Algebra

A1. Let n be an integer, and let A be a subset of $\{0, 1, \cdots, 5^n\}$ 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 $a_1 < \cdots < a_m$ 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 $i = 1, \cdots, n$ and $j = 1, \cdots, n$.

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

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

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

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

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

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 $k = 1, \cdots, n$. This is precisely when $n+1$ is prime.

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

$$\lfloor \frac{a_1}{1} \rfloor + \cdots + \lfloor \frac{a_n}{n} \rfloor$$

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

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

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

$a_{2^m}, \cdots, a_{\min(2^{m+1}-1,n)}$ is $\min(2^{m+1}-1,n), 2^m, \cdots, \min(2^{m+1}-1,n)-1$, 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 $a_1, \cdots, a_m$ are distinct positive integers, then then $\lfloor \frac{a_1}{1} \rfloor + \cdots + \lfloor \frac{a_m}{m} \rfloor \geq f(m)$:*

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

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

□

In particular, this would be the case when $(a_1, \cdots, a_n)$ is a permutation of $1, \cdots, n$. (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 $\lfloor \frac{a_{m+1}}{m+1} \rfloor + \cdots + \lfloor \frac{a_n}{n} \rfloor \geq 1$, so

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

  $f(m)$ 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 $a_1, \cdots, a_m$; we have $n' \leq m \leq \frac{n}{2}$. If we define $a'_i = \begin{cases} n' & i = \ell \\ a_i & \text{otherwise} \end{cases}$ then

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

  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

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

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 $C_1, C_2, \cdots, C_n$, 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 $i = 1, \cdots, n$.

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 $g = 0, \cdots, n-2$, 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 $i = 1, 2, \cdots, n$, 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 2. *There exists a diverse collection of path from A to B with maximal number, such that all paths in the form of $A \to v \to B$ are included (here $\to$ means directed edge).*

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

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

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

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

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

$$A \to v \Rightarrow B \qquad A \Rightarrow v \to B$$

such that $A \Rightarrow v$ and $v \Rightarrow B$ are two paths with disjoint roads, and also disjoint from edges $A \to v$ and $v \to B$. 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 $A \to v \to B$.

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

Now, referencing to towns A and B, each vertex can be categorized into exactly one of the following: $\vec{AB}$-type ($A \to v \to B$), $\vec{BA}$-type ($B \to v \to A$), in-type ($A \to v \leftarrow B$) and out-type ($A \leftarrow v \to B$). Regardless of the members of the collection, either $A \to B$ or $B \to A$ 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 $A \to v \to B$ for all $\vec{AB}$-type vertices v. Thereafter, any new path starting with $A \to v'$ must have v' an in-type and any new path ending with $v'' \to B$ must have v'' an out-type. Now we claim the following:

Lemma 3. *A maximally diverse collection of paths from A to B containing $A \to v \to B$ for all $\vec{AB}$-type vertices v. Then the remaining paths are the maximal possible-sized set of paths in the form $A \to v_1 \Rightarrow v_2 \to B$, 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 $A \to v_1$ and $B \to v_2$ condition.

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

To finish, denote C_{AB} as the quantity described in Lemma 3. 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,

$$N_{AB} = C_{AB} + 1\{A \to B\} + |\{v : \vec{AB}\text{−type}\}| \qquad N_{BA} = C_{BA} + 1\{B \to A\} + |\{v : \vec{BA}\text{−type}\}|$$

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

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

as desired.

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, ..., 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 $1, \cdots, 2n$ (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 $|\sigma_1(k) - \sigma_2(k)|$ 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 $\{1, \cdots, 2n\}$ into equivalence classes determined by following: we say $\sigma_1 \sim \sigma_2$ if and only if for all $i = 1, \cdots, n$, $\{2i-1, 2i\}$ are in the same two positions for σ_1, σ_2, though could be swaped. (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 $\{1, \cdots, 2n\}$ into n pairs $\{a_1, b_1\}, \cdots, \{a_n, b_n\}$ such that for a permutation σ in this class, $\{\sigma(a_i), \sigma(b_i)\} = \{2i - 1, 2i\}$ for all $i = 1, \cdots, n$. 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 $\{a_1, b_1\}, \cdots, \{a_n, b_n\}$ 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 $\{1, \cdots, 2n-2\}$. 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 $\{1, \cdots, 2n-2\}$ (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 paralleogram 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 vy some angle chasing we have

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

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.

