Problem 1. – *Julian Lyczak, IST Austria*
Let p be a prime. A subset $X \subseteq \mathbb{F}_p^\times$ satisfies the following two properties.

- *The sum $x + y$ of two distinct element $x, y \in X$ lies in $\mathbb{F}_p^\times$.*
- *Any element $s \in \mathbb{F}_p^\times$ can be uniquely written as the sum of two distinct elements of X.*

Prove that $p = 11$ and X is either the quadratic residues modulo 11, or the quadratic non-residues.

Solution by Julian Lyczak and Carlo Pagano. Let $x_1, \ldots, x_r$ be the distinct elements of X. We begin with the following remarks.
By the conditions we see that $\{x_i + x_j \mid i < j\}$ and $\mathbb{F}_p^\times$ are equals as multisets. The first multiset contains $\binom{r}{2}$ elements and the second $p-1$. We derive that $p - 1 = \frac{r(r-1)}{2}$. In particular we find that $p > 3$.
If a subset $X \subseteq \mathbb{F}_p^\times$ which satisfies the conditions of the problem, then it is easily checked that the subset $aX := \{a \cdot x \mid x \in X\}$ also satisfies the conditions for any $a \in \mathbb{F}_p^\times$.

Now let $\zeta = e^{\frac{2\pi i}{p}}$ be a primitive p-th root of unity and consider the element

$$w_Y = \sum_{x \in Y} \zeta^x$$

for any subset $Y \in \mathbb{F}_p$. We will compute the norm of the complex number w_X in two ways. The first method will prove that $|w_X| \leq 2$ and the second that $|w_X|^2 = r - 2$.
For the subset X in the problem we find

$$\begin{aligned} w_X^2 &= \left(\sum_{x \in X} \zeta^x\right)^2 \\ &= \sum_{x \in X} \zeta^{2x} + \sum_{\substack{x \neq y \\ x, y \in X}}^{r} \zeta^{x+y} \\ &= \sum_{x \in X} \zeta^{2x} + 2(\zeta + \zeta^2 + \ldots + \zeta^{p-1}) \\ &= w_{2X} - 2. \end{aligned}$$

Consider the function $f \cdot \mathbb{C} \to \mathbb{C}, x \mapsto x^2 + 2$. Since $2X$ also satisfies the conditions of the problem we find

$$f^{p-1}(w_X) = w_{2^{p-1}X} = w_X.$$

Hence w_X is a periodic point of f. Now assume that a complex number z satisfies $|z| > 2$. We will show that z is not a periodic point of f. This follows from

$$|f(z)| = |z^2 + 2| \geq |z^2| - |2| > 2|z| - 2 > |z|.$$

This proves that $|w_X| \leq 2$.
To compute the norm of w_X exactly in terms of r we use the following lemma.

Lemma. *Any element $\mathbb{F}_p^\times$ can be written in precisely two ways as the difference of two elements in X.*

Proof. Assume that we can write an element of $d \in \mathbb{F}_p^\times$ as the difference in two distinct ways, say $d = a_1 - b_1 = a_2 - b_2$ with $a_i, b_i \in X$ with $a_1 \neq a_2$ and equivalently $b_1 \neq b_2$. Since d is invertible modulo p we also see that $a_1 \neq b_1$ and $a_2 \neq b_2$. We will prove that either $a_1 = b_2$ or $a_2 = b_1$. Rewrite to $a_1 + b_2 = a_2 + b_1$ and call this sum $s \in \mathbb{F}_p$. If $s \neq 0$ then we have two ways two write $s \in \mathbb{F}_p^\times$ as the sum of two elements in X. This is only possible if at least one of the sums has two equal terms, due to the second condition. This proves that $a_1 = b_2$ or $a_2 = b_1$. Now note that both equalities can not hold since $p \neq 2$.
Let us prove that no element $d \in \mathbb{F}_p^\times$ can be written as the difference of elements in X in three ways, say

