if  $B := A \cdot \xi_1 + \dots + A \cdot \xi_k$ , then  $1000B := B + B + \dots + B = F$  (again by the Cauchy-Davenport inequality, Theorem 1.1).  $\square$

Another way of stating the conclusion of this Theorem is that there is a linear surjection  $\pi : A^k \rightarrow F$ , defined by

$$\pi(a_1, a_2, \dots, a_k) = \sum_{i=1}^k a_i \xi_i$$

for some  $\xi_i \in F$ . Our goal, then, is to replace  $A^k$  with a polynomial expression in  $A$ , and we do this one step at a time:

**Lemma 2.2.** *Let  $B \subseteq F$  be a nonempty subset of  $F = \mathbb{Z}/p\mathbb{Z}$  ( $p$  prime), and suppose that there is a linear surjection  $f : B^k \rightarrow F$  for some  $k > 1$ , say  $f(b_1, \dots, b_k) = \sum b_i \xi_i$  for some  $\xi_i \in F$ . Then there is a linear surjection  $\tilde{B}^{k-1} \rightarrow F$  where*

$$\tilde{B} = B \cdot (B - B) + B \cdot (B - B)$$

*Proof.* First notice that  $f$  cannot be injective since, if it were, then  $|F| = |B|^k$ , a contradiction since  $k > 1$ . Therefore there are  $(b_1, \dots, b_k) \neq (b'_1, \dots, b'_k) \in B^k$  such that

$$(b_1 - b'_1)\xi_1 + \dots + (b_k - b'_k)\xi_k = 0$$

Suppose WLOG that  $b_k \neq b'_k$ . We know that  $F = B \cdot \xi_1 + \dots + B \cdot \xi_k$ , so since  $F$  is a field, we also know that

$$\begin{aligned}
F &= F(b_k - b'_k) \\
&= B \cdot \xi_1(b_k - b'_k) + \dots + B \cdot \xi_k(b_k - b'_k) \\
&= B \cdot \xi_1(b_k - b'_k) + \dots + B \cdot \xi_{k-1}(b_k - b'_k) - B \cdot \xi_1(b_1 - b'_1) - \dots - B \cdot \xi_{k-1}(b_{k-1} - b'_{k-1}) \\
&= \xi_1 \cdot B \cdot (b_k - b'_k) - \xi_1 \cdot B \cdot (b_1 - b'_1) + \dots + \xi_{k-1} \cdot B \cdot (b_k - b'_k) - \xi_{k-1} \cdot B \cdot (b_{k-1} - b'_{k-1}) \\
&\subseteq \xi_1 \cdot (B \cdot (B - B) + B \cdot (B - B)) + \dots + \xi_{k-1} \cdot (B \cdot (B - B) + B \cdot (B - B))
\end{aligned}$$

Thus we conclude that  $F = \tilde{B}\xi_1 + \dots + \tilde{B}\xi_{k-1}$ .  $\square$

Putting it all together for the sake of proving the BKT result (Theorem 0.1), let  $\delta > 0$  be given, and suppose  $A \subseteq F$  with  $p^\delta < |A| < p^{1-\delta}$ . Then Lemma 2.1 implies that  $F = A \cdot \xi_1 + \dots + A \cdot \xi_k$  for some  $\xi_i \in F$  and  $k \sim 1/\delta$ . If we iterate Lemma 2.2  $k$  times, we get a polynomial  $P$  depending only on  $\delta$  such that  $F = P(A, A, \dots, A)$ ! We will dedicate the next three lectures to showing that if the BKT theorem is false, then  $|P(A, \dots, A)| \ll |F|$  for all polynomials  $P$  to arrive at a contradiction. This is sort of what one might expect, at least according to the notation: if  $|A + A|$  and  $|A \cdot A|$  are both small, then any polynomial expression in  $A$  should be small, too.

