

Algebra

- A1. Let n be an integer, and let A be a subset of $\{0, 1, \dots, 5^n\}$ consisting of $4n + 2$ numbers. Prove that there exist $a, b, c \in A$ such that $a < b < c$ and $c + 2a > 3b$.

Solution. Suppose A is a counterexample of the condition above. Here, we order the numbers as $a_1 < \dots < a_m$ with $m = 4n + 2$. Then we get the following identity: for all $i \leq 4n = m - 2$ we have

$$2a_i + a_m \leq 3a_{i+1} \Rightarrow (a_m - a_{i+1}) \leq 2(a_{i+1} - a_i) \Rightarrow \frac{a_m - a_i}{a_m - a_{i+1}} = 1 + \frac{a_{i+1} - a_i}{a_m - a_{i+1}} \geq 1 + \frac{1}{2} = \frac{3}{2}$$

Repeating this procedure, we get

$$\frac{a_m - a_1}{a_m - a_{m-1}} \geq \left(\frac{3}{2}\right)^{m-2} = \left(\frac{3}{2}\right)^{4n} = \left(\frac{81}{16}\right)^n > 5^n$$

which contradicts $0 \leq a_1$ and $a_m \leq 5^n$.

- A2. For every integer $n \geq 1$ consider the $n \times n$ table with entry $\lfloor \frac{ij}{n+1} \rfloor$ at the intersection of row i and column j , for every $i = 1, \dots, n$ and $j = 1, \dots, n$.

Determine all integers $n \geq 1$ for which the sum of the n^2 entries in the table is equal to $\frac{1}{4}n^2(n-1)$.

Answer. All n such that $n+1$ is prime.

Solution. Let $r(x)$ be the remainder of an integer x when divided by $n+1$, thus $0 \leq x \leq n$. $\lfloor \frac{ij}{n+1} \rfloor = \frac{1}{n+1}(ij - r(ij))$. This gives the sum as

$$\frac{1}{n+1} \sum_{i=1}^n \sum_{j=1}^n (ij - r(ij)) = \frac{1}{n+1} \left(\sum_{i=1}^n i \right)^2 - \frac{1}{n+1} \sum_{i=1}^n \sum_{j=1}^n r(ij) = \frac{n^2(n+1)}{4} - \frac{1}{n+1} \sum_{i=1}^n \sum_{j=1}^n r(ij)$$

It follows that $\sum_{i=1}^n \sum_{j=1}^n r(ij) = (n+1) \left(\frac{n^2(n+1)}{4} - \frac{n^2(n-1)}{4} \right) = \frac{n^2(n+1)}{2}$.

Now we consider each row k . Suppose that $\gcd(k, n+1) = \ell$. Then $r(ki)$ for $i = 1, \dots, n$ is just ℓ copies of $\ell, 2\ell, \dots, \ell(\frac{n+1}{\ell} - 1)$. It then follows the sum of $r(ki)$ here is given by

$$\frac{1}{2} \ell^2 \left(\frac{n+1}{\ell} \right) \left(\frac{n+1}{\ell} - 1 \right) = \frac{1}{2} \cdot (n+1)(n+1-\ell)$$

This is upper bounded by $\frac{n(n+1)}{2}$, which means the sum of all the remainders cannot exceed $\frac{n^2(n+1)}{2}$. Equality holds if and only if $\ell = 1$ for all such k , i.e. $\gcd(k, n+1) = 1$ for $k = 1, \dots, n$. This is precisely when $n+1$ is prime.

- A3. Given a positive integer n , find the smallest value of

$$\left\lfloor \frac{a_1}{1} \right\rfloor + \dots + \left\lfloor \frac{a_n}{n} \right\rfloor$$

over all permutations (a_1, \dots, a_n) of $(1, \dots, n)$.

Answer. $\lfloor \log_2 n \rfloor + 1$.

Solution. Let's first do the easier part: finding such a construction. Indeed, let $2^k \leq n < 2^{k+1}$. Consider the following construction:

$$a_\ell = \begin{cases} \min(2\ell - 1, n) & \exists m \geq 0 : \ell = 2^m \\ \ell - 1 & \text{otherwise} \end{cases}$$

Then $\lfloor \frac{a_\ell}{\ell} \rfloor$ is 1 when $\ell = 2^m$ and 0 otherwise, so the sum is indeed $k + 1 = \lfloor \log_2 n \rfloor + 1$. One can also verify that the construction above is a permutation: indeed for each $m \leq k$,

$a_{2^m}, \dots, a_{\min(2^{m+1}-1, n)}$ is $\min(2^{m+1}-1, n), 2^m, \dots, \min(2^{m+1}-1, n)-1$, i.e. permutation within this interval.

To establish the lower bound, we denote $f(n)$ as our desired answer, and it suffices to show that $f(n) \geq f(\lfloor \frac{n}{2} \rfloor) + 1$ for all $n \geq 2$. Observe that $f(1) = 1$. We now consider this lemma:

Lemma 1. *If a_1, \dots, a_m are distinct positive integers, then $\lfloor \frac{a_1}{1} \rfloor + \dots + \lfloor \frac{a_m}{m} \rfloor \geq f(m)$:*

Proof. If b_i is the position of a_i when arranged in sorted order then $b_i \leq a_i$ and b_1, \dots, b_m is a permutation of $1, \dots, m$, so

$$\lfloor \frac{a_1}{1} \rfloor + \dots + \lfloor \frac{a_m}{m} \rfloor \geq \lfloor \frac{b_1}{1} \rfloor + \dots + \lfloor \frac{b_m}{m} \rfloor \geq f(m)$$

□

In particular, this would be the case when (a_1, \dots, a_n) is a permutation of $1, \dots, n$. (I.e. we look at the “prefix” of the first m entries).

Now fix $m = f(\lfloor \frac{n}{2} \rfloor)$, and we have the two cases:

- $a_k \geq k$ for some $k > m$. Then $\lfloor \frac{a_{m+1}}{m+1} \rfloor + \dots + \lfloor \frac{a_n}{n} \rfloor \geq 1$, so

$$\lfloor \frac{a_1}{1} \rfloor + \dots + \lfloor \frac{a_n}{n} \rfloor \geq f(m) + 1$$

$f(m)$ for the first m terms; 1 for the rest.

- $a_k < k$ for some $k > m$. It then follows that $a_\ell = n$ for some $\ell \leq m$. Now let n' be the smallest number not in a_1, \dots, a_m ; we have $n' \leq m \leq \frac{n}{2}$. If we define

$$a'_i = \begin{cases} n' & i = \ell \\ a_i & \text{otherwise} \end{cases} \quad \text{then}$$

$$\lfloor \frac{a'_1}{1} \rfloor + \dots + \lfloor \frac{a'_m}{m} \rfloor \geq f(m)$$

by Lemma 1. In addition, $n - n' \geq \frac{n}{2} \geq \ell$ so $\lfloor \frac{n}{\ell} \rfloor - \lfloor \frac{n'}{\ell} \rfloor \geq 1$. Therefore

$$\lfloor \frac{a_1}{1} \rfloor + \dots + \lfloor \frac{a_m}{m} \rfloor \geq 1 + \lfloor \frac{a'_1}{1} \rfloor + \dots + \lfloor \frac{a'_m}{m} \rfloor \geq f(m) + 1$$

A4. (IMO 2) Show that the inequality

$$\sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i - x_j|} \leq \sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i + x_j|}$$

holds for all real numbers x_1, \dots, x_n .

Solution. The main idea is to move all the x_i 's by a constant (say $\frac{c}{2}$): here, the LHS remains the same, while the RHS varies. The precise formulation is as follows:

Lemma 2. *Suppose that*

$$c_0 \in \arg \min_c \sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i + x_j + c|}$$

(i.e. c_0 is one of the minimizers above). Then there exists i and j such that $x_i + x_j + c_0 = 0$.

Proof. For each c with $x_i + x_j + c \neq 0$ for all i, j , we have

$$\frac{d}{dc} \sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i + x_j + c|} = \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \text{sign}(x_i + x_j + c) |x_i + x_j + c|^{-1/2}$$

where $\text{sign}(x) = 1$ if $x > 0$ and -1 if $x < 0$ (let's not worry about the $x = 0$ case here). Differentiating once more, we have

$$\frac{d^2}{dc^2} \sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i + x_j + c|} = -\frac{1}{4} \sum_{i=1}^n \sum_{j=1}^n (\text{sign}(x_i + x_j + c))^2 |x_i + x_j + c|^{-3/2} < 0$$

since $|x_i + x_j + c| > 0$. Therefore, if such c is a minimum point, we must have the first derivative as $= 0$ and second derivative as ≥ 0 , which is impossible. It then follows that all such c cannot be a minimum point. \square

Now we may proceed by induction on n . For $n = 0$ there's nothing to prove; for $n = 1$ we're showing $0 \leq \sqrt{|2x_1|}$ which is trivial.

Suppose for some n our desired inequality holds for k variables for all $k \leq n-1$. Consider, now, n variables x_1, \dots, x_n , and let y_1, \dots, y_n be such that $y_i = x_i + \frac{c}{2}$ for some c , and such that $\sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i + y_j|}$ is minimal. Then we have

$$\sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i - x_j|} = \sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i - y_j|} \quad \sum_{i=1}^n \sum_{j=1}^n \sqrt{|x_i + x_j|} \geq \sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i + y_j|}$$

so it suffices to show $\sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i - y_j|} \geq \sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i + y_j|}$.

By our lemma, there exists i_0, j_0 such that $y_{i_0} + y_{j_0} = 0$. If $i_0 = j_0$, then essentially $y_{i_0} = 0$ and

$$\sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i - y_j|} = \sum_{i \neq i_0} \sum_{j \neq i_0} \sqrt{|y_i - y_j|} + 2 \sum_{i=1}^n \sqrt{|y_i|}$$

and

$$\sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i + y_j|} = \sum_{i \neq i_0} \sum_{j \neq i_0} \sqrt{|y_i + y_j|} + 2 \sum_{i=1}^n \sqrt{|y_i|}$$

but then we have $\sum_{i \neq i_0} \sum_{j \neq i_0} \sqrt{|y_i - y_j|} \leq \sum_{i \neq i_0} \sum_{j \neq i_0} \sqrt{|y_i + y_j|}$ by the inductive hypothesis (with $n-1$ variables).

Similarly, when $i_0 \neq j_0$ we have $y_{i_0} = v, y_{j_0} = -v$ for some real v . Therefore

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i - y_j|} &= \sum_{i \neq i_0, j_0} \sum_{j \neq i_0, j_0} \sqrt{|y_i - y_j|} + \sum_{i=1}^n \sqrt{|y_i - v|} + \sum_{j=1}^n \sqrt{|y_j + v|} \\ \sum_{i=1}^n \sum_{j=1}^n \sqrt{|y_i + y_j|} &= \sum_{i \neq i_0, j_0} \sum_{j \neq i_0, j_0} \sqrt{|y_i + y_j|} + \sum_{i=1}^n \sqrt{|y_i - v|} + \sum_{j=1}^n \sqrt{|y_j + v|} \end{aligned}$$

and again the inequality $\sum_{i \neq i_0, j_0} \sum_{j \neq i_0, j_0} \sqrt{|y_i - y_j|} \leq \sum_{i \neq i_0, j_0} \sum_{j \neq i_0, j_0} \sqrt{|y_i + y_j|}$ follows from inductive hypothesis with $n-2$ variables.