$$d = a_1 - b_1 = a_2 - b_2 = a_3 - b_3.$$

Without loss of generality we find $a_1 = b_2$, because if $a_2 = b_1$ we can consider $-d$. If we now had $b_2 = a_3$ we would have $a_1 = a_3$ and hence $(a_1, b_1) = (a_3, b_3)$. So we find $a_2 = b_3$ and we conclude that

$$3d = (a_1 - b_1) + (a_2 - b_2) + (a_3 - b_3) = 0.$$

Since $p \neq 3$ this contradicts the fact that $d \in \mathbb{F}_p^\times$.
We have $p-1$ elements $d \in \mathbb{F}_p^\times$ and $2\binom{r}{2}$ differences $x-y$ for distinct $x, y \in X$. Since $p-1 = \binom{r}{2}$ and every d can be written in at most two ways as a difference, we see that every $d \in \mathbb{F}_p^\times$ can be written in exactly two ways as a difference of elements in X. $\square$

The lemma implies that

$$\begin{aligned} |w_X|^2 &= \left(\sum_{x \in X} \zeta^x\right)\left(\sum_{x \in X} \zeta^{-x}\right) \\ &= \sum_{x \in X} \zeta^x \zeta^{-x} + \sum_{\substack{x \neq y \\ x,y \in X}}^{r} \zeta^{x-y} \\ &= r + 2(\zeta + \zeta^2 + \ldots + \zeta^{p-1}) \\ &= r - 2. \end{aligned}$$

We conclude that $r - 2 = |w_X|^2 \leq 2^2$ and hence $r \leq 6$. We consider the remaining cases separate. If r is one of the values $1, 3$, or 6 then $p = \binom{r}{2} + 1$ is not a prime number. For $r = 2$ we find $p = 2$ which is also not possible. The remaining cases are $r = 3$ and $p = 7$, and $r = 5$ and $p = 11$. Let us make the following general remarks to prove the first case yields no solutions and the second case gives two possible subsets X.
If a subset X satisfies the conditions and contains an element a, then the subset $a^{-1}X \subseteq \mathbb{F}_p^\times$ also works and contains $1 \in \mathbb{F}_p^\times$. So we can assume that X contains 1.
We know that the difference 1 occurs twice between elements of X, let say $x, x+1, y, y+1 \in X$ with $x \neq y$. Since $x + (y+1) = (x+1) + y$ these four elements are not all distinct. Without loss of generality we have $x = y + 1$ and hence X contains three consecutive elements.
Now consider an X with $r = 3$ and $p = 7$ which contains $1 \in \mathbb{F}_7^\times$. The conditions on X imply that $6 \notin X$ and that X contains either 2 or 5, and it contains either 3 or 4. Since X also contains three consecutive numbers the only possibility is $X = \{1, 2, 3\}$ which does work.
For $r = 5$ we have $p = 11$ and X contains precisely one of x and $-x$ for all $x \in \mathbb{F}_p^\times$. Again assume that X contains $1 \in \mathbb{F}_{11}^\times$. Consider the possibilities of three consecutive numbers in X.

- X contains $\{1, 2, 3\}$. Then X can not contain 8, 9 and 10. It also can not contain 4, since $1 + 4 = 2 + 3$. So the remaining two elements of X come from $\{5, 6, 7\}$. These elements can not be consecutive, so X must be $\{1, 2, 3, 5, 7\}$, but $1 + 7 = 3 + 5$ so this does not satisfy the conditions of the problem.
- X contains $\{2, 3, 4\}$. However, X also contains 1 and $1 + 4 = 2 + 3$.
- X contains $\{3, 4, 5\}$. Now X can not contain 2, 6, 7, 8 and 10. So the remaining element of X must be 9. This gives $X = \{1, 3, 4, 5, 9\}$ which is the set of quadratic residues modulo 11.
- X contains $\{5, 6\}$. Now we have $5 + 6 \equiv 0 \mod 11$.
- X contains $\{6, 7, 8\}$. The set X can not contain 3, 4, 5 and 10. Neither 2 nor 9 completes X to a correct set.
- X contains $\{7, 8, 9\}$. Now 2, 3, 4 and 10 are excluded. Again, neither 5 nor 6 works.

So X is a coset of the quadratic residues modulo 11. $\square$