Interesting problem solutions, storage

Victor Wang

October 23, 2013

1. (Miklos Schweitzer, 1987/1) The numbers $1, 2, \dots, n$ have been colored in three colors, so that every color is assigned to more than $n/4$ numbers. Prove that there exist numbers x, y, z of three different colors such that $x + y = z$.

   Solution. If we color the odds with one color and split the other two colors evenly among the evens, we get an approximate equality case.

   Go by contradiction. Analyzing any two colors alone and saying $(a, b) \in A \times B \implies a \pm b \notin C$ is not a powerful condition used directly.

   However, a potentially useful idea is pigeonhole, if we can find a number in $(A - B) \cap (B - C) \cap (C - A)$ (where difference sets are defined by absolute value). (*)

   First we WLOG $1 \in A$. This means nothing in B borders a C, so strings of b's and c's are separated by a's. Now it's more obvious why (*) is helpful. If we have a substring bba or abb, for instance, cac is forbidden. Similarly, bba forbids acc and abb forbids cca.

   This is a very powerful condition. First it tells us that we can't have both a bb and a cc, or else if WLOG the bb comes before the cc, they're separated by an a and we have bba and acc at the same time.

   However, suppose we have bb but no cc; then we can't have cac ahead or behind of the bb, since some a must lie between any b and c which means we get one of bba and abb in addition fo cac. This means that each c is bordered by two a's (or one, if it's on the border), yet is distance at least two from every other a. Thus no a is bordered by two c's, so $|A| \geq 2|C| - 1$ (how to consider the border: we start with an a, but we also might end with a c). But then $n - |B| = |A| + |C| \geq 2|C| - 1 + |C|$ forces $n + 1 \geq 4(n + 1)/4 = n + 1$ with equality only when $n \equiv 3 \pmod 4$ and $|B| = |C| = (n + 1)/4$ and $|A| = 2|C| - 1 = (n - 1)/2$. Hence we have $(n - 3)/4$ strings of aca and one string of ac (at the end), with strings of b's in between. By pigeonhole or our assumption that a bb exists, we must have $acabb$ somewhere. But then we get an a and b of difference 2, contradicting the fact that we start with aca and so $2 \in C$.

   On the other hand, if there are no bb's and cc's, we have at least $n/2$ a's and thus at most $n/2$ b's and c's in all. But we have at least $(n + 1)/4$ of each, contradiction.

2. If T is a subset of $\{1, 2, \dots, n\}$ such that for all distinct $i, j \in T$, i does not divide $2j$, prove that $|T| \leq 4n/9 + \log_2 n + 2$.

   Solution. We generalize the classic problem by considering $S_{r,m} = \{r4^m3^a2^b : (a, b) \in \{0, 1, 2, \dots\} \times \{0, 1\}\}$ for $r \equiv \pm 1 \pmod 6$ and $m \geq 0$. Indeed, $S_{r,m} \cap T$ contains at most one number, so if $g(n) = \{4^m r : m \geq 0, r \in \{1, 7, \dots\} \cap \{5, 11, \dots\}\} \cap [1, n]$, then

   $$g(n) = \lfloor (n + 5)/6 \rfloor + \lfloor (n + 1)/6 \rfloor + g(n/4) \leq n/3 + 1 + g(n/4),$$

   whence the conclusion follows easily by induction.

3. Let a, b, m, n be positive integers with $a \leq m < n < b$. Prove that there exists a nonempty subset S of $\{ab, ab + 1, \dots, ab + a + b\}$ such that $(\prod_{x \in S} x)/mn$ is the square of a rational number.

   Solution. The idea is that this is algebraic rather than number theoretic. If $(m, n), (n, p)$ can be reached, then so can mp (except when mp is a perfect square, we may need to pay more attention).

(Simplifications like this are very important to make the problem conditions easier to work with, since it's very hard to make things explicit – also, this is the best way to use the messiness of the rational condition.)

