Problem 11666
(American Mathematical Monthly, Vol.119, October 2012)

Proposed by Dmitry G. Fon-Der-Flaass (Russia) and Max. A. Alekseyev (USA).

Let m be a positive integer, and let A and B be nonempty subsets of $\{0,1\}^m$. Let n be the greatest integer such that $|A|+|B| > 2^n$. Prove that $|A+B| \geq 2^n$. (Here, $|X|$ denotes the number of elements in X, and $A+B$ denotes $\{a+b : a \in A, b \in B\}$, where addition of vectors is componentwise modulo 2.)

Solution proposed by Roberto Tauraso, Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy.

We will prove a more general statement.

Let p be a prime and let A and B be nonempty subsets of the abelian group $\mathbb{Z}_p^m$.
If $|A| + |B| > p^n$ then $|A + B| \geq p^n$.

We divide the proof in several claims:

i) If $|A| = 1$ then $|A| + |B| > p^n$ implies that $|B| \geq p^n$ and

$$|A + B| = |a + B| = |B| \geq p^n.$$

ii) Assume that $|A| > 1$. If B intersects A *properly* that is if

$$A \cap B \neq \emptyset \quad \text{and} \quad A \setminus B \neq \emptyset$$

then let $A' = A \cap B$ and let $B' = A \cup B$ so that $|A'| < |A|$, and $|A'|+|B'| = |A|+|B|$. Moreover if $a' + b' \in A' + B'$ then

$$a' + b' \in A + B \text{ for } b' \in A \text{ and } a' + b' \in B + A \text{ for } b' \in B$$

which imply that $A' + B' \subset A + B$ and $|A' + B'| \leq |A + B|$. Hence it suffices to prove the required property for A' and B' with $1 \leq |A'| < |A|$.

iii) If B does not intersect A properly, take $A' = A + (p-1)a + b$ with $a \in A$ and $b \in B$ then $b = a + (p-1)a + b \in A' \cap B \neq \emptyset$. If there is $b \in B$ such that $A' \setminus B \neq \emptyset$ then B intersects A' properly and we can apply i) with A replaced by A'.

iv) If at each step it is possible to apply iii) and ii), we are able to reduce the size of the set A until we can use i) and the proof is complete. Thus it suffices to consider the case when at some step we can not apply iii): $A' \setminus B = \emptyset$ for all $b \in B$, that is $(A + (p-1)a) + B \subset B$. Since $0 \in (A+(p-1)a)$ it follows that $B \subset (A+(p-1)a)+B$ and therefore $(A+(p-1)a)+B = B$. Consider the set $S(B) = \{x \in \mathbb{Z}_p^m : x + B = B\}$. It is easy to verify that $S(B)$ is a subgroup of $\mathbb{Z}_p^m$, and $(A + (p-1)a) + B = B$ implies that $(A + (p-1)a) \subset S(B)$ and B is the union of cosets of $S(B)$. Hence $|A| = |(A + (p-1)a)| \leq |S(B)| = p^d$, $|B| = r|S(B)| = rp^d$ for some integers $d \geq 0$ and $r \geq 1$ and

$$|A + B| = |(A + (p-1)a) + B| = |B| = rp^d \quad , \quad |A| + |B| = |(A + (p-1)a)| + |B| \leq (r+1)p^d.$$

Now $rp^d = |A + B| < p^n < |A| + |B| \leq (r+1)p^d$ yields the contradiction $1 \leq r < p^{n-d} < r+1$ (p^{n-d} is an integer!). Therefore $|A + B| \geq p^n$.

□