Lec 9/1

Friday, September 1, 2017 14:13

find errata for book

<u>Szemerédi</u>: $A \subseteq \mathbb{N}$. If $\bar{\partial}(A) = \limsup \frac{|A \cap \{1, \dots, N\}|}{N} > 0$ then A is AP-rich.

(Meaning A contains arbitrarily long arithmetic progressions)

($\{a, a+d, \dots a+(k-1)d\}$ is a length k AP when $d \neq 0$)

Is it true that if $\bar{\partial}(A) > 0$ then $\exists d$ s.t. A contains arbitrarily long APs with step size d. (Exercise: No)

Roth: for progressions of length 3

<u>Sárközy</u>: If $\bar{\partial}(A) > 0$, then $\exists x, y \in A$, $\exists n \in \mathbb{N}$ s.t. $\underline{x - y = n^2}$.

can also get $x - y = p - 1$ for some $p \in \mathbb{P}$.

Very important question:

what are interesting properties of the set

$$R_k(A) = \{ d : \exists a \text{ s.t. } \{a, a+d, \dots, a+(k-1)d\} \subset A \}$$

Thm: $R_k(A) \ni n^2 \quad \forall k \in \mathbb{N}, \forall A$ w/ $\bar{\partial}(A) > 0$

$\quad\quad\ \ \uplus$

$\quad\quad p - 1$

$R_k(A) \cap R_k(A_2) \ni n^2$?

$S \subset \mathbb{N}$ is syndetic if finitely many shifts of

S cover $\mathbb{N}$.

$\bar{d}(A) > 0 \Rightarrow \forall k \; \exists d$ s.t.

$$A \cap (A-d) \cap \dots \cap (A-(k-1)d) \neq \emptyset$$

(equiv. to result of Szemeredi theorem)

$$\mathbb{1}_A(n) := \begin{cases} 1 & n \in A \\ 0 & n \notin A \end{cases} \qquad \mathbb{1}_B \cdot \mathbb{1}_A = \mathbb{1}_{B \cap A}$$

$$\mathbb{1}_A \in \{0,1\}^{\mathbb{N}}$$

$\forall k \exists d$ $\quad A \cap (A-d^2) \cap \dots \cap (A-(k-1)d^2) \neq \emptyset$

$\forall k \exists p$ $\quad A \cap (A-(p-1)) \cap \dots \cap (A-(k-1)(p-1)) \neq \emptyset$

<u>Fermat's Theorem</u> If $p \in \mathbb{P}$, $a^p \equiv a \mod p$

<u>Proof (Leibniz)</u> $a^p = (\underbrace{1 + \dots + 1}_{a})^p \equiv \underbrace{1 + 1 + \dots + 1}_{a} + p \cdot c \equiv a$ ∎

Exercise multinomial coeffs in $(1 + \dots + 1)^p$ are divisible by p.

<u>Proof 2</u> Ivory

$\underbrace{a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \mod p}$ $\Rightarrow \underbrace{a^{p-1} \equiv 1 \mod p}_{\text{Little Fermat Thm.}}$

show $k\{1, \dots, p-1\} = \{1, \dots, p-1\} \mod p$

from 5520H

Proof multiplication by $[k]$ injective.

If $[k][x] = [k][y]$ then $[kx] = [ky]$ so $kx - ky = np \Rightarrow k(x-y) = np$ for some n

p not divisible by k, so n divisible by k meaning $x - y = mp$ for some m

so $[x] = [y]$.

$\mathbb{Z}_p$, $p \in \mathbb{P}$ are finite fields.

In a general field, it may happen that for some $n \in \mathbb{N}$,

$$\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0. \quad (*)$$

Claim: If this happens then the least such $n \in \mathbb{P}$.

<u>Proof</u>: assume (i) n is the smallest number satisfying $(*)$

(ii) $n = n_1 n_2$, $n_1, n_2 > 1$.

$$0 = \underbrace{1 + 1 + \cdots + 1}_{n_1 n_2} = \underbrace{(1 + \cdots + 1)}_{n_1} \underbrace{(1 + \cdots + 1)}_{n_2}.$$

If $\exists\, n$ like this, the field has finite characteristic.

(Exercise) Show there are infinitely many fields of characteristic p for any p

Hint: prove field of size p^n has characteristic p.

(Exercise) are there uncountably many? Maybe yes?

$$\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}_5 \right\}$$ has characteristic 5.