- A5. Let $n \geq 2$ be an integer and let a_1, a_2, \dots, a_n be positive real numbers with sum 1. Prove that

$$\sum_{k=1}^n \frac{a_k}{1 - a_k} (a_1 + a_2 + \dots + a_{k-1})^2 < \frac{1}{3}.$$

Solution. For each k , denote $s_k = a + 1 + \cdots + a_k$, with $s_0 = 0$, $s_n = 1$, and s_k strictly increasing. Then the LHS is now equivalent to

$$\sum_{k=1}^n \frac{s_k - s_{k-1}}{1 - (s_k - s_{k-1})} s_{k-1}^2$$

We first notice that $0 < s_k \leq 1$ for all k , so $s_k - s_{k-1} \leq \frac{s_k - s_{k-1}}{s_k} = 1 - \frac{s_{k-1}}{s_k}$. Therefore,

$$\begin{aligned} \sum_{k=1}^n \frac{s_k - s_{k-1}}{1 - (s_k - s_{k-1})} s_{k-1}^2 &\leq \sum_{k=1}^n \frac{s_k - s_{k-1}}{\left(\frac{s_{k-1}}{s_k}\right)} s_{k-1}^2 \\ &= \sum_{k=1}^n s_{k-1} s_k (s_k - s_{k-1}) \\ &\leq \sum_{k=1}^n \frac{1}{3} (s_k^2 + s_k s_{k-1} + s_{k-1}^2) s_k (s_k - s_{k-1}) \\ &= \sum_{k=1}^n \frac{1}{3} (s_k^3 - s_{k-1}^3) \\ &= \frac{1}{3} \end{aligned}$$

It now remains to show that the equality cannot hold. Indeed, for $k = 1$ we have the LHS as 0 since $s_0^2 = 0$, while the RHS is $\frac{1}{3}(s_1^3 - s_0^3) > 0$ since $s_1 > 0$. This means either one of the \leq inequality is, in fact, strict for $k = 1$.

Combinatorics

- C1. Let S be an infinite set of positive integers, such that there exists four pairwise distinct $a, b, c, d \in S$ with $\gcd(a, b) \neq \gcd(c, d)$. Prove that there exist three pairwise distinct $x, y, z \in S$ such that

$$\gcd(x, y) = \gcd(y, z) \neq \gcd(z, x)$$

Solution. By dividing each number by the same common divisor d as necessary, we may assume $\gcd(S) = 1$ (i.e. for each prime p there's $s \in S$ with $p \nmid s$). We now consider the following two cases:

Case 1. There exists a prime p such that $p \mid s$ for infinitely many primes p . By the $\gcd(S) = 1$ assumption we may assume that there exists y such that $p \nmid y$. Let $S_p = \{s \in S : p \mid s\}$, and we see that:

$$\{\gcd(y, x) : x \in S_p\} \subseteq \{d : \text{positive divisors of } y\}$$

Since $|S_p|$ is infinite, while the set of positive divisors of y is finite, by pigeonhole principle we have $\gcd(x, y) = \gcd(z, y)$ for some $x \neq z \in S_p$. Here we have $p \mid x, z$ while $p \nmid y$, so $\gcd(x, y) \neq \gcd(x, z)$, as desired.

Case 2. Now we have each prime dividing only finitely many members in S . The $\gcd(a, b) \neq \gcd(c, d)$ condition means $\gcd(x, z) > 1$ for some $x \neq z \in S$. We note that the set of primes p dividing xz is finite, so in this case, we have

$$|\{s \in S : \gcd(s, xz) > 1\}| < \infty$$

Thus we may take $y \in S$ such that $\gcd(y, xz) = 1$. It then follows that $\gcd(y, x) = \gcd(y, z) = 1$.

- C2. Let $n \geq 3$ be an integer. An integer $m \geq n+1$ is called n -colorful if, given infinitely many marbles in each of n colours C_1, C_2, \dots, C_n , it is possible to place m of them around a circle so that in any group of $n+1$ consecutive marbles there is at least one marble of colour C_i for each $i = 1, \dots, n$.

Prove that there are only finitely many positive integers which are not n -colourful, and find the largest among them.

Answer. The largest number that's not n -colorful is $n^2 - n - 1$.

Solution. We first show that $n^2 - n - 1$ is not n -colorful. Indeed, one of the color, say C_j , is used at most $\lfloor \frac{n^2-n-1}{n} \rfloor = n-2$ times. Since $n^2 - n - 1 = (n-2)(n+1) + 1$, it follows that if we iterate through the marbles in clockwise fashion, the gap of some two of them (possibly cyclic repetition) is at least $n+2$. This means the $\geq n+1$ marbles in between them has no colour C_j .

Conversely, we show that any $m \geq n^2 - n$ is colorful. Let g be the remainder of m when divided by n (i.e. $0 \leq g \leq n-1$). We consider the following arrangement:

$$\underbrace{(C_1 C_2 \cdots C_n C_1)}_{g \text{ copies}} \quad \underbrace{(C_1 C_2 \cdots C_n)}_{(m-g(n+1))/n \text{ copies}}$$

For all $n^2 - n$, we have $g(n+1) \leq m$ since $g(n+1) < n^2 - n$ for all $g = 0, \dots, n-2$, and when $g = n-1$, $m \geq n^2 - 1 = g(n+1)$. Next, the i -th color of each group (either in $(C_1 C_2 \cdots C_n C_1)$ or $(C_1 C_2 \cdots C_n)$) are of color C_i for $i = 1, 2, \dots, n$, and are either spaced n or $n+1$ apart, which guarantees that any $n+1$ consecutive marbles would cover this C_i .

- C3. (IMO 5) Two squirrels, Bushy and Jumpy, have collected 2021 walnuts for the winter. Jumpy numbers the walnuts from 1 through 2021, and digs 2021 little holes in a circular pattern in the ground around their favourite tree. The next morning Jumpy notices that Bushy had placed one walnut into each hole, but had paid no attention to the numbering. Unhappy, Jumpy decides to reorder the walnuts by performing a sequence of 2021 moves. In the k -th move, Jumpy swaps the positions of the two walnuts adjacent to walnut k .

Prove that there exists a value of k such that, on the k -th move, Jumpy swaps some walnuts a and b such that $a < k < b$.

Solution. W.l.o.g. let the arc length of circle be 2021 and each adjacent walnuts have arc length 1 between them. Suppose that the conclusion doesn't hold. That is, on each k -th move, the walnuts being swapped are either both greater than k or both smaller than k . Now an observer squirrel (say Humpy) would simply mark the k -th walnut at the k -th move, starting from all unmarked walnuts. If, in addition, the two walnuts swapped are smaller than k , then Humpy colours the arc containing the three walnuts black (i.e. arc length 2).

A few observations are in order. First, we see that after k moves, a walnut is marked iff the value is $\leq k$. Next, at k -th move, the two walnuts adjacent to k will both be unmarked (if both bigger than k) or both be marked (if both smaller than k). This means that apart from the walnut numbered k , the positions of other marked and unmarked walnut doesn't change. Finally, notice that by the segment colouring protocol, we see that an arc is coloured if and only if the two endpoints are marked walnuts (indeed, Humpy either marks a walnut with two unmarked neighbours and do not colour any segment, or with two marked neighbours and colour this segment).

Finally, the total length of black arcs increased by 0 or 2 after iteration, hence even. At the end of the procedure, however, we see that the number of black arcs must be 2021 since all the walnuts would have been marked. This is a contradiction.

- C4. The kingdom of Anisotropy consists of n cities. For every two cities there exists exactly one direct one-way road between them. We say that a path from X to Y is a sequence of roads such that one can move from X to Y along this sequence without returning to an already visited city. A collection of paths is called diverse if no road belongs to two or more paths in the collection.

Let A and B be two distinct cities in Anisotropy. Let N_{AB} denote the maximal number of paths in a diverse collection of paths from A to B . Similarly, let N_{BA} denote the maximal number of paths in a diverse collection of paths from B to A . Prove that the equality $N_{AB} = N_{BA}$ holds if and only if the number of roads going out from A is the same as the number of roads going out from B .

Solution. Let's first show the following:

Lemma 3. *There exists a diverse collection of path from A to B with maximal number, such that all paths in the form of $A \rightarrow v \rightarrow B$ are included (here \rightarrow means directed edge).*

Proof. Let's consider any such diverse collection \mathcal{C} with N_{AB} such paths. Consider any v such that $A \rightarrow v \rightarrow B$ is not included. We consider these cases:

Case 0. Neither $A \rightarrow v$ nor $v \rightarrow B$ are in any path contained in \mathcal{C} . Then we may even add $A \rightarrow v \rightarrow B$ directly.

Case 1a. $A \rightarrow v$ belongs to some path contained in \mathcal{C} but not $v \rightarrow B$. Now, if the path is $A \rightarrow v \Rightarrow B$ where \Rightarrow denotes a path from v to B , then we may replace the paths in $v \Rightarrow B$ to $v \rightarrow B$, that gives $A \rightarrow v \rightarrow B$.

Case 1b. $v \rightarrow B$ belongs to some path contained in \mathcal{C} but not $A \rightarrow v$. Similar case: if this is $A \Rightarrow v \rightarrow B$ we may replace $A \Rightarrow v$ with $A \rightarrow v$.

Case 2. Both $A \rightarrow v$ and $v \rightarrow B$ are part of the collection but in different paths. This means there exists the two paths

$$A \rightarrow v \Rightarrow B \quad A \Rightarrow v \rightarrow B$$

such that $A \Rightarrow v$ and $v \Rightarrow B$ are two paths with disjoint roads, and also disjoint from edges $A \rightarrow v$ and $v \rightarrow B$. Call these two paths U and V . Thus $A \Rightarrow v \Rightarrow B$ does contain a path that's subset of $U \cup V$ (basically, take the union, and remove all cycles), so we may replace the two original paths with this path and $A \rightarrow v \rightarrow B$.

So considering all cases above it means we can indeed include $A \rightarrow v \rightarrow B$ into the collection, for all such eligible v . \square

Now, referencing to towns A and B , each vertex can be categorized into exactly one of the following: \vec{AB} -type ($A \rightarrow v \rightarrow B$), \vec{BA} -type ($B \rightarrow v \rightarrow A$), in-type ($A \rightarrow v \leftarrow B$) and out-type ($A \leftarrow v \rightarrow B$). Regardless of the members of the collection, either $A \rightarrow B$ or $B \rightarrow A$ must also be in a maximally-constructed diverse collection.

By above we may assume that we can construct a maximally constructed path by including all paths of the form $A \rightarrow v \rightarrow B$ for all \vec{AB} -type vertices v . Thereafter, any new path starting with $A \rightarrow v'$ must have v' an in-type and any new path ending with $v'' \rightarrow B$ must have v'' an out-type. Now we claim the following:

Lemma 4. *A maximally diverse collection of paths from A to B containing $A \rightarrow v \rightarrow B$ for all \vec{AB} -type vertices v . Then the remaining paths are the maximal possible-sized set of paths in the form $A \rightarrow v_1 \Rightarrow v_2 \rightarrow B$, where v_1 is in-type, v_2 is out-type, and any two paths of the form $v_1 \Rightarrow v_2$ have disjoint paths and starting and ending vertices.*

Proof. The disjoint edges condition follows from definition; the disjoint starting and ending vertices follow from $A \rightarrow v_1$ and $B \rightarrow v_2$ condition.