For each $0 \le i \le b-a-2$, we find positive k_i such that $ab \le (a+i)k_i < (a+i+1)k_i \le ab+a+b$. To do this, it's enough to show that (use $\lfloor x \rfloor = -\lceil -x \rceil$)

$$\lfloor (ab+a+b)/(a+i+1) \rfloor \ge \lceil ab/(a+i) \rceil \iff \lfloor (ab+a+b)/(a+i+1) \rfloor + \lfloor -ab/(a+i) \rfloor \ge 0,$$

or equivalently,

$$\lfloor (a-bi)/(a+i+1) \rfloor + \lfloor bi/(a+i) \rfloor \ge 0.$$

Let $b = a+i+2+r$ for $r \ge 0$; this reduces to

$$1+\lfloor (a-i(r+1))/(a+i+1) \rfloor + \lfloor (i(r+1)-a)/(a+i) \rfloor = \lfloor (a-i(r+1))/(a+i+1) \rfloor + \lfloor i(r+2)/(a+i) \rfloor \ge 0,$$

which is trivial (with the second expression) when $a - i(r+1) \ge 0$. When $a-i(r+1) < 0$, we use the fact that $\lfloor x \rfloor + \lfloor y \rfloor \ge \lfloor x+y \rfloor - 1$, which follows from $\{x\}+\{y\}-\{x+y\} \le \{x\}+\{y\} < 1+1$. But $1/(a+i) > 1/(a+i+1)$, so we're done.

The only possible issue arises when mn is a perfect square. But this is easy to fix: suppose for contradiction that $x^2 < ab < ab+a+b < (x+1)^2$, so $2x > a+b \ge 2\sqrt{ab}$. But then $ab > x^2 > ab$, contradiction.

4. For a positive real x, let $A(X) = \{\lfloor nx \rfloor : n \in \mathbb{N}\}$. Find all irrational numbers $\alpha > 1$ satisfying the following: if a positive real number β satisfies $A(\alpha) \supset A(\beta)$, then $\frac{\beta}{\alpha}$ is integer.

   Solution. It helps to consider $A(\alpha') = \mathbb{N} \backslash A(\alpha)$, where $\frac{1}{\alpha} + \frac{1}{\alpha'} = 1$, since $A(\beta) \subseteq A(\alpha)$ iff $A(\beta) \cap A(\alpha') = \emptyset$.

   If $A(\beta) \subseteq A(\alpha)$, then for every $n \in \mathbb{N}$, there exists m such that $\lfloor m\alpha \rfloor = \lfloor n\beta \rfloor$, or equivalently, $[\lfloor n\beta \rfloor/\alpha, \lfloor n\beta + 1 \rfloor/\alpha)$ contains an integer for every n. Weakening, this means $((n\beta-1)/\alpha, (n\beta+1)/\alpha)$ has an integer for all $n \ge 1$. If β/α is irrational, then if $2/\alpha \le 1$ we can make this not work. If β/α is rational but noninteger, then β is irrational; for some arithmetic progression of n we can make $\{n(\beta/\alpha)\} = 1/q \le 1/2 < 1 - 1/\alpha$ (where $\beta/\alpha = p/q$ and $q > 1$), and then using equidistribution theorem we can get $\{n\beta\}$ arbitrarily close to 0 on this arithmetic progression so that $0 < \{n(\beta/\alpha) - \{n\beta\}/\alpha\} \le 1 - 1/\alpha$.

   This is, however, a messy condition, so we also need to consider the complement/dual with $A(\alpha')$. Note that our condition above means that $\beta/\alpha, \beta, 1$ are linearly dependent for any counterexample. We want to show that if $1 < \alpha < 2$, there don't exist n, i, j such that $n/\beta < i < (n+1)/\beta$ and $n/\alpha' < j < (n+1)/\alpha'$. We know $1/\beta, 1/\alpha, 1$ are lineraly dependent, or equivalently, $1/\beta, 1/\alpha', 1$ are linearly dependent. If we take $1/\beta + 1/\alpha' = 1/2$, we get an easy contradiction since $2 \mid n$ or $2 \mid n+1$, so we're done ($\beta/\alpha = 2/(2-\alpha)$).

