Algebra

A1 (IMO 4) Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that, for all integers a, b, c that satisfy $a + b + c = 0$, the following equality holds:

$$f(a)^2 + f(b)^2 + f(c)^2 = 2f(a)f(b) + 2f(b)f(c) + 2f(c)f(a).$$

Answer. There are three families of functions, with c denoting any integer constant:

- $f(n) = cn^2$.
- $f(n) = 0$ if n even, or c if n odd.
- $f(n) = c$ if n odd, $4c$ if $4 \mid n - 2$, 0 if $4 \mid n$.

We can verify that those work (although in the actual IMO a detail verification is needed...erm screw that).
Solution. Plugging $a = b = c = 0$ gives $3f(0)^2 = 6f(0)^2$ which forces $f(0) = 0$. Plugging $(a, b, c) = (0, n, -n)$ gives $f(n)^2 + f(-n)^2 = 2f(n)f(-n)$, i.e. $(f(n) - f(-n))^2 = 0$. This forces $f(n) = f(-n)$, so f is an even function.

Now we proceed with the following by considering $c = -(a + b)$, bearing in mind that $f(c) = f(-c)$, too. We now have the following:

$$f(a+b)^2 - 2f(a+b)(f(a) + f(b)) + (f(a)^2 + f(b)^2 - 2f(a)f(b)) = 0$$

which is essentially solving the quadratic equation on $f(a+b)$. Using the quadratic formula (and bearing in mind that $f(a)^2 + f(b)^2 - 2f(a)f(b) = (f(a) - f(b))^2$) we have:

$$\begin{aligned} f(a+b) &= \frac{2(f(a) + f(b)) \pm \sqrt{4(f(a) + f(b))^2 - 4(f(a) - f(b))^2}}{2} \\ &= (f(a) + f(b)) \pm \sqrt{4f(a)f(b)} \\ &= (f(a) + f(b)) \pm 2\sqrt{f(a)f(b)} \end{aligned}$$

In particular, if $f(b) = 0$ then $f(a + b) = f(a)$ so f is of period b. Hence $f(1) = 0$ implies $f \equiv 0$ (which can be put into any category above). We thus assume that $f(1) \neq 0$ in the future.

Now we see what happens when we fix $f(1)$. We have $f(2) = 2f(1) \pm 2\sqrt{f(1)^2} = 2f(1) \pm 2f(1)$, i.e. $f(2) = 0$ or $f(2) = 4f(1)$. In the first case, by setting $b = 2$ we have $f(a + 2) = f(a) \pm 2\sqrt{0} = f(a)$, so $f(a + 2) = f(a)$. We now infer that $f(a) = 0$ if a even, and $f(a) = f(1)$ if a odd.

Otherwise, we assume that $f(2) = 4f(1)$. Then $f(3) = f(1) + f(2) \pm \sqrt{f(1)f(2)}$, and setting $f(2) = 4f(1)$ we have $5f(1) \pm \sqrt{2}4f(1)^2 = 5f(1) \pm 4f(1)$, so we have two cases, depending whether $f(3) = f(1)$ or $f(3) = 9f(1)$.

In the first case, $f(3) = f(1)$. We have $f(4) = f(1) + f(3) \pm 2\sqrt{f(1)f(3)} = 2f(1) \pm 2f(1)$, which is equal to either 0 or $4f(1)$. Also $f(4) = f(2) + f(2) \pm 2\sqrt{f(2)^2} = 2f(2) \pm 2f(2)$ which is either 0 or $4f(2) = 16f(1)$. Since both $f(4) \in \{0, 4f(1)\}$ and $f(4) \in \{0, 16f(1)\}$, we have $f(4) = 0$ and therefore f is of period 4, in the form $c, 4c, c, 0$, etc.

Otherwise, $f(3) = 9f(1)$. Now $f(k) = k^2 f(1)$ for $k = 0, 1, 2, 3$. We now show that this is true for all integer k. Since f is even, we only need to prove this for all $k > 0$. We use induction: suppose that $f(n) = n^2 f(1)$ for all $n = 0, 1, \cdots, k$, with $k \geq 3$. We now consider $f(k + 1)$:

- considering $f(1)$ and $f(k)$, we have $f(k+1) = f(1) + f(k) \pm 2\sqrt{f(1)f(k)} = f(1) + k^2 f(1) \pm 2\sqrt{k^2 f(1)} = f(1)(1 + k^2 \pm 2k) = f(1)(k \pm 1)^2$, i.e. either $f(1)(k+1)^2$ or $f(1)(k-1)^2$.

- considering $f(2)$ and $f(k-1)$, we have $f(k+1) = f(2)+f(k-1)\pm 2\sqrt{f(2)f(k-1)} = f(1)(2^2+(k-1)^2\pm 2(2)(k-1)) = f(1)((k-1)\pm 2)^2$, i.e. $f(1)(k+1)^2$ or $f(1)(k-3)^2$.

We thus infer than $f(k+1) = f(1)(k+1)^2$, done.

A2 Let $\mathbb{Z}$ and $\mathbb{Q}$ be the sets of integers and rationals respectively.

(a) Does there exist a partition of $\mathbb{Z}$ into three non-empty subsets A, B, C such that the sets $A+B, B+C, C+A$ are disjoint?

(b) Does there exist a partition of $\mathbb{Q}$ into three non-empty subsets A, B, C such that the sets $A+B, B+C, C+A$ are disjoint?

Answer. (a): yes; (b): no.

Solution. The construction for (a) is

$$A = \{3k+1 : k \in \mathbb{Z}\} \qquad B = \{3k+2 : k \in \mathbb{Z}\} \qquad C = \{3k : k \in \mathbb{Z}\}$$

Now we show that (b) cannot work. Let d be any rational number. For a set A we say that A is d-existent if there exists $a, b \in A$ such that $a - b = d$. We say that A is d-abundant if for any $a \in A$, $a + d \in A$.

We first show that if A is d-existent, then all A, B, C are d-abundant. Indeed, let $a_1, a_2 \in A$ such that $a_2 - a_1 = d$. Since B and C are nonempty, choose $b \in B$ and $c \in C$. By the problem condition, since $a_1 + b, a_2 + b \in A + B$, they cannot be in $A + C$ or $B + C$, so both the numbers $a_1 + b - c$ and $a_2 + b - c$ are in C. Operating on these numbers again, we have $(a_2 + b) - (a_1 + b - c) = c + (a_2 - a_1) = c + d \in C$. Repeating this argument on any $c \in C$, we have C as d-abundant, and similarly so for B. Finally, since B and C are nonempty and d-abundant, they are also d-existent. Therefore we may repeat the logic above to deduce that A is d-abundant, too.

Now choose $a \in A$ and $b \in B$, and suppose that $d = b - a$. Then since $b \notin A$, A cannot be d-abundant, and therefore by our lemma above, A, B, C cannot be d-existent. On the other hand, consider the four numbers $0, \frac{1}{6}d, \frac{1}{3}d, \frac{1}{2}d$. By pigeonhole principle, two of the numbers must be in the same partition, meaning that this partition must be $\frac{d}{k}$-existent (where $k \in \{2, 3, 6\}$). Thus by our lemma, A, B, C are all $\frac{1}{k}$-abundant. Notice, however, a d-abundant set is also a kd-abundant set for all integers k (we have $a \in A \to a + d, a + 2d, a + 3d, \cdots, a + kd \in A$), so all the three sets are d-abundant, contradiction.

A3 (IMO 2) Let $n \geq 3$ be an integer, and let $a_2, a_3, \ldots, a_n$ be positive real numbers such that $a_2 a_3 \cdots a_n = 1$. Prove that

$$(1 + a_2)^2 (1 + a_3)^3 \cdots (1 + a_n)^n > n^n.$$

Solution. As per official solution, we will show that $f_k(x) = \frac{(x+1)^k}{x} \geq \frac{k^k}{(k-1)^{k-1}}$ with equality if and only if $x = \frac{1}{k-1}$. Consider the derivative w.r.t. x:

$$f_k'(x) = \frac{xk(x+1)^{k-1} - (x+1)^k}{x^2} = \frac{(x+1)^{k-1}}{x^2}(xk - (x+1)) = \frac{(x+1)^{k-1}}{x^2}((k-1)x - 1)$$

Since $\frac{(x+1)^{k-1}}{x^2} > 0$, we have $f_k'(x) > 0$ iff $(k-1)x - 1 > 0$, i.e. $x > \frac{1}{k-1}$. Also $f_k'(x) < 0$ iff $(k-1)x - 1 < 0$, i.e. $x < \frac{1}{k-1}$. Thus f_k is increasing when $x > \frac{1}{k-1}$ and f_k is decreasing when $x < \frac{1}{k-1}$. We conclude that f_k attains it minimum point at $x = \frac{1}{k-1}$, with $f_k(\frac{1}{k-1}) = \frac{(1+1/(k-1))^k}{1/(k-1)} = \frac{k^k}{(k-1)^{k-1}}$.

Now, having established this, we have

$$\prod_{k=2}^{n}(1+a_k)^k = \prod_{k=2}^{n}\frac{(1+a_k)^k}{a_k} \geq \prod_{k=2}^{n}\frac{k^k}{(k-1)^{k-1}} = \frac{n^n}{1^1} = n^n$$

(since $\prod a_k = 1$). However, if the equality were to hold, we have $a_k = \frac{1}{k-1}$, so $\prod a_k = \frac{1}{(k-1)!} < 1$, which is a contradiction. Hence the equality cannot hold, so the inequality must be strict.

A4 Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.

Solution. Let $p_1 < p_2 < \cdots$ be a sequence of prime numbers and $\{r_k\}_{k\geq 1}$ be the sequence of rational numbers, such that $(p_n f + g)(r_n) = 0$.

We first show that the sequence $\{r_n\}$ must be bounded. Notice that $\{p_k\}_{k\geq 0} \to \infty$, and $p_n|f(r_n)| = |g(r_n)|$. Let M_1 be a real number such that $f(x), g(x) \neq 0$ for all $x > M_1$, and let M_2 be a real number such that $|f(x)| > |g(x)|$ for all $x > M_2$ (this is true since $\deg(f) > \deg(g)$ and therefore $\frac{|f|}{|g|} \to \infty$). From $p_n|f(r_n)| = |g(r_n)|$ (since $p_n \geq 1$ for primes p_n) we have $|f(r_n)| \leq |g(r_n)|$ since $|\cdot|$ is nonnegative. We therefore know that $r_n \leq \max\{M_1, M_2\}$ for all $n \geq 1$, and therefore $\{r_n\}$ is bounded.

Now, since $\{r_n\}$ is bounded, it has a convergent subsequence. By extracting the convergent subsequence and the corresponding p_n responsible for them, may as well assume that $\{r_n\}$ is itself convergent, and let $\{r_n\} \to r_0$. We show that r_0 is rational and $f(r_0) = 0$. Now that f and g are polynomials, they are continuous functions. Suppose that $f(r_0) > 0$. Since $\{r_n\} \to r_0$, there exists an N such that $f(r_n) > \frac{f(r_0)}{2}$. Since $\{r_n\}$ is also convergent (and bounded), $\{g(r_n)\}$ is also bounded: let N be such that $|g(r_n)| < N$ for all $n \geq 1$. Since $\{p_n\}$ is increasing sequences of primes, it's also unbounded. Thus, there exists p_n that's greater than $\frac{2N}{f(r_0)}$. Now, $p_n|f_n(r_n)| = |g_n(r_n)|$. However,

$$p_n|f_n(r_n)| > p_n|\frac{f(r_0)}{2}| > \frac{2N}{f(r_0)} \cdot \left|\frac{f(r_0)}{2}\right| = N > |g_n(r_n)|$$

which is a contradiction. Hence we cannot have $f(r_0) > 0$. Similarly we cannot have $f(r_0) < 0$. Therefore $f(r_0) = 0$.

