

C7. Let $P_1, \dots, P_s$ be arithmetic progressions of integers, the following conditions being satisfied:

- (i) each integer belongs to at least one of them;
- (ii) each progression contains a number which does not belong to other progressions.

Denote by n the least common multiple of steps of these progressions; let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be its prime factorization. Prove that

$$s \geq 1 + \sum_{i=1}^k \alpha_i (p_i - 1).$$

(Germany)

Solution 1. First, we prove the key lemma, and then we show how to apply it to finish the solution.

Let $n_1, \dots, n_k$ be positive integers. By an $n_1 \times n_2 \times \dots \times n_k$ grid we mean the set $N = \{(a_1, \dots, a_k) : a_i \in \mathbb{Z}, 0 \leq a_i \leq n_i - 1\}$; the elements of N will be referred to as *points*. In this grid, we define a *subgrid* as a subset of the form

$$L = \{(b_1, \dots, b_k) \in N : b_{i_1} = x_{i_1}, \dots, b_{i_t} = x_{i_t}\}, \quad (1)$$

where $I = \{i_1, \dots, i_t\}$ is an arbitrary nonempty set of indices, and $x_{i_j} \in [0, n_{i_j} - 1]$ ($1 \leq j \leq t$) are fixed integer numbers. Further, we say that a subgrid (1) is *orthogonal* to the i th coordinate axis if $i \in I$, and that it is *parallel* to the i th coordinate axis otherwise.

Lemma. Assume that the grid N is covered by subgrids $L_1, L_2, \dots, L_s$ (this means $N = \bigcup_{i=1}^s L_i$) so that

- (ii') each subgrid contains a point which is not covered by other subgrids;
- (iii) for each coordinate axis, there exists a subgrid L_i orthogonal to this axis.

Then

$$s \geq 1 + \sum_{i=1}^k (n_i - 1).$$

Proof. Assume to the contrary that $s \leq \sum_i (n_i - 1) = s'$. Our aim is to find a point that is not covered by $L_1, \dots, L_s$.

The idea of the proof is the following. Imagine that we expand each subgrid to some maximal subgrid so that for the i th axis, there will be at most $n_i - 1$ maximal subgrids orthogonal to this axis. Then the desired point can be found easily: its i th coordinate should be that not covered by the maximal subgrids orthogonal to the i th axis. Surely, the conditions for existence of such expansion are provided by Hall's lemma on matchings. So, we will follow this direction, although we will apply Hall's lemma to some subgraph instead of the whole graph.

Construct a bipartite graph $G = (V \cup V', E)$ as follows. Let $V = \{L_1, \dots, L_s\}$, and let $V' = \{v_{ij} : 1 \leq i \leq k, 1 \leq j \leq n_i - 1\}$ be some set of s' elements. Further, let the edge (L_m, v_{ij}) appear iff L_m is orthogonal to the i th axis.

For each subset $W \subset V$, denote

$$f(W) = \{v \in V' : (L, v) \in E \text{ for some } L \in W\}.$$

Notice that $f(V) = V'$ by (iii).

Now, consider the set $W \subset V$ containing the maximal number of elements such that $|W| > |f(W)|$; if there is no such set then we set $W = \emptyset$. Denote $W' = f(W)$, $U = V \setminus W$, $U' = V' \setminus W'$.

By our assumption and the Lemma condition, $|f(V)| = |V'| \geq |V|$, hence $W \neq V$ and $U \neq \emptyset$. Permuting the coordinates, we can assume that $U' = \{v_{ij} : 1 \leq i \leq \ell\}$, $W' = \{v_{ij} : \ell+1 \leq i \leq k\}$.

Consider the induced subgraph G' of G on the vertices $U \cup U'$. We claim that for every $X \subset U$, we get $|f(X) \cap U'| \geq |X|$ (so G' satisfies the conditions of Hall's lemma). Actually, we have $|W| \geq |f(W)|$, so if $|X| > |f(X) \cap U'|$ for some $X \subset U$, then we have

$$|W \cup X| = |W| + |X| > |f(W)| + |f(X) \cap U'| = |f(W) \cup (f(X) \cap U')| = |f(W \cup X)|.$$

This contradicts the maximality of $|W|$.

