Problem 7. Let p be a prime number and $k < p$ a positive integer. Let $m = \left\lceil \frac{p}{k+1} \right\rceil$. Show that there is a set $A \subseteq \{1, 2, \ldots, p-1\}$ with at most 2m elements such that for every $a \in \{1, 2, \ldots, p-1\}$ there are $b \in A$ and $c \in \{1, 2, \ldots, k\}$ such that p divides $a - bc$.

Solution. Recall that for any $a \in \{1, 2, \ldots, p-1\}$ there is unique $b \in \{1, 2, \ldots, p-1\}$ such that p divides $ab - 1$. We call b the inverse of a modulo p. Let A be the set of all numbers in $\{1, 2, \ldots, p-1\}$ whose inverse is either in $\{1, 2, \ldots, m\}$ or in $\{p-1, p-2, \ldots, p-m\}$. Thus A has at most $2m$ elements (it has exactly $2m$ elements if $k > 1$ and $p > 2$). We will prove that A has the required property. Note that A has the follwing property:

$$\text{for any non-zero integer } d \in [-m, m] \text{ there is } b \in A \text{ such that } p \text{ divides } bd - 1. \tag{1}$$

Consider now any $a \in \{1, 2, \ldots, p-1\}$. Let

$$T_j = \{j(k+1) + 1, \ldots, j(k+1) + (k+1) = (j+1)(k+1)\}.$$

The union of the sets $T_0, T_1, \ldots, T_{m-1}$ contains the set $\{1, 2, \ldots, p\}$. Indeed, this follows from the fact that $m(k+1) \geq \frac{p}{k+1}(k+1) = p$. We say that an integer l if of type j if the unique $r \in \{1, 2, \ldots, p\}$ such that $l - r$ is divisible by p belongs to T_j. Thus we have m different types. It follows that two of the $m+1$ integers $a, 2a, \ldots, (m+1)a$ are of the same type. Let us say that sa and ta are of type j for some j and some $1 \leq s, t \leq m+1$, $s \neq t$. This means that $sa - u$ and $ta - w$ are divisible by p for some $u, w \in T_j$. Without loss of generality, we may assume that $u < w$. Let $c = w - u$ We see that $(t-s)a - (w-u) = (t-s)a - c$ is divisible by p. Note that $0 \neq t - s \in [-m, m]$ and $1 \leq c \leq k$. By (1), there is $b \in A$ such that p divides $b(t-s) - 1$. The numbers

$$b((t-s)a - c) = b(t-s)a - bc = (b(t-s) - 1)a + a - bc \text{ and } b(t-s) - 1$$

are both divisible by p. It follows that $a - bc$ is divisible by p. Since a was arbitrary and $b \in A$, $c \in \{1, 2, \ldots, k\}$, this completes our proof that A has the required property.

Remark. We wrote the solution using just the language of divisibility. It would be more natural to use the concept of congruences. In fact, even more natural would be to note that the residues modulo p form a finite field $\mathbb{F}_p$. The non-zero residues form a group $\mathbb{F}_p^\times$ under multiplication. Let $S = \{1, 2, \ldots, k\} \subseteq \mathbb{F}_p^\times$. For any $t \in \mathbb{F}_p^\times$ the set $tS = \{ta : a \in S\}$ is called the translate of S by t. Our problem can be now phrased as follows: the group $\mathbb{F}_p^\times$ can be covered by at most $2m$ translates of S. This leads to the following concept. Let G ba a group and S a subset of G. The covering number $\tau(S, G)$ of S is the smallest number of translates of S which cover G (it can be infinite). For a nice discussion of the covering number we recommend the following paper (clickable link):

On covering by translates

(Béla Bollobás, Svante Janson, and Oliver Riordan, *ON COVERING BY TRANSLATES OF A SET*)

As a good excercise, we suggest solving the following problem (using Problem 7 as a key tool).

Problem. Let p be a prime. Prove that elements of the set $\{1, 2, \ldots, p-1\}$ can be colored in at most $2 + \lceil \sqrt{2p} \rceil$ colors so that for any non-empty subset A of $\{1, 2, \ldots, p-1\}$ which consists of numbers of the same color, the sum of all elements in A is not divisible by p. Hint: take k to be the largest integer smaller than $(\sqrt{8p+9} - 1)/2$.