1

PEN O35

(Romania TST 1998) Let n be a prime and $a_1 < a_2 < \ldots < a_n$ be integers. Prove that $a_1, a_2, \ldots, a_n$ is an arithmetic progression if and only if there exists a partition of $\mathbb{N}_0 = \{0, 1, 2, \ldots,\}$ into n sets $A_1, A_2, \ldots, A_n$ so that

$$a_1 + A_1 = a_2 + A_2 = \ldots = a_n + A_n,$$

where $x + A = \{x + a | a \in A\}$.

Vasile Pop

First Solution. Assume firstly that $a_1, a_2, \ldots, a_n$ is an arithmetic progression. Define $A_i = \{knr + ir + j | k \in \mathbb{N}_0, 0 \le j \le n-1\}$. It is easy to see that $\mathbb{N}_0 = A_1 \cup A_2 \ldots \cup A_n$ and $A_i \cap A_j = \emptyset$ for $i \neq j$.

The converse part is much more difficult. For convenience of notations, let $B_i = A_{n-i}$ and $r_i = a_n - a_{n-i}$. Hence $B_i = B_0 + r_i$ and $\mathbb{N}_0 = B_0 \cup B_1 \cup \ldots \cup B_{n-1}$. Call a segment of length k of a subset B_i a set $S \subset B_i$ of the form $\{m+1, \ldots, m+k\}$, where $m, m+k+1 \notin B_i$.

Lemma 1. *Any segment of any subset B_i has length $r = r_1$.*

Proof. Note that if B_i for some $i > 0$ contains a segment of length different from r, then so must B_0, since $B_i = B_0 + r_i$. Hence it is enough to show that B_0 consists only of segments of length r. Indeed, note that if $m \in B_0$ then $m + r \in B_1$, hence any segment of B_0 has length at most r. Assume to the contrary that there is at least one segment of length less than r in B_0. Among all such segments, let $S = \{m+1, \ldots, m+k\} \subset B_0$ with $k < r$ be the one with smallest m (the 'first' one). Then $\{m+1+r, m+2+r, \ldots, m+k+r\}$ is a segment of B_1. Since $m+k+1 \notin B_0$, $m + r \notin B_1$, and the set $\{m+k+1, \ldots, m+r\}$ has $r - k > 0$ elements it follows that there is a segment $T \subset \{m+k+1, \ldots, m+r\}$ of some B_i, $i > 0$ of length at most $r - k$. Hence $T - r_i = \{m+k+1-r_i, \ldots, m+r-r_i\}$ is a segment of length at most $r - k < r$ of B_0. Since $m + k + 1 - r_i < m$, this contradicts the definition of S. □

Lemma 2. *Each B_i starts with the segment $S_i = \{ir, ir+1, \ldots, ir+r-1\}$.*

Proof. We prove the statement by induction on i. It is clear that $S_0 = \{0, 1, \ldots, r-1\} \subset B_0$, which is the base of our induction. Assume the statement true for $0 \le i < k$. We are going to show the statement for $i = k$.

So $S_i \subset B_i$, $i = \overline{0, k-1}$. Let $S_k \subset B_j$ and assume, to the contrary, that $j \neq k$. From $a_1 < a_2 < \ldots < a_n$ we get $r_1 < r_2 < \ldots < r_n$. This implies $j < k$. But then S_k is already the second segment of B_j (after S_j) which is impossible for $j > 0$, since we haven't reached the second segment of B_0 yet. Hence $j = 0$, so $S_k \in B_0$. Note that for $j < k$ we have $r_j = jr$. Then it follows that $S_i \subset B_{i-k}$ for $i = k, k+1, \ldots, 2k-1$. Again, S_{2k} must be a subset of either B_0 or B_k. If $S_{2k} \subset B_0$ then we apply the above argument again to obtain $S_i \in B_{i-2k}$ for $i = 2k, 2k+1, \ldots, 3k-1$. Repeating this process, we obtain that the first segment of B_k must be of the form S_{tk}, for some t. This implies $r_k = tk$.