Conversely, if we have such a collection of $A \rightarrow v_1 \Rightarrow v_2 \rightarrow B$, then these collections have edges disjoint from $A \rightarrow v \rightarrow B$, so such addition is valid. It therefore means we can pick the collection with maximum number of paths. \square

To finish, denote C_{AB} as the quantity described in Lemma 4. Such paths do not depend on A and B other than that we have in- and out-types of edges, so $C_{AB} = C_{BA}$. Therefore,

$$N_{AB} = C_{AB} + 1\{A \rightarrow B\} + |\{v : \vec{AB}\text{-type}\}| \quad N_{BA} = C_{BA} + 1\{B \rightarrow A\} + |\{v : \vec{BA}\text{-type}\}|$$

where $1\{A \rightarrow B\}$ means there's a directed edge $A \rightarrow B$. so $N_{AB} - N_{BA} = 1\{A \rightarrow B\} + |\{v : \vec{AB}\text{-type}\}| - (1\{B \rightarrow A\} + |\{v : \vec{BA}\text{-type}\}|)$. Given also that the out degree of A , $\text{out}(A)$ is given by $1\{A \rightarrow B\} + |\{v : \vec{AB}\text{-type}\}| + |\{v : \text{out-type}\}|$, we have

$$N_{AB} - N_{BA} = \text{out}(A) - \text{out}(B)$$

as desired.

- C6. A hunter and an invisible rabbit play a game on an infinite square grid. First the hunter fixes a colouring of the cells with finitely many colours. The rabbit then secretly chooses a cell to start in. Every minute, the rabbit reports the colour of its current cell to the hunter, and then secretly moves to an adjacent cell that it has not visited before (two cells are adjacent if they share an edge). The hunter wins if after some finite time either:

- the rabbit cannot move; or
- the hunter can determine the cell in which the rabbit started.

Decide whether there exists a winning strategy for the hunter.

Answer. Yes, the hunter can win.

Solution. Disclaimer: this solution deliberately wastes colour (to make analysis easier) since we aren't interested in optimizing the number of colours.

Assume that the grid is infinite in both directions for both coordinates (if it's only infinite in one direction the problem would just get easier). We may then denote the coordinates as (x, y) with $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$. In our solution we denote x -gap of two cells as distance in x -coordinates; define y -gap analogously.

Now consider the following attributes of the squares:

- $x \pmod{3}$, $y \pmod{3}$ (call these $M3x$ and $M3y$).
- Binary variable on whether $x \geq 0$, and whether $y \geq 0$ (call these $x0$ and $y0$).
- Binary variable on whether $|x|$ is a power of 2, and $|y|$ is a power of 2 (call these $P2x$ and $P2y$).
- We encode the following into one of $\{s, 0, 1\}$. For each (x, y) , let ℓ_x be the number of digits of $|x|$ in binary representation (thus $\ell_x = 1$ for $x = -1, 0, 1$). Let r be the remainder of y when divided by $\ell_x + 1$, then if $r = 0$ we encode s (call this separator); otherwise we encode the r -th digit of x . (Call this D_x). Repeat the same with (x, y) reversed, call this D_y .
- Finally, for each (x, y) we also encode where y is divisible by $\ell_x + 2$, and also whether x is divisible by $\ell_y + 2$. (Call these N_x, N_y respectively).

These would put them into $3^2 \times 2^2 \times 2^2 \times 3^2 \times 2^2 = 5084$ classes, thus the hunter may colour according to the classes.

We now show that the farmer can obtain victory after the rabbit travels finitely many steps, via the following protocol:

- Determine the trajectory (and track it all the time)
- Determine one of its coordinates
- Determine the other coordinate

The trajectory can be determined via $M3x$ and $M3y$ at all times, hence the farmer only needs to learn the current coordinate of the rabbit. Next, as the rabbit is only permitted to visit squares it has not visited before, either the x -coordinate or the y -coordinate has to be unbounded in one of the directions. W.l.o.g. we assume that the x -coordinate it visits is unbounded.

We first claim that the farmer can learn the x -coordinate of the rabbit, given that the x -coordinate it visits is unbounded. If the rabbit ever crosses both the negative and nonnegative region, then the indicator $x0$ will be flipped at $-1 \leftrightarrow 0$ region, allowing the farmer to learn the x -coordinate immediately. Otherwise, we assume that the rabbit it's in one region only; w.l.o.g. it's only in the nonnegative region. Since x -coordinate of the rabbit's trajectory is unbounded, and that the coordinate they visit have to be consecutive, it has to pass through both $2^k, 2^{k+1}$ for some $k \geq 1$. The farmer can then determine k via $P2x$, where the two consecutive cells with $P2x$ turned on have x -distance 2^k (which the farmer knows).

It now remains to determine the y -coordinate. Using similar logic as the x -coordinate case, if the y -coordinate ever changes sign, or the rabbit ever lands on two cells with different y -coordinates with $P2y$ turned on, then the farmer can determine this y -coordinate. Hence we assume it's not the case here. Similar as before, we assume that the y -coordinate is nonnegative throughout.

We divide our analysis into whether the rabbit lands on a cell (say, c_0 , with y coordinate y_0) with $P2y$ turned on. If this is the case, then the hunter knows that the cell with y -coordinate a power of 2. It therefore remains to just learn the number of digits. Here's where the separator variable comes in: via N_y and D_y . If the rabbit goes below c_0 (i.e. strictly lower y -coordinate) then the farmer focuses on N_y ; otherwise the farmer focuses on D_y : whether a separator is turned on (not the digits 0 or 1) (call these 'variable of interest' here). In any case, the flag of interest is on if and only if the x -coordinate (which the farmer knows by now) is divisible by $\ell_{y_0} + 1$. The hunter can learn ℓ_{y_0} by looking at the of the x -gap of the consecutive cells (of different x -coordinate) with the variable of interest turn on (which will exist as x -coordinate of the rabbit is unbounded).

Otherwise, if the rabbit never steps on cells with y -coordinate that's a power of 2, then ℓ_y is constant throughout. Since the x -coordinate of the rabbit is unbounded, the farmer can first learn ℓ_y by identifying the two 'consecutive' cells with different y -coordinates that have s (separator) variable encoded (so $\ell_y + 1$ is the x -gap). Then, the rabbit will have to traverse the whole spectrum where x -coordinate has remainder $0, 1, \dots, \ell_y$ when divided by $\ell_y + 1$. Although the y -coordinate itself changes across steps, the farmer can use the trajectory of the rabbit to determine the corresponding digits (starting from the unit digits, and then 2, 4, \dots). This enables the hunter to learn the precise y -coordinates, eventually.

- C7. Consider a checkered $3m \times 3m$ square, where m is an integer greater than 1. A frog sits on the lower left corner cell S and wants to get to the upper right corner cell F . The frog can hop from any cell to either the next cell to the right or the next cell upwards.

Some cells can be sticky, and the frog gets trapped once it hops on such a cell. A set X of cells is called blocking if the frog cannot reach F from S when all the cells of X are sticky. A blocking set is minimal if it does not contain a smaller blocking set.

- Prove that there exists a minimal blocking set containing at least $3m^2 - 3m$ cells.
- Prove that every minimal blocking set contains at most $3m^2$ cells.

Solution. Throughout the solution, we denote the phrase B is “reachable” from A by the meaning that there’s a path from cell A to cell B with only upwards and rightwards moves, without passing through any cell in X .

A construction for (a) is as follows: we partition our checkered square into m subsquares with 3 rows each (and $3m$ columns). Then for each of these subsquares, we block off:

- the second cell from the left for the top row;
- all except the leftmost two and the rightmost two for the middle row;
- the second cell from the right for the bottom row.

	x							
		x	x	x	x	x		
							x	

Table 1: An illustration of one of the $3 \times 3m$ subsquare when $m = 3$

As a short justification on why this works, we have a total of $m(3m - 2) = 3m^2 - 2m$ cells. Within each subsquare, the blocking cells partition the non-blocking cells into “bottom-left” (BL) and “top right” (TR) region; when travelling from BL region of a subsquare, the frog either goes to another cell of the BL region of this subsquare or the BL region of the subsquare above it, hence keep staying in BL region. This proves blockingness since S is in BL region while F is in TR region (of their respective subsquare). Finally, removal of any x ’s above allows the frog to traverse from BL to TR region. Given that any cell in BL region of any subsquare is reachable from S while F is reachable from any cell in TR region of any subsquare, this proves minimality.

For (b), we consider the following characteristics of any minimal blocking set X . For each $x \in X$ we see the following:

- $X \setminus \{x\}$ is non-blocking, so there’s a valid path that passes through no cell in X other than x .
- X is blocking, so this path must pass through x (and no other cell in X).

Now let Y be the set reachable by S , and Z be the set where F is reachable from. Since X is blocking, Y and Z are disjoint. We’ll show that $|Y| \geq |X| - 1$ and $|Z| \geq |X| - 1$. This would then imply

$$9m^2 \geq |X| + |Y| + |Z| \geq 3|X| - 2 \quad (1)$$

which means $|X| \leq 3m^2$.

To do so we appeal to the following graph theory formulation.

Lemma 5. *Let G be a directed acyclic graph. If $u \rightarrow v$ is an edge, we say u is a parent of v , and v is a child of u . We say that a node is a root if it has no parent, and a node is a leaf if it has no children.*

Suppose that G has exactly one root and each node has at most two children. let k be the number of leaf and ℓ the number of non-leaf. Then $k - \ell \leq 1$.

Proof. Denote a path by a sequence of nodes connected by directed edge, and a reverse path as the sequence reversed (traversed by reverse edge). We now proceed by induction on the graph. Base case is where we have a single node; here $k = 1, \ell = 0$.

Inductive step: suppose that for some G , this statement holds for all graphs G' with fewer nodes than G . We see that by traversing from any node in reverse direction it will reach the root eventually (since there’s only one root and our graph is acyclic). Consider a non-leaf p in G such that all its children are leaves; this choice exist by considering an arbitrary

topological ordering of G and we choose p that's ranked last among the non-leaves (there must be one non-leaf if G has > 1 node since we only have one root). Denote G' as G with all the children of p deleted. This means G' also has a single root (as all the nodes deleted are leaves).

Since p (and possibly some other node that shares children with p) is now a leaf, $\ell' \leq \ell - 1$. Meanwhile, given that p has no more than two children (which got deleted) while p is now a leaf, we have $k' \geq k - 1$. By induction hypothesis, $k' - \ell' \leq 1$, so $k - \ell \leq (k' + 1) - (\ell' + 1) \leq 1$, as desired. \square

Now to complete the solution, consider the cells $X \cup Y$, and cell u is a parent of cell v if v is next cell right or next cell upwards to u , and u, v not both in X . By our construction, each cell in X cannot have any child (and hence must be all the leaves), and each cell in Y can have at most two child. Finally, the only root can be S : all cells in $X \cup Y$ are reachable from S . Take $x \in X \cup Y$ and y be the cell immediately before x in the path from S to x , $y \in Y$ and therefore y is a parent of x ($y \notin Z$ since X is blocking). Thus our lemma is applicable here, and $|X| - |Y| \leq 1$. Analogously, we may consider $Z \cup X$ and cell u is parent of cell v if v is cell left or bottom to u , and adjacent to u , and u, v not both in X (we can similarly show that F is the only root). Similar to the previous case, we have a generalized binary tree and so $|X| - |Z| \leq 1$.