Next week, we will prove the first main ingredient in the second half of the proof: sumset estimates. This says that if  $A$  is essentially  $B$ -invariant, then  $|nB - mB|$  cannot be much larger than  $|A|$  (in a way we will make explicit next week). This is a corollary to Plünnecke's Theorem, which says that if  $|A + B| \leq K|A|$  for some  $K \geq 1$ , then there is a nonempty subset  $A' \subseteq A$  such that  $|A' + B + B| \leq K^2|A'|$ . Although this is a very nice, concrete result, it leaves something to be desired since  $A'$  could be very small; for more on this, see lecture 1 in [?].

In order to prepare to prove Plünnecke's theorem, we need to introduce some notions from graph theory. Let  $Z$  be an abelian group. A **commutative graph** (of depth 2) is a directed graph with vertex sets  $V_0, V_1, V_2 \subset Z$  and edge sets  $E_{0 \rightarrow 1}, E_{1 \rightarrow 2}$  such that 1) for all edges  $e \in E_{i \rightarrow i+1}$ , the initial point of  $e$  is in  $V_i$  and the terminal point is in  $V_{i+1}$  and 2) if  $(a \rightarrow a+b) \in E_{0 \rightarrow 1}$  and  $(a+b \rightarrow a+b+c) \in E_{1 \rightarrow 2}$ , then  $(a \rightarrow a+c) \in E_{0 \rightarrow 1}$  and  $(a+c \rightarrow a+b+c) \in E_{1 \rightarrow 2}$ . The second condition is called the **commuting square property**.

Given two commutative graphs  $G$  and  $\tilde{G}$ , one can define their Cartesian product  $G \times \tilde{G}$  to have vertex sets  $V_0 \times \tilde{V}_0, V_1 \times \tilde{V}_1$ , and  $V_2 \times \tilde{V}_2$  (where the  $V_i$  and  $\tilde{V}_i$  are the vertex sets of  $G$  and  $\tilde{G}$ , respectively) and edge sets  $E_{0 \rightarrow 1} \times \tilde{E}_{0 \rightarrow 1}$  and  $E_{1 \rightarrow 2} \times \tilde{E}_{1 \rightarrow 2}$ , where the product of two edges  $(a \rightarrow b), (\tilde{a} \rightarrow \tilde{b})$  is

$$(a \rightarrow b) \times (\tilde{a} \rightarrow \tilde{b}) = ((a, \tilde{a}) \rightarrow (b, \tilde{b}))$$

**Exercise 2.1.** Show that if  $G$  and  $\tilde{G}$  are commutative graphs, then  $G \times \tilde{G}$  is as well.

For example, let  $A, B \subseteq Z$  and define  $G[A, B]$  to be the commutative graph with vertex sets  $A, A+B, s$  and  $A+B+B$  and all obvious possible edges from  $A$  to  $A+B$  and from  $A+B$  to  $A+B+B$ . Then by working through the definitino one can show that  $G[A, B] \times G[A', B'] = G[A \times A', B \times B']$  for any  $A', B' \subseteq Z$ . Note that if we let  $G(X)$  denote all the points in  $V_1$  that are endpoints of edges starting at  $X \subseteq V_0$ , and similarly  $G^2(X)$  be those points in  $V_2$  that are reachable via paths starting in  $X \subseteq V_0$ , then we may restate the conclusion of Plünnecke's theorem this

way: there is a  $A' \subseteq A$  such that  $|G[A, B]^2(A')| \leq K^2|A'|$ . We will prove a more general statement about commutative graphs next time.

We require one more notion to facilitate next week's lesson. Let  $A$  and  $B$  be subsets of a finite graph  $G$ . Define  $MAXFLOW(A \rightarrow B, G)$  to be the maximum number of disjoint paths connecting a vertex in  $A$  to one in  $B$ . Also define  $MINCUT(A \rightarrow B, G)$  to be the minimum number of vertices one must remove from  $G$  to disconnect  $A$  from  $B$ .

**Exercise 2.2** (Menger's Theorem).  $MAXFLOW(A \rightarrow B, G) = MINCUT(A \rightarrow B, G)$ .

Next time, we will use these ideas to prove Plünnecke's theorem using graph theory. Then, using the Ruzsa bound on  $|A+B|$  that we proved last week (Lemma 1.3), we will derive the sunset estimates as a corollary.

**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.