Thus, applying Hall's lemma, we can assign to each $L \in U$ some vertex $v_{ij} \in U'$ so that to distinct elements of U , distinct vertices of U' are assigned. In this situation, we say that $L \in U$ corresponds to the i th axis, and write $g(L) = i$. Since there are $n_i - 1$ vertices of the form v_{ij} , we get that for each $1 \leq i \leq \ell$, not more than $n_i - 1$ subgrids correspond to the i th axis.

Finally, we are ready to present the desired point. Since $W \neq V$, there exists a point $b = (b_1, b_2, \dots, b_k) \in N \setminus (\cup_{L \in W} L)$. On the other hand, for every $1 \leq i \leq \ell$, consider any subgrid $L \in U$ with $g(L) = i$. This means exactly that L is orthogonal to the i th axis, and hence all its elements have the same i th coordinate c_L . Since there are at most $n_i - 1$ such subgrids, there exists a number $0 \leq a_i \leq n_i - 1$ which is not contained in a set $\{c_L : g(L) = i\}$. Choose such number for every $1 \leq i \leq \ell$. Now we claim that point $a = (a_1, \dots, a_\ell, b_{\ell+1}, \dots, b_k)$ is not covered, hence contradicting the Lemma condition.

Surely, point a cannot lie in some $L \in U$, since all the points in L have $g(L)$ th coordinate $c_L \neq a_{g(L)}$. On the other hand, suppose that $a \in L$ for some $L \in W$; recall that $b \notin L$. But the points a and b differ only at first ℓ coordinates, so L should be orthogonal to at least one of the first ℓ axes, and hence our graph contains some edge (L, v_{ij}) for $i \leq \ell$. It contradicts the definition of W' . The Lemma is proved. $\square$

Now we turn to the problem. Let d_j be the step of the progression P_j . Note that since $n = \text{l.c.m.}(d_1, \dots, d_s)$, for each $1 \leq i \leq k$ there exists an index $j(i)$ such that $p_i^{\alpha_i} \mid d_{j(i)}$. We assume that $n > 1$; otherwise the problem statement is trivial.

For each $0 \leq m \leq n - 1$ and $1 \leq i \leq k$, let m_i be the residue of m modulo $p_i^{\alpha_i}$, and let $m_i = \overline{r_{i\alpha_i} \dots r_{i1}}$ be the base p_i representation of m_i (possibly, with some leading zeroes). Now, we put into correspondence to m the sequence $r(m) = (r_{11}, \dots, r_{1\alpha_1}, r_{21}, \dots, r_{k\alpha_k})$. Hence $r(m)$ lies in a $\underbrace{p_1 \times \dots \times p_1}_{\alpha_1 \text{ times}} \times \dots \times \underbrace{p_k \times \dots \times p_k}_{\alpha_k \text{ times}}$ grid N .

Surely, if $r(m) = r(m')$ then $p_i^{\alpha_i} \mid m_i - m'_i$, which follows $p_i^{\alpha_i} \mid m - m'$ for all $1 \leq i \leq k$; consequently, $n \mid m - m'$. So, when m runs over the set $\{0, \dots, n - 1\}$, the sequences $r(m)$ do not repeat; since $|N| = n$, this means that r is a bijection between $\{0, \dots, n - 1\}$ and N . Now we will show that for each $1 \leq i \leq s$, the set $L_i = \{r(m) : m \in P_i\}$ is a subgrid, and that for each axis there exists a subgrid orthogonal to this axis. Obviously, these subgrids cover N , and the condition (ii') follows directly from (ii). Hence the Lemma provides exactly the estimate we need.

Consider some $1 \leq j \leq s$ and let $d_j = p_1^{\gamma_1} \dots p_k^{\gamma_k}$. Consider some $q \in P_j$ and let $r(q) = (r_{11}, \dots, r_{k\alpha_k})$. Then for an arbitrary q' , setting $r(q') = (r'_{11}, \dots, r'_{k\alpha_k})$ we have

$$q' \in P_j \iff p_i^{\gamma_i} \mid q - q' \text{ for each } 1 \leq i \leq k \iff r_{i,t} = r'_{i,t} \text{ for all } t \leq \gamma_i.$$

Hence $L_j = \{(r'_{11}, \dots, r'_{k\alpha_k}) \in N : r_{i,t} = r'_{i,t} \text{ for all } t \leq \gamma_i\}$ which means that L_j is a subgrid containing $r(q)$. Moreover, in $L_{j(i)}$, all the coordinates corresponding to p_i are fixed, so it is orthogonal to all of their axes, as desired.