Now since $\{r_n\}$ is a rational sequence, let's write $r_n = \frac{u_n}{v_n}$ with p_n, q_n integers. By the rational root theorem, we have $v_n \mid p_n a_k$ and $u_n \mid p_n a_0 + b_0$ where a_k is the leading coefficient of f (recall that $\deg f > \deg g$) and a_0, b_0 the constant coefficient of f and g, respectively. For clarity, let's focus on all n such that $p_n > a_k$. Since p_n is increasing sequence of primes, there's a N such that $p_n > a_k$ for all $n \geq N$. We may now assume that $N = 1$ (by truncating all the first $N-1$ terms) and that $p_n > a_k$ for all $n \geq 1$.

If $p_n \nmid v_n$ for infinitely many v_n, then $v_n \mid a_k$ for those all those n's. Since there are infinitely many of those n's, and a_k has only finitely many divisors, there must be infinitely many v_n's that are the same. Let $\{r_{n_k}\}$ be the subsequence such that v_{n_k} are the same, say v_0. Since this subsequence also converges to r_0, u_{n_k} must be the same (say u_0) for sufficiently large k, too. This forces $r_0 = u_0/v_0$, and is thus rational.

Thus $p_n \mid v_n$ for all but finitely many v_n. Again by extracting the appropriate subsequence we may assume $p \mid v_n$ for all n. Let $v_n = p_n w_n$, then from $v_n \mid pa_k$ we have $w_n \mid a_k$. Again by the logic above, there are infinitely w_n that are the same, say, w_0. Since $u_n \mid p_n a_0 + b_0$, we can write $u_n = \frac{p_n a_0 + b_0}{d_n}$, and therefore we have $r_n = \frac{u_n}{v_n} = \frac{p_n a_0 + b_0}{d_n p_n w_n}$, with infinitely many of the w_n equal to w_0. In other words we have yet another subsequence $r_n = \frac{p_n a_0 + b_0}{d_n p_n w_0}$ converging to r_0, i.e. $\frac{p_n a_0 + b_0}{d_n p_n} = \frac{a_0}{d_n} + \frac{b_0}{d_n p_n}$ converging to $r_0 w_0$. If d_n is unbounded, this gives a subsequence of $\frac{p_n a_0 + b_0}{d_n p_n}$ converging to 0, so $r_0 = 0$. Otherwise, there exists infinitely many d_n that's the same, say d_0, so we have $\frac{p_n a_0+b_0}{d_n p_n} = \frac{p_n a_0+b_0}{d_0 p_n}$ which converges to $\frac{a_0}{d_0}$ and therefore $r_0 = \frac{a_0}{d_0 w_0}$, establishing the claim.

Combinatorics

C1 Several positive integers are written in a row. Iteratively, Alice chooses two adjacent numbers x and y such that $x > y$ and x is to the left of y, and replaces the pair (x, y) by either $(y + 1, x)$ or $(x - 1, x)$. Prove that she can perform only finitely many such iterations.

Solution. Let M be the maximum of the n numbers. We first notice that at each step, the two numbers $y < x \leq M$ is changed to either $y+1$ and x or $x-1$ and x. Since $y < x$, $y + 1 \leq x \leq M$, so neither $y + 1, x, x - 1$ can exceed M. Thus after any iterations, no number can exceed M, and thus the sum of the n numbers is bounded by Mn. On the other hand, after each iteration, the sum of the n numbers either increases by 1 (in the case of $(y + 1, x)$), or $x - y - 1$ (in the case of $(x - 1, x)$). Since $x - y - 1 \geq 0$ (as $x > y$), the sum of the numbers never decrease. But since the sum of the numbers cannot exceed Mn either, it can only increase finitely many times (each increase adds to the sum by at least 1 since the numbers are all positive integers).

Thus if Alice were to do it infinitely many times, after one point the sum of the numbers remain the same. This falls into the case of $(x, y) \to (x-1, x)$ and when $x-y-1 = 0$, i.e. $y = x-1$. This is basically swapping the two adjacent numbers $(x, y) \to (y, x)$, subject to the constraint $y = x - 1$. We see that the set of the numbers (along with their frequency) do not change, so all those iterations are basically permutations of the numbers.

Let's now order the permutations of n numbers in the following way: if σ and γ are two permutations, let k_0 be the leftmost index such that $\sigma(k_0) \neq \gamma(k_0)$. We say that $\sigma < \gamma$ iff $\sigma(k_0) < \gamma(k_0)$. Since $y < x$, each iteration changes the arrangement of the n numbers to a smaller permutation. But since there are only $n!$ permutation, there's only finitely many possible such iterations too. This proves the problem.

C2 Let $n \geq 1$ be an integer. What is the maximum number of disjoint pairs of elements of the set $\{1, 2, \ldots, n\}$ such that the sums of the different pairs are different integers not exceeding n?

Answer. $\lfloor \frac{2n-1}{5} \rfloor$

Solution. Suppose that we have k such pairs of numbers, then the $2k$ numbers must have sum at least $1 + 2 + \cdots + 2k = k(2k + 1)$. Since these k pairs have sum that are different integers not exceeding n, the sum is at most $n+(n-1)+\cdots+(n-k+1) = \frac{k}{2} \cdot (2n-k+1)$. Thus, $k(2k+1) \leq \frac{k}{2} \cdot (2n-k+1)$, which is the same as $2(2k+1) \leq 2n-k+1$. Rearranging yields $5k \leq 2n - 1$, i.e. $k \leq \frac{2n-1}{5}$. Since k must be an integers, $k \leq \frac{2n-1}{5}$.

Now we show that this is an attainable bound, which we split into two cases:

- For $n = 5m + 1$ and $5m + 2$, we have (in both cases) $\lfloor \frac{2n-1}{5} \rfloor = 2m$. Consider the first $4m$ numbers and we pair them in the following fashion:

  $$(1, 4m-1), (2, 4m-3), \cdots, (m, 2m+1), (m+1, 4m), (m+2, 4m-2), \cdots, (2m, 2m+2)$$

  these give the sum as following:

  $$4m, 4m - 1, \cdots, 3m + 1, 5m + 1, 5m, \cdots, 4m + 2$$

  so these are $2m$ pairs of sum $3m+1, 3m+2, \cdots, 4m, 4m+2, 4m+3, \cdots, 5m, 5m+1$ which are all distinct and at most $5m + 1 \leq n$.

- Now for $n = 5m+3, 5m+4, 5m+5$, $\lfloor \frac{2n-1}{5} \rfloor = 2m+1$. We now need the first $4m+2$ numbers and consider the following pairing:

  $$(1, 3m+2), (2, 3m+3), \cdots, (m+1, 4m+2), (m+2, 2m+2), (m+3, 2m+3), \cdots, (2m+1, 3m+1)$$

  these give the sum as the following:

  $$(3m+3), (4m+5), \cdots, (5m+1), (5m+3), (3m+4), (3m+6), \cdots, (5m+2)$$

  which are the distinct $2m+1$ sums of all integers in the range $3m+3, 3m+4, \cdots, 5m+3$.

C4 Players A and B play a game with $N \geq 2012$ coins and 2012 boxes arranged around a circle. Initially A distributes the coins among the boxes so that there is at least 1 coin in each box. Then the two of them make moves in the order $B, A, B, A, \ldots$ by the following rules:
(a) On every move of his B passes 1 coin from every box to an adjacent box.
(b) On every move of hers A chooses several coins that were not involved in B's previous move and are in different boxes. She passes every coin to an adjacent box.

Player A's goal is to ensure at least 1 coin in each box after every move of hers, regardless of how B plays and how many moves are made. Find the least N that enables her to succeed.

Answer. $2(2012) - 2 = 4022$.
Solution. (Modified from the solution submitted as homework) The condition that A can only move coins that are not involved in B's previous moves and are in different boxes can be reformulated as, A can choose boxes that had two coins before B's immediate prior move, and move one coin from each chosen boxes to an adjacent box.

We will now design a strategy for A when $N = 4022$ by having her to maintain the following invariant after each step of hers: all boxes have exactly two coins except two of them, say, box B_x and B_y, and $x \not\equiv y \pmod 2$. Now, for each of the 2010 boxes B_k that are not B_x or B_y, A can do the following: if B moved a coin from B_k to $B_{k+\epsilon}$ with $\epsilon = \pm 1$, then A moves a coin from B_k to $B_{k-\epsilon}$. To show that this invariant is maintained, suppose, for time being, that the boxes B_x and B_y are involved in A's move as well. For each box B_k, each A and B moves a coin from B_k to an adjacent box, so there's an outflow of two coins by this consideration. Nevertheless, considering the move from B_{k-1}, among the two moves $B_{k-1} \to B_k$ and $B_{k-1} \to B_{k-2}$, exactly one move is done by B and the other by A. Same goes to the two moves $B_{k+1} \to B_k$ and $B_{k+1} \to B_{k+2}$, so these give a total inflow of two coins by the two players. Hence the net flow of coins is zero, which restores our configuration to the initial configuration before B's move. Now, excluding B_x and B_y from the operation means that we need to undo the moves by B_x and B_y to an adjacent box. That is, moving an adjacent coin from $B_{x\pm1}$ to B_x and $B_{y\pm1}$ to B_y. Since x and y are of different parity, $B_{x\pm1}$ and $B_{y\pm1}$ cannot be the same regardless of the choices of the signs, and moreover $x \pm 1$ and $y \pm 1$ have different signs. Therefore, $B_{x\pm1}$ and $B_{y\pm1}$ are the only two boxes with one coin each, and our invariant is maintained.

Next, we design a strategy for B when $N \leq 2n-3$. Notice that if some N gives a winning strategy for A, then so will $N + k$ for any $k \geq 0$ (A can technically add the extra k coins anywhere and 'pretend' that those coins don't exist). We assume an arbitrary starting state for B and break B's algorithm into the following:

Step 1: we first show that B can force two adjacent boxes with 1 coin each, after some A's move. The algorithm is to find an arc starting and ending with boxes of 1 coin and having 2 coins *on average* for boxes in between, and then shorten this arc. We'll also use the fact that, if $B_1, \cdots, B_k$ with $k \geq 2$ has at least 1 coin each but total coin $\leq 2k-2$, then there's one such arc within these k boxes.

Given $N = 2n-3$, the starting state (or any state that prevents A from losing) must have one box with exactly one coin. Let this box be B_0 (indices modulo n).

Let k be the minimal index such that the sum of coins in $B_1, \cdots, B_k$ is less than $2k$. By the minimality of k, B_k has 1 exactly coin; since $B_1, \cdots, B_{n-1}$ has $2n-4 < 2(n-1)-1$ coins in total, $k \le n-2$. This means $B_0, \cdots, B_k$ has length $k+1$ and is one of the arcs we've described.