Remark. The construction of (a) is motivated by mazes.

C8. Determine the largest integer N for which there exists a table T of integers with N rows and 100 columns that has the following properties:

- Every row contains the numbers $1, 2, \dots, 100$ in some order.
- For any two distinct rows r and s , there is a column c such that $|T(r, c) - T(s, c)| \geq 2$. (Here $T(r, c)$ is the entry in row r and column c .)

Answer. $N = \frac{100!}{2^{50}}$.

Solution. In general, we can view the rows as a permutation of $1, \dots, 2n$ (here $n = 50$), and therefore we need to find the maximal number of such permutation set S such that for any pairs $\sigma_1 \neq \sigma_2 \in S$ we have $|\sigma_1(k) - \sigma_2(k)| \geq 2$ for some k . Denote such number as $f(n)$, and we claim $f(n) = \frac{(2n)!}{2^n}$.

Upper bound. Group the set S_{2n} of all permutations of $\{1, \dots, 2n\}$ into equivalence classes determined by following: we say $\sigma_1 \sim \sigma_2$ if and only if for all $i = 1, \dots, n$, $\{2i - 1, 2i\}$ are in the same two positions for σ_1, σ_2 , though could be swapped. (For example, when $n = 2$, the permutations $(1234), (1243), (2134), (2143)$ are all the permutations in the same equivalence class). In other words, each class is characterized by partitioning $\{1, \dots, 2n\}$ into n pairs $\{a_1, b_1\}, \dots, \{a_n, b_n\}$ such that for a permutation σ in this class, $\{\sigma(a_i), \sigma(b_i)\} = \{2i - 1, 2i\}$ for all $i = 1, \dots, n$. Then, for any two permutations σ_1, σ_2 in this class, for each k there's an i such that $\{\sigma_1(k), \sigma_2(k)\} \subseteq \{2i - 1, 2i\}$, hence having $|\sigma_1(k) - \sigma_2(k)| \leq 1$. It then follows that for each class we can only choose at most one such permutation, giving the upper bound $\frac{(2n)!}{2^n}$ since there are 2^n elements in each class (given such partitions $\{a_1, b_1\}, \dots, \{a_n, b_n\}$ there are two ways to place $\{2i - 1, 2i\}$ for each i).

Construction. We use induction on n , where base case $n = 1$ we just need (12) .

Inductive step: suppose for some $n \geq 2$ we have $f(n - 1) = \frac{(2n - 2)!}{2^{n - 1}}$ such permutations of $\{1, \dots, 2n - 2\}$. Consider, now, such collection $U_{n - 1}$ of permutations. The key idea is as follows:

- Notice that $(123), (231), (312)$ (the even permutations of S_3) itself would satisfy our condition, and so will the similar idea applied to their counterparts in $\{2n - 2, 2n - 1, 2n\}$ (we'll see why it's important later).

- Group each permutation into $T_{x,y}$ where $x < y$ denote the positions of $\{2n-1, 2n\}$ (again, can be swapped within).

Concretely, our construction for the set U_n is as follows: for each $1 \leq x < y \leq 2n$, we consider each $\sigma \in U_{n-1}$, insert a blank space at position x , and then a blank space at position y . E.g. if $n = 3, x = 2, y = 5, \sigma = (2341)$ then we have $(2?34?1)$ with $?$ being the blank space. Then we insert $2n-1, 2n$ in the blank space according to the position of $2n-2$: we make $2n-1$ to come before $2n$ if and only if $2n-2$ is between the two blank spaces. Hence the relative order of the three numbers are one of the following: $(2n-2, 2n-1, 2n)$, $(2n-1, 2n, 2n-2)$, or $(2n, 2n-2, 2n-1)$ (or if you like, these three are cyclic shifts of each other). This would give $|U_n|$ is $\frac{(2n-2)!}{2^{n-1}} \cdot \binom{2n}{2} = \frac{(2n)!}{2^n}$, the optimal number.

Finally to verify, consider any σ_1, σ_2 in U_n . Consider the following cases depending on their class $T_{x,y}$ as denoted before.

Case 1. For some $x < y$ we have $\sigma_1, \sigma_2 \in T_{x,y}$. Then by induction hypothesis on the first $2n-2$ numbers these two permutations are valid by judging only on the positions of $\{1, \dots, 2n-2\}$ (since they both come from U_{n-1} , and shifted at the same two positions for $\{2n-1, 2n\}$).

Case 2. For some four pairwise distinct $x_1 < y_1, x_2 < y_2$ we have $\sigma_1 \in T_{x_1, y_1}$ and T_{x_2, y_2} . Here, we have either $\sigma_1(x_1) = 2n$ or $\sigma_1(y_1) = 2n$, but $\sigma_2(x_1)$ and $\sigma_2(y_1)$ both $\leq 2n-2$.

Case 3. Same $x_1 < y_1, x_2 < y_2$ but with exactly one overlap, say z where $z \in \{x_1, y_1\}$ and $z \in \{x_2, y_2\}$. If $\sigma_1(z) = 2n-1$ then $\sigma_1(w) = 2n$ where w is such that $\{w, z\} = \{x_1, y_1\}$. But then by our assumption (of one overlap), $\sigma_2(w) \leq 2n-2$. A similar verification can be done in case $\sigma_2(z) = 2n$.

Hence $\sigma_1(z) = \sigma_2(z) = 2n$, which leaves some $w_1 \neq w_2$ such that $\sigma_1(w_1) = \sigma_2(w_2) = 2n-1$. For a condition violation to happen, we'll need $\sigma_1(w_2) = \sigma_2(w_1) = 2n-2$ (they cannot be $2n$ since the spot is taken at position z for both). Such a construction, however, means σ_1 and σ_2 restricted to positions w_1, w_2, z (and elements $\{2n-2, 2n-1, 2n\}$) are obtained by swapping a pair of elements from each other, hence having different permutation parity. This is a contradiction of the cyclic shift construction we discussed earlier.

Geometry

- G1. Let $ABCD$ be a parallelogram such that $AC = BC$. A point P is chosen on the extension of the segment AB beyond B . The circumcircle of the triangle ACD meets the segment PD again at Q , and the circumcircle of the triangle APQ meets the segment PC again at R .

Prove that the lines CD, AQ , and BR are concurrent.

Solution. Denote T as $CD \cap AQ$ and $R' = CP \cap BT$. Our goal is to show that R' is on circle APQ .

Here we have $AC = BC = AD$ (from the definition of parallelogram), and by some angle chasing we have

$$\angle QAC = \angle TAC = \angle TDP = \angle CDP = \angle DPA \quad \angle CTA = \angle TAB$$

so triangles CTA and ADP are similar. It then follows that $CT \cdot AP = AD \cdot AC = AC^2 = BC^2$. Given also that $\angle TCA = \angle CBA = \angle CAB$, we have triangles CBT and APC similar, so $\angle TBC = \angle CPA$, which in turn becomes $\angle TR'C = \angle TQC$. Therefore $TCQR'$ is cyclic. This means:

$$\angle QAP = \angle QTC = \angle QR'C$$

and so $APR'Q$ is indeed cyclic.

- G2. (IMO 4) Let Γ be a circle with centre I , and $ABCD$ a convex quadrilateral such that each of the segments AB, BC, CD and DA is tangent to Γ . Let Ω be the circumcircle of the triangle AIC . The extension of BA beyond A meets Ω at X , and the extension of BC beyond C meets Ω at Z . The extensions of AD and CD beyond D meet Ω at Y and T , respectively. Prove that

$$AD + DT + TX + XA = CD + DY + YZ + ZC.$$

Solution. Here, IA is the external angle bisector of $\angle XAY$, and since X, A, I, Y are all on Ω , I is equidistant from X and Y . Similarly, T and Z are equidistant from I . This gives $TX = YZ$ and we're therefore left to prove

$$AD + DT + XA = CD + DY + ZC$$

Now, let $p(A)$ be the length of tangent from A to Γ (only defined for points outside Γ). Then the tangent of AD to Γ is in between A and D , but not between A and X (with X further). Therefore, $AD = p(A) + p(D)$ and $XA = p(X) - p(A)$. Similarly, $DT = p(T) - p(D)$, $DC = p(D) + p(C)$, $DY = p(Y) - p(D)$ and $CZ = p(Z) - p(C)$. This gives

$$AD + DT + XA = p(A) + p(D) + p(X) - p(A) + p(T) - p(D) = p(X) + p(T)$$

$$CD + DY + ZC = p(C) + p(D) + p(Y) - p(D) + p(Z) - p(C) = p(Y) + p(Z)$$

but since $IT = IZ$, $p(T)^2 = IT^2 - r^2 = IZ^2 - r^2 = p(Z)^2$ (here r is the radius of Γ). So $p(T) = p(Z)$ and similarly $p(X) = p(Y)$. Therefore $p(X) + p(T) = p(Y) + p(Z)$ as desired.

- G3. Let n be a fixed positive integer, and let \mathcal{S} be the set of points (x, y) on the Cartesian plane such that both coordinates x and y are nonnegative integers smaller than $2n$ (thus $|\mathcal{S}| = 4n^2$). Assume \mathcal{F} is a set consisting of n^2 quadrilaterals such that all their vertices lie in \mathcal{S} , and each point in \mathcal{S} is a vertex of exactly one of the quadrilaterals in \mathcal{F} . Determine the largest possible sum of areas of all n^2 quadrilaterals in \mathcal{F} .

Answer. $\frac{n^2(2n-1)(2n+1)}{3}$

Solution. The center (say, point O), is at coordinate $(n - \frac{1}{2}, n - \frac{1}{2})$. For a given quadrilateral $A_1A_2A_3A_4$, the area is bounded by (indices taken modulo 4)

$$\frac{1}{2} \sum_{i=1}^4 A_i O \cdot A_{i+1} O \cdot \sin \angle A_i O A_{i+1} \leq \frac{1}{4} \sum_{i=1}^4 (A_i^2 + A_{i+1}^2) = \frac{1}{2} \sum_{i=1}^4 A_i^2$$

with equality iff O lies in all the four triangles formed by the triangulation of the quadrilateral (and all the inequalities are equality). It therefore follows that the area sum is bounded by half the sum of squared distance from O to the $4n^2$ points, i.e.

$$\begin{aligned} & \frac{1}{2} \sum_{i=0}^{2n-1} \sum_{j=0}^{2n-1} (i - (n - \frac{1}{2}))^2 + (j - (n - \frac{1}{2}))^2 = 2n \sum_{i=0}^{2n-1} (i - (n - \frac{1}{2}))^2 \\ & = 2n \left(\frac{(2n-1)(2n)(4n-1)}{6} - n(2n-1)^2 + \frac{n(2n-1)^2}{2} \right) = \frac{n^2(2n-1)(2n+1)}{3} \end{aligned}$$

Equality can hold by the following construction: for each point A in \mathcal{S} and in the bottom left quadrant (i.e. both coordinates are less than those of O), consider the square with center O (such square is uniquely formed once A and O are fixed), then the all the four vertices of the square are in \mathcal{S} and in 4 different quadrants. It then follows that we can form such n^2 quadrilaterals fulfilling the problem formulation.

- G4. Let $ABCD$ be a quadrilateral inscribed in a circle Ω . Let the tangent to Ω at D intersect the rays BA and BC at points E and F , respectively. A point T is chosen inside the triangle ABC so that $TE \parallel CD$ and $TF \parallel AD$. Let $K \neq D$ be a point on the segment DF such that $TD = TK$.

