

## 6. KONYAGIN'S EXTENSION (PRESENTED BY VLADO)

Today we will prove the following extension of the BKT theorem due to Konyagin [2], and we will follow a proof by Ben Green in his notes from MIT [1]:

**Theorem 6.1.** *For all  $\delta > 0$ , there exists a constant  $c = c(\delta)$  such that for all primes  $p$  and for all subsets  $A \subseteq \mathbb{Z}/p\mathbb{Z}$  such that  $|A| < p^{1-\delta}$ , we have*

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

This is a very nice result because it gets rid of the assumption that  $A$  is relatively big. Its proof relies on three results that we have seen previously: sunset/product-set estimates (Theorem 3.3), approximate subrings have small difference of products (Theorem 5.1), and small difference of products implies small polynomial expressions (Theorem 4.1). We begin our proof by defining a rational expression that grows well in general, and is analogous to the set  $B \cdot (B - B) + B \cdot (B - B)$  that we encountered in Lemma 2.2. We define the rational expression  $J$  by

$$J(A) = \left\{ a_5 \left( \frac{a_1 a_2 - a_3 a_4}{a_3 - a_1} - a_6 \right) : a_i \in A, a_1 \neq a_3 \right\}$$

As usual, let  $F := \mathbb{Z}/p\mathbb{Z}$ . We begin with a lemma, which is very similar in spirit to our Theorem 5.1.

**Lemma 6.2.** *If  $|A + A|$  and  $|A \cdot A|$  are both less than or equal to  $K|A|$ , then there is an  $A'' \subseteq A$  such that  $|A''| \geq K^{-c}|A|$  and  $|J(A'')| \leq K^c|A|$ .*

*Proof.* By Lemma 5.1, there is a subset  $A' \subseteq A$  such that the difference of products is small:  $|A'A' - A'A'| \leq K^c$  for some  $c$ . Let  $X = P(A', \dots, A')$  where  $P(X_1, \dots, X_6) = X_5(X_1 X_2 - X_3 X_4 + X_6 X_3 - X_6 X_1)$ , and fix  $x \in X$  with  $x \neq 0$ . Then we may define a bijection by right multiplication by  $1/x^2$ :

$$f : \frac{X}{(A' - A') \setminus \{0\}} \hookrightarrow \frac{X}{X \setminus \{0\}}, \quad f\left(\frac{x_0}{a_1 - a_2}\right) = \frac{x_0}{x^2(a_1 - a_2)}$$

Then we have the following estimates, where  $Y := X \setminus \{0\}$ :

$$|J(A')| \leq \left| \frac{X}{(A' - A') \setminus \{0\}} \right| \leq \left| \frac{X}{X \setminus \{0\}} \right| \leq C \left| \frac{Y}{Y} \right|$$

So, by Theorem 4.1, we have

$$|X \cdot X| \leq K^c|A'| \leq K^c|X|$$

Therefore, by product-set estimates,  $|Y/Y| \leq K^c|Y| \leq K^{c'}|A'|$  as needed. (Note that the constant  $c$  may change from step to step, but it's still just a constant.)  $\square$

Now we state the main proposition, from which Konyagin's main result will follow quite easily:

**Proposition 6.3.** *For  $A \subseteq \mathbb{Z}/p\mathbb{Z}$ ,*

- *if  $|A| \leq \sqrt{p}$ , then  $|J(A)| \geq |A|^3/(2|A - A|)$ ;*
- *if  $|A| > \sqrt{p}$ , then  $|J(A)| \geq p/2$ .*

We will say that  $\xi \in F$  is **involved with**  $A$  if  $|A(A + \xi)| < |A|^2$ . We require a basic lemma (cf. Lemma 2.2).

**Lemma 6.4.** *Suppose that  $\xi$  is involved with  $A$ . Then  $J(A)$  contains  $A(A + \xi)$ .*

*Proof.* Since  $\xi$  is involved, there are  $(a_1, a_2) \neq (a_3, a_4)$  such that

$$a_1(a_2 + \xi) = a_3(a_4 + \xi)$$

Therefore  $\xi = \frac{a_1 a_2 - a_3 a_4}{a_3 - a_1}$ , so for all  $a_5, a_6 \in A$  we have  $a_5(a_6 + \xi) \in J(A)$  by the definition of  $J$ .  $\square$

Now we use the Cauchy-Schwartz inequality to make an averaging argument (cf. Lemma 2 in [2]):

**Lemma 6.5.** *Suppose that  $A \subset F$ . Then there is a  $\xi \in F$  such that*

$$|A \cdot (A + \xi)| \geq \frac{|A|^2 p}{|A|^2 + p}$$

*Proof.* See [1], Lemma 5.3.  $\square$

We also omit the proof of the next lemma, which we have taken directly from [1] as well:

**Lemma 6.6.** *Suppose that  $A \subseteq F$  satisfies  $|A| \leq \sqrt{p}$  and  $|A - A| \leq K|A|$ . Then there is some  $\xi \in F$  such that  $\xi$  is involved with  $A$  but not very involved, i.e.*

$$\frac{|A|^2}{2K} \leq |A \cdot (A + \xi)| < |A|^2$$

*Proof.* See [1], lemma 5.4.  $\square$

*Proof of Proposition 6.3.* Suppose first that  $|A| > \sqrt{p}$ . Since  $A \cdot (A + \xi) \subseteq F$  and  $|F| < |A|^2$ , every value of  $\xi$  is involved with  $A$ . So, by Lemma 6.5, there is some  $\xi \in F$  such that

$$p/2 \leq |A \cdot (A + \xi)| < |A|^2$$

Then by Lemma 6.4, we know that  $p/2 \leq |A \cdot (A + \xi)| \leq |J(A)|$ , so we're done with the first case. For the second, apply Lemma 6.6 to find a  $\xi$  that is involved but not very involved and then apply Lemma 6.4 again to conclude that

$$|A|^2/2K \leq |A \cdot (A + \xi)| \leq |J(A)|$$

where  $K = |A - A|/|A|$ . This completes the proof of the proposition.  $\square$

To finish, we outline a proof of the main theorem; details are left as an exercise, and one is encouraged to use arguments similar to those found at the end of section 4.

*Proof of Theorem 6.1.* Suppose that  $A \subseteq F$  is an approximate subring. Then by Lemma 6.2, there is a subset  $A' \subseteq A$  with  $|A'| \geq K^{-c}|A|$  and  $|J(A')| \leq K^c|A|$ . By sumset estimates, we also know that  $|A' - A'| \leq |A - A| \leq K|A|$ , so by Proposition 6.3, we know that either  $|J(A)| \geq p/2$  or

$$|J(A)| \geq |A|^3/2|A - A| = O(|A|^2)$$

so  $|J(A')| \gg \min(p, K^{-c}|A|^2)$ . By comparing this and the other bound above on  $|J(A)|$ , one should get a contradiction... these are the details that I leave to the reader.  $\square$

So we have seen that the lower bound on  $A \subseteq F$  is unnecessary in the BKT theorem. Clearly, one cannot hope to get rid of the upper bound on  $A$ , so the Konyagin extension of the BKT theorem seems best possible. For a great, self-contained proof of the full theorem, see [1].

**References.**

- [1] Ben Green. Sum-product estimates.
- [2] S.V. Konyagin. A sum-product estimate in fields of prime order, 2003.