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

$$\angle TDE = \angle TDU + \angle UDE = \angle TVU + (180^\circ - \angle UAE) = \angle FVC + \angle CAB$$

$$= \angle FDC + \angle CAB = \angle DAC + \angle CAB = \angle DAB$$

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

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

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 $O_B O_D$.

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 $\Omega, \omega_B, \omega_D$, respectovely. 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

$$\angle E_B B B_1 = \frac{\angle T_B B B_1}{2} = \frac{\angle BAC - \angle BCA}{2} = \frac{\angle BDC - \angle BAC}{2} = \angle BDD_1$$

and therefore $BE_B DD_1$ is cyclic. Similarly $DE_D BB_1$ is cyclic. This gives us

$$\angle DE_B D_1 = \angle DBD_1 = \angle BDB_1 = \angle BE_D B_1$$

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 $E_B DB_1$ and $E_D BD_1$ 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 $\angle E_B B B_1 = 90^\circ$ and $BT_B = T_B B_1$, so T_B is the midpoint of $E_B B_1$. Similarly, T_D is the midpoint of $E_D D_1$. Thus combined with $E_B DB_1 \sim E_D BD_1$ we also have $DT_B \parallel BT_D$.

Finally, $T_B B_1^2 = T_B B^2 = T_B A \cdot T_B C$ (first equality by angle chasing, second equality follows from $T_B B$ 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 $T_B D \parallel T_D B$.

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 $n \geqslant 100$ be an integer. Ivan writes the numbers $n, n + 1, \ldots, 2n$ 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 $(d_1, d_2, \cdots, d_k)$ such that for every $i = 1, 2, \cdots, k$, the number $d_1 + \cdots + d_i$ 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 4. *Let x_i be the positive integer such that $x_i^2 = d_1 + \cdots + d_i$. Then $x_{i-1} = \frac{d_i-1}{2}$ and $x_i = \frac{d_i+1}{2}$ must hold.*

Proof of Lemma 4. 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 $x_1, x_2, \cdots, x_k$, 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 ther other hand, we can solve:

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

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

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 $r^{b_1}, r^{r_1}, r^{r_2}, r^{b_2}, \cdots$ 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 $r^{r_1}, r^{b_2}, r^{r_2}, \cdots$, 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 $b_2, \cdots, b_\ell$ in the following manner: suppose that $r^{b_2} + \cdots + r^{b_i} + r_{r_1} + \cdots + r_{r_\ell} = -\frac{(\ell+1)^k}{\ell^{k-1}}$ 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 $r^{b_{i+1}} + \cdots + r^{b_\ell}$ 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 $b_2, b_3, \cdots, b_\ell$ to be $M-1, M-2, \cdots, 1, 0, 0, \cdots, 0$. 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 $n \geqslant 2$ with the following property: every n pairwise distinct integers whose sum is not divisible by n can be arranged in some order $a_1, a_2, \ldots, a_n$ so that n divides $1 \cdot a_1 + 2 \cdot a_2 + \cdots + n \cdot a_n$.

Answer. All odd numbers and powers of 2.

Solution. Henceforth denote the quantity $S = a_1 + \cdots + a_n$, and $T = (1 \cdot a_1 + 2 \cdot a_2 + \cdots + n \cdot a_n)$. Let's first give an example of the case $n = 2^k a$ where $a > 1$ odd and $k \geq 1$. Let $b_1, \cdots, b_n$ be n positive integers whose sum is not divisible by a, and the n positive inegers be $\{2^k b_i + 1\}$ for $i = 1, \cdots, n$. 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

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

and therefore not divisible by n.

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

Lemma 5. *Let $d = \gcd(n, S) < n$. Suppose n is power of 2 or odd number, then we can rearrange $a_1, \cdots, a_n$ 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 $a_1, \cdots, a_n$. 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 rearragement 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 $a_{x+1}, \cdots, a_{x+s}$ for some x. If $p_{u+1}^{\ell+1} \nmid a_{x+1} + \cdots + a_{x+s}$ 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:

$$(a_{x+1}, \cdots, a_{x+s}) \to (a_{x+s-m+1}, \cdots, a_{x+s}, a_{x+1}, \cdots, a_{x+s-m})$$

where now T changes by

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

Now consider $k = 0, d', \cdots, s - d'$ (notice the last quantity is the same as $d'(p_{u+1}^{e_{u+1}} - 1)$). Here, T remains devisible 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

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

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

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

$$(a_1, \cdots, a_n) \to (a_{n-k+1}, \cdots, a_n, a_1, \cdots, a_{n-k})$$

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

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 $P^m(1), \cdots, P^m(n)$ leave exactly $\lceil n/2m \rceil$ distinct remainders when divided by n.