Let's prove now by induction on l, that if $lk < n$ then each apparition of a segment from B_{lk} is followed by a sequence of segments belonging to the sets $B_{lk+1}, \ldots, B_{lk+-1}$, implying that $(l+1)k \leq n$. Moreover, if $(l+1)k \leq n$ then the first segment of $B_{(l+1)k}$ is of the form S_{tk} for some t.

For $l = 0$ the statement of trivial. Assume now the statement true for all $l < u$ and let's prove it for $l = u$. Assume $lk < n$. Applying the inductive hypothesis for $l = u-1$, we get that the first segment of $B_{(u+1)k} = B_{lk}$ is of the form S_{tk} for some t. Take the segment S_{tk+i}, $0 < i < k$. Let's prove that it belongs to a new segment B_{lk+i}. Indeed assume $S_{tk+i} \in B_j$ for some j. Assume B_j has appeared before. The inductive hypothesis shows that each B_{xk+i}, $x < l$, $0 \leq i < k$ has only segments of the form $S_{x'k+i}$, for some x'. Hence $r_{xk+i} = Mrk + ri$, for some M. Also, the inductive hypothesis shows that $r_{xk} + ri = r_{xk+i}$, $0 \leq i < k$. It follows that $j = t'k + i$, for some $t' < l$ and that $r_{t'k} = r_j - ri$. Since $S_{tk+i} \in B_j$ has been obtained by adding r_j to some segment $S_{hk} \in B_0$, it follows that when adding $r_{t'k} = r_j - ri$ to S_{hk} we should obtain a segment belonging to $B_{t'k}$. However $S_{hk} + r_j - r_i = S_{tk+i} - ri = S_{tk} \in B_{lk}$. Contradiction because $t' < l$.

From the last result, we infer that $k|n$, which is impossible for $1 < k < n$. Hence the proof of Lemma 2 is ended. □

Lemma 2 states that $S_i \subset B_i$, for $i = 0, 1, \ldots, n-1$, hence $r_i = ir$ for all i, implying that $a_1, a_2, \ldots, a_n$ is an arithmetical progression with term difference r.

□

Second Solution. If $a_1, \ldots, a_n$ is an arithmetical progression, proceed like in the previous solution. Let's prove the converse. Again, let $B_i = A_{n-i}$ and $r_i = a_n - a_{n-i}$, hence $B_i = B_0 + r_i$. Let $f(m,i)$ be the number of nonnegative integers $\leq m$ which are in B_i. Clearly $f(m,i) = f(m-r_i, 0)$. Because the sets (B_i) cover the set of nonnegative integers, $m+1 = f(m,0) + f(m,1) + \ldots + f(m, n-1)$. Define $x_i = f(i,0)$ for $i \geq 0$ and $x_i = 0$ for $i < 0$. Using the above remark, we obtain

$$x_m + x_{m-r_1} + \ldots + x_{m-r_{n-1}} = m+1,$$

for $m \geq 0$. Adding the above relation for $m-1$, $m+1$ and subtracting it twice for m, we obtain

$$t_m + t_{m-r_1} + \ldots + t_{m-r_{n-1}} = 0,$$

where $t_i = x_{i+1} + x_{i-1} - 2x_i$.

From the definition of t_i and x_i we observe that $t_i \in \{-1, 0, 1\}$. This and the recurrence relation for the sequence (t_i) implies that (t_i) is a periodic sequence. Let M be the length of its smallest period. Then $t_{i+1} + t_{i+2} + \ldots + t_{i+M}$ is a constant value. Let's prove that this value equals 0. Indeed, let $C = t_{i+1} + t_{i+2} + \ldots + t_{i+M}$. Let N be a positive integer. Sum up the recurrence relation for $m = 0$ to N. We obtain

$$0 = n(t_0 + \ldots + t_{N-r_{n-1}}) + E,$$

where E consists of finitely many t_i's (for example, less than $(r_{n-1}+1)^2$ t_i's), hence it is bounded: $|E| < h$ for some constant h implying that $t_0 + \ldots + t_{N-r_{n-1}}$ is bounded for all N. On the other side $t_0 + \ldots + t_{kM-1} = kC$ as it is the sum of k blocks of t_i's. If $C \neq 0$ for large enough k we have $|kC| > h$. Impossible. So $C = 0$.