Comment 1. The estimate in the problem is sharp for every n . One of the possible examples is the following one. For each $1 \leq i \leq k$, $0 \leq j \leq \alpha_i - 1$, $1 \leq k \leq p - 1$, let

$$P_{i,j,k} = kp_i^j + p_i^{j+1}\mathbb{Z},$$

and add the progression $P_0 = n\mathbb{Z}$. One can easily check that this set satisfies all the problem conditions. There also exist other examples.

On the other hand, the estimate can be adjusted in the following sense. For every $1 \leq i \leq k$, let $0 = \alpha_{i0}, \alpha_{i1}, \dots, \alpha_{ih_i}$ be all the numbers of the form $\text{ord}_{p_i}(d_j)$ in an increasing order (we delete the repeating occurrences of a number, and add a number $0 = \alpha_{i0}$ if it does not occur). Then, repeating the arguments from the solution one can obtain that

$$s \geq 1 + \sum_{i=1}^k \sum_{j=1}^{h_i} (p^{\alpha_j - \alpha_{j-1}} - 1).$$

Note that $p^\alpha - 1 \geq \alpha(p - 1)$, and the equality is achieved only for $\alpha = 1$. Hence, for reaching the minimal number of the progressions, one should have $\alpha_{i,j} = j$ for all i, j . In other words, for each $1 \leq j \leq \alpha_i$, there should be an index t such that $\text{ord}_{p_i}(d_t) = j$.

Solution 2. We start with introducing some notation. For positive integer r , we denote $[r] = \{1, 2, \dots, r\}$. Next, we say that a set of progressions $\mathcal{P} = \{P_1, \dots, P_s\}$ *cover* $\mathbb{Z}$ if each integer belongs to some of them; we say that this covering is *minimal* if no proper subset of $\mathcal{P}$ covers $\mathbb{Z}$. Obviously, each covering contains a minimal subcovering.

Next, for a minimal covering $\{P_1, \dots, P_s\}$ and for every $1 \leq i \leq s$, let d_i be the step of progression P_i , and h_i be some number which is contained in P_i but in none of the other progressions. We assume that $n > 1$, otherwise the problem is trivial. This implies $d_i > 1$, otherwise the progression P_i covers all the numbers, and $n = 1$.

We will prove a more general statement, namely the following

Claim. Assume that the progressions $P_1, \dots, P_s$ and number $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} > 1$ are chosen as in the problem statement. Moreover, choose some nonempty set of indices $I = \{i_1, \dots, i_t\} \subseteq [k]$ and some positive integer $\beta_i \leq \alpha_i$ for every $i \in I$. Consider the set of indices

$$T = \left\{ j : 1 \leq j \leq s, \text{ and } p_i^{\alpha_i - \beta_i + 1} \mid d_j \text{ for some } i \in I \right\}.$$

Then

$$|T| \geq 1 + \sum_{i \in I} \beta_i (p_i - 1). \quad (2)$$

Observe that the Claim for $I = [k]$ and $\beta_i = \alpha_i$ implies the problem statement, since the left-hand side in (2) is not greater than s . Hence, it suffices to prove the Claim.

1. First, we prove the Claim assuming that all d_j 's are prime numbers. If for some $1 \leq i \leq k$ we have at least p_i progressions with the step p_i , then they do not intersect and hence cover all the integers; it means that there are no other progressions, and $n = p_i$; the Claim is trivial in this case.

Now assume that for every $1 \leq i \leq k$, there are not more than $p_i - 1$ progressions with step p_i ; each such progression covers the numbers with a fixed residue modulo p_i , therefore there exists a residue $q_i \pmod{p_i}$ which is not touched by these progressions. By the Chinese Remainder Theorem, there exists a number q such that $q \equiv q_i \pmod{p_i}$ for all $1 \leq i \leq k$; this number cannot be covered by any progression with step p_i , hence it is not covered at all. A contradiction.

