Sum-free sets

A set of integers S is said to be sum-free if $\forall x, y \in S$, $x+y \notin S$. [x, y may not be distinct]

Example ① $S = \{2, 3, 7, 8, 9\}$

② $S = \{-5, -3, 100\}$

Q. Given $B = \{b_1, b_2, \ldots, b_n\}$ be a set of n integers. How large a subset of B can you get that is sum-free?

27 September 2020 18:35

Examples

(1) $B = \{1, 2, 3, 4, 5, \underline{6, 7, 8, 9, 10}\}$

$S = \{6, 7, 8, 9, 10\} \subseteq B$

$\longrightarrow$ sum-free.

(2) $B = \{1, 2, 4, 8, 16, 32\}$

$S = \{1, 4, 16\}$

Theorem [Erdos, 1965] Every set $B=\{b_1,\dots,b_n\}$ of n non-zero integers contains a sum-free subset A of size $|A| > \frac{n}{3}$.

Proof: Let $p = 3k+2$ (for some k) be a prime number such that

$p > b_1$, $p > b_2$, ..., $p > b_n$.

$p = 3k+2$.

$C = \{k+1, k+2, \dots, 2k+1\}$, $|C| = k+1$

Claim: C is a sum-free subset of the Abelian group $\mathbb{Z}_p$.

$(X, \circ)$ → set, → binary op, is a group

if $\forall x_1, x_2, x_3 \in X$,

(i) $x_1 \circ x_2 \in X$ ← closure

(ii) $x_1 \circ (x_2 \circ x_3) = (x_1 \circ x_2) \circ x_3$

$\hookrightarrow$ Associativity

(iii) $\exists e$ s.t. $\forall x \in X$, $x \circ e = x$

$\hookrightarrow$ Identity

(iv) $\forall x \in X$, $\exists x^{-1} \in X$, s.t. $x \circ x^{-1} = e$

$\hookrightarrow$ Inverse.

$(X, \circ)$ is an Abelian group if

$\forall x_1, x_2 \in X$, $x_1 \circ x_2 = x_2 \circ x_1$

$(\mathbb{Z}, +)$

$\mathbb{Z}$: integers

$(\mathbb{Z}_p, +)$ $(\{0, 1, 2, \dots, p-1\}, +)$

p : prime

$+$: addition modulo p.

27 September 2020 18:53

$p = 3k+2 \quad (\{0,1,\dots,3k+1\}, +)$

$C = \{k+1, k+2, \dots, 2k+1\}$, $|C| = k+1$

Claim: C is a sum-free subset of $\mathbb{Z}_p$.

Proof: do it yourself.

$\cancel{(k+1)+(k+1)} = 2k+2 \notin C.$

$\cancel{(2k+1)+(2k+1)} = 4k+2 \pmod{p}$

$\equiv k \pmod{p}$

$\notin C.$

$k+1+x$, $0 \leq x \leq k$

$0 \leq y \leq k$

$(k+1+x)+(k+1+y) \pmod{3k+2}$

$\equiv 2k+2+\underbrace{(x+y)}$

$0 \text{———} 2k$

$\notin C.$

Given: $B = \{b_1, b_2, \dots, b_n\} \to$ n non-zero integers

To show: a sum-free subset of B of size $> \frac{n}{3}$.

Proof: Let $p = 3k+2$ be a prime with $p > b_1$, $p > b_2, \dots, p > b_n$.

We showed that

$C = \{k+1, k+2, \dots, 2k+1\}$ is a sum-free subset of $\mathbb{Z}_p$. $|C| = k+1$

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

$1, 2, \dots, p-1$

non-zero elmts in $\mathbb{Z}_p$.

of size $> \frac{p-1}{3}$.

Choose an x uniformly at random from $\{1, 2, \dots, p-1\}$.

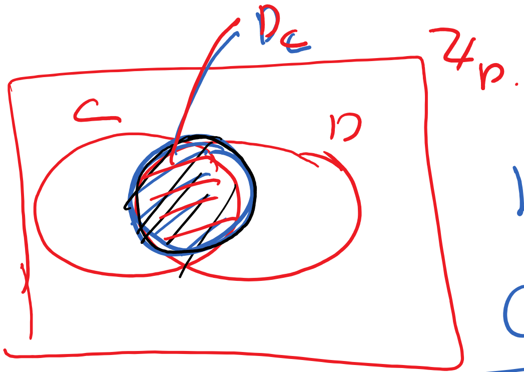
For every $b_i \in B$.

$d_i \equiv b_i \cdot x \pmod p$. cannot be a multiple of p.

So $0 < d_i \leq p-1$.

$$D = \{d_1, d_2, \ldots, d_n\} \subseteq \{1, 2, \ldots, p-1\}$$

We know $C = \{k+1, k+2, \ldots, 2k+1\} \subseteq \{1, 2, \ldots, p-1\}$ → sum-free.



Let $D_C = \{d_1, d_2, \ldots, d_k\}$

Clearly D_C is a sum-free subset of D.

Claim $\{b_1, b_2, \ldots, b_k\}$ is a sum-free subset of B.

Proof of Claim: Suppose not.

Suppose $b_1 + b_2 = b_3$.

Then, clearly $b_1 x + b_2 x = b_3 x$

$$\Rightarrow \quad b_1 x + b_2 x \equiv b_3 x \pmod{p}$$

i.e. $d_1 + d_2 \equiv d_3 \pmod{p}$

But this contradicts the fact that

$\{d_1, d_2, \dots, d_k\} = C \cap D$ is a sum-free subset.

Hence, the claim is ~~true~~

What is left: To show that for some choice of $x \in [p-1]$, the set $D \cap C$ is large $\to > \frac{n}{3}$.

$B = \{b_1, \dots, b_n\}$

$p = 3k+2$, $C = \underline{\{k+1, \dots, 2k+1\}}$ — sum-free.

$D = \{d_1, \dots, d_n\}$ was constructed by choosing x UAR from $[p-1]$ and then $d_i \equiv b_i x \pmod p$.

Take any $b_i \in B$

For any two $\underline{\text{distinct}}$ $x, y \in [p-1]$

$$b_i x \not\equiv b_i y \pmod p$$

Therefore, $\{\underline{b_i 1 \pmod p, b_i 2 \pmod p}, \dots, \underline{b_i(p-1) \pmod p}\} = [p-1]$.

Choosing x uniformly at random from $[p-1]$

$$\Pr[\underbrace{b_i x \pmod p}_{d_i} \in C] = \frac{|C|}{p-1} > \frac{1}{3}!$$

Random Variable X_i

$$X_i = \begin{cases} 1, & \text{if } \underline{d_i \in C} \end{cases}$$

$$X_i = \begin{cases} 1, & \text{if } a_i \in C \\ 0, & \text{otherwise} \end{cases}$$

$$E[X_i] > \frac{1}{3} \cdot 1 + 0 \cdot 0$$

$$> \frac{1}{3}$$

$$X_1, X_2, \ldots, X_n.$$

$$X = X_1 + X_2 + \cdots + X_n$$

$$E[X] = E[X_1 + X_2 + \cdots + X_n]$$

$$= \sum_{i=1}^{n} E[X_i] \quad \text{(by linearity of expectation)}$$

$$> \frac{n}{3}.$$

$\square$