Conjectured answer. All the powers of 2 and prime numbers.

Partial Solution. Throughout we assume P is a polynomial with integer coefficients. The following identity will be used profusely: 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 $P^m(\cdot \pmod{n})$.

We define $\sigma(P, m, n)$ as the number of distinct reimainders of $P^m(1), \cdots, P^m(n)$ when devided by n. A preliminary observation would be that for any polynomials P and integers m and n, $\sigma(P, m+1, n) \leq \sigma(P, m, n)$, with equality if and only if $\sigma(P, M, n) = \sigma(P, m, n)$ for all $M \geq m$.

We break down our solution into the following.

Lemma 6. *Let p and q be any integers such that $\gcd(p, q) = 1$. Then for any polynomial P, $\sigma(P, m, pq) = \sigma(P, m, p) \cdot \sigma(P, m, q)$.*

Proof. Consider the mapping $r : \mathbb{N}_{pq} \to \mathbb{N}_p \times \mathbb{N}_q$ by the following: for each x with $0 \leq x \leq pq - 1$, if $x \equiv y \pmod{p}$ and $x \equiv z \pmod{q}$ then $r(x) = (y, z)$. Since $\gcd(p, q) = 1$, this mapping is bijective via Chinese Remainder Theorem.

Now if $r(x) = (y, z)$, then $r(P^m(x) \pmod{pq}) = (P^m(y) \pmod{p}, P^m(z) \pmod{q})$, since $p \mid x - y$ implies $p \mid P^m(x) - P^m(y)$ (and similarly for q and z). It then follows that

$$\begin{aligned} |\{P^m(x) \pmod{pq} : x \in \mathbb{N}\}| &= |\{(P^m(y) \pmod{p}, P^m(z) \pmod{q}) : y, z \in \mathbb{N}\}| \\ &= |\{P^m(y) \pmod{p} : y \in \mathbb{N}\}| \cdot |\{P^m(z) \pmod{q} : z \in \mathbb{N}\}| \end{aligned}$$

as desired. □

Now if n is divisible by at least two primes, it can be written as $n = pq$ with $1 < p, q < n$. The problem condition implies that $\sigma(P, m, n) = 1$ for some (sufficiently large) n, so $\sigma(P, m, p) = 1 = \sigma(P, m, q) = 1$ for sufficiently large m. Let m_p (respectively m_q) be the minimum index such that $\sigma(P, m, p)$ (respectively $\sigma(P, m, q)$) is 1; we have $m_p, m_q \geq 1$. W.l.o.g, also, that $m_p \leq m_q$. Then by the lemma 6 we have

$$\begin{aligned} \sigma(P, m_p, q) = \sigma(P, m_p, p) \cdot \sigma(P, m_p, q) = \sigma(P, m_p, n) &= \left\lceil \frac{\sigma(P, m_p - 1, n)}{2} \right\rceil \\ &= \left\lceil \frac{\sigma(P, m_p - 1, p)\sigma(P, m_p - 1, q)}{2} \right\rceil \end{aligned}$$

By the minimality of m_p, $\sigma(P, m_p - 1, p) \geq 2$, and $\sigma(P, m_p - 1, q) > \sigma(P, m_p, q)$, so

$$\left\lceil \frac{\sigma(P, m_p - 1, p)\sigma(P, m_p - 1, q)}{2} \right\rceil \geq \left\lceil \frac{2(\sigma(P, m_p, q) + 1)}{2} \right\rceil \geq \sigma(P, m_p, q) + 1$$

i.e. a contradiction. This effectively reduces n to the cases of prime powers. For $n = 2^k$, the polynomial $P(x) = 2x$ would do the job; for $n = p$ an odd prime number, consider

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

which by Fermat's little theorem satisfies $P(x) \equiv \lfloor \frac{x}{2} \rfloor$ for $x = 0, \cdots, p-1$. It then follows that the set $\{P^m(x)\}$ for $x = 0, \cdots, p-1$ is $0, \cdots, \lfloor \frac{p-1}{2^m} \rfloor$ for each m, which contains $1 + \lfloor \frac{p-1}{2^m} \rfloor = \lceil \frac{p}{2^m} \rfloor$ distinct entries.

It then remains to consider $n = p^k$ for some odd prime p and $k \geq 2$. (TODO: this is the harder part.)