Prove that the lines AC, DT and BK intersect at one point.

Solution. Let AC intersect TE and TF at U and V , respectively. Using some angle chasing, we can get

$$\angle UEF = \angle TEF \angle FDC = \angle DAC$$

and therefore $DEAU$ is cyclic. Similarly, $EDVC$ is cyclic. Moreover, since $\angle DCB + \angle DAB = 180^\circ$, we have

$$180^\circ = \angle FCD + \angle EAD = \angle FVD + \angle EUD$$

angle therefore $DUTV$ is also cyclic. This gives

$$\begin{aligned} \angle TDE &= \angle TDU + \angle UDE = \angle TVU + (180^\circ - \angle UAE) = \angle FVC + \angle CAB \\ &= \angle FDC + \angle CAB = \angle DAC + \angle CAB = \angle DAB \end{aligned}$$

Meanwhile, $TD = TK$ would mean $\angle TKE = 180^\circ - \angle TDE$, and $\angle BDE = \angle DCB = 180^\circ - \angle DAB = 180^\circ - \angle TDE$, therefore we may conclude $BD \parallel TK$.

Now let BD intersect AC at G , and DT intersect AC at W . We have

$$\frac{FK}{KE} = \frac{BF \sin \angle FBK}{BE \sin \angle EBK} \quad \frac{FW}{WE} = \frac{BC \sin \angle FBW}{BA \sin \angle EBW}$$

so showing that B, W, K collinear is the same as showing

$$\frac{FK}{KE} : \frac{BF}{BE} = \frac{CW}{WA} : \frac{BC}{BA}$$

Given also that D, G, B collinear, we have

$$\frac{FD}{DE} : \frac{BF}{BE} = \frac{CG}{GA} : \frac{BC}{BA}$$

Hence it suffices to show

$$\frac{FK}{KE} : \frac{FD}{DE} = \frac{CW}{WA} : \frac{CG}{GA}$$

For the first ratio, looking at triangle TFE and cevians TD, TK we have

$$\frac{FK}{KE} : \frac{FD}{DE} = \frac{TF \sin \angle FTK}{TE \sin \angle ETK} : \frac{TF \sin \angle FTD}{TE \sin \angle ETD} = \frac{\sin \angle ADB}{\sin \angle CDB} : \frac{\sin \angle FTD}{\sin \angle ETD}$$

where $\angle FTK = \angle ADB$ follows from $TK \parallel BD$ and $TF \parallel AD$ (and similarly for $\angle ETK = \angle CDB$). Similarly by looking at triangle CDA and cevians DW, DG we have

$$\frac{CW}{WA} : \frac{CG}{GA} = \frac{CD \sin \angle CDW}{DA \sin \angle ADW} : \frac{CD \sin \angle CDG}{DA \sin \angle ADG} = \frac{\sin \angle ETD}{\sin \angle FTD} : \frac{\sin \angle CDB}{\sin \angle ADB}$$

Here, $\angle CDW = \angle CDT = \angle ETD$ follows from $CD \parallel TE$ and similarly $\angle ADW = \angle ADT = \angle FTD$ follows from $AD \parallel TF$.

Thus both ratios turn out to be $\sin \angle ADB \sin \angle ETD : \sin \angle CDB \sin \angle FTD$, as desired.

- G5. Let $ABCD$ be a cyclic quadrilateral whose sides have pairwise different lengths. Let O be the circumcenter of $ABCD$. The internal angle bisectors of $\angle ABC$ and $\angle ADC$ meet AC at B_1 and D_1 respectively. Let O_B be the centre of the circle which passes through

B and is tangent to AC at D_1 . Similarly, let O_D be the centre of the circle which passes through D and is tangent to AC at B_1 .

Assume that $BD_1 \parallel DB_1$. Prove that O lies on the line O_BO_D .

Solution. Let E be the intersection between diagonals AC and BD , and denote the circle $ABCD$, circle with center O_B and tangent to AC , and circle with center O_D and tangent to AC as $\Omega, \omega_B, \omega_D$, respectively. Then the condition $BD_1 \parallel DB_1$ implies that E must be between B_1 and D_1 . W.l.o.g. let A, B_1, E, D_1, C be in that order, then $\angle ACD = \angle ABE > \angle CBE = \angle DAC$, so $AD > DC$, and similarly $BC > AB$.

Now we have

$$\angle E_BB_1 = \frac{\angle T_BB_1}{2} = \frac{\angle BAC - \angle BCA}{2} = \frac{\angle BDC - \angle BAC}{2} = \angle BDD_1$$

and therefore $BE_BB_1DD_1$ is cyclic. Similarly DE_DBB_1 is cyclic. This gives us

$$\angle DE_BB_1 = \angle DBD_1 = \angle BDB_1 = \angle BE_D B_1$$

middle equality is due to $BD_1 \parallel DB_1$. Thus we in fact have $DE_B \parallel BE_D$. Now that $BD_1 \parallel DB_1$ and $DE_B \parallel BE_D$, triangles E_BDB_1 and E_DBD_1 are similar.

Now let T_B, T_D be on AC such that lines BT_B and DT_D are tangent to circle Ω . Let the external bisectors of $\angle ABC$ and $\angle ADC$ intersect line AC at E_B and E_D , respectively. Then $\angle E_BB_1 = 90^\circ$ and $BT_B = T_BB_1$, so T_B is the midpoint of E_BB_1 . Similarly, T_D is the midpoint of E_DD_1 . Thus combined with $E_BDB_1 \sim E_DBD_1$ we also have $DT_B \parallel BT_D$.

Finally, $T_BB_1^2 = T_BB^2 = T_BA \cdot T_BC$ (first equality by angle chasing, second equality follows from T_BB tangent to Ω). With ω_D tangent to AC at B_1 this means that T_B has same power of point to Ω and ω_D . Since D is on both circles, DT_B is the radical axis of Ω and ω_D . Similarly, BT_D is the radical axis of Ω and ω_B . With $DT_B \parallel BT_D$, the centers of the three circles, O, O_B, O_D are collinear, as desired.

Remark: one way to say $BD_1 \parallel DB_1$ is to say

$$\frac{1}{AB^2} - \frac{1}{BC^2} = \frac{1}{DC^2} - \frac{1}{AD^2}$$

which can also be used to show $T_BD \parallel T_DB$.

- G7. (IMO 3) Let D be an interior point of the acute triangle ABC with $AB > AC$ so that $\angle DAB = \angle CAD$. The point E on the segment AC satisfies $\angle ADE = \angle BCD$, the point F on the segment AB satisfies $\angle FDA = \angle DBC$, and the point X on the line AC satisfies $CX = BX$. Let O_1 and O_2 be the circumcenters of the triangles ADC and EXD , respectively. Prove that the lines BC, EF , and O_1O_2 are concurrent.

Solution. Let T be the intersection point of BC and EF , Z be the second intersection of circles ADC and EXD . Let M be the second intersection of AD and circumcircle of triangle ABC , and N be the point diametrically opposite it. Then the task O_1, O_2, T collinear is equivalent to showing that $D \neq Z$ (i.e. ADC and EXD are not tangent to each other) and that $TD = TZ$. Our approach is broken down into the following steps:

Lemma 6. T is the center of the Apollonius' circle of triangle DBC passing through D .

Proof. Consider the following:

$$\frac{AE}{EC} = \frac{|\triangle ADE|}{|\triangle DEC|} = \frac{\frac{1}{2}AD \cdot DE \cdot \sin \angle ADE}{\frac{1}{2}DE \cdot DC \cdot \sin \angle CDE} = \frac{AD \cdot \sin \angle BCD}{DC \cdot \sin \angle CDE}$$

and similarly,

$$\frac{AF}{FB} = \frac{AD \cdot \sin \angle DBC}{DB \cdot \sin \angle FDB}$$

We also notice that by sine rule, $\frac{DB}{DC} = \frac{\sin \angle DCB}{\sin \angle DBC}$. In addition, $\angle FDB + \angle CDE = 360^\circ - \angle FDA - \angle ADE - \angle BDC = 360^\circ - \angle DBC - \angle BCD - \angle BDC = 180^\circ$. This means, $\sin \angle FDB = \sin \angle CDE$. By Menelaus' theorem applied on triangle ABC and line FET (without taking signs into consideration), we have

$$1 = \frac{CE}{EA} \cdot \frac{AF}{FB} \cdot \frac{TB}{TC} = \frac{DC \cdot \sin \angle CDE}{AD \cdot \sin \angle BCD} \cdot \frac{AD \cdot \sin \angle DBC}{DB \cdot \sin \angle FDB} \cdot \frac{TB}{TC} = \frac{DC}{DB} \cdot \frac{\sin \angle DBC}{\sin \angle DCB} \cdot \frac{TB}{TC} = \frac{DC^2}{DB^2} \cdot \frac{TB}{TC}$$

so $\frac{TB}{TC} = \frac{DB^2}{DC^2}$. Given also that E and F are on the segments AC and AB respectively, we have T lying outside of segment BC . The point T' on BC with $T'D$ tangent to circumcircle of DBC must satisfy $\frac{DB}{DC} = \frac{T'D}{T'C} = \frac{T'B}{T'D}$ which means that $\frac{T'B}{T'C} = \frac{DB^2}{DC^2}$. Thus $T' = T$ and TD is tangent to the circumcircle of DBC , hence being the center of an Apollonius circle. \square

Lemma 7. X, A, N, Z are concyclic.

Proof. Using directed angles, we have

$$\begin{aligned} \angle(XZ, ZC) &= \angle(XZ, ZD) + \angle(ZD, ZC) = \angle(XE, ED) + \angle(AD, AC) \\ &= \angle(AC, ED) + \angle(AD, AC) = \angle(AD, ED) \end{aligned}$$

where we used Z, X, E, D concyclic and Z, D, A, C concyclic. Analogously we have

$$\angle(XZ, ZA) = \angle(ZX, ZC) + \angle(ZC, ZA) = \angle(AD, ED) + \angle(CD, DA) = \angle(CD, ED)$$

Recall that we have $\angle(DC, CB) = \angle(DE, DA)$ from the problem condition (and taking care of the clockwise/anticlockwise direction). This gives

$$\angle(CD, ED) = \angle(CD, DA) + \angle(DA, DE) = \angle(CD, DA) + \angle(BC, CD) = \angle(BC, DA)$$

In addition, X, M, N collinear and perpendicular to BC , and $\angle NAM = 90^\circ$ since NM is the diameter of the circle ABC . This gives

$$\begin{aligned} \angle(XN, NA) &= \angle(XM, BC) + \angle(BC, DA) + \angle(DA, NA) \\ &= 90^\circ + \angle(BC, DA) + 90^\circ = \angle(BC, DA) = \angle(XZ, ZA) \end{aligned}$$

since directed angles are modulo 180° . \square

Lemma 8. Let DZ intersect MN at Q . Then line QC is tangent to the circle ADC at C .