   Rational β may pose a small issue but it's trivial to fix.

   There's another construction for the latter part. Note that $A(\beta) \subseteq A(\alpha)$ iff $A(\beta) \cap A(\alpha') = \emptyset$ iff $A(\alpha') \subseteq A(\beta')$, so we might as well take $\beta' = \alpha'/n$ for some integer $n \ge 1$, as long as $\alpha'/n > 1$. Then if this all works out, we easily compute $\beta/\alpha = 1/(n - \alpha(n-1))$, so if $n \ge 2$ gives a valid β' we know that α doesn't work; this occurs iff $\alpha' > 2 \iff \alpha < 2$, so we can finish the $\alpha \ge 2$ case as above.

5. Given a positive integer $n \ge 3$, colour each cell of an $n \times n$ square array with one of $\lfloor (n+2)^2/3 \rfloor$ colours, each colour being used at least once. Prove that there is some 1×3 or 3×1 rectangular subarray whose three cells are coloured with three different colours.

   Solution. KEY IDEA: EVERY TROMINO CONTAINS A PAIR (EITHER NORMAL OR DISJOINT)

   approach 1:

   1. natural to try 3x3 (nice way is to consider first row, then next two add at most 2)

2. extend (1) to 3xn to get an asymptotically 1/3 # squares bound, which allows for an inductive solution

3. alternatively to get to 2, want to understand mxn for small m, n ($m = 1, 2$ are obvious though, and don't allow for each induction if the leading quadratic constant is 1/3)

approach 2:

1. global approaches difficult; note that each tromino has ≥ 2 squares of some color, so because $2 + 2 > 3$, exactly one color with ≥ 2 squares

2. want to analyze each color separately, so consider # x's and # trominos "bearin" x and do some sums (each row, column independently)

3. alternatively to get to 2, consider number of normal pairs and disjoint pairs, then note that to count these pairs we want to sum over triples

6. On the cartesian plane are drawn several rectangles with the sides parallel to the coordinate axes. Assume that any two rectangles can be cut by a vertical or a horizontal line. Show that it's possible to draw one horizontal and one vertical line such that each rectangle is cut by at least one of these two lines.

Solution. Hmm... I think the key is to elaborate on the idea of considering the leftmost right and rightmost left sides (which comes from the one-dimensional analog).

Let $l(\mathcal{R}), r(\mathcal{R}), b(\mathcal{R}), t(\mathcal{R})$ denote the left, right, bottom, and top coordinates of rectangle $\mathcal{R}$. Two rectangles are *connected* if they can be cut by a line; *vertical and horizontal connectivity* refer to the orientation of the line. (Although it doesn't really matter, in this solution we'll include the boundary in the "interior" of a rectangle.)

Suppose we have $n \geq 3$ rectangles ($n \leq 2$ is trivial), and order them according to $r(\mathcal{R}_1) \leq r(\mathcal{R}_2) \leq \cdots \leq r(\mathcal{R}_n)$. If $\mathcal{R}_i$ and $\mathcal{R}_j$ are horizontally connected for all $1 \leq i < j \leq n$, we're done by the one-dimensional analog. Otherwise, let $2 \leq k \leq n-1$ denote the smallest index such that there exists $1 \leq i \leq k-1$ with $\mathcal{R}_i, \mathcal{R}_k$ horizontally disconnected. For $k+1 \leq m \leq n$, place $\mathcal{R}_m$ in set S_- if $l(\mathcal{R}_m) \leq r(\mathcal{R}_k)$ and S_+ if $l(\mathcal{R}_m) > r(\mathcal{R}_k)$.

For all $\mathcal{R}_m \in S_-$, $l(\mathcal{R}_m) \leq r(\mathcal{R}_k) \leq r(\mathcal{R}_m)$, so we place a vertical line at $r(\mathcal{R}_k)$ to account for $\{\mathcal{R}_k\} \cup S_-$.