If $k = 1$ we're done with this step. Otherwise, let B do the following:

$$B_0 \to B_{-1} \qquad B_1 \to B_0 \qquad B_{-1} \to B_{-2} \qquad B_k \to B_{k+1} \qquad B_{k+1} \to B_{k+2}$$

and additionally, if $k \ge 3$, we do $B_{k-1} \to B_k$. If $k = 2$, the initial state must be $B_0 = 1$, $B_1 = 2$ and $B_2 = 1$; after B's move it will be $B_0 = 1, B_1 = 1, B_2 = 0$. As A isn't allowed to move coin from B_0 and B_2, B_1 cannot gain any coin and therefore $B_1 = 1$ remains. Given also that $B_2 = 0$ before A's move, it can gain at most one coin from B_1 and B_3, however B_1 has no coin to be moved so $B_2 \le 1$ must hold, which then means $B_1 = B_2 = 1$ after A's move, i.e. achieving the goal of two adjacent boxes of 1 coin each.

Else, $k \ge 3$. The flow of B_1 to B_0 and $B_{k-1} \to B_k$ means that there's a net outflow of at least 2 coins among boxes $B_1, \cdots, B_{k-1}$. Since B_0 and B_k had 1 coin before B's move, A cannot move any coin from B_0 or B_k, thus maintaining the status at least a net outflow of 2 coin among $B_1, \cdots, B_{k-1}$. By the minimality of k, we have $B_1 + \cdots B_{k-1} = 2(k-1)$ before B's move, so now we have $2(k-1) - 2$ coins among $B_1, \cdots, B_{k-1}$, which means there will be an arc among $B_1, \cdots, B_{k-1}$, so we have effectively shortened the arc from $k+1$ to at most $k-1$. Continuing this algorithm yields an arc of minimal possible length, i.e. 2 (with adjacent boxes with only 1 coin each).

Step 2: now that we have two adjacent boxes, say B_0 and B_1 of 1 coin each, B wants to force three adjacent boxes of 1 coin each after some A's turn. We first note that this initial condition can be maintained: at every step of B, just move $B_0 \to B_{-1}$ and $B_1 \to B_2$. This means B_0 and B_1 have no coins and A is forced to move the coins back from B_2 to B_1 and B_{-1} to B_0, if this is even allowed.

Next, since the total number of coins is $2n-3$, there's a minimal index k such that $B_2, \cdots, B_k$ together contain fewer than $2(k-1)$ coins. If $k = 2$ we're done. Otherwise, this means that $B_2, \cdots, B_{k-1}$ contains exactly $2(k-2)$ coins and B_k contains one coin. All B needs to do now is

$$B_{k-1} \to B_k \qquad B_k \to B_{k+1}$$

We claim that regardless of how A moves, there's an index $k' < k$ such that $B_2, \cdots, B_{k'}$ contains at most $2(k'-1)-1$ coins in total. Again we consider the arc

$$B_2, \cdots, B_{k-1}$$

At B's move, B_2 receives a coin from B_1 and B_{k-1} gives a coin to B_k. This means that the net flow of coins is 0 after B's move. Now, B_1 has 0 coin so A must do $B_1 \to B_2$; B_k had 1 coin before B's turn so A cannot move coin from B_k to B_{k-1}. This results in a net outflow of at least one. This means after B's and A's move we have $2(k-2) = 2(k-1)-1$ coins among $B_2, \cdots, B_{k-1}$, as desired. Thus all B needs to do is repeat this iteration until the minimal such k becomes 2, and we have B_0, B_1, B_2 all having 1 coin exactly.

Step 3: now B can win the game with B_0, B_1, B_2 jhaving 1 coin each. Simply do

$$B_0 \to B_{-1}, B_1 \to B_2, B_2 \to B_3$$

which means B_1 is now empty. As B_0 and B_2 both have 1 coin before B's move, A cannot transfer coin from either box to B_1. Hence B_1 remains empty.

C5 The columns and the row of a $3n \times 3n$ square board are numbered $1, 2, \ldots, 3n$. Every square (x, y) with $1 \leq x, y \leq 3n$ is colored asparagus, byzantium or citrine according as the modulo 3 remainder of $x + y$ is $0, 1$ or 2 respectively. One token colored asparagus, byzantium or citrine is placed on each square, so that there are $3n^2$ tokens of each color.

Suppose that one can permute the tokens so that each token is moved to a distance of at most d from its original position, each asparagus token replaces a byzantium token, each byzantium token replaces a citrine token, and each citrine token replaces an asparagus token. Prove that it is possible to permute the tokens so that each token is moved to a distance of at most $d + 2$ from its original position, and each square contains a token with the same color as the square.

Solution. Let asparagus $= A$, byzantium $= B$, and citrine $= C$, and call a token A-token, B-token, C-token based on its colour (and similarly, A-square, B-square, C-square based on its colour). For each token, call a square u-good w.r.t. the token if the square is at most distance u away and has the same colour as the token. Then by Hall's lemma, it suffices to show that for any subset S of the $9n^2$ tokens, the number of squares that are $d + 2$-good to at least one token in S is at least $|S|$. Since a good square-token pair must have the same colour, it suffices to consider the case where S is all of the same colour.

Consider the case where S as a subset of A-tokens, with $k \triangleq |S| \leq 3n^2$. Denote S_B be the set of k B-tokens that each token in S_A can replace within d steps, and S_C the set of k C-tokens that replaces each token in S_A within d steps. Denote, now, T as $S \cup S_B \cup S_C$. Also denote $D_u(U)$ as the set of A-squares that are u-good to at least one token in U.

We first show that $|D_2(U)| \geq \frac{|U|}{3}$ for any subset U of the $9n^2$ tokens. Consider each triple of coordinates $\{(x, 3y-2), (x-3y-1), (x, 3y)\}$, where $x = 1, \cdots, 3n$ and $y = 1, \cdots, n$. We see that each such triple has exactly one A-square. Suppose $\ell \leq 3n^2$ of these triples have at least one token in U occupying a space in one of these coordinates. For each of these ℓ triples, the A-square has distance at most 2 with the token in U (since $|3y - (3y-2)| \leq 2$). Thus this A-square is in $D_2(U)$, so $|D_2(U)| \geq \ell$. Meanwhile, $|U| \leq 3\ell$ since the squares in U must be in these ℓ triples. This gives $|D_2(U)| \geq \frac{|U|}{3}$.

In particular, $|D_2(T)| \geq \frac{|T|}{3} = \frac{3k}{3} = k$. We'll now show that $D_2(T) \subseteq D_{d+2}(S)$. Indeed, for each A-square in $D_2(T)$, if it's 2-close with a token in S then it's in $D_2(S) \subseteq D_{d+2}(S)$; if it's in 2-close with a token in S_B or S_C, this token is of distance $\leq d$ with some A-token (either replaces or being replaced), and hence $d + 2$-close to that A-token. Therefore it's in $D_{d+2}(S)$. We therefore conclude that $|D_{d+2}(S)| \geq k = |S|$, as desired.

C6 (IMO 3) The liar's guessing game is a game played between two players A and B. The rules of the game depend on two positive integers k and n which are known to both players.

At the start of the game A chooses integers x and N with $1 \leq x \leq N$. Player A keeps x secret, and truthfully tells N to player B. Player B now tries to obtain information about x by asking player A questions as follows: each question consists of B specifying an arbitrary set S of positive integers (possibly one specified in some previous question), and asking A whether x belongs to S. Player B may ask as many questions as he wishes. After each question, player A must immediately answer it with yes or no, but is allowed to lie as many times as she wants; the only restriction is that, among any $k + 1$ consecutive answers, at least one answer must be truthful.

After B has asked as many questions as he wants, he must specify a set X of at most n positive integers. If x belongs to X, then B wins; otherwise, he loses. Prove that:

(a) If $n \geq 2^k$, then B can guarantee a win.

(b) For all sufficiently large k, there exists an integer $n \geq (1.99)^k$ such that B cannot guarantee a win.

Solution. The query-answer protocol is the same as B partitioning $\{1, \cdots, N\}$ into two parts and A says which set x belongs to (which we call the correct set, as opposed to wrong set) B can guarantee a win iff for all but n numbers y, A says y doesn't belong to the correct set for $k+1$ consecutive times.

This motivates the following formulation of the problem: let $a_1, \cdots, a_N$ be written on the board. Initially, all numbers are equal to 0. Thereafter, B and A play the following: B chooses a partition $\{1, \cdots, N\}$ into two parts, and A chooses one part, say U and set $a_i = 0$ for $i \in U$, while for the other part (say V) she replaces a_i by $a_i + 1$ for all $i \in V$. If $a_i = k+1$, then the number is erased from the board permanently.

The game ends when there are $\leq n$ numbers on the board, where B wins. We'll need to prove the winning conditions.

Part 1, $n = 2^k$. Let's first consider $N = n+1$, so B's goal is to remove one number from the board. We consider the following two phases (a bit lengthy compared to the official but easier to think of).

Phase 1: we show that B can maintain the invariant that at step ℓ (starting with step 0), the size of $A_\ell = \{i \in 1, \cdots, N : a_i \geq \ell\}$ is at least $2^{k-\ell}$ regardless of A's strategy. Indeed, $|A_0| = N = n+1 > 2^k$, and with A_ℓ at hand, at step $\ell+1$ for $k < \ell$, B would simply partition $\{1, \cdots, N\}$ into U and V such that the sizes $|A_\ell \cap U|$ and $|A_\ell \cap V|$ differ by no more than 1 (i.e. as evenly as possible). Then no matter how A acts, either $A_\ell \cap U$ or $A_\ell \cap V$ has all its a_i increased by 1, thereby forming part of $A_{\ell+1}$. Finally, $|A_{\ell+1}| \geq \min\{|A_\ell \cap U|, |A_\ell \cap V|\}$, but since we have already have $|A_\ell| \geq 2^{k-\ell}$, according our partition we have both $A_\ell \cap U, A_\ell \cap V$ of size $\geq 2^{k-\ell-1}$. This proves the induction. In particular, A_k is nonempty.

Phase 2: if $|A_k| \geq 2$, then B is done: simply make sure the two elements in A_k are in different partitions in the next step and one of them, say j, will be forced to become $a_j = k+1$. Otherwise, w.l.o.g. we have $A_k = \{N\}$ (so we have $a_N = k$ here). B can now partition into $\{1, \cdots, N-1\}$ and $\{N\}$. If A picks N to increase count by 1, we're done. Otherwise, after this step $a_i \geq 1$ for all $i = 1, \cdots, N-1 = n$. Thus here we have $A_1 = \{1, \cdots, n\}$.

We may repeat the protocol above: this time ensuring that at step ℓ, $|A_\ell| \geq 2^{k-\ell+1}$, noting that $|A_1| = n = 2^k$ here. Eventually, $|A_{k+1}| \geq 1$, as desired.

To generalize $N = n+1$ to arbitrary N, if $N \leq n$ there's nothing to prove. For all bigger N, so long as there are $> n$ numbers on the board, B can choose any set $n+1$ numbers to play the game with A and eliminate 1 number at one time.