Proof. let the circle DQC intersect AM again at R , and let MRC intersect NM again at S . Then we have:

$$\angle AZC = \angle MDC = \angle RDC = \angle RQC \quad \angle ACZ = \angle ADZ = \angle QDR = \angle QCR$$

so triangles AZC and RQC are similar. Similarly, S, R, C, M are concyclic, and then N, A, C, M are also concyclic. This means,

$$\angle SRC = 180^\circ - \angle SMC = 180^\circ - \angle NMC = \angle NAC \quad \frac{SR}{RC} = \frac{\sin \angle SMR}{\sin \angle RMC} = \frac{\sin \angle NMA}{\sin \angle AMC} = \frac{NA}{AC}$$

so triangles SRC and NAC are also similar. Thus this gives us

$$\frac{QR}{RS} = \frac{QR}{RC} \cdot \frac{RC}{RS} = \frac{AZ}{AC} \cdot \frac{AC}{NA} = \frac{AZ}{NA}$$

and

$$\angle QRS = 360^\circ - \angle QRC - \angle SRC = 360^\circ - \angle ZAC - \angle NAC = \angle NAZ$$

so triangles NAZ and SRQ are also similar. This gives

$$\angle MQR = \angle SQR = \angle MXA = \angle NZA = \angle NXA = \angle MXA$$

so lines AC and QR are parallel. This would entail $\angle QRA = \angle DAC$. Since D, A, C, Z are concyclic, $\angle DAC = \angle DZC$ and with Q, D, R, C concyclic, $\angle QRD = \angle QCD$. Thus $\angle QCD = \angle DZC$ so QC is indeed tangent to circle DZC . \square

Now we can complete the solution. First, $D \neq Z$: otherwise, D would have lied on circle XNA . We have D on internal angle bisector (segment) AM of $\angle BAC$, but segment AM only intersects circle XNA at point A . Next, with QC tangent to circle $ADCZ$ and Q on line DZ , Q is the center of Apollonius circle of CDZ passing through C . But since Q is on NM , $QB = QC$ so Q is also the center of Apollonius circle of BDZ passing through B . This gives us

$$\frac{CD}{CZ} = \sqrt{\frac{QD}{QZ}} = \frac{BD}{BZ}$$

or in other words, $\frac{BD}{CD} = \frac{BZ}{CZ}$. This means D and Z both lie on the same Apollonius circle, or $TD = TZ$, as desired.

Number Theory

- N1. Determine all integers $n \geq 1$ for which there exists a pair of positive integers (a, b) such that no cube of a prime divides $a^2 + b + 3$ and

$$\frac{ab + 3b + 8}{a^2 + b + 3} = n$$

Answer. $n = 2$ is the only solution, realized by $a = 2, b = 2$.

Solution. By solving equations on both sides we have $(a + 3 - n)b = na^2 + 3n - 8$. If both sides are 0 then $a + 3 - n = na^2 + 3n - 8 = 0$. This means we either have $n = 1$ or $n = 2$ (since we need $8 \geq 3n$). $n = 2$ has been shown to be possible, so we consider $n = 1$, i.e. $a^2 = 5$, which is impossible. We therefore have $a + 3 - n \neq 0$, and $b = \frac{na^2 - 5}{a + 3 - n}$. Using this, we have

$$a^2 + b + 3 = a^2 + \frac{na^2 - 5}{a + 3 - n} + 3 = \frac{(a + 1)^3}{a + 3 - n}$$

Now consider any prime p dividing $a + 1$. By the “no cube” condition we need $3v_p(a + 1) - (a + 3 - n) \leq 2$, so $(a + 3 - n) \geq 3v_p(a + 1) - 2 \geq v_p(a + 1)$ since $v_p(a + 1) \geq 1$. It then follows that $a + 3 - n$ is divisible by $a + 1$, and since $a + 3 - n > 0$, $a + 3 - n \geq a + 1$. In particular, $n \leq 2$. To see why we cannot have $n = 1$, we have $\frac{(a+1)^3}{a+2}$ an integer, but since $a + 1 \equiv -1 \pmod{a + 2}$ we have $a + 2 \mid -1$. This is impossible since $a \geq 1$.

- N2. (IMO 1) Let $n \geq 100$ be an integer. Ivan writes the numbers $n, n + 1, \dots, 2n$ each on different cards. He then shuffles these $n + 1$ cards, and divides them into two piles. Prove that at least one of the piles contains two cards such that the sum of their numbers is a perfect square.

Solution. Consider the numbers $a = 2((k - 1)^2 - 1)$, $b = 2k^2 + 1$, $c = 2((k + 1)^2 - 1)$ for some positive integer k . Then $a + b = (2k - 1)^2$, $a + c = (2k)^2$ and $b + c = (2k + 1)^2$. Hence if $n \leq a$ and $c \leq 2n$, by pigeonhole principle two of the three numbers above must be in the same pile.

It then remains to show that we can find such a k such that $n \leq a$ and $c \leq 2n$. Let k be the least integer such that $n \leq a$, i.e. $n \leq 2((k-1)^2 - 1)$. This also means that $n > 2((k-2)^2 - 1)$. For $100 \leq n \leq 126$, we may pick $k = 9$, resulting in $a = 126$ and $b = 198$. For $n \geq 127$ we have $k \geq 10$, and therefore

$$c = 2((k+1)^2 - 1) = 2((k-2)^2 - 1) \cdot \frac{(k+1)^2 - 1}{(k-2)^2 - 1} < n \cdot \frac{k}{k-3} \cdot \frac{k+2}{k-1} \leq n \cdot \frac{10}{7} \cdot \frac{12}{9} < 2n$$

as desired.

- N3. Find all positive integers n with the following property: the k positive divisors of n have a permutation (d_1, d_2, \dots, d_k) such that for every $i = 1, 2, \dots, k$, the number $d_1 + \dots + d_i$ is a perfect square.

Answer. $n = 1, 3$. We have $d_1 = 1$ for the former, and $d_1 = 1, d_2 = 3$ for latter.

Solution. By our condition, d_i is a difference between two squares, which follows that $d_i \not\equiv 2 \pmod{4}$. In particular, $d_i \neq 2$ for any d_i , so n cannot be even.

We now proceed with the following:

Lemma 9. Let x_i be the positive integer such that $x_i^2 = d_1 + \dots + d_i$. Then $x_{i-1} = \frac{d_i-1}{2}$ and $x_i = \frac{d_i+1}{2}$ must hold.

Proof of Lemma 9. We perform induction on the divisors d_i of n on the size of d_i itself: when $d_i = 1$, we use the fact that the only way to write $1 = x^2 - y^2$ is when $x = 1$ and $y = 0$ to conclude. This also means $d_1 = 1$.

Now for some d_i , suppose we have that for all d_j 's with $j < i$, the lemma holds. Consider, now, writing $d_i = (x_i - x_{i-1})(x_i + x_{i-1})$. If $a = x_i - x_{i-1}$ and $b = x_i + x_{i-1}$, then a, b are both divisors of d_i , and hence n . Suppose that $1 < a, b < d_i$. It then follows that $a = d_j$ and $b = d_k$ for some j, k . By our assumption, $x_{j-1} = \frac{a-1}{2}$ and $x_j = \frac{a+1}{2}$, given the monotonicity of x_1, x_2, \dots, x_k , we have x_{i-1} and x_i either both $\leq x_{j-1} = \frac{a-1}{2}$, or $\geq x_{j-1} = \frac{a+1}{2}$. Similarly, either $x_i \leq \frac{b-1}{2}$, or $x_{i-1} \geq \frac{b+1}{2}$. On the other hand, we can solve:

$$x_{i-1} = \frac{b-a}{2} \quad x_i = \frac{b+a}{2}$$

So x_i is \geq both $\frac{a+1}{2}$ and $\frac{b+1}{2}$, which then follows that $\frac{b-a}{2} \geq \frac{b+1}{2}$ too. This is absurd as it implies $a \leq 1$.

Hence we have $a = 1, b = d_i$. This readily implies $x_{i-1} = \frac{d_i-1}{2}$ and $x_i = \frac{d_i+1}{2}$. □

To finish off the problem, we have $x_i - x_{i-1} = 1$ for all i , which then follows that $x_i = i$ and $d_i = 2i - 1$. This means the divisors of n are all the odd numbers leading to n . In particular we have $n - 2 \mid n$ for $n > 1$, which only makes sense when $n = 3$.

- N4. Alice is given a rational number $r > 1$ and a line with two points $B \neq R$, where the point R contains a red bead and point B contains a blue bead. Alice plays a solitaire game by performing a sequence of moves. In every move, she chooses a (not necessarily positive) integer k , and a bead to move. If that bead is placed at point X , and the other bead is placed at Y , then Alice moves the chosen bead to point X' with $Y\vec{X}' = r^k Y\vec{X}$.

Alice's goal is to move the red bead to the point B . Find all rational numbers $r > 1$ such that Alice can reach her goal in at most 2021 moves.

Answer. $r = 1 + \frac{1}{\ell}, \ell = 1, 2, \dots, 1010$.

Solution. W.l.o.g. let B be at 1 and R be at 0. To show that the r given above is feasible, Alice can move in the following manner: in alternate fashion, Alice moves blue

bead with $k = 1$ and then red bead with $k = -1$. Then after each pair of moves the red bead is moved by $\frac{1}{\ell}$ to the right. Thus it will reach 1 after $2\ell \leq 2020$ moves.

Now let's consider $r = \frac{x}{y}$, with $\gcd(x, y) = 1$. Suppose that $d \triangleq x - y \geq 2$. We now consider modulo d on all rational numbers with both numerator and denominator relatively prime to d , such that $\frac{x'}{y'} \equiv k$ for integer k if $x'k \equiv y'$. Then $r \equiv 1 \pmod{d}$, and so is all its power. Since $r^k - r^\ell \equiv 0 \pmod{d}$ for any pairs of integers k, ℓ , the positions of the two beads modulo d won't change regardless of the moves by Alice (given that the distances of the beads will always be r^x). In particular, the position of red bead will always be congruent to 0 \pmod{d} , i.e. cannot reach 1.

We're left to consider $r = 1 + \frac{1}{\ell}$ for some ℓ , so our goal now becomes showing that $\ell \leq 1010$. Consider, now, the following problem formulation instead: starting at distance 1 between the two beads, we may move the beads such that the ordering is preserved (blue always to the right of the red), and the distance is r^m for some m . This means moving the same bead more than once in consecutive moves can be unified into one move, and we may then assume that every consecutive move would move beads of different colour. Consider the following cases:

Case 1. Blue goes first. If the chosen distance is $r^{b_1}, r^{r_1}, r^{b_2}, \dots$ then after $2p$ or $2p + 1$ moves. Suppose also that $p < \ell$, then the position of red bead is

$$P = \sum_{i=1}^p r^{b_i} - \sum_{j=1}^p r^{r_j}$$

if $b_i = r_i = 0$ for all i then the red bead remains at 0. If $b_i = r_j$ for some i, j then these two moves could be removed (while the number of steps cannot increase). Hence we may assume $b_i \neq r_j$ for any $i, j \leq p$.

Consider $M = \max\{b_i, r_j\}$. If $M > 0$, w.l.o.g. let M appear on the b side (i.e. positive sign). Since r^M appears at most $p < \ell$ times overall, we have $P = \frac{x}{y}$ where $\ell^M \mid y$ and $\ell \nmid x$, which means $P \neq 1$. In a similar fashion, if $M = \min\{b_i, r_j\} < 0$ then again w.l.o.g. let M appear on the b side. With r^M appears at most $p < \ell$ times overall, $P = \frac{x}{y}$ where $(\ell + 1)^{|M|} \mid y$ but $\ell + 1 \nmid x$, which also means $P \neq 1$.