Since $t_{i+1} + \ldots + t_{i+M} = (x_i - x_{i+1}) - (x_{i+M} - x_{i+M+1}) = 0$, we have the implication: if $i \in B_0$ then $i + M \in B_0$. Moreover, if $i \in B_j$ then $i + M \in B_j$ for $j = \overline{0, n-1}$. Let B be the subset of B_0 having all elements less than M. Let's prove that

$$B \cup B + r_1 \cup \ldots \cup B + r_{n-1} = \{0, 1, \ldots, M-1\}.$$

It is obvious that every $m \in \{0, 1, 2, \ldots, M-1\}$ belongs to some $B + r_i$. For the converse, let $x = y + r_i$, for some $y \in B$. Assume, to the contrary, that $x \geq M$. Let $x = qM + r$, $q \geq 1$, $M - 1 \geq r \geq 0$. Then $r \in B + r_i$, hence $r - r_i \in B$, hence $r \geq r_i$. Since $y + r_i = qm + r \geq qm + r_i$, we obtain $y \geq qm \geq m$. Impossible since $y \in B$.

Denote now by R the set $\{0, r_1, \ldots, r_{n-1}\}$. Define set addition as $X + Y = \{x + y | x \in X, y \in Y\}$. We are to show that if $B + R = \{0, 1, \ldots, M-1\}$ and $|R|$ is a prime number, then $0, r_1, \ldots, r_{n-1}$ form an arithmetic progression.

We will make use of the following Lemma, which proves better than anything the power of the Extremal Principle:

Lemma 3. *Let X and Y be two sets so that $X + Y = \{0, 1, \ldots, M-1\}$. Let $m = \min(Y \setminus \{0\})$. Then $|X|$ is a multiple of m and there exist sets X' and Y' so that $X' + Y' = \left\{0, 1, \ldots, \frac{M}{m} - 1\right\}$ and $X = mX' + \{0, 1, \ldots, m-1\}$, $Y = mY'$.*

Proof. Let's show firstly that every element of Y is a multiple of m. Indeed, note firstly that $\{0, 1, \ldots, m-1\} \subseteq X$. Note also that every element from $\{0, 1, \ldots |X| \cdot |Y| - 1\}$ can be uniquely written as $x + y$, where $x \in X$ and $y \in Y$. Assume to the contrary that there is an $y = qm + r \in Y$, with $0 < r < m$. Among all such numbers, take the one with smallest q. If $qm \in Y$, since $r \in X$ then $qm + r = (qm + r) + 0$ are two representations of the same number as $x + y$, $x \in X$, $y \in Y$. Impossible. Hence $qm \notin Y$. Also, $qm \notin X$, because otherwise $qm + m = (qm + r) + (m - r)$. Hence $qm \notin X, Y$. Since $qm < qm + r$ and all elements less than $qm + r$ in Y are multiples of m, we deduce the existence of a positive u so that $um \in Y$ and $(q - u)m \in X$. Let's prove now that: if $km \in X$ for some $k < q - u$ then $km + r \in X$, for all $0 < r < m$; and if $km + r \in X$ for some $0 < r < m; k < q - u$ then $km \in X$. Assume to the contrary that there is a pair (k, r) so that $km \in X$ and $km + r \notin X$ or $km \notin X$ and $km + r \in X$. Among all such pairs take the one with the smallest k. Assume firstly $km \in X$ and $km + r \notin X$. Consider the number $z = km + r$. By our choice $z \notin X$. By the minimality of q, we obtain $z \notin Y$, hence $z \notin X, Y$. Hence there is a positive $x < q$ such that $z = xm + (k - x)m + r$, where $xm \in Y$ and $(k - x)m + r \in X$. *By our choice of k and r, we have $(k - x)m \in X$.* Since $km \in X$ and $xm \in Y$, we obtain two distinct representations: $km = km + 0 = (k - x)m + xm$. Impossible. The second case is treated in an analogous way. Consider now the number $Z = (q - u)m + r$. If $Z \in X$, then $Z + um = (qm + r) + 0$, impossible. Also from the minimality of q, $Z \notin Y$. Hence there exist $x \in X$ and $y \in Y$ so that $Z = x + y$. Because $Z < qm + r$, $x = tm$ for some $t > 0$, and $y = (q - u - t)m + r$. From what was proved above, we obtain that $(q - u - t)m \in X$. But then $(q - u - t)m + um = (q - u)m + 0$ are two distinct representations of $(q - u)m$ as sum $x + y$, $x \in X$ and $y \in Y$. Contradiction.