Part 2. Consider any β with $1.99 < \beta < 2$, and $n = \lceil \beta^k \rceil$ Pick α such that $\beta < \alpha < 2$, and k such that $(1 - \frac{\alpha}{2})\alpha^{k+1} > \beta^k$ (this would work so long as $k > \frac{-\log(\alpha(1-\frac{\alpha}{2}))}{\log \alpha - \log \beta}$). Assuming $N > n$, A just need to predetermine $n+1$ numbers to 'protect' (say, $S = \{1, \cdots, n+1\}$). Then A's strategy will be, regardless of the partitions U and V by B, A considers the following expressions and choose the smaller one:

$$\sum_{i \in U \cap S} \alpha^{a_i} \qquad \sum_{i \in V \cap S} \alpha^{a_i}$$

First, note that we start with value of $n + 1 = \lceil \beta^k \rceil + 1 < \alpha^k$. Let's now show that the value $\sum_{i \in S} \alpha^{a_i}$ will always be less than α^{k+1} under this strategy. Indeed, suppose that

$$\sum_{i \in U \cap S} \alpha^{a_i} + \sum_{i \in V \cap S} \alpha^{a_i} = \sum_{i \in S} \alpha^{a_i} < \alpha^{k+1}$$

Then, if U contributes less compared to V, after A's move the value now becomes

$$\begin{aligned}\sum_{i\in U\cap S}\alpha^{a_i+1}+\sum_{i\in V\cap S}\alpha^0 &= \alpha\sum_{i\in U\cap S}\alpha^{a_i}+|V\cap S| \\ &\le \frac{\alpha^{k+2}}{2}+\beta^k \\ &< \frac{\alpha^{k+2}}{2}+(1-\frac{\alpha}{2})\alpha^{k+1} \\ &= \alpha^{k+1}\end{aligned}$$

as desired. In particular, at any time all a_i's are $\le k$, hence will not be erased. This means that B cannot tell which one among $\{1,\cdots,n+1\}$ is not equal to x.

Comment. Using such an analysis, when $\beta = 1.99$ the optimal α (that results in the lowest threshold k) is around 1.9987, and the required k is around 1523. Such n will then be enormously large for the game to be played in real life.

Geometry

G1 (IMO 1) Given triangle ABC the point J is the centre of the excircle opposite the vertex A. This excircle is tangent to the side BC at M, and to the lines AB and AC at K and L, respectively. The lines LM and BJ meet at F, and the lines KM and CJ meet at G. Let S be the point of intersection of the lines AF and BC, and let T be the point of intersection of the lines AG and BC. Prove that M is the midpoint of ST.

Solution. We first show that A, F, L, J lie on a circle. Now that BK and BM are both tangent to the excircle ω of ABC, we have $\angle BKJ = BMJ = 90^\circ$, and moreover $MJ = MK$, so M and K are symmetric w.r.t. BJ. This means, $BJ \perp MK$. By some angle chasing we have

$$\begin{aligned}\angle JFL &= \angle JFM \\ &= 90^\circ - \angle KMF \\ &= 90^\circ - (180^\circ - \angle KML) \\ &= 90^\circ - 180^\circ + (180^\circ - \frac{1}{2}\angle KJL) \\ &= 90^\circ - \frac{1}{2}(180^\circ - \angle KAL) \\ &= \frac{1}{2}\angle KAL \\ &= \angle LAJ\end{aligned}$$

so A, F, L, J are indeed concyclic. Since $\angle ALJ = 90^\circ$, $\angle AFJ = 90^\circ$, too, and thus $AS \perp BJ$. Combined with $MK \perp BJ$ we have $AS \parallel MK$. But then $BK = BM$ so $BA = BS$, too. This gives $MS = MB + BS = BK + BA = AK$.

Similarly, $MT = AL$. Since AK and AL are both tangents to ω, we have $AK = AL$, so $MS = MT$. Since M, S, T are all on BC, they are collinear, so M is indeed the midpoint of ST.

G2 Let $ABCD$ be a cyclic quadrilateral whose diagonals AC and BD meet at E. The extensions of the sides AD and BC beyond A and B meet at F. Let G be the point such that $ECGD$ is a parallelogram, and let H be the image of E under reflection in AD. Prove that D, H, F, G are concyclic.

Solution. Since G and H lie on the different side of DF, we are proving that $\angle DHF + \angle DGF = 180°$, which is the same as proving $\angle DEF + \angle DGF = 180°$.

There are a few ways to prove this (one of which is the trigonometric bash I submitted as my homework), but one way is to explore the similarities arising from the fact that $ABCD$ is cyclic. Now, by some angle chasing we have (note the use of equal angle at parallelograms, and the use of exterior angle $\angle EDC + \angle ECD = \angle AED$ and $\angle FDE + \angle AED = \angle FAE$)

$$\angle FDG = \angle FDE + \angle EDC + \angle CDG = \angle FDE + \angle EDC + \angle ECD$$

$$= \angle FDE + \angle AED = \angle FAE = \angle FBE$$

with the last equality following from the $ABCD$ is cyclic. In addition,

$$\begin{aligned}\frac{FD}{DG} &= \frac{FD}{CE} \\ &= \frac{FB \sin\angle FBD/\sin\angle FDB}{BE \sin\angle EBC/\sin\angle BCE} && \text{(sin rule on triangle } FBD) \\ &= \frac{FB \sin\angle EBC/\sin\angle BCE}{BE \sin\angle EBC/\sin\angle BCE} && (\angle BCE = \angle FDB) \\ &= \frac{FB}{BE}\end{aligned}$$

so together with $\angle FDG = \angle FBE$, we can conclude that triangles FDG and FBE are similar. In particular, $\angle DGF = \angle BEF$. But since B, E, D are on a straight line in that order, we have $\angle BEF + \angle FED = 180°$, and therefore $\angle DGF + \angle FED = 180°$.

G3 In an acute triangle ABC the points D, E and F are the feet of the altitudes through A, B and C respectively. The incenters of the triangles AEF and BDF are I_1 and I_2 respectively; the circumcenters of the triangles ACI_1 and BCI_2 are O_1 and O_2 respectively. Prove that I_1I_2 and O_1O_2 are parallel.

Solution. There are two things we need to prove:

- Let I be the incenter of triangle ABC. Then $CI \perp I_1I_2$.
- CI is also the radical axis of the circumcircles of ACI_1 and BCI_2.

Once we establish the two, it will follow that $CI \perp O_1O_2$, and therefore with $CO \perp I_1I_2$ we have $O_1O_2 \parallel I_1I_2$.

We will in fact show an overarching claim: ABI_2I_1 is cyclic. We have learned so many times that $DFCB$ is cyclic because $\angle CFB = \angle CDB = 90°$, therefore $\angle ADF = \angle ACB$, meaning that triangles ADF and ACB are similar. Moreover, their similitude is $\frac{AF}{AB} = \cos\angle CAB$. Thus, $\frac{AI_1}{AI} = \cos\angle CAB$, too. But then I and I_1 both lie on the internal angle bisector of $\angle CAB$, so we have

$$II_1 = IA - I_1A = IA(1 - \cos\angle CAB) = IA(2\sin^2\frac{\angle CAB}{2}) = 2IA\sin^2\angle IAB$$

(notice the use of double angle formula: $\cos 2x = 1 - 2\sin^2 x$) and similarly $II_2 = 2IB\sin^2\angle IBA$. Thus we now have

$$\frac{II_1 \cdot IA}{II_2 \cdot IB} = \frac{2IA\sin^2\angle IAB \cdot \angle IA}{2IB\sin^2\angle IBA \cdot IB} = \frac{IA^2}{IB^2} \cdot \frac{\sin^2\angle IAB}{\sin^2\angle IBA} = \frac{\sin^2\angle IBA}{\sin^2\angle IAB} \cdot \frac{\sin^2\angle IAB}{\sin^2\angle IBA} = 1$$

(notice the use of sine rule on triangle IAB in the second last equality). Thus $II_1 \cdot IA = II_2 \cdot IB$, and so by power of point theorem I_1ABI_2 is cyclic. Moreover, the power of point from I to the circumcircle of ACI_1 and BCI_2 are $II_1 \cdot IA$ and $II_2 \cdot IB$, respectively. Since these two are equal, I has equal power from the two circles, and hence lie on the radical axis of the two circles. Since C lies on both the circles, CI is the radical axis of these two circles. Finally, if G is the intersection from CI to I_1I_2 then (the second equality is the exterior angle)

$$\angle I_1IG+\angle II_1G=(\angle ICA+\angle IAC)+\angle IBA=\frac{\angle BCA+\angle BAC+\angle CBA}{2}=\frac{180^\circ}{2}=90^\circ$$

which shows that CI and I_1I_2 are indeed perpendicular.

G4 Let ABC be a triangle with $AB \neq AC$ and circumcenter O. The bisector of $\angle BAC$ intersects BC at D. Let E be the reflection of D with respect to the midpoint of BC. The lines through D and E perpendicular to BC intersect the lines AO and AD at X and Y respectively. Prove that the quadrilateral $BXCY$ is cyclic.

Solution. W.L.O.G. assume $AB < AC$. We first notice that, if M is the second intersection of the angle bisector AD of $\angle BAC$ and the circumcircle of ABC, then $BM = MC$, and therefore the perpendicular from M to BC (say, M_1) will be the midpoint of BC. Since $DM_1 = M_1E$, we also have $DM = MY$.

We now show that $AD\cdot DM = XD\cdot EY$. Now, $EY = DY\cos\angle DYE = 2DM\cos\angle DYE$. Moreover, we can use the well-known fact that the perpendicular from A to BC and AO are the isogonal conjugate (i.e. the reflection in AD) and since $DX \perp BC$, we have $\angle XAD = \angle XDA$. Since $XD \perp EY$, too, $\angle XDA = \angle EYD$. This also means $DX = XA$, and that $AD = 2DX\cos\angle EYD$, and thus $DX = \frac{AD}{2\cos\angle EYD}$. Therefore we have

$$XD\cdot EY=\frac{AD}{2\cos\angle EYD}\cdot 2DM\cos\angle DYE=AD\cdot DM$$

but by the power of point theorem (since $ABMC$ is cyclic) we have $AD\cdot DM = BD\cdot DC$. It follows that $XD\cdot EY = BD\cdot DC$ too.

Now reflect Y in the perpendicular bisector of BC to get Y' and we have $XD\cdot DY' = BD\cdot DC$ since X, D, Y' would be collinear. It follows that $BXCY'$ is cyclic. But then $BCYY'$ is also cyclic (isoceles trapezoid), so the conclusion follows.

G5 (IMO 5) Let ABC be a triangle with $\angle BCA = 90^\circ$, and let D be the foot of the altitude from C. Let X be a point in the interior of the segment CD. Let K be the point on the segment AX such that $BK = BC$. Similarly, let L be the point on the segment BX such that $AL = AC$. Let M be the point of intersection of AL and BK.