2. Now, we assume that the general Claim is not valid, and hence we consider a counterexample $\{P_1, \dots, P_s\}$ for the Claim; we can choose it to be minimal in the following sense:

- the number n is minimal possible among all the counterexamples;
- the sum $\sum_i d_i$ is minimal possible among all the counterexamples having the chosen value of n .

As was mentioned above, not all numbers d_i are primes; hence we can assume that d_1 is composite, say $p_1 \mid d_1$ and $d'_1 = \frac{d_1}{p_1} > 1$. Consider a progression P'_1 having the step d'_1 , and containing P_1 . We will focus on two coverings constructed as follows.

(i) Surely, the progressions $P'_1, P_2, \dots, P_s$ cover $\mathbb{Z}$, though this covering is not necessarily minimal. So, choose some minimal subcovering $\mathcal{P}'$ in it; surely $P'_1 \in \mathcal{P}'$ since h_1 is not covered by $P_2, \dots, P_s$, so we may assume that $\mathcal{P}' = \{P'_1, P_2, \dots, P_{s'}\}$ for some $s' \leq s$. Furthermore, the period of the covering $\mathcal{P}'$ can appear to be less than n ; so we denote this period by

$$n' = p_1^{\alpha_1 - \sigma_1} \dots p_k^{\alpha_k - \sigma_k} = \text{l.c.m.}(d'_1, d_2, \dots, d_{s'}).$$

Observe that for each $P_j \notin \mathcal{P}'$, we have $h_j \in P'_1$, otherwise h_j would not be covered by $\mathcal{P}$.

(ii) On the other hand, each nonempty set of the form $R_i = P_i \cap P'_1$ ($1 \leq i \leq s$) is also a progression with a step $r_i = \text{l.c.m.}(d_i, d'_1)$, and such sets cover P'_1 . Scaling these progressions with the ratio $1/d'_1$, we obtain the progressions Q_i with steps $q_i = r_i/d'_1$ which cover $\mathbb{Z}$. Now we choose a minimal subcovering $\mathcal{Q}$ of this covering; again we should have $Q_1 \in \mathcal{Q}$ by the reasons of h_1 . Now, denote the period of $\mathcal{Q}$ by

$$n'' = \text{l.c.m.}\{q_i : Q_i \in \mathcal{Q}\} = \frac{\text{l.c.m.}\{r_i : Q_i \in \mathcal{Q}\}}{d'_1} = \frac{p_1^{\gamma_1} \dots p_k^{\gamma_k}}{d'_1}.$$

Note that if $h_j \in P'_1$, then the image of h_j under the scaling can be covered by Q_j only; so, in this case we have $Q_j \in \mathcal{Q}$.

Our aim is to find the desired number of progressions in coverings $\mathcal{P}$ and $\mathcal{Q}$. First, we have $n \geq n'$, and the sum of the steps in $\mathcal{P}'$ is less than that in $\mathcal{P}$; hence the Claim is valid for $\mathcal{P}'$. We apply it to the set of indices $I' = \{i \in I : \beta_i > \sigma_i\}$ and the exponents $\beta'_i = \beta_i - \sigma_i$; hence the set under consideration is

$$T' = \left\{ j : 1 \leq j \leq s', \text{ and } p_i^{(\alpha_i - \sigma_i) - \beta'_i + 1} = p_i^{\alpha_i - \beta_i + 1} \mid d_j \text{ for some } i \in I' \right\} \subseteq T \cap [s'],$$

and we obtain that

$$|T \cap [s']| \geq |T'| \geq 1 + \sum_{i \in I'} (\beta_i - \sigma_i)(p_i - 1) = 1 + \sum_{i \in I} (\beta_i - \sigma_i)_+(p_i - 1),$$

where $(x)_+ = \max\{x, 0\}$; the latter equality holds as for $i \notin I'$ we have $\beta_i \leq \sigma_i$.

