07 December 2020 14:13

Sum-sets

Let A, B be sets whose elements are from a field $\mathbb{F}$. The sum-set of A and B is defined as:-

$$A+B = \{ a+b : a \in A, \ b \in B \}$$

Theorem [Cauchy–Davenport] If p is a prime and A, B are non-empty subsets of $\mathbb{F}_p$, (i.e. $\{0, 1, \ldots, p-1\}$ $\leftarrow$:) then

$$|A+B| \geq \min\{ p, |A|+|B|-1 \}$$

Example

$p = 7$. $\mathbb{F}_p = (\{0,1,2,3,4,5,6\}, +, \cdot)$

$A = \{1, 3\}$, $B = \{2, 5\}$, $B' = \{1, 4, 3\}$

$A+B = \{3, 6, 5, 1\}$ $\quad x = 3$, $\quad \{x\} - B = \{1, 5\}$

$A+B' = \{2, 3, 4, 5, 6\}$

$|A+B'| = 5 \geq |A|+|B|-1 = 2+3-1 = 4.$

$|A+B| = 4 \geq |A|+|B|-1 = 2+2-1 = 3.$

$|A+B| = 4 \geq |A| + |B| - 1 = 2+2-1 = 3$.

Proof: Con 1 If $|A|+|B| > p$, then the proof is easy. This is because $\forall x \in \mathbb{F}_p$, A and $\{x\} - B$ 'intersect/overlap'.

$\{x-b : b \in B\}$

This implies every $x \in \mathbb{F}_p$ is present in $A+B$. To explain in detail,

Let $x \in \mathbb{F}_p$. Suppose $c \in A$ and $c \in \{x\} - B$.

Then $\exists\, b \in B$ such that $x - b = c$.

So $b + c = x$.

So $|A+B| \geq p$.

Con 2: $|A| + |B| \leq p$.

In this case, we will show that

$$|A+B| \geq |A| + |B| - 1$$

We prove by contradiction. Suppose this is not true. That is, suppose

$|A+B| < |A| + |B| - 2$

$$|A+B| \le |A| + |B| - 2.$$

In that case, take an $(|A|+|B|-2)$-sized subset C of $\mathbb{F}_p$ such that

$A+B \subseteq C$. We have,

$$f(x,y) = \prod_{c \in C} (x+y-c) \bmod p,$$

when $x, y \in \mathbb{F}_p$.

Note, $f(x,y) = 0$, when $x \in A$ and $y \in B$.

Claim:

$$\deg(f(x,y)) = |C| = |A| + |B| - 2$$

We show that the monomial $x^{|A|-1} y^{|B|-1}$ has a non-zero coefficient.

coefficient of

$$\binom{|A|+|B|-2}{|A|-1}$$

To show $\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod p$

$|A|-1$ $\quad$ 1

Claim. $\binom{q}{r}$ is non-zero in $\mathbb{F}_p$, if $q < p$.

Suppose $\binom{q}{r} \equiv 0 \pmod p$.

Then, $\frac{q!}{r!(q-r)!} = kp$, for some k.

That is, $q! = kp\, r!\,(q-r)!$. That is, $p \mid q$ or $p \mid (q-1)$ or $p \mid (q-2)$ or ... or $p \mid 1$. We know none of them is true. So our assumption that $\binom{q}{r} \equiv 0 \pmod p$ is FALSE.

Thus, by combinatorial nullstellensatz, $\exists\, x \in A,\ y \in B$ such that $f(x,y) \neq 0$, which is a contradiction. Hence our assumption that $|A+B| \leq |A| + |B| - 2$ is FALSE. This proves the theorem.

□

What we are not doing.

Cauchy-Davenport Thm can be applied to prove (Erdős-Ginzburg-Ziv)-Theorem

END OF COURSE