Solution. Let Y to be the orthocenter of triangle AXB. Since YX is perpendicular to AB, Y, X, C, D are collinear. Now, consider the circle ω_A centered at A with radius AC, and circle ω_B centered at B with radius BC. We now consider the pole P' of BX with respect to ω_A. This pole P' lies on the polar of B. Since $\angle BCA = 90^\circ$, BC is tangent to ω_A and since CD is perpendicular to AB, CD is indeed to polar of B and P' is on CD. Moreover, by the definition of pole, P' also lies on perpendicular line from A to BX. Thus $P'A \perp BX$ and $P'X \perp AB$, showing that P' is the orthocenter of AXB. Thus $P' = Y$, too, i.e. Y is the pole of BX w.r.t. ω_A. Similarly Y is also the pole of AX w.r.t. ω_B. But since L is on both BX and ω_A, YL is tangent to ω_A, and similarly YK is tangent to ω_B. But since Y is on CD, the radical axis of ω_A and ω_B, we have $YK = YL$. Finally, $MK^2 = YM^2 - YK^2 = YM^2 - YL^2 = ML^2$ so $MK = ML$ (we use the fact that $\angle YKM = \angle YLM = 90^\circ$).

G6 Let ABC be a triangle with circumcenter O and incenter I. The points D, E and F on the sides BC, CA and AB respectively are such that $BD + BF = CA$ and $CD + CE = AB$. The circumcircles of the triangles BFD and CDE intersect at $P \neq D$. Prove that $OP = OI$.

Solution. (Modified from the solution I submitted to my homework for the IMO 2013 training camp). Let M_A, M_B, M_C be the midpoints of sides BC, CA, AB, respectively, and let D', E', F' be the reflections of D, E, F in M_A, M_B, M_C, respectively. We first show that the circumcircles of $AE'F', BF'D'$ and $CD'E'$ intersect at I.

By Miquel's theorem, they do have a common point. We first show that I lies on the circumcircle of $AE'F'$; the other two facts would be similar. From the length relation above, we have $AD + AE = BC$, so $AD' + AE' = (AB + AC) - BC$ by the definition of "reflection in the midpoint". If T_A, T_B, T_C denotes the tangency points of the incircle of ABC with the sides BC, CA, AB, then we also have $ATB + AT_C = (AB + AC) - BC$ (exercise :P). Therefore, $T_BE' = T_CF'$, and moreover E' lies on the segment AT_B if and only if F' lies on the segment T_CB (refer this as the "side manipulation" later). From the fact that $IT_B = IT_C$ and $\angle IT_BA = \angle IT_CA$ we can then conclude that $\angle IE'T_B = \angle IF'T_C$ since the triangle $IE'T_B$ and $IF'T_C$ would be similar. By the "side manipulation" fact, however, we get $\angle AF'I$ and $\angle AE'I$ supplementary, so the lemma follows.

Now to prove the main problem, we shall make a bolder claim as follows. By the definition of reflection again, reflecting any line passing through D' in the perpendicular bisector of BC will produce a line passing through D (infer similarly for the other two). Now reflect the lines $D'I, E'I, F'I$ in the perpendicular bisectors of BC, CA, AB, respectively to get lines ℓ_A, ℓ_B, ℓ_C passing through D, E, F. We will prove that these three lines intersect at I.

To show this, from before we have (using oriented angles from now on) $\angle(IT_C, IT_B) = \angle(AB, AC) = \angle(F'I, E'I)$ by the cyclicity of $AE'IF'$ and AT_BIT_C, so by doing some appropriate substraction we have $\angle(F'I, I_TC) = \angle(E'I, IT_B) = \angle(D'I, IT_A)$ (we extend the claim to something analogous). By the definition of reflection, $\angle(F'I, IT_C), \angle(E'I, IT_B), \angle(D'I, IT_A)$ are each equal to $\angle(IT_C, \ell_C), \angle(IT_B, \ell_B), \angle(IT_A, \ell_A)$, which are in turn equal to $\angle(OM_C, \ell_C), \angle(OM_B, \ell_B), \angle(OM_A, \ell_A)$ since OM_A and IT_A are both perpendicular to BC (similarly to the other two). These angle must all be the same, as it turns out.

Now assume, for a moment, that the lines ID' and OM_A intersect at K_A, then K_A is on ℓ_A, too. Define ℓ_B and ℓ_C similarly. By the angle condition above, K_A, K_B, K_C could simultaneously be the point of infinity; in this case it's not hard to show that P is the reflection of I in O, hence $OP = OI$ must hold here. We would therefore now assume that this is not the case, so K_A, K_B, K_C are all points in the non-projective plane. Now we have the following refined equality:

$$\angle(F'I, IT_C) = \angle(IK_C, K_CM_C) = \angle(IK_C, K_CO) = \angle(E'I, IT_B) = \angle(IK_B, K_BM_B) = \angle(IK_B, K_BO)$$

where we used the fact that the perpendicular bisectors of the sides concur at O. We therefore have K_B, K_C, I, O concyclic, and similarly K_A would be on this circle too. If P' is another point on this circle with $OP' = OI$ then it's not hard to see that P' is on the three lines ℓ_A, ℓ_B, ℓ_C, and moreover P' is on the circles AEF, BDF, CDE. It follows that $P' = P$ and therefore $OI = OP$. Q.E.D.

G7 Let $ABCD$ be a convex quadrilateral with non-parallel sides BC and AD. Assume that there is a point E on the side BC such that the quadrilaterals $ABED$ and $AECD$ are circumscribed. Prove that there is a point F on the side AD such that the quadrilaterals $ABCF$ and $BCDF$ are circumscribed if and only if AB is parallel to CD.

Solution. Let BC and AD meet at P, and w.l.o.g. we let P be on rays CB and DA beyond B and A, respectively. Then the incircles of $ABED$ and $ACED$ are the excircle of triangle PBA (opposite P) and incircle of triangle PCD, respectively. Let the centers be I_1 and I_2, respectively.

We'll generalize the problem a bit: let P, A, B, C, D, I_1, I_2 as defined, and let E_1 and E_2 on line BC be such that ABE_1D and AE_2CD are circumscribed (that is, let the tangent from D to the first circle that's not AD to meet BC at E_1), and F_1 and F_2 on line AD be such that $BCDF_2$ and $ABCF_1$ are circumscribed. Then $\frac{PE_1}{PE_2} = \frac{PF_1}{PF_2}$ if and only if $AB \parallel CD$. Thus the problem is a special case where $\frac{PE_1}{PE_2} = 1$.

Suppose, first, that $AB \parallel CD$. We'll claim that $AE_2 \parallel CF_1$ and similarly $BF_2 \parallel DE_1$. Notice that:

$$\angle PBI_1 = 180^\circ - \angle CBI_1 = 180^\circ - \frac{\angle CBA}{2} = 90^\circ + \frac{\angle PBA}{2}$$

and

$$\angle PI_2D = 180^\circ - \angle I_2PD - \angle PDI_2 = 180^\circ - \frac{\angle CPD}{2} - \angle\frac{PDC}{2} = 90^\circ + \frac{\angle PCD}{2} = 90^\circ + \frac{\angle PBA}{2}$$

so these two angles are essentially equal. Combined with $\angle BPI_1 = \angle DPI_2$ we have triangles PBI_1 and PI_2D similar. This gives:

$$\frac{PB}{PI_2} = \frac{PB}{PI_1} \cdot \frac{PI_1}{PI_2} = \frac{PI_2}{PD} \cdot \frac{PI_1}{PI_2} = \frac{PI_1}{PD}$$

and therefore PBI_2 and PI_1D are also similar. Finally,

$$\angle PBF_2 = 180^\circ - 2\angle CBI_2 = 2\angle PBI_2 - 180^\circ \qquad \angle PDE_1 = 2\angle PDI_1$$

and therefore

$$\angle PBF_2 + \angle PDE_1 = 2\angle PBI_2 + 2\angle PDI_1 - 180^\circ = 2(180^\circ - \angle BPI_2) - 180^\circ = 180^\circ - \angle BP_A$$

which does show that BF_2 and DE_1 are parallel. Similarly, BF_2 and DE_1 are parallel. Therefore:

$$\frac{PE_2}{PE_1} = \frac{PE_2}{PC}\frac{PC}{PD}\frac{PD}{PE_1} = \frac{PA}{PF_1}\frac{PB}{PA}\frac{PF_2}{PB} = \frac{PF_2}{PF_1}$$

as desired.

Now consider the case where AB and CD are not parallel. Fixing the circles with centers I_1 and I_2, consider D' on AD and C' on BC such that $C'D' \parallel AB$ and PCD and $PC'D'$ share the same incircles. Let E_0 and F_0 on BC and AD, respectively, such that ABE_0D' and BAF_0C' are circumscribed. Then $\frac{PE_2}{PE_0} = \frac{PF_2}{PF_0}$ as per above. According to our arrangement, since PCD and $PC'D'$ share the same circle, if $PC < PC'$, then $PF_0 < PF_1$, $PD' < PD$ and $PE_1 < PE_0$ and so

$$\frac{PE_2}{PE_1} > \frac{PE_2}{PE_0} = \frac{PF_2}{PF_0} > \frac{PF_2}{PF_1}$$

so the desired equality no longer holds. The opposite inequality will hold if $PC' < PC$. This proves the other direction of the inequality.

G8 Let ABC be a triangle with circumcircle ω and ℓ a line without common points with ω. Denote by P the foot of the perpendicular from the center of ω to ℓ. The side-lines BC, CA, AB intersect ℓ at the points X, Y, Z different from P. Prove that the circumcircles of the triangles AXP, BYP and CZP have a common point different from P or are mutually tangent at P.

Solution. Let AD, BE, CF be the radical axis of ω and circles AXP, BYP and CZP, respectively, with D, E, F on ℓ. Since P does not lie on ω, each of D, E, F must be distinct from P. We show that these three lines concur: if Q is the common intersection point, then it will be on the radical center of the three circles AXP, BYP, CZP. Then both P and Q are on the radical center, showing that these three circles are indeed coaxial.

To start with, for each point Q denote by $f(Q) = OQ^2 - r^2$ the power of point of point Q with respect to ω, with O being the center of ω and r its radius. If Q is on ℓ, we also have $f(Q) = OQ^2 - r^2 = PQ^2 + PO^2 - r^2 = PQ^2 + f(P)$. Now consider point D, with $f(D) = PD^2 + f(P)$. Since it's on the radical axis of ω and AXP, we have $f(D) = DP \cdot DX$. Since $f(D) = PD^2 + f(P) > PD^2$ (because $f(P) > 0$: P is outside ω), we have $DA > DP$ and we can write $DX = DP + PX$ (i.e. P lies between D and X). Thus $PD^2 + f(P) = DP \cdot (DP + PX) = DP^2 + DP \cdot PX$, and therefore $f(P) = DP \cdot PX$. Similarly we have

$$f(P) = DP \cdot PX = EP \cdot PY = FP \cdot PZ(*)$$

with P lying between E and Y, between F and Z, too.