So every element of Y is a multiple of m and writing $Y = mY'$, for some set Y' makes sense. We'll now prove in a completely similar way as above that if $km \in X$ for some k, then $km+r \in X$, for $0 < r < m$; and conversely, if $km + r \in X$ for some $0 < r < m$, then $km \in X$. Among all such *bad* pairs, take the one with the least k. For the sake of completeness we shall now treat the second case. Assume that $km + r \in X$ for some $0 < r < m$ and that $km \notin X$. It is easy to see that $km \notin Y$, otherwise $km + r = (km + r) + 0$. Hence there is a positive x so that $xm \in Y$ and $(k - x)m \in X$. By the choice of our k, we obtain that $(k - x)m + r \in X$. But then $(km + r) + 0 = [(k - x)m + r] + xm$ are two distinct representations. Contradiction. So we can write $X = mX' + \{0, 1, \ldots, m - 1\}$.

It remains to prove that $X'+Y' = \left\{0, 1, 2, \ldots, \dfrac{M}{m} - 1\right\}$. Indeed, let $k \in \left\{0, 1, 2, \ldots, \dfrac{M}{m} - 1\right\}$ and take consider $z = km \in \{0, 1, \ldots, M - 1\}$. Since the representation $z = x + y$ in $X + Y$ is unique and $m|y$ we also have $m|x$, so the reprezentation $k = x/m + y/m = x' + y'$ where $x' \in X'$, $y' \in Y'$ is unique. □

Note that Lemma 3 is symmetrical wrt X and Y.

Let's now finish the problem. We will prove by induction on $|B|$ that if $B \cup R = \{0, 1, \ldots, |B| \cdot |R| - 1\}$ then $0, r_1, \ldots, r_{n-1}$ form an arithmetical progression.

If $|B| = 1$, then $B = \{0\}$ and $B+R = B = \{0, 1, \ldots, n-1\}$ so $r_i = i$ and we are done. Assume now the statement true for all sets B having less than b elements. We have two cases:

If $1 \in R$, then $m = \min(B \setminus \{0\}) > 1$ and from Lemma 3, $m|n$. Since n is a prime number, it follows that $m = n$. Then it follows that $|R'| = 1$, $R' = \{0\}$, so $R = mR' + \{0, 1, \ldots, m - 1\} = \{0, 1, \ldots, m - 1\}$ and the statement is true.

If $1 \notin R$, then $m = \min(R \setminus \{0\}) = r_1|b$. By Lemma 3, $R = mR'$ and $B = mB' + \{0, 1, \ldots, m - 1\}$. R' and B' have the properties that $|R'| = |R|$ is a prime, $R' + B' = \{0, 1, \ldots, |R'| \cdot |B'| - 1\}$ and $|B'| = \dfrac{b}{m} < b$, hence by the induction hypothesis the elements of R' form an arithmetical progression. Because $R = mR'$ the same holds for $0, r_1, \ldots, r_{n-1}$. □