

# Combi Mean Free Subset

March 13, 2025

**Problem.** Let  $p$  be a prime,  $A$  is an infinite set of integers. Prove that there is a subset  $B$  of  $A$  with  $2p-2$  elements, such that arithmetic mean of any pairwise distinct  $p$  elements in  $B$  does not belong in  $A$ .

**Solution.** For notation we define  $P(B,A)$  to be true iff  $A$  is an infinite set of integers and  $B$  is a subset of  $A$  with  $2p-2$  elements s.t. arithmetic mean of any pairwise distinct  $p$  elements in  $B$  does not belong in  $A$ . We have to prove that for each  $A$  there exists a  $B$  s.t.  $P(B,A)$  is true

We will prove the result for all infinite natural number sets  $A$ . First of all let's prove that it's sufficient to prove the result for all natural sets. Let's assume the proposition is true for all natural sets, then we will prove it's true for all integer sets. Let's define If  $A$  has infinite natural numbers then consider the set  $A^+ = \{x : x > 0, x \in A\}$ . Consider the subset  $B^+$  s.t.  $P(B^+, A^+)$  is true, then so is  $P(B^+, A)$ . If  $A$  has infinite negative numbers consider the set  $A^- = \{-x : x < 0, x \in A\}$ , consider the set  $B^-$  s.t.  $P(B^-, A^-)$  is true, consider the set  $C = \{-x : x \in B^-\}$ , we have  $P(C, A)$  to be true. Therefore it suffices to prove the result for  $A$  which are an infinite set of natural numbers.

Let  $A$  be an infinite set of natural numbers. Note that if a set  $C$  which is a subset of set  $T = \{x : x > t, x \in A\}$  and satisfies  $P(C, T) = \text{true}$  then we must also have  $P(C, A) = \text{true}$ . Let's index our set  $A$  s.t. its elements are arranged in increasing order so  $A = \{A_i : i \in \mathbb{N}, A_1 < A_2 < \dots\}$

Consider all the numbers in  $A$  modulo  $p$ . If there are 2 residues which have at least  $p-1$  integers modulo equal to them (let's call them  $a$  and  $b$ ), then choose  $p-1$  integers whose residue  $= a \pmod p$  and  $p-1$  integers whose residue  $= b \pmod p$ . It's clear that mean of any  $p$ -subset of this set is not an integer hence we can set  $B$  to be equal to this set and it satisfies the original condition.

Now if that's not the case consider the function  $f_k : A \rightarrow \mathbb{Z}/p^k\mathbb{Z}$  where  $f_k(a) = a \pmod{p^k}, \forall a \in A$ . Now since  $\mathbb{Z}/p^k\mathbb{Z}$  is a finite set it must have at least one integer whose inverse image is infinite. If for some  $k$  there are at least 2 integers whose inverse image is an infinite set then choose minimum such  $k$ . let's call these 2 integers  $a$  and  $b$ . Clearly  $k > 1$ , so numbers modulo  $p^{k-1}$  will have infinite inverse image for one number and finite for every other modulo. let's call this number which has

infinite inverses in mapping modulo  $p^{k-1}$  be  $t$ . So after a finite number  $N$ , we have  $A_i \equiv t \pmod{p^{k-1}}$  for all  $i \geq N$  let's consider the set  $S_1 = \{A_j : j > N, A_j \equiv a \pmod{p^k}\}$  and  $S_2 = \{A_j : j > N, A_j \equiv b \pmod{p^k}\}$ . Consider a set  $S$  which has  $p-1$  numbers from  $S_1$  and  $p-1$  from  $S_2$ , then we claim that  $P(S, A)$  is true. This is true as any mean of  $p$  numbers of  $S$  will be greater than  $A_N$  but the mean will not have a residue  $= t \pmod{p^{k-1}}$  but all numbers greater than  $A_N$  in  $A$  will have residue  $= t \pmod{p^{k-1}}$ .

Now consider that there is not a single  $k$  for which we have 2 residues occuring infinite number of times. Then let's define  $G : \mathbb{N} \rightarrow \mathbb{N}$  s.t.  $G(k) = a$  where  $a$  is the residue occurs infinitely many times modulo  $p^k$ .

Let's define the sequence  $T_i = \max(\{j : A_j \not\equiv G(i) \pmod{p^i}\})$  where  $\max$  of empty set is 0, note that  $T_i$  is an non-decreasing sequence ( as the  $i+1$  th set is superset of  $i$  th set). Note that the sequence  $T_i$  is also unbounded ( if it's eventually constant then after some  $N$ ,  $A_i \equiv A_j \pmod{p^t}$  for all  $t$  which is a contradiction). Now choose set  $C = \{A_{T_i} : i > 10, T_i > T_{i-1}\}$ , choose any  $2p-2$  subset of  $C$ , let's call it  $B$ . We claim that  $P(B, A)$  is true.

Let's choose  $p$  elements from  $B$ , let's call them  $A_{T_{j_1}}, A_{T_{j_2}} \dots A_{T_{j_p}}$  where  $j_1 < j_2 < \dots < j_p$ . Now note that their mean is greater than  $A_{T_{j_1}}$  hence their value modulo  $p^{j_1-1}$  must be equal to  $G(j_1-1)$  if it is in  $A$ . But to consider the residue of mean of  $p$  numbers modulo  $p^{j_1-1}$  we only have to consider these numbers modulo  $p^{j_1}$  since all other terms wont affect the value of mean modulo  $p^{j_1-1}$ . Now note that  $G(j_1) \equiv G(j_1-1) \pmod{p^{j_1-1}}$ , so  $G(j_1) = G(j_1-1) + p^{j_1-1}y$  where  $y < p$ , similarly  $A_{T_{j_1}} = G(j_1-1) + p^{j_1-1}x$  as  $T_{j_1} > T_{j_1-1}$  where  $x < p, x \neq y$

$$\sum_{k=1}^{k=p} \frac{A_{T_{j_k}}}{p} \equiv (G(j_1-1)p + y(p-1)p^{j_1-1} + xp^{j_1-1})/p \equiv (G(j_1-1) + p^{j_1-2}(x + (p-1)y)) \not\equiv G(j_1-1) \pmod{p^{j_1-1}}$$

last inequation holds as  $x \neq y \pmod{p}$ . Hence mean does not have a residue of  $G(j_1-1)$  modulo  $p^{j_1-1}$ , therefore  $P(B, A)$  is true.

*QED*

**Exploration.**  $p$ -base numbers to the rescue, thinking in base- $p$  helped give the solution a direction

**Tags.** Combinatorics , Number Theory , primes , mean , subset ,  $2p-2$