Now we can proceed by the trigonometric version of Ceva's version. But we somehow need to be careful about the sign convention here. We'll have these in mind:

- To prove concurrency of AD, BE, CF we will need (considering sign conventions)

$$\frac{\sin \angle BAD}{\sin \angle CAD} \cdot \frac{\sin \angle ACF}{\sin \angle BCF} \cdot \frac{\sin \angle CBE}{\sin \angle ABE} = 1$$

- Considering the triangle ZAY with cevian AD:

$$\frac{AZ}{AY} \cdot \frac{\sin \angle BAD}{\sin \angle CAD} \sigma(A) = \frac{ZD}{DY}$$

  with $\sigma(A)$ being 1 if the angle domain $\angle BAC$ is the same (or opposite) as the angle domain $\angle YAZ$ and -1 they are adjacent, and similarly

$$\frac{CY}{CX} \cdot \frac{\sin \angle ACF}{\sin \angle BCF} \sigma(C) = \frac{YF}{FX} \qquad \frac{BX}{BZ} \cdot \frac{\sin \angle CBE}{\sin \angle ABE} \sigma(B) = \frac{XE}{EZ}$$

- Above, we have AZ, AY, CY, CZ, BX, BZ all unsigned (positive) but fraction $\frac{ZD}{DY}$ is positive iff D lies between Z and Y and negative otherwise (i.e. follow the normal rule of signed convention). Also, by sine rule on triangle AYZ we have $\frac{AZ}{AY} = \frac{\sin \angle AYZ}{\sin \angle AZY}$ and similarly $\frac{BX}{BZ} = \frac{\sin \angle BZX}{\sin \angle BXZ}$ and $\frac{CY}{CX} = \frac{\sin \angle CXY}{\sin \angle CYX}$. But since B, C, X are collinear, we have $\angle CXY$ and $\angle BXZ$ either equal or complementary (depending on the sides of ℓ where Y and Z lie on). In either case $\sin \angle CXY = \sin \angle BXZ$. Similarly, $\sin \angle CYX = \sin \angle AYZ$ and $\sin \angle AZY = \sin \angle BZX$. This gives

$$\frac{AZ}{AY} \cdot \frac{BX}{BZ} \cdot \frac{CY}{CX} = \frac{\sin \angle AYZ}{\sin \angle AZY} \cdot \frac{\sin \angle BZX}{\sin \angle BXZ} \cdot \frac{\sin \angle CXY}{\sin \angle CYX} = 1$$

Thus it all reduces to proving that

$$\sigma(A)\sigma(B)\sigma(C) = \frac{XE}{EZ} \cdot \frac{YF}{FX} \cdot \frac{ZD}{DY}$$

We first determine the ratio of right hand side in terms of linear coordinates (as they all lie on ℓ). W.L.O.G, too, let P to have coordinate 0, and let the coordinates of X, Y, Z to be x, y, z. Then by the property (*), we have the coordinates d, e, f of D, E, F as

$$-\frac{f(P)}{x} \qquad -\frac{f(P)}{y} \qquad -\frac{f(P)}{z}$$

respectively. We also know that the sign convention of length ratio goes as, $\frac{XE}{EZ}$ is positive if and only if E lies on the segment XZ. So the ratio now becomes

$$\frac{XE}{EZ} \cdot \frac{YF}{FX} \cdot \frac{ZD}{DY} = \frac{e-x}{z-e} \cdot \frac{f-y}{x-f} \cdot \frac{d-z}{y-d} = \frac{-\frac{f(P)}{y} - x}{z + \frac{f(P)}{y}} \cdot \frac{-\frac{f(P)}{z} - y}{x + \frac{f(P)}{z}} \cdot \frac{-\frac{f(P)}{x} - z}{y + \frac{f(P)}{x}} = -1$$

To play around with the values $\sigma(A), \sigma(B), \sigma(C)$, however, we need to determine them with respect to the positions of X, Y, Z (e.g. where X is at ray BC beyond C or ray CB beyond B). From Menelaus' theorem applied to ℓ and triangle ABC we have, in unsigned terms,

$$\frac{|ZA|}{|ZB|} \cdot \frac{|YC|}{|YA|} \cdot \frac{|XB|}{|XC|} = 1$$

We say a ratio is big if it's > 1 and small if it's -1. Two big or two small ratios are in the same category, and a big ratio is in a different category than a small one.

We have $\dfrac{|ZA|}{|ZB|} > 1$ iff Z on ray AB beyond B and < 1 iff on ray BA beyond A. Now, $\sigma(A)$ depends on the positions of Y and Z: angle domain $\angle YAZ$ on the angle domain $\angle BAC$ iff Y and Z are both "far away" from A (Y on ray AC beyond C, Z on ray AB beyond B), and therefore $\dfrac{|ZA|}{|ZB|} > 1$ and $\dfrac{|YC|}{|YA|} < 1$. Similarly, we can deduce that these two angle domains are opposite of each other if $\dfrac{|ZA|}{|ZB|} < 1$ and $\dfrac{|YC|}{|YA|} > 1$ and adjacent to each other iff the ratios are both > 1 or < 1. Therefore, $\sigma(A) = -1$ iff the corredponsing ratios are in the same category, and 1 iff different. Similar for the other two. Since the three ratios have product 1, we must have one big two small, or two big one small. Either way, from the three pairs of ratios, two of them are of the different category and the other pair same (i.e. for (big, big, small) we have two (big, small) pair and one (big, big) pair). Thus one of $\sigma(A), \sigma(B), \sigma(C)$ is -1 and the other two 1, and $\sigma(A)\sigma(B)\sigma(C) = -1$.

Remark: I gave a solution involving inverting around P to a math olympiad tutoring class. The solution turned out to be essentially the same, but that way it's more natural to see how should the ratios be manipulated.

Number Theory

N1 Call admissible a set A of integers that has the following property: If $x, y \in A$ (possibly $x = y$) then $x^2 + kxy + y^2 \in A$ for every integer k. Determine all pairs m, n of nonzero integers such that the only admissible set containing both m and n is the set of all integers.

Answer. All (m, n) satisfying $\gcd(m, n) = 1$.
Solution. First, let $d = \gcd(m, n)$. The set $d\mathbb{Z} = \{dn : n \in \mathbb{Z}\}$ contains m and n, and is admissible since $d \mid x$ and $d \mid y$ implies that for all $k \in \mathbb{Z}$ we have x^2, kxy, y^2 are all divisible by d, so $d \mid x^2 + kxy + y^2$. So we need $d = 1$ for $d\mathbb{Z} = \mathbb{Z}$.

On the other hand, suppose $\gcd(m, n) = 1$. Letting $x = y = m$ we have $m^2 + km^2 + m^2 = (k+2)m^2 \in A$, so $m^2\mathbb{Z} \subseteq A$, and similarly $n^2\mathbb{Z} \subseteq A$. Since $\gcd(m^2, n^2) = 1$ too, we can find a and b such that $am^2 + bn^2 = 1$, by Euclidean theorem. Also am^2, bn^2 both $\in A$. Now let $x = am^2$ and $y = bn^2$ and $k = 2$ we have $(x+y)^2 = x^2 + 2xy + y^2 \in A$ but since $x + y = 1$ we have $1 \in A$. Finally, letting $x = y = 1$ we have $1 + k + 1 = k + 2 \in A$ for every integer k, so $A = \mathbb{Z}$.

N2 Find all triples (x, y, z) of positive integers such that $x \le y \le z$ and

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

Answer. The only such triple is $(2, 251, 252)$.
Solution. The left hand side is divisible by x while the right hand side is congruent to $2012(2) = 4024$ modulo x. We therefore have $x \mid 4024 = 503 \times 2^3$, with 503 being a prime. Next, we show that x cannot be divisible by 4. Suppose it is, then the left-hand-side is divisible by $4^3 = 64$, and $4 \mid x$ implies $503 \times 2^3 \times 2^2 = 2012(4) \mid 2012xyz$ so $2012xyz$ is

divisible by $2^5 = 32$. It then follows that 4024 is divisible by 32 (since $32 \mid 64$) too, which is a contradiction. Finally, we show that x cannot be greater than $\sqrt[3]{2012}$. For all $x \geq 2$ we have $xyz + 2 \leq z^3 + 2 < z^3 + y^3$ since $x \leq y \leq z$, so either $x = 1$ or $x^3 < 2012$, as claimed. Thus the maximal possible x is 11, but since it also has to be a divisor of 8×503 and cannot be divisible by 4, we have either $x = 1$ or $x = 2$.

If $x = 1$, we essentially have $y^3 + z^3 = 2012(yz + 2)$, and notice that $y^3 + z^3$ is divisible by 2012. Since 503 is a prime that's $\equiv 2 \pmod 3$, we have $y^3 \equiv z^3 \pmod{503} \to y \equiv z \pmod{503}$, so here $y^3 \equiv (-z)^3 \to y \equiv -z$, meaning $503 \mid y + z$. In addition, $y^3 + z^3$ is even, so $y + z$ must also be even (y and z must be of the same parity). It then follows that $y + z$ is divisible by 1006. Let $y + z = 1006k$, and $y^3 + z^3 = (y + z)(y^2 - yz + z^2) = 1006k(y^2 - y(1006k - y) + (1006k - y)^2)$ while $2012(yz + 2) = 2012(y(1006k - y) + 2)$. This gives $k(y^2 - y(1006k - y) + (1006k - y)^2) = 2(y(1006k - y) + 2)$.

- If $k = 1$, we have $(y^2 - y(1006 - y) + (1006 - y)^2) = 2(y(1006 - y) + 2)$, i.e. $3y^2 - 3018y + 1006^2 = -2y^2 + 2012y + 4$, i.e. $5y^2 - 5030y + (1006^2 - 4) = 0$. This reduces to a quadratic equation in y with discriminant $5030^2 - 4(5)(1006^2 - 4) = 5 \times 1006^2 + 80 = 4(5)(503^2 + 4)$. We see that $503^2 + 4 \equiv 4 + 4 \equiv 3$ modulo 5, so this discriminant is divisible by 5 but not 5^2, and thus not a perfect square. It follows that this quadratic equation has no integer solution.
- If $k = 2$ we have $y^2 - y(2012 - y) + (2012 - y)^2 = y(2012 - y) + 2$, so $3y^2 - 3(2012)y + 2012^2 = 2012y - y^2 + 2$, i.e. $4y^2 - 4(2012)y + (2012^2 - 2) = 0$. Again we treat it as a quadratic equation with discriminant $4^2(2012^2) - 4(2012^2 - 2) = 4(4(2012^2) - (2012^2 - 2))$. Since $4 \mid 2012$, we see the term $4(2012^2) - (2012^2 - 2)$ is divisible by 2 but not 4, hence cannot be a perfect square. This also means that $4(4(2012^2) - (2012^2 - 2)) = 2^2(4(2012^2) - (2012^2 - 2))$ cannot be a perfect square, showing that once again this qudratic equation cannot have solution.
- Let's see what happens as $k \geq 3$. We have $y + z = 1006k$ and therefore by the power-mean inequality, $y^3 + z^3 \geq 2(\frac{y+z}{2})^3 = \frac{(1006k)^3}{4} = 2 \times 503^3 \times k^3$. On the other hand, on the right hand side we have $2012(yz + 2) \leq 2012(\frac{(y+z)^2}{4} + 2) = 2012(\frac{(1006k)^2}{4} + 2) = 2012(503^2k^2 + 2)$. Combining these two inequalities give

  $$2 \times 503^3 \times k^3 \leq 2012(503^2k^2 + 2) \overset{\div 1006}{\to} 503^2 \times k^3 \leq 2(503^2k^2 + 2)$$

  This means, $503^2k^2(k - 2) \leq 4$, and we see that this inequality fails when $k \geq 3$, so no solution for $k \geq 3$.

