

Material in this lecture comes from

Sum-product estimates and exponential sums over subgroups arXiv

Theorem: (Bourgain-Katz-120) Let $\delta > 0$ and suppose $A \subseteq \mathbb{F}_p$

has $p^\delta \leq |A| \leq p^{1-\delta}$. Then there is $\delta' = \delta'(\delta) > 0$

such that $\max(|A+A|, |A-A|) \geq p^{\delta'} |A|$

Remark: The requirement $|A| \geq p^\delta$ subsequently removed by

Bourgain-?..? The result \Rightarrow the class. of K -approximate

subfield \mathbb{F}_p noted last time...

(missed end of remark).

Theorem: (Bourgain-Glibichuk-Konyagin). Let $H \leq \mathbb{F}_p^*$ be a subgroup. Suppose $|H| \geq p^\delta$. Then $\exists \delta' = \delta(\delta) > 0$ such that

Lemma 1: Suppose $A \subseteq \mathbb{F}_p$. Then $\exists \xi \in \mathbb{F}_p^*$ such that $|A + \xi \cdot A| \geq \frac{1}{2} \min(|A|^2, p)$.

Pr: We'll look at additive energy

$\sum_{\xi \in \mathbb{F}_p^*} \omega(A, \xi \cdot A)$. This is equal to

$\frac{1}{|A|^3}$ times the # of $a_1, a_2, a_3, a_4 \in A$,

$\xi \in \mathbb{F}_p^*$ with $a_1 + a_2 = \xi(a_3 + a_4)$.

If $a_1 \neq a_2, a_3 \neq a_4$ there is unique ξ satisfying this.

If $a_1 = a_2$ and $a_3 = a_4$ then any ξ will do.

So the # of solutions is $|A|^2(|A-1)^2 + |A|^2(p-1)$.

Hence there is some $\xi \in \mathbb{F}_p^*$ with $\omega(A, \xi A) \leq \frac{1}{|A|} + \frac{(|A-1)^2}{p-1}$

$$\leq \frac{1}{|A|} + \frac{|A|^2}{p} \leq 2 \max\left(\frac{1}{|A|}, \frac{|A|}{p}\right).$$

~~$\sup_{\xi \neq 0} \frac{1}{|H|} \left| \sum_{x \in H} e\left(\frac{x\xi}{p}\right) \right| < p^{\delta'}$~~

$$\sup_{\xi \neq 0} \frac{1}{|H|} \left| \sum_{x \in H} e\left(\frac{x\xi}{p}\right) \right| < p^{\delta'}$$

Now use the fact (Cauchy-Schwarz) that $\exists [A, B] \omega [A, B] \leq 1$
 (we saw this before). II

Lemma 2: Suppose $A \subseteq \mathbb{F}_p$, then $|\mathcal{Z}A^2 - \mathcal{Z}A^2| \geq \frac{1}{2} \min(|A|^2, p)$.

[Here ~~$\mathcal{Z}A^2$~~ $A^2 = A \cdot A = \{a_1 a_2 : a_1, a_2 \in A\}$
 $\mathcal{Z}X - \mathcal{Z}X = \{x_1 + x_2 + x_3 - x_4 - x_5 - x_6 : x_i \in X\}$]

Proof: ~~Two cases:~~ ~~Case 1:~~ Write $\frac{A \cdot A}{A \cdot A} = \left\{ \frac{a_1 a_2}{a_3 a_4} : \begin{matrix} a_i \in A \\ a_3 \neq a_4 \end{matrix} \right\}$.

Note that $\mathcal{Z} \in \frac{A \cdot A}{A \cdot A} \iff |A + \mathcal{Z} \cdot A| < |A|^2$.

(Indeed, $|A + \mathcal{Z} \cdot A| \leq |A|^2$ with equality iff the sums $a_1 + \mathcal{Z} a_2$ are all distinct).

Case 1: $\frac{A \cdot A}{A \cdot A} \neq \mathbb{F}_p^*$. Then $\exists \mathcal{Z} \in \frac{A \cdot A}{A \cdot A}$ such that $\mathcal{Z} + 1 \notin \frac{A \cdot A}{A \cdot A}$.