WLOG $b(\mathcal{R}_i) > t(\mathcal{R}_k)$. For all $\mathcal{R}_m \in S_+$, $l(\mathcal{R}_m) > r(\mathcal{R}_k) \implies \mathcal{R}_m$ is vertically disconnected from $\mathcal{R}_1, \ldots, \mathcal{R}_k$ and thus horizontally connected to each of $\mathcal{R}_1, \ldots, \mathcal{R}_{k-1}, \mathcal{R}_k$ (including $\mathcal{R}_i, \mathcal{R}_k$!). Furthermore, $\mathcal{R}_1, \ldots, \mathcal{R}_{k-1}$ are pairwise horizontally connected by the minimality of k, while $\mathcal{R}_{m_1}, \ldots, \mathcal{R}_{m_\ell}$ (where $|S_+| = \ell$) are pairwise horizontally connected by the horizontal lines in $[t(\mathcal{R}_k), b(\mathcal{R}_i)]$ (which belong to the vertical "gap" in between $\mathcal{R}_k$ and $\mathcal{R}_i$), so by the one-dimensional analog, there exists a horizontal line in

$$[\max(b(\mathcal{R}_1), \ldots, b(\mathcal{R}_{k-1}), b(\mathcal{R}_{m_1}), \ldots, b(\mathcal{R}_{m_\ell})), \min(t(\mathcal{R}_1), \ldots, t(\mathcal{R}_{k-1}), t(\mathcal{R}_{m_1}), \ldots, t(\mathcal{R}_{m_\ell}))],$$

as desired (because $\mathcal{R}_1, \ldots, \mathcal{R}_{k-1}, \mathcal{R}_{m_1}, \ldots, \mathcal{R}_{m_\ell}$ are pairwise horizontally connected).

Does this extend to arbitrary dimensions using a similar induction idea?

vector fields solution

There is a less explicit way to do the same thing. Take a minimal counterexample, which must clearly have at least two rectangles. Remove an arbitrary rectangle R; by minimality, we can assume the x and y axes satisfy the remaining $n-1$ rectangles and R is in the first quadrant. Assume the x- and y-axes are "maximal", i.e. we can't move either up or to the right without leaving some previously covered rectangle. Then some rectangle R_x has top edge the x-axis and is not covered by y-axis; similarly we can find R_y with right edge the y-axis and not covered by x-axis. By the condition on R, R_x and R, R_y, we have R_x, R_y in the lower right and upper left quadrants, so R_x, R_y don't satisfy the problem condition, contradiction.

7. Let $p \geq 3$ be a prime number and $a_1, \ldots, a_{p-2}$ a sequence of integers such that $p \nmid a_i, a_i^i - 1$ for each i. Prove that some distinct terms multiply to $2 \pmod{p}$.

   Solution. The first thing we notice is that the 2 is very arbitrary multiplicatively. So we want to show that we can get everything modulo p. Even 1 is difficult to get directly, unless we assume that one of the residues $2, 3, \ldots, p-1$ cannot be reached (then use pigeonhole on $a_1, a_1a_2, \ldots$).

   We can try to convert the problem by taking a primitive root and passing to a sum problem modulo $p-1$ (and generalize this to arbitrary n), but this is not obviously useful either: it's only very easy to do when n is prime (e.g. CNS shows we can get every residue). (On a random note, if the problem had started from this direction, the appearance of $\phi(d)$ for all $d \mid n$ can sometimes be better behaved when we order the integers and consider their gcd with n.)

   But keeping all equivalent problems in mind is always a good idea. Here, we notice that 2^{p-2} gives us a LOT of choices.

   There are two ways to look at the last step. Either we want to try a greedy approach (since there is very little obvious structure but so many options) or work backwards. If we start backwards, suppose that x cannot be reached; then x/a_i cannot be reached by subsets not involving a_i, etc. – we can try to extend this logic to eventually get a contradiction. But it still boils down to doing the greedy approach backwards. Indeed, including the empty set as product 1, we start with $S_1 = \{1, a_1\}$ as the set of products generated by the first term. Now it's easy to show that $|S_k| \geq k+1$ for each k by induction, which is where the a_k^k comes into play (it cannot permute a set of k elements upon multiplication, so when multiplied to a set of k elements it makes it larger).