We now proceed to the second case: $x = 2$, i.e. $8(y^3 + z^3) = 2012(2yz + 2)$, or $y^3 + z^3 = 503(yz + 1)$. By the same logic as above, we need $503 \mid y + z$. If $y + z = 503k$ then by the power-mean inequality (again) we have $y^3 + z^3 \geq \frac{503^3k^3}{4}$ and $503(yz + 1) \leq 503(\frac{503^2k^2}{4} + 1)$, so

$$\frac{503^3k^3}{4} \leq 503(\frac{503^2k^2}{4} + 1) \overset{\times 4 \div 503}{\to} 503^2k^3 \leq 503^2k^2 + 4$$

which implies $503^2k^2(k - 1) \leq 4$, as well. Again from here we can see $k \leq 1$ so we only need to care about this case. Knowing this, we have $x + y = 503$ and therefore $y^2 - yz + z^2 = yz + 1$ becomes $(y - z)^2 = 1$. Since $z \geq y$, we have $z - y = 1$ and $z + y = 503$. This implies $y = 251$ and $z = 252$. We can check that this triple $(x, y, z) = (2, 251, 252)$ fulfills the problem condition, and is thus the only triple of our interest.

N3 Determine all integers $m \geq 2$ such that every n with $\frac{m}{3} \leq n \leq \frac{m}{2}$ divides the binomial coefficient $\binom{n}{m-2n}$.

Answer. All m's that are prime.

Solution. We use the following formula to calculate the highest power of a prime p

dividing $n!$:

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

and notice that $\binom{n}{m-2n} = \frac{n!}{(m-2n)!(3n-m)!}$.

We first see what happens when m is prime. Then for all n within the stipulated condition we have $n < m$ and so $\gcd(n, m) = 1$. Choose any n arbitrary, subject to the inequality constraint. Let p to be any prime dividing n and let $k_0 = v_p(n)$. We now have

$$v_p\left(\frac{n!}{(m-2n)!(3n-m)!}\right) = v_p(n!) - v_p((m-2n)!) - v_p((3n-m)!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m-2n}{p^k} \right\rfloor - \left\lfloor \frac{3n-m}{p^k} \right\rfloor$$

We first notice that for each k, $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m-2n}{p^k} \right\rfloor - \left\lfloor \frac{3n-m}{p^k} \right\rfloor \geq 0$ since $\lfloor a+b \rfloor \geq \lfloor a \rfloor + \lfloor b \rfloor$ for all real numbers a and b. It now remains to show that for all $k \leq k_0$ we have $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m-2n}{p^k} \right\rfloor - \left\lfloor \frac{3n-m}{p^k} \right\rfloor \geq 1$. Since $p^{k_0} \mid v_p(n)$, $\frac{n}{p^k}$ is an integer and therefore $\left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n}{p^k}$. However, as $\gcd(n, m) = 1$, m is not divisible by p and so neither is $m - 2n$ nor $3n - m$. We therefore have $\left\lfloor \frac{m-2n}{p^k} \right\rfloor < \frac{m-2n}{p^k}$ and $\left\lfloor \frac{3n-m}{p^k} \right\rfloor < \frac{3n-m}{p^k}$. Therefore,

$$\begin{aligned}
\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m-2n}{p^k} \right\rfloor - \left\lfloor \frac{3n-m}{p^k} \right\rfloor &= \frac{n}{p^k} - \left\lfloor \frac{m-2n}{p^k} \right\rfloor - \left\lfloor \frac{3n-m}{p^k} \right\rfloor \\
&> \frac{n}{p^k} - \frac{m-2n}{p^k} - \frac{3n-m}{p^k} \\
&> 0
\end{aligned}$$

and since the floor functions are integers, so is the differences and sums among them. Therefore $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m-2n}{p^k} \right\rfloor - \left\lfloor \frac{3n-m}{p^k} \right\rfloor \geq 1$ for all $k \leq k_0$, establishing the claim. Therefore this identity holds when m is prime.

Next, let's see what happens if m is composite. If m is divisible by 2, choosing $n = \frac{m}{2}$ gives $\binom{n}{m-2n} = \binom{n}{0} = 1$ so we have $n \nmid 1$. If m is divisible by 3, choosing $m = \frac{m}{3}$ gives $\binom{n}{m-2n} = \binom{n}{n} = 1$ so we have $n \nmid 1$, too. We can therefore assume that the smallest prime dividing m is at least 5.

Having this in mind, let m composite and p any prime divisor. Let $m = pq$ and since m is divisible by neither 2 nor 3, $q \geq 5$. Consider, now, plugging $n = p\left(\frac{q-1}{2}\right)$. Then given $p \mid n$, we have $p \mid \binom{n}{m-2n} = \binom{p\left(\frac{q-1}{2}\right)}{p}$. By Lucas' theorem, this is the same as $\binom{\left(\frac{q-1}{2}\right)}{1} = \frac{q-1}{2}$ modulo p. We therefore need $p \mid q-1$. Assuming this, and given p and q both odd, we have $q \geq 2p+1 \geq 2(5)+1 = 11$. This means, $\frac{q-3}{2} > \frac{q}{3}$ (equality holds when $q = 9$ here), so we can now consider $n = p\left(\frac{q-3}{2}\right)$, giving rise to $p \mid \binom{n}{m-2n} = \binom{p\left(\frac{q-3}{2}\right)}{3p}$. Since $3 \nmid p$, by Lucas' theorem again this is congruent to $\binom{\left(\frac{q-3}{2}\right)}{3}$ modulo p. But then

$$\binom{\left(\frac{q-3}{2}\right)}{3} = \frac{(q-3)(q-5)(q-7)}{2^3 \cdot 3!}$$

so one of $q-3, q-5, q-7$ must be divisible by p. With $q \equiv 1 \pmod p$ as assumed, this is the same as saying that either 2, 4, 6 must be divisible by p contradicting that p is a prime greater than 3.

N4 An integer a is called friendly if the equation $(m^2+n)(n^2+m) = a(m-n)^3$ has a solution over the positive integers.
a) Prove that there are at least 500 friendly integers in the set $\{1, 2, \ldots, 2012\}$.
b) Decide whether $a = 2$ is friendly.

Solution. (a) Plugging $m = 2k-1$ and $n = k-1$ gives $a = 4k-3$ which works for all $k \geq 2$ so we have $5, 9, 13, \cdots, 2009$ all friendly, i.e. a total of 502 of them here.

Nb. if you ask "what's the motivation behind?" then all I can tell is, set $m-n = k$ and we want the left hand size to be divisible by k^3. We need, now, $k \mid n+2+n+k$ so $n \equiv 0, -1 \pmod k$. But then $n \equiv -1$ has the bonus of making it divisible by k^2, and turned out, $k \mid m^2+n$ in this case too.

(b) The answer is no. Like above, write $m = n+k$ and we need to solve $((n+k)^2 + n)(n^2+n+k) = 2k^3$. Writing in cubic equation in k, this gives

$$k^3 - n(n+3)k^2 - n(n+1)(2n+1)k - n^2(n+1)^2 = 0$$

and we need to find $n > 0$ such that the equation has an integer root in k. From $k^3 - n(n+3)k^2 > 0$ we have $k > n(n+3)$ (since k and n are both positive).

On the other hand the polynomial $P(k) = k^3 - n(n+3)k^2 - n(n+1)(2n+1)k - n^2(n+1)^2$ has derivative $P'(k) = 3k^2 - 2n(n+3)k - n(n+1)(2n+1)$. Note that P' has minimum point at $k = \frac{n(n+3)}{3}$ and for $k \geq n(n+3)$,

$$P'(k) \geq P'(n(n+3)) = 3n^2(n+3)^2 - 2n^2(n+3)^2 - n(n+1)(2n+1) = n(n^3+4n^2+6n-1) > 0$$

so P is increasing at $k \geq n(n+3)$. We also have

$$P(n(n+5)) = 6n^4 + 32n^3 - 6n^2 = 2n^2(3n^2+16n-3) > 0$$

so P is positive for $k \geq n(n+5)$. This means all positive roots k must be between $n(n+3)$ and $n(n+5)$.

Setting $b = k - n(n+3)$ we have the equation becomes $bk^2 - n(n+1)(2n+1)k - n^2(n+1)^2 = 0$. Now this becomes quadratic in k with discriminant

$$n^2(n+1)^2(2n+1)^2 + 4bn^2(n+1)^2 = n^2(n+1)^2((2n+1)^2 + 4b)$$

so $(2n+1)^2 + 4b$ must be an integer. We already had $b > 0$ and the next square with same parity as $(2n+1)^2$ is $(2n+3)^2$. This means

$$4b \geq (2n+3)^2 - (2n+1)^2 = 2(4n+4) = 8(n+1)$$

so $b \geq 2(n+1)$. This means $k \geq n(n+3) + 2(n+1) > n(n+5)$, which is another contradiction.

N5 For a nonnegative integer n define $\operatorname{rad}(n) = 1$ if $n = 0$ or $n = 1$, and $\operatorname{rad}(n) = p_1 p_2 \cdots p_k$ where $p_1 < p_2 < \cdots < p_k$ are all prime factors of n. Find all polynomials $f(x)$ with nonnegative integer coefficients such that $\operatorname{rad}(f(n))$ divides $\operatorname{rad}(f(n^{\operatorname{rad}(n)}))$ for every nonnegative integer n.

Answer. All polynomials in terms of $f(n) := cn^k$ for any $c, k \in \mathbb{N}_0$.
Solution. If f has a positive coefficient a_k at x^k (meaning that f is nonzero), then $f(n) \geq a_k n^k > 0$ for all $n > 0$. Hence, for all $n > 0$ this essentially means that for any prime p, $p \mid f(n) \to p \mid f(n^{\operatorname{rad}(n)})$.

We first see what happens when $p \nmid n$ but $p \mid f(n)$ for some n. Here' an important identity on polynomials with integer coefficient that I would like to quote:

$$m - n \mid f(m) - f(n), \forall m, n \in \mathbb{Z} \cdots (*)$$

Having this in mind, let $p - 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime decomposition of $p - 1 = \phi(p)$. We are to create a sequence of numbers $n_0 = n, n_1, \cdots n_{\alpha_1 + \cdots + \alpha_k}$ such that:

- for each i, $p \mid f(n_i)$.
- Let $i = \alpha_1 + \cdots + \alpha_m + c$ with $m \leq k$ and $c \leq \alpha_{m+1}$ (or $m = k$ and $c = 0$), then n_i is a $p_1^{\alpha_1} \cdots p_m^{\alpha_m} \cdot p_{m+1}^c$-th residue of p.