This means at least 2ℓ moves is necessary, forcing $\ell \leq 1010$.

Case 2. Now red goes first. Let the chosen distance be $r^{r_1}, r^{b_2}, r^{r_2}, \dots$, then after $2p - 1$ moves ($p \leq \ell$) we have the position of red bead as

$$P = 1 + \sum_{i=2}^p r^{b_i} - \sum_{j=1}^p r^{r_j}$$

where the first 1 is due to the initial position of the blue bead. Using the similar analysis, we would get $P \neq 1$, unless $M = \max\{b_i, r_j\} > 0$ and appear at least ℓ times. With $p \leq \ell$, this means we need $p = \ell$ and this M must appear on the r side. We then in fact have

$$\sum_{j=1}^p r^{r_j} = \sum_{j=1}^{\ell} \left(\frac{\ell + 1}{\ell} \right)^M = \sum_{j=1}^{\ell} \frac{(\ell + 1)^M}{\ell^{M-1}}$$

Notice that if $M' = \min\{b_i, r_j\} < 0$ this would also land us problem as this M' cannot appear $\ell + 1$ times, hence all exponents have to be nonnegative here.

We now determine b_2, \dots, b_ℓ in the following manner: suppose that $r^{b_2} + \dots + r^{b_i} + r_{r_1} + \dots + r_{r_\ell} = -\frac{(\ell+1)^k}{\ell^{k-1}}$ for some k . Then:

- If $k = 1$ then we need $b_j = 0$ for all $j > i$.

- If $k > 1$ then we need one of the remaining numbers (say b_{i+1}) to be $k - 1$.

For the first case, we need $r^{b_{i+1}} + \dots + r^{b_\ell}$ to be an integer (here i could be 1), so by the analysis before all b_i 's have to be 0. For the second case, a similar analysis means all the remaining b_j 's have to be $\leq k - 1$, and we need one exactly $k - 1$ to match the denominator coefficient, hence the result. Given this, we have

$$-\frac{(\ell+1)^k}{\ell^{k-1}} + \frac{(\ell+1)^{k-1}}{\ell^{k-1}} = \frac{(\ell+1)^{k-1}(1-\ell-1)}{\ell^{k-1}} = -\frac{(\ell+1)^{k-1}}{\ell^{k-2}}$$

i.e. the telescoping sum.

To summarize, given $r_i = M$ for all i 's, we need b_2, b_3, \dots, b_ℓ to be $M-1, M-2, \dots, 1, 0, 0, \dots, 0$. At the end of telescoping we have $-\frac{(\ell+1)^k}{\ell^{k-1}} = -(\ell+1)$, so $P = C - (\ell+1)$ where $C = 1 + (\ell - 1 - (M-1))$ so $P \leq -1 - (M-1) \leq -1$, also a contradiction.

- N6. Determine all integers $n \geq 2$ with the following property: every n pairwise distinct integers whose sum is not divisible by n can be arranged in some order a_1, a_2, \dots, a_n so that n divides $1 \cdot a_1 + 2 \cdot a_2 + \dots + n \cdot a_n$.

Answer. All odd numbers and powers of 2.

Solution. Henceforth denote the quantity $S = a_1 + \dots + a_n$, and $T = (1 \cdot a_1 + 2 \cdot a_2 + \dots + n \cdot a_n)$. Let's first give an example of the case $n = 2^k a$ where $a > 1$ odd and $k \geq 1$. Let b_1, \dots, b_n be n positive integers whose sum is not divisible by a , and the n positive integers be $\{2^k b_i + 1\}$ for $i = 1, \dots, n$. Then $S = \sum_{i=1}^n (2^k b_i + 1) \equiv 2^k \sum_{i=1}^n b_i \pmod{n}$ is not divisible by b , and therefore not divisible by n . However, regardless of how we permute the n numbers, we have

$$T = 1 \cdot a_1 + 2 \cdot a_2 + \dots + n \cdot a_n \equiv (1 + 2 + \dots + n) = 2^{k-1} b(2^k b + 1) \equiv 2^{k-1} \pmod{2^k}$$

and therefore not divisible by n .

For n in the other category, let's consider the following. Denote a_1, \dots, a_n as our n integers. The main idea, both inside and outside the lemma, is the cyclic shift.

Lemma 10. Let $d = \gcd(n, S) < n$. Suppose n is power of 2 or odd number, then we can rearrange a_1, \dots, a_n such that $d \mid T$.

Proof. Consider the following prime factorization of d :

$$d = \prod_{i=1}^k p_i^{e_i}$$

Consider an arbitrary arrangement of a_1, \dots, a_n . Consider, also, the maximal index u such that the resulting T is divisible by $d' = \prod_{i=1}^u p_i^{e_i}$. If $u = k$ we're done. Here, d is either power of 2, or is odd. It then follows that d' has to be odd.

Now we focus on the prime power $p_{u+1}^{e_{u+1}}$. Denote $p_{u+1}^\ell = \gcd(p_{u+1}^{e_{u+1}}, \gcd(a_i - a_j))$, the inner gcd taken across all i, j with $d' \mid i - j$. Then w.r.t. p_{u+1}^ℓ we have

$$T \equiv \sum_{i=1}^{d'} a_i \left(\sum_{j=0}^{\frac{n}{d'}-1} (d'j + i) \right) \equiv \sum_{i=1}^{d'} a_i \left(\frac{n}{d'} + d' \cdot \frac{1}{2} \frac{n}{d'} \cdot \left(\frac{n}{d'} - 1 \right) \right) \equiv 0 \pmod{p_{u+1}^\ell}$$

The equality follows from that $\frac{n}{d'} = \prod_{i=u+1}^k p_i^{e_i}$ is divisible by $p_{u+1}^{\ell+1}$, and so is $\frac{1}{2} \frac{n}{d'} \left(\frac{n}{d'} - 1 \right)$: this wouldn't be an issue if p_{u+1} is odd; if $p_{u+1} = 2$ then we have $d' = 1$, $n = 2^{\ell'}$ for some $\ell' > \ell$ so $\frac{1}{2}n$ is also divisible by 2^ℓ .

Next, we claim that we can do some rearrangement such that there exists a segment of length $s = d'p_{u+1}^{e_{u+1}}$ such that the sum of a_i 's is not divisible by $p_{u+1}^{\ell+1}$. Notice that by the definition of ℓ , there exists i_0, j_0 such that $p_{u+1}^\ell = \gcd(p_{u+1}^{e_{u+1}}, a_{i_0} - a_{j_0})$, and $d' \mid i_0 - j_0$. W.l.o.g. suppose $i_0 < j_0$, and consider any such segment of length s containing only i_0 and not j_0 , or vice versa. Such a segment exists since $n \geq 2s$:

- If $j_0 \geq s$, then we may take a segment ending at a_{i_0} (or if $i_0 < s$, take segment starting at a_1).
- Otherwise, we may just take segment starting at a_{j_0} (or if $j_0 + s > n$, take segment ending at a_n).

Let this segment be a_{x+1}, \dots, a_{x+s} for some x . If $p_{u+1}^{\ell+1} \nmid a_{x+1} + \dots + a_{x+s}$ we're done. Otherwise, we may just swap a_{i_0} and a_{j_0} , and the conclusion follows from that exactly one of a_{i_0}, a_{j_0} is in the segment, and also $p_{u+1}^{\ell+1} \nmid a_{i_0} - a_{j_0}$. Notice that T is now changed by $(i_0 - j_0)(a_{i_0} - a_{j_0})$, which by our assumption the difference is divisible by d' since $d' \mid i_0 - j_0$. So T remains divisible by d' .

We're now ready to show that we can shift this segment around to make T divisible by s . Consider the following m -step cyclic shift:

$$(a_{x+1}, \dots, a_{x+s}) \rightarrow (a_{x+s-m+1}, \dots, a_{x+s}, a_{x+1}, \dots, a_{x+s-m})$$

where now T changes by

$$m(a_{x+1} + \dots + a_{x+s}) - s(a_{x+s-m+1} + \dots + a_{x+s}) \equiv m(a_{x+1} + \dots + a_{x+s}) \pmod{s}$$

Now consider $k = 0, d', \dots, s - d'$ (notice the last quantity is the same as $d'(p_{u+1}^{e_{u+1}} - 1)$). Here, T remains divisible by d' after any such shifts, so it suffices to consider modulo $p_{u+1}^{e_{u+1}}$. Moreover, we also have $p_{u+1}^\ell \mid T$, and so the solution

$$md'(a_{x+1} + \dots + a_{x+s}) + T \equiv 0 \pmod{p_{u+1}^{e_{u+1}}}$$

has a solution m given that $p_{u+1}^{\ell+1} \nmid d'(a_{x+1} + \dots + a_{x+s})$. This completes the induction step. \square

Now, the extension from the lemma to the whole problem is now straightforward: given $\gcd(S, n) = d$, we may first rearrange a_1, \dots, a_n such that $d \mid T$. Thereafter, we do cyclic shift on the whole interval:

$$(a_1, \dots, a_n) \rightarrow (a_{n-k+1}, \dots, a_n, a_1, \dots, a_{n-k})$$

where T is now changed by $k(a_1 + \dots + a_n) \pmod{n}$. Since $T \mid \gcd(a_1 + \dots + a_n, n)$, it then follows that we can find such k such that $k(a_1 + \dots + a_n) + T \equiv 0 \pmod{n}$.

- N8. For a polynomial $P(x)$ with integer coefficients let $P^1(x) = P(x)$ and $P^{k+1}(x) = P(P^k(x))$ for $k \geq 1$. Find all positive integers n for which there exist a polynomial $P(x)$ with integer coefficients such that for every integer $m \geq 1$, the numbers $P^m(1), \dots, P^m(n)$ leave exactly $\lceil \frac{n}{2^m} \rceil$ distinct remainders when divided by n .

Answer. All the powers of 2 and prime numbers.

Solution. We first provide examples for the said answers above. For $n = 2^k$, considering $P(x) \equiv 2x$ means $\{P^m(x) \pmod{n} : x = 1, \dots, n\}$ are $\{u2^{\min\{m, k\}} \pmod{n} : u = 0, 1, \dots, 2^{\max\{0, k-m\}} - 1\}$. For n any odd prime p , define

$$P(x) = \sum_{i=0}^{p-1} \left\lfloor \frac{i}{2} \right\rfloor (1 - (x - i)^{p-1})$$

By Fermat's little theorem, $P(x) \equiv \lfloor \frac{x}{2} \rfloor \pmod{p}$, and therefore the set $\{P^m(x) \pmod{p}\}$ for $x = 0, \dots, p-1$ is $0, \dots, \lfloor \frac{p-1}{2^m} \rfloor$ for each m . Since p is odd, $\{P^m(x) \pmod{p}\}$ then has $\lceil \frac{p-1}{2^m} \rceil$ elements.

It now remains to show that these are the only answers. First, for any $m \geq 0$ and integers $x \neq y$ we have

$$x - y \mid P^m(x) - P^m(y)$$

Thus we may (sometimes) consider $P^m(\cdot \pmod{n})$. Define $S_n(P^m) = \{P^m(1), \dots, P^m(n) \pmod{n}\}$, and $\sigma_n(P^m) = |S_n(P^m)|$. We see that $S_n(P^m) \subseteq S_n(P^{m+1})$, with equality if and only if $S_n(P^m) = S_n(P^M)$ for all $M \geq m$. It then follows that $\sigma_n(P^m)$ monotonically decreases with m before being constant.

