Let $p$ be a prime number at least three and let $k$ be a positive integer smaller than $p$. Given $a_1, \ldots, a_k \in \mathbb{F}_p$ and distinct elements $b_1, \ldots, b_k \in \mathbb{F}_p$, prove that there exists a permutation $\sigma$ of $[k]$ such that the values of $a_i + b_{\sigma(i)}$ are distinct modulo $p$.

**Solution.** See [1]. We take advantage of the following lemmas.

**Lemma 1** (Combinatorial Nullstellensatz). Let $F$ be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree $\deg(f)$ of $f$ is $\sum_{i=1}^{n} t_i$, where each $t_i$ is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in $f$ is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of $F$ with $|S_i| > t_i$, there are $s_1 \in S_1, \ldots, s_n \in S_n$ so that $f(s_1, \ldots, s_n) \neq 0$.

**Proof.** Refer to [2].

**Lemma 2** (Vandermonde determinant). Let

$$V = \begin{bmatrix} x_1^{j-1} \\ x_2^{j-1} \\ \vdots \\ x_n^{j-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}$$

be a square Vandermonde matrix. Then

$$\det(V) = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

**Proof.** Refer to [3].

Let $f = f(x_1, \ldots, x_k)$ be a polynomial over $\mathbb{F}_p$ defined as

$$f(x_1, \ldots, x_k) = \prod_{1 \leq i < j \leq k} (x_i - x_j) \prod_{1 \leq i < j \leq k} [(a_i + x_i) - (a_j + x_j)].$$

Let $B$ be a subset of $\mathbb{F}_p$ with $|B| = k$. If we can apply Lemma 1 with $S_1 = \cdots = S_k = B$, then there are $b_i \in B$ (with indices possibly different from the ones given in the problem) such that

$$f(b_1, \ldots, b_k) = \prod_{1 \leq i < j \leq k} (b_i - b_j) \prod_{1 \leq i < j \leq k} [(a_i + b_i) - (a_j + b_j)] \neq 0.$$

Thus, the elements $b_i$ of $B$ are pairwise distinct, and so are the values of $a_i + b_i$ as desired.

It remains to check the conditions of the lemma. Let $t_1 = t_2 = \cdots = t_k = k - 1$. Note that

$$\deg(f) = \binom{k}{2} + \binom{k}{2} = k(k - 1) = \sum_{i=1}^{k} t_i.$$

Consider the monomial $g = \prod_{i=1}^{k} x_i^{k-1} = k(k - 1)$. Since $\deg(f) = \deg(g) = k(k - 1)$, the constants $a_i$ are irrelevant to the coefficient of $g$. Hence, it coincides with the one of $g$ in the polynomial

$$\prod_{1 \leq i < j \leq k} (x_i - x_j) \prod_{1 \leq i < j \leq k} (x_i - x_j) = \prod_{1 \leq i < j \leq k} (x_i - x_j)^2.$$
By Lemma 2,
\[
\prod_{1 \leq i < j \leq k} (x_i - x_j) = (-1)^{\binom{k}{2}} \prod_{1 \leq i < j \leq k} (x_j - x_i)
\]
\[
= (-1)^{\binom{k}{2}} \begin{vmatrix}
1 & 1 & \cdots & 1 \\
x_1 & x_2 & \cdots & x_k \\
\vdots & \vdots & \ddots & \vdots \\
x_1^{k-1} & x_2^{k-1} & \cdots & x_k^{k-1}
\end{vmatrix} = (-1)^{\binom{k}{2}} \sum_{\sigma \in \mathbb{S}_n} \text{sgn}(\sigma) \prod_{i=1}^{k} x_{\sigma(i)}^{i-1} = \sum_{\sigma \in \mathbb{S}_n} \text{sgn}(\sigma) \prod_{i=1}^{k} x_{\sigma(i)}^{k-i}.
\]

We have
\[
\left( \prod_{1 \leq i < j \leq k} (x_i - x_j) \right)^2 = (-1)^{\binom{k}{2}} \left[ \sum_{\sigma \in \mathbb{S}_n} \text{sgn}(\sigma) \prod_{i=1}^{k} x_{\sigma(i)}^{i-1} \right] \left[ \sum_{\sigma \in \mathbb{S}_n} \text{sgn}(\sigma) \prod_{i=1}^{k} x_{\sigma(i)}^{k-i} \right].
\]

Therefore, the coefficient of \( g \) is \((-1)^{\binom{k}{2}} k!\), which is nonzero modulo \( p \) because \( p \) is an odd prime and \( k < p \). This completes the proof. \( \square \)

References