8. (Bulgaria 1997) Let $n \geq 4$ be an even integer, and $A \subseteq [n]$ a subset with more than $n/4$ elements. Show that there exist elements $a, b, c \in A$ (not necessarily distinct) with one of the numbers $a+b, a+b+c, a+b-c$ divisible by n.

   Solution. Assume that $x \in A \implies x \notin A$ and $\pm a \pm b \pm c$ is not divisible by n for any $a, b, c \in A$ and choice of signs. This is a very useful symmetry observation for the signs, because it's then clear that we can exchange x and $-x$ if we want, and one may be easier to analyze than the other. So we can assume $A \subseteq \{1, 2, \ldots, m-1\}$, where $n = 2m$. But A is sum-free, so $m - 1 \geq |A| + \frac{|A-A|-1}{2} \geq 2|A| - 1$ forces $|A| \leq \frac{m}{2} = \frac{n}{4}$, contradiction.

   Alternatively, let k be the smallest element of A and use the fact taht $x, x+k$ can't both be in A. (This is uglier though.)

9. (Gabriel Carroll MOP Handout) Let $a_1, \ldots, a_n$ be positive integers with the followinng property: for any nonempty subset $S \subseteq [n]$, there exists $s \in S$ with $a_s \leq \gcd(S)$. Prove that $a_1a_2\cdots a_n \mid n!$.

   Solution. We use prime counting for every $p \leq n$. This is enough since taking S to be any one element gives $a_s \leq s$. If $p^k \leq n$ (for some fixed p, k) divides $a_{r_1}, \ldots, a_{r_\ell}$ for some indices $r_1 < \cdots < r_\ell$ and $\ell \geq 1 + \lfloor n/p^k \rfloor$ (we're going by contradiction), then taking $S = \{r_1, \ldots, r_\ell\}$ first gives $r_1 \geq p^k$. By the Euclidean algorithm we also have the bound $p^k \leq \frac{r_\ell - r_1}{\ell - 1} \leq \frac{n-p^k}{\ell-1}$, whence $\ell \leq \frac{n}{p^k}$, contradiction.

   Another idea is to find a bijection $f : [n] \to [n]$ such that $a_s \mid f(s)$ for every s. To do this, start from the largest a_i and move down in size. Suppose that we can't continue this procedure at some point: say we've picked all the multiples of a_m; then there exist $\lfloor n/a_m \rfloor$ indices k (say they form a set T) such that $a_k \geq a_m$ (since we go in decreasing order of a_i) and $a_m \mid f(k)$. But then $a_m \leq \gcd(T \cup \{m\}) < a_m$ (either the smallest index is less than a_m or there is a gap less than a_m).

   The second solution can be reworded in terms of Hall's marriage theorem, since if $a_{i_1} \leq \cdots \leq a_{i_r}$, then $a_{i_1} \leq \gcd(i_1, \ldots, i_r) \leq n/r$ means there are at least r multiples of a_{i_1} less than or equal to n.

   All three of these solutions have the same spirit, however.

10. (Vietnam 1997) Find the largest real number α for which there exists an infinite sequence $a_1, a_2, \ldots$ of positive integers such that $a_n > 1997^n$ and $a_n^\alpha \leq \gcd\{a_i + a_j \mid i + j = n\}$ for each $n \geq 1$.

    Solution. Note that $\alpha = 0$ works for any sequence with $a_n > 1997^n$ for all n, so we can assume $\alpha > 0$.

If $\alpha \geq 1$ then $a_n \leq a_1 + a_{n-1}$ shows that $a_n = O(n)$, so $\alpha < 1$. Furthermore, $a_{2n} \leq a_n + a_n$ shows that $a_{2^k} \leq 2^{\alpha^{-1}} a_{2^{k-1}}^{\alpha^{-1}}$, so by induction

$$a_{2^k} \leq 2^{\alpha^{-1}+\cdots+\alpha^{-k}} a_1^{\alpha^{-k}} \implies 1997^{(2\alpha)^k} \leq 2^{1+\alpha+\cdots+\alpha^{k-1}} a_1 < 2^{1/(1-\alpha)} a_1.$$

Thus $2\alpha \leq 1$.

