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 $\lfloor \frac{ij}{n+1}$ 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 $\lfloor \frac{a_\ell}{\ell}$ 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

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

$\square$

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:

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

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.

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. $\square$

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. $\square$

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.

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.

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.

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 $a \geq 1$.

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 $\vec{YX'} = r^k \vec{YX}$.

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 $\ell \leq 1010$. (TODO)

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.

Answer. All the prime powers p^k for some prime p and $k \geq 0$.

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 5. *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

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

$$= |\{P^m(y) \pmod{p} : y \in \mathbb{N}\}| \cdot |\{P^m(z) \pmod{q} : z \in \mathbb{N}\}|$$

as desired. $\square$

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 5 we have

$$\sigma(P, m_p, q) = \sigma(P, m_p, p) \cdot \sigma(P, m_p, q) = \sigma(P, m_p, n) = \lceil \frac{\sigma(P, m_p - 1, n)}{2} \rceil$$

$$= \lceil \frac{\sigma(P, m_p - 1, p)\sigma(P, m_p - 1, q)}{2} \rceil$$

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

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

i.e. a contradiction. This effectively reduces n to the cases of prime powers, which we consider in the following:

Lemma 6. *Let $n = p^d$ for some prime p, and $a_1, \cdots, a_n$ be such that for each $k \leq d$, $p^k \mid x - y$ implies $p^k \mid a_x - a_y$. Then there exists a polynomial P with integer coefficients such that $P(x) \equiv a_x \pmod{n}$ for $x = 1, \cdots, n$.*

Proof. We do induction on d. For base case $d = 0$ there's nothing to prove since any polynomial would work.

Now suppose that for some $d \geq 1$, the conclusion above holds for $d - 1$, i.e. there exists $P(x)$ such that $P(x) \equiv a_x \pmod{p^{d-1}}$ for all $x = 1, \cdots, p^{d-1}$. Consider the number $r_x = P(x) - a_x$, which is divisible by p^{d-1} for $x = 1, \cdots, p^{d-1}$ (and therefore for all $x \in \mathbb{Z}$).

(LOL this lemma is wrong :(will fix stuff later) □

Now we can finish the proof. Here, consider $n = p^d$. Consider the function $s(\cdot)$ that maps $\{0, 1, \cdots, p-1\}$ to itself such that,

$$0 \leq a_i \leq p - 1, \ell = \sum_{i=0}^{d-1} a_i p^i \Rightarrow s(\ell) = \sum_{i=0}^{d-1} a_{d-i-1} p^i$$

I.e. $s(\ell)$ is the number obtained by reversing the digits of ℓ written in base p (with leading zeros until there are d digits in total). By Lemma 6, there exists a polynomial P satisying

$$P(x) \equiv s(\lfloor \frac{s(x)}{2} \rfloor) \pmod{n}, \forall x = 0, 1, \cdots, n-1$$

Indeed, if $p^k \mid x - y$, then:

- x and y have identical last k digits;
- $s(x)$ and $s(y)$ have identical first k digits;
- $\lfloor \frac{s(x)}{2} \rfloor$ and $\lfloor \frac{s(y)}{2} \rfloor$ have identical first k digits
- $s(\lfloor \frac{s(x)}{2} \rfloor)$ and $s(\lfloor \frac{s(y)}{2} \rfloor)$ have identical last k digits

which then means $p^k \mid P(x) - P(y)$. Finally, given that s is bijective with $s(s(x)) = x$, the distinct values of $P^m(x) \bmod n$ are $s(\lfloor \frac{x}{2^m} \rfloor), \forall x = 0, 1, \cdots, n - 1$, thus giving us $1 + \lfloor \frac{n-1}{2^m} \rfloor = \lceil \frac{n}{2^m} \rceil$ distinct values, as desired.