We have then, $|A + (\mathcal{Z} + 1)A| = |A|^2$. Write $\mathcal{Z} = \frac{a_1 a_2}{a_3 a_4}$, then

$$\left| A + \left(\frac{a_1 a_2}{a_3 a_4} + 1 \right) \cdot A \right| = \left| (a_3 a_4) \cdot A + (a_1 a_2 + a_3 a_4) \cdot A \right| = |A|^2.$$

But $(a_3 a_4) \cdot A + (a_1 a_2 + a_3 a_4) \cdot A \subseteq \mathcal{Z}A^2 - \mathcal{Z}A^2$.

Case 2: $\frac{A-A}{A-A} = \mathbb{F}_p^*$. Use Lemma 1 to find ξ with $|A+\xi A| \geq \frac{1}{2} \min(|A|^2, p)$

Write $\xi = \frac{a_1 - a_2}{a_3 - a_4}$ and proceed similarly. \square

Corollary 3: Suppose that $A \subseteq \mathbb{F}_p^*$ with $|A| \geq p^\delta$. Then there is $k = k(\delta)$ such that $kA^k - kA^k = \mathbb{F}_p$.

[Remark: the proof gives $k(\delta) \sim \exp(\frac{1}{\delta^c})$.]

Pf: Herstein lemma 2 gives some k_0 such that $|k_0 A^{k_0} - k_0 A^{k_0}| > \frac{p}{2}$

But if $X \subseteq \mathbb{F}_p$ has $|X| > \frac{p}{2}$ then $X+X = \mathbb{F}_p$ (exercise). \square

Let $K \geq 2$ be a parameter. Define $\text{Alg}_K(A) := \{ \xi \in \mathbb{F}_p^* : |A+\xi A| \leq K|A| \}$

The following follows from Ruzsa calculus: If $\xi_1, \xi_2 \in \text{Alg}_K(A)$

then $\xi_1, \xi_2, \xi_1^{-1}, \xi_2^{-1}, \xi_1 + \xi_2$ lie in $\text{Alg}_{K^c}(A)$.

(For example if $\xi_1, \xi_2 \in \text{Alg}_K(A)$ then $|A + (\xi_1 + \xi_2)A| \leq |A + \xi_1 A + \xi_2 A| \leq K^c |A|$ by Ruzsa's third inequality.)

Lemma 1: Let $A, B \subseteq \mathbb{F}_p$ have $|A| = p^\alpha$, $|B| = p^\beta$. Then there is $b \in B$ such that $|A + b \cdot A| \geq |A|^{1 + c_{\alpha, \beta}}$ where $c_{\alpha, \beta} > 0$ depends only on α, β .

Pr: Suppose ~~that~~ that $B \subseteq \text{Alg}_K(A)$, i.e. $|A + b \cdot A| \leq K|A|$.

Choose $k = k(p)$ such that $kB^k - kB^k = \mathbb{F}_p$ (cf. Corollary 3).

By the remark just made it follows that $kB^k - kB^k \subseteq \text{Alg}_{K^k}(A)$.
 $\mathbb{F}_p \subseteq$

but that contradicts $K = |A|^{\frac{1}{10c_k}}$ (say), since by Lemma 1

$\mathbb{F}_p^* \not\subseteq \text{Alg}_{\frac{1}{2}|A|}(A)$. \square

Exponential sums over subgroups: If $A \subseteq \mathbb{F}_p$ and $\delta > 0$ is a parameter we write $\text{Spec}_\delta(A)$ for the set $\left\{ z \in \mathbb{F}_p^* : \frac{1}{|A|} \left| \sum_{x \in A} e\left(\frac{xz}{p}\right) \right| \geq \delta \right\}$

" δ -large spectrum". B-G-K result is equivalent to showing that

if $H \leq \mathbb{F}_p^*$ is a subgroup of size p^δ then $\text{Spec}_{p^{-\delta'}}(H) = \{0\}$

for some $\delta' = \delta'(\delta) > 0$.

Note that $\text{Spec}_\eta(H)$ is H -invariant for any η (i.e. if $\xi \in \text{Spec} \Rightarrow h\xi \in \text{Spec}$ for all h .)

It turns out that for any set A the sets $\text{Spec}_S(A)$ have (weak) additive closure properties.

Proposition: Let $B \subseteq \text{Spec}_S(A)$. Then for a proportion at least $\frac{\delta^2}{2}$ of the pairs $x, y \in B$ we have $x + y \in \text{Spec}_{S+K}(A)$.