We first consider the case $n = pq$ where $\gcd(p, q) = 1$, $p > 1$ and $q > 1$. Observe that by Chinese Remainder Theorem, there is a bijection from $\mathbb{N}_n \rightarrow \mathbb{N}_p \rightarrow \mathbb{N}_q$ by $(x \pmod{n}) \rightarrow (x \pmod{p}, x \pmod{q})$. This also implies that there is a bijection from $S_n(P^m)$ to $(S_p(P^m), S_q(P^m))$ and therefore $\sigma_n(P^m) = \sigma_p(P^m) \cdot \sigma_q(P^m)$. From the problem condition, for $m > \log_2(n)$ we have $\sigma_n(P^m) = 1 = \sigma_p(P^m) \cdot \sigma_q(P^m)$. On the other hand, $\sigma_p(P^0) = p$ and $\sigma_q(P^0) = q$. This means we can choose $m_p = \min\{m : \sigma_p(P^m) = 1\}$ and $m_q = \min\{m : \sigma_q(P^m) = 1\}$. W.l.o.g. let $m_p \leq m_q$. This means we have

$$\sigma_n(P^{m_p-1}) = \sigma_p(P^{m_p-1}) \cdot \sigma_q(P^{m_p-1}) \geq 2 \cdot (\sigma_q(P^{m_p}) + 1) > 2 \cdot \sigma_q(P^{m_p}) = 2\sigma_n(P^{m_p})$$

where the inequality is due to $\sigma_p(P^{m_p-1}) > \sigma_p(P^{m_p}) = 1$, and $\sigma_p(P^{m_q-1}) > \sigma_p(P^{m_q})$ due to the monotone strict decrease (before stabilizing). By the problem condition, however, we must have $2\sigma_n(P^{m_p}) - \sigma_n(P^{m_p-1}) \in \{0, 1\}$, contradiction.

It then remains to consider $n = p^k$ for some odd prime p and $k \geq 2$. Consider, now, $A_u = \{u, p+u, \dots, p(p^{k-1}-1)+u \pmod{p^k}\}$, $u = 0, 1, \dots, p-1$, we see that by $x-y \mid P(x) - P(y)$ there exists $v \in \{0, \dots, p-1\}$ such that $P(A_u) \subseteq A_v$. We now start with the following lemma.

Lemma 11. *For each u , consider v such that $P(A_u) \subseteq A_v$. Then we have either $P(A_u) = A_v$ (i.e. $|P(A_u)| = p^{k-1}$), or $1 \leq |P(A_u)| \leq p^{k-2}$.*

Proof. Expand $P(x) = \sum_{i=0}^n a_i x^i$ (where n is the degree of P), and define $Q(x) = \sum_{i=1}^n i a_i x^{i-1}$. A quick computation yields that for any b, ℓ with $\ell \geq 1$ we have

$$P(u + bp^\ell) - P(u) = \sum_{i=1}^n a_i \sum_{j=1}^i \binom{i}{j} u^{i-j} (bp^\ell)^j \equiv \sum_{i=1}^n b i a_i p^\ell = bp^\ell Q(u) \pmod{p^{\ell+1}}$$

If $p \nmid Q(u)$, then $p^k \nmid P(u + bp^\ell) - P(u)$ whenever $p^k \nmid bp^\ell$. Extending this logic to any $u', u' + bp^\ell \in A_u$ we see that $P(u')$ takes different values in A_v for all $u' \in A_u$, hence $|P(A_u)| = |A_u| = |A_v|$ and therefore $P(A_u) = A_v$. Conversely, if $p \mid Q(u)$, then $p^k \mid P(u' + bp^{k-1}) - P(u')$ for all $u' \in A_u$. Thus $P(A_u) = \{P(u') : u' = u, \dots, p^{k-1} - p + u\}$, which has at most p^{k-2} elements. \square

Now we state a related corollary. Denote the following quantities (as usual all quantities in mod p^k)

$$R_m = \{u \in \{0, 1, \dots, p-1\} : u' \in \text{Range}(P^m), \forall u' \in u\} \quad \ell_m = |R_m|$$

$$s_m = |\text{Range}(P^m) \pmod{p^k} \setminus \cup_{u \in R_m} A_u|$$

One may deduce that $|\text{Range}(P^m) \pmod{p^k}|$ is $\ell_m p^{k-1} + s_m$. We now show that $t_m \triangleq \ell_m p^{k-2} + s_m$ cannot increase w.r.t. m . Indeed, let a and b be such that among the elements

$A_u \in R_m$, a of them have $P(A_u) = A_v$ for some v , and b of them have $|P(A_u)| \leq p^{k-2}$. Then we have $\ell_{m+1} \leq a$ and $s_{m+1} \leq bp^{k-2} + s_m$ and therefore

$$t_{m+1} \leq ap^{k-2} + bp^{k-2} + s_m = t_m$$

as desired. (We note that it's possible that some of the $bp^{k-2} + s_m$ elements might form a complete A_v , but that will mean a decrease of s_{m+1} by p^k and increase of ℓ_{m+1} by 1, which will not increase t_{m+1}). In particular, $t_0 = p(p^{k-2}) = p^{k-1}$, so $t_i \leq p^{k-1}$.

Now, by the problem condition, $\lceil \frac{p^k}{2^m} \rceil = \ell_m p^{k-1} + s_m$. We see that for each number t with $0 \leq t \leq p^k$, with the exception of $t = p^{k-1}$ (with $(0, p^{k-1})$ or $(1, 0)$), the other t has at most one representation of $t = ap^{k-1} + b$ with (a, b) nonnegative integers, such that $ap^{k-2} + b \leq p^{k-1}$.

Suppose we're given such P ; we see that by setting $m = 1$, we have $\lceil \frac{p^k}{2} \rceil = \frac{p-1}{2}p^{k-1} + \lceil \frac{p^{k-1}}{2} \rceil$, i.e. $\ell_1 = \frac{p-1}{2}$, $s_1 = \lceil \frac{p^{k-1}}{2} \rceil$. We first see that under this condition, there must be at least $\frac{p-1}{2}$ numbers $u \in \{0, \dots, p-1\}$ such that $|P(A_u)| = p^{k-1}$; let these u 's be U_1 . Also, the s_1 residues must come from at least $\lceil \frac{s_1}{p^{k-2}} \rceil = \frac{p+1}{2}$ other A_u 's; let these u 's be V_1 . Since $\frac{p-1}{2} + \frac{p+1}{2} = p$, the equality must then hold. It follows that:

- The $\frac{p-1}{2}$ numbers u in U_1 must have $P(A_u)$ occupying different A_v 's (in other words, $u \neq u' \in U_1$ means $p \nmid u - u'$).
- Consider the set $W = \cup_{u \in U_1} P(A_u)$. If $P(A_u) \subseteq W$ for some $u \in V_1$, then $s_1 \leq p^{k-2}(|V_1| - 1) = p^{k-2}(\frac{p-1}{2}) < \lceil \frac{p^{k-1}}{2} \rceil$, which is impossible. It then follows that each of the $\frac{p-1}{2}$ sets $P(A_u) : u \in U_1$, and also the single set $\cup_{u \in V_1} P(A_u)$, are disjoint.

Since $|\{P^m \pmod{p^k}\}| = 1$ for all $m > k \log_2 p$, this also means $|\{P^m \pmod{p}\}| = 1$ for all $m > k \log_2 p$. It then follows that there is a unique u_0 such that $P(u_0) \equiv u_0 \pmod{p}$, which then also means that $|P(A_{u_0})| \leq p^{k-2}$ (otherwise, $P(A_{u_0}) = A_{u_0}$ and then $|\{P^m \pmod{p^k}\}| = p^{k-1}$ for all m , contradiction). In addition, there must exist another $u'_0 \neq u_0 \pmod{p}$ such that $P(u'_0) \equiv u_0$ (otherwise, for all m $P^m \pmod{p}$ takes at least two values). Since $u_0 \equiv P(u_0) \not\equiv u \pmod{p}$ for all $u \in U_1$, it then follows that this u'_0 must be in V_1 . This means that:

$$|A_{u_0} \cap \{P(x) \pmod{p^k}\}| \geq \lceil \frac{p^{k-1}}{2} \rceil - \frac{p-3}{2}(p^{k-2}) = \lceil \frac{3p^{k-2}}{2} \rceil$$

By the property of u_0 , however, we see that these $|A_{u_0} \cap \{P(x) \pmod{p^k}\}|$, when applied P , will only produce at most p^{k-2} distinct residues. It then follows that the s_1 u 's will produce at most $s_1 - (\lceil \frac{3p^{k-2}}{2} \rceil - p^{k-2}) = s_1 - \lceil \frac{p^{k-1}}{2} \rceil$ when applied P once more. This gives

$$t_2 \leq t_1 - \lceil \frac{p^{k-2}}{2} \rceil = p^{k-2}(\frac{p-1}{2}) + \lceil \frac{p^{k-1}}{2} \rceil - \lceil \frac{p^{k-2}}{2} \rceil = p^{k-1} - p^{k-2} = p^{k-2}(p-1)$$

Consider, now, the following two cases, each of which we provide a contradiction.

- For some m we have $\lceil \frac{p^k}{2^m} \rceil = ap^{k-1} + b$ with $a \geq 2$ even. Then by the ℓ_m, s_m uniqueness, $\ell_m = a$ and $s_m = b$. Since a is even, we have $\ell_{m+1} = \frac{a}{2}$ and $s_{m+1} = \lceil \frac{b}{2} \rceil$, meaning that $t_{m+1} \leq \lceil \frac{t_m}{2} \rceil \leq \lceil \frac{p^{k-1}}{2} \rceil$. Now consider the minimal m_1 with $\lceil \frac{p^k}{2^{m_1}} \rceil < p^{k-1}$. Since p is odd, we have $\ell_{m_1} = 0$ and $\lceil \frac{p^{k-1}}{2} \rceil \leq s_{m_1} < p^{k-1}$. Since $t_{m+1} \leq \lceil \frac{p^{k-1}}{2} \rceil$, we have $s_{m_1} = \lceil \frac{p^{k-1}}{2} \rceil$. Considering step $m_1 - 1$, however, we get $(\ell, s) = (1, 0), (1, 1), (0, p^{k-1})$, with t_{m_1} being p^{k-2}, p^{k-1} , or $p^{k-2} + 1$, none of which can be equal to $\lceil \frac{p^{k-1}}{2} \rceil$ and therefore violates the monotonicity.

- We now have $\lceil \frac{p^k}{2^m} \rceil = ap^{k-1} + b$ where either a is odd or $a = 0$. For this to happen, by considering $a = \lfloor \frac{p}{2^m} \rfloor$ we have $p = 2^q - 1$ for some q . Now in this case we have $\lceil \frac{p^k}{2^m} \rceil = (2^{q-2} - 1)p^{k-1} + \lceil \frac{3p^{k-2}}{4} \rceil$, resulting in

$$t_2 = (2^{q-2} - 1)p^{k-2} + \lceil \frac{3p^{k-1}}{4} \rceil = (\frac{p-3}{4})p^{k-2} + \lceil \frac{3p^{k-1}}{4} \rceil > p^{k-2}(p-1),$$

which contradicts $t_2 \leq p^{k-2}(p-1)$ earlier on.