Observe that $x = (x - y)_+ + \min\{x, y\}$ for all x, y . So, if we find at least

$$G = \sum_{i \in I} \min\{\beta_i, \sigma_i\}(p_i - 1)$$

indices in $T \cap \{s' + 1, \dots, s\}$, then we would have

$$|T| = |T \cap [s']| + |T \cap \{s' + 1, \dots, s\}| \geq 1 + \sum_{i \in I} ((\beta_i - \sigma_i)_+ + \min\{\beta_i, \sigma_i\})(p_i - 1) = 1 + \sum_{i \in I} \beta_i(p_i - 1),$$

thus leading to a contradiction with the choice of $\mathcal{P}$. We will find those indices among the indices of progressions in $\mathcal{Q}$.

3. Now denote $I'' = \{i \in I : \sigma_i > 0\}$ and consider some $i \in I''$; then $p_i^{\alpha_i} \nmid n'$. On the other hand, there exists an index $j(i)$ such that $p_i^{\alpha_i} \mid d_{j(i)}$; this means that $d_{j(i)} \nmid n'$ and hence $P_{j(i)}$ cannot appear in $\mathcal{P}'$, so $j(i) > s'$. Moreover, we have observed before that in this case $h_{j(i)} \in P'_1$, hence $Q_{j(i)} \in \mathcal{Q}$. This means that $q_{j(i)} \mid n''$, therefore $\gamma_i = \alpha_i$ for each $i \in I''$ (recall here that $q_i = r_i/d'_1$ and hence $d_{j(i)} \mid r_{j(i)} \mid d'_1 n''$).

Let $d'_1 = p_1^{\tau_1} \dots p_k^{\tau_k}$. Then $n'' = p_1^{\gamma_1 - \tau_1} \dots p_k^{\gamma_k - \tau_k}$. Now, if $i \in I''$, then for every β the condition $p_i^{(\gamma_i - \tau_i) - \beta + 1} \mid q_j$ is equivalent to $p_i^{\alpha_i - \beta + 1} \mid r_j$.

Note that $n'' \leq n/d'_1 < n$, hence we can apply the Claim to the covering $\mathcal{Q}$. We perform this with the set of indices I'' and the exponents $\beta''_i = \min\{\beta_i, \sigma_i\} > 0$. So, the set under consideration is

$$\begin{aligned} T'' &= \left\{ j : Q_j \in \mathcal{Q}, \text{ and } p_i^{(\gamma_i - \tau_i) - \min\{\beta_i, \sigma_i\} + 1} \mid q_j \text{ for some } i \in I'' \right\} \\ &= \left\{ j : Q_j \in \mathcal{Q}, \text{ and } p_i^{\alpha_i - \min\{\beta_i, \sigma_i\} + 1} \mid r_j \text{ for some } i \in I'' \right\}, \end{aligned}$$

and we obtain $|T''| \geq 1 + G$. Finally, we claim that $T'' \subseteq T \cap (\{1\} \cup \{s' + 1, \dots, s\})$; then we will obtain $|T \cap \{s' + 1, \dots, s\}| \geq G$, which is exactly what we need.

To prove this, consider any $j \in T''$. Observe first that $\alpha_i - \min\{\beta_i, \sigma_i\} + 1 > \alpha_i - \sigma_i \geq \tau_i$, hence from $p_i^{\alpha_i - \min\{\beta_i, \sigma_i\} + 1} \mid r_j = \text{l.c.m.}(d'_1, d_j)$ we have $p_i^{\alpha_i - \min\{\beta_i, \sigma_i\} + 1} \mid d_j$, which means that $j \in T$. Next, the exponent of p_i in d_j is greater than that in n' , which means that $P_j \notin \mathcal{P}'$. This may appear only if $j = 1$ or $j > s'$, as desired. This completes the proof.

Comment 2. A grid analogue of the Claim is also valid. It reads as following.

Claim. Assume that the grid N is covered by subgrids $L_1, L_2, \dots, L_s$ so that

- (ii') each subgrid contains a point which is not covered by other subgrids;
- (iii) for each coordinate axis, there exists a subgrid L_i orthogonal to this axis.

Choose some set of indices $I = \{i_1, \dots, i_t\} \subset [k]$, and consider the set of indices

$$T = \{j : 1 \leq j \leq s, \text{ and } L_j \text{ is orthogonal to the } i\text{th axis for some } i \in I\}.$$

Then

$$|T| \geq 1 + \sum_{i \in I} (n_i - 1).$$

This Claim may be proved almost in the same way as in Solution 1.