We do induction on i, with $i = 0$ being true: the second point is vacuously true, and the first point follows from the assumption. Next, suppose that n_i satisfies these conditions. Since each p_j is a divisor of $p - 1$, they are relatively prime to p. Hence, for each j, we can find ℓ such that $n_i + \ell p$ is divisibly by p_j. Denote, for now, $m = n_i + \ell p$. But by the condition (*), $\ell p \mid f(n_i + \ell p) - f(n_i)$, and with $p \mid f(n_i)$ we have $p \mid f(n_i + \ell p) = f(m)$ and therefore $p \mid f(m^{\text{rad}(m)})$. Since n_i (and m) are $p_1^{\alpha_1} \cdots p_m^{\alpha_m} \cdot p_{m+1}^c$-th residue of p, $m^{\text{rad}(m)}$, having $\text{rad}(m)$ divisible by p_j, is then a $p_1^{\alpha_1} \cdots p_m^{\alpha_m} \cdot p_{m+1}^c \cdot p_j$-th residue of p. We can then assign p_j according to the following cases:

- If $i = \alpha_1 + \cdots + \alpha_{m+1}$ for some m (i.e. $c = \alpha_{m+1}$) we can assign $j = m + 2$.
- Otherwise, $0 \leq c < m + 2$ so $j = m + 1$.

This finishes the induction step.

Now, $m = n_{\alpha_1 + \cdots \alpha_k}$ is a $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ residue of p, hence must be congruent to 1 modulo p by Fermat's Little Theorem. Since we also have $p \mid f(m)$ and $p \mid m - 1$, by the identity (*) we have $p \mid m - 1 \mid f(m) - f(1)$ so $p \mid f(1)$. We therefore conclude that if f is a nonzero polynomial, all primes p with $p \mid f(n)$ for some n with $p \nmid n$ must also satisfy $p \mid f(1)$, hence there must be finitely many of them.

Finally, for nonzero f we write $f = x^k g$ for some k with $g(0) \neq 0$. We claim that g must be constant. Let $a_0 \neq 0$ (i.e. $a_0 > 0$) be the constant term of g. Let $h(n) = g(na_0|)/a_0$, then $h(0) = 1$ and if g_k is the coefficient of x^k in $g(x)$, we have $g_k(na_0)^k/a_0 = g_k a_0^k n^k / a_0$, so the coefficient of x^k in $h(k)$ is $g_k a_0^{k-1}$. Thus h is also a polynomial with integer coefficients. If h is nonconstant, by Schur's theorem there exists infinitely prime p such that $p \mid h(n)$ for some n, i.e. $p \mid g(na_0) \mid f(na_0)$. Moreover, since $h(0) = 1$, we have $p \nmid n$. This means there are infinitely many prime p with $p \mid f(na_0)$ but $p \nmid n$. Since a_0 is nonzero, it has only finitely many prime divisors, and therefore infinitely many of the prime p satisfying the previous condition do not divide $f(na_0)$ either. This would make those p divide $f(1)$, which is a contradiction. Hence, h must be a constant, which means g is also a constant too. We now have $f(n) = cx^k$, as desired.

N6 Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

Solution. As the first step, we show that, if $x > 1$, then for each k, ℓ satisfying $1 < k < 2^\ell$ and k odd, the set of prime numbers dividing $x^{2^n} - 1$ for some x is finite. To see this, we do the following expansion:

$$x^{2^n} - 1 = (x - 1)(x + 1)(x^2 + 1) \cdots (x^{2^{n-1}} + 1)$$

We now claim that all odd primes dividing $x^{2^k} + 1$ must have remainder 1 modulo 2^{k+1}. To see this, let p odd and $p \mid x^{2^k} + 1$ for some x, so -1 is a 2^k-th power residue modulo p. If ℓ is the highest power of 2 dividing $p - 1$ (meaning $\frac{p-1}{2^\ell}$) is odd then from $x^{2^k} \equiv -1$ we have $(x^{2^k})^{\frac{p-1}{2^\ell}} \equiv (-1)^{\frac{p-1}{2^\ell}} = -1$. If $\ell \leq k$ then $(x^{2^k})^{\frac{p-1}{2^\ell}} = x^{(p-1)(2^{k-\ell})}$ with exponent divisible by $p-1$, hence $x^{(p-1)(2^{k-\ell})} \equiv 1$ by Fermat's Little theorem, which is a contradiction to this equivalence actually being -1. So we need $\ell > k$, i.e. $p-1$ must be divisible by 2^{k+1}, as claimed.

Thus from above, if $p \mid x^{2^n} - 1$, and $2^k \nmid p-1$, then from $p \nmid x^{2^\ell} + 1$ for all $\ell \geq k$ we have $p \mid (x-1)(x+1)(x^2+1)\cdots(x^{2^{k-1}}+1) = x^{2^k} - 1$. This means that if $p \mid x^{2^n} - 1$ for some n then p is a positive divisor of $x^{2^k} - 1$. This last number is positive if $x > 1$, hence having finitely many positive divisors (and so finitely many p satisfies this property).

The next step is to show that there exists a k such that there are infinitely many primes p with $p \not\equiv 1 \pmod{2^k}$, and that $p \mid 2^n y + 1$ for some n. We consider now the sequence $(a_n)_{n\geq 1}$. Since $2^n y$ is an integer when $n \geq -v_2(y)$, we may backtrack to $(a_n)_{n \geq -v_2(y)+1}$. In other words, we may assume that y is odd.

Suppose that there's only finitely many primes $p_1, \cdots, p_k$ with $p_i \equiv 3 \pmod 4$ that divides at least one term in the sequence (a_n). Let b_i be the highest power of p_i dividing $2y+1$ for each i. Set $n = \prod_{i=1}^{k} \phi(p_i^{b_i+1})$ where $\phi(x)$ is the number of elements in $\{1, 2, \cdots, x\}$ relatively prime to x. This means $2^n \equiv 1 \pmod{p_i^{b_i+1}}$, and from b_i being the highest power of p_i dividing $2y+1$ we have the same for $2^{n+1}y+1$, too. This means, we can write out the following terms:

$$2y+1 = u\prod_{i=1}^{k} p_i^{b_i} \qquad 2^{n+1}y+1 = v\prod_{i=1}^{k} p_i^{b_i}$$

where u, v are divisible by none of $p_1, \cdots, p_k$. Since y is odd, $2y+1 \equiv 3 \pmod 4$ so $u \equiv 1 \pmod 4$. Since $n > 0$, $2^{n+1}y + 1 \equiv 1 \pmod 4$ so $v \equiv 1 \pmod 4$. But this means v has to be divisible by some prime $q \equiv 3 \pmod 4$, which cannot be $p_1, \cdots, p_k$. This contradicts our initial assumption.

N7 (IMO 6) Find all positive integers n for which there exist non-negative integers $a_1, a_2, \ldots, a_n$ such that

$$\frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \cdots + \frac{1}{2^{a_n}} = \frac{1}{3^{a_1}} + \frac{2}{3^{a_2}} + \cdots + \frac{n}{3^{a_n}} = 1.$$

Answer. All n such that $n \equiv 1, 2 \pmod 4$.

Solution. We see that the condition above is necessary: indeed multiply the second term by 3^M where $M = \max\{a_i\}$ we have $3^M = \sum_{k=1}^n k3^{M-a_k}$, and in modulo two we have $1 \equiv \sum_{k=1}^n k = \frac{n(n+1)}{2}$, the last term odd if and only if $n \equiv 1, 2 \pmod 4$.

Now let's show that these n would work. We first need the following examples:

- $n = 1 : a_1 = 0$
- $n = 5 : (2, 1, 3, 4, 4)$

For the rest, we make the following observation:

$$\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}} \quad \frac{c}{3^k} = \frac{c}{3^{k+1}} + \frac{2c}{3^{k+1}} (*)$$

This means taking $k = a_{2\ell+1}$ and $c = 2\ell+1$ means that, if $(a_1, \cdots, a_{4\ell+1})$ is a valid sequence, then so is $(a_1, \cdots, a_{2\ell}, a_{2\ell+1}+1, \cdots, a_{4\ell+1}, a_{2\ell+1}+1)$, so if we have such a sequence for $n = 4\ell+1$ we have the same for $4\ell+2$ too.

Next, notice also that for any x, y, z with $y + z = 6x$:

$$\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+2}} + \frac{1}{2^{k+2}} \quad \frac{x}{3^k} = \frac{x}{3^{k+1}} + \frac{y}{3^{k+2}} + \frac{z}{3^{k+2}} (**)$$

Having this, we consider the following iterative mindset: we consider some 'candidate' construction $(a_1, \cdots, a_n)$ where a_i could be integer or ? (placeholder), such that

$$\sum_{a_i \neq ?} 2^{-a_i} = \sum_{a_i \neq ?} i \cdot 3^{-a_i} = 1$$

We first construct $n = 9$ based on $n = 1$:

- Start with $a_1 = 0$, now we have $(0, ?, ?, ?, ?, ?, ?, ?, ?)$.
- Apply $*$ to $c = 1$, then $c = 2$, then $c = 4$, which gives

$$(1, 1, ?, ?, ?, ?, ?, ?, ?) \to (1, 2, ?, 2, ?, ?, ?, ?, ?) \to (1, 2, ?, 3, ?, ?, ?, 3, ?)$$

- Apply $**$ using $(x, y, z) = (2, 3, 9)$, and then $(2, 5, 7)$, giving

$$(1, 2, ?, 3, ?, ?, ?, 3, ?) \to (1, 3, 4, 3, ?, ?, ?, 3, 4) \to (1, 4, 4, 3, 5, ?, 5, 3, 4)$$

- Finally apply $*$ to $c = 3$, give the final construction

$$(1, 4, 5, 3, 5, 5, 5, 3, 4)$$

and from $n = 9$ to $n = 13$: start with $(1, 4, 5, 3, 5, 5, 5, 3, 4, ?, ?, ?, ?)$, apply * to $c = 5$ and $c = 6$ to get

$$(1, 4, 5, 3, 6, 6, 5, 3, 4, 6, ?, 6, ?)$$

and then ** to $(x, y, z) = (4, 11, 13)$ to get

$$(1, 4, 5, 4, 6, 6, 5, 3, 4, 6, 5, 6, 5)$$

Now let's go from $4\ell + 1$ to $4\ell + 13$ for $\ell \geq 1$ using the following algorithm: consider a valid sequence $(a_1, \cdots, a_{4\ell+1})$. Let our candidate be $(a_1, \cdots, a_{4\ell+1}, ?, \cdots, ?)$ (with 12 ?s in the end). Among the 12 numbers $4\ell + 2, \cdots, 4\ell + 13$, pair them such that each pair has two numbers divisible by 6. (In particular, we need the two numbers divisible by 6 to be paired, and the two numbers $\equiv 3 \pmod 6$ to be paired. The others can have more flexibility).

Now in each of the 6 steps, choose a pair (y, z) with $a_y = a_z = ?$. Notice that if $x = \frac{y+z}{6}$ then with $\ell \geq 1$,

$$x = \frac{y + z}{6} \leq \lfloor \frac{4\ell + 12 + 4\ell + 13}{6} \rfloor = \lfloor \frac{4\ell}{3} \rfloor + 4 < 4\ell + 2$$

i.e. $x \leq 4\ell + 1$ so $a_x \neq ?$. Then we can apply (**) on this x, y, z and do the following:

$$a_y, a_z \leftarrow a_x + 2, a_x \leftarrow a_x + 1$$

Thus we do have $4n + 1 \to 4n + 13$. Together with the examples $1, 5, 9, 13$, and the way to go from $4n + 1$ to $4n + 2$, the solution is complete.