To find a construction for $\alpha = 1/2$, we use "sum-to-product" identities (motivated by Chebyshev polynomials, Fibonacci numbers, etc.): set $\alpha = N + \sqrt{N^2-1}$ (so $\alpha^{-1} = N - \sqrt{N^2-1}$) for some large integer N and define $b_n = \alpha^n + \alpha^{-n}$ for all $n \geq 0$ (clearly these are all positive integers); letting $a_n = \alpha^{2n} + \alpha^{-2n}$ for each $n \geq 1$, we have

$$a_i + a_j = \alpha^{2i} + \alpha^{2j} + \alpha^{-2i} + \alpha^{-2j} = (\alpha^{i+j} + \alpha^{-i-j})(\alpha^{i-j} + \alpha^{j-i}) = b_{i+j} b_{|i-j|}.$$

For N sufficiently large, clearly $a_n > \alpha^{2n} > 1997^n$ for each n, and

$$\begin{aligned} \gcd\{a_i + a_j \mid i+j=n\} &\geq b_n = \alpha^n + \alpha^{-n} \\ &= \sqrt{\alpha^{2n} + \alpha^{-2n} + 2} > \sqrt{\alpha^{2n} + \alpha^{-2n}} = a_n^{1/2}, \end{aligned}$$

as desired.

11. Let $k \geq 1$ be a positive integer and G a tournament such that for every k-element subset S of V, there is a vertex $v_0 \in V \setminus S$ such that $v_0 \to v$ for all $v \in S$. Show that $|G| \geq (k+2)2^{k-1} - 1$.

Solution. One may observe that such bounds are most easily generated through recursion. It will be convenient to let $f(S)$ denote the intersection of $N^{-1}(v)$ for all $v \in S$.

So our condition, in other words, states that $|f(v_1, \ldots, v_k)| \geq 1$ for all $(v_1, \ldots, v_k) \in V^k$ (note that redundancies are fine). Let $F(k)$ be the best greatest lower bound we can put on $|G|$. Clearly $F(1) = 3$.

So first we can try direct induction. The idea is that if we fix v_1, then for all $(v_2, \ldots, v_k) \in V^{k-1}$ we have $f(v_2, \ldots, v_k) \cap f(v_1) \neq \emptyset$. In particular, $|f(v_2, \ldots, v_k)| \geq 1$ for all $(v_2, \ldots, v_k) \in f(v_1)^{k-1}$, so by the inductive hypothesis $|f(v_1)| \geq F(k-1)$. If we take v_1 to have minimal indegree, then we can show that $F(k) \geq 2F(k-1) + 1$; however, this is too weak for our desired bound. (*)

Why is this direct bound weak? Because when we focus so much on v_1 we lose a lot of information, even if minimality does give us significant bounds. We should try to incorporate more variety into the picture by fixing $k-1$ vertices and playing around with this. Suppose we have $|S| = k-1$. We can try to use the same idea as (*), but this is too weak: all we get is that $|f(S)| \geq F(1) = 3$. So we should use a new idea: for every $v \in G$, $f(v) \cup f(S) = f(v \cup S) \neq \emptyset$ means that something in $f(S)$ points to v. Equivalently, v does not point to everything in $f(S)$. This holds for all $v \in G$, however, whence $|f(S)| \geq k+1$ by the hypothesis. This is good progress because while we have weakened the condition from k vertices to $k-1$, we have improved the bound from 1 to $k+1$, which is extremely helpful if we want to get the extra $(k+2)$ factor in our bound! (**)

We should continue this promising logic: let $|S| = k-2$ for some S. Directly using the idea from (**), we get that some $k+1$ vertices in $f(S)$ point to v (for fixed $v \in G$), or equivalently, that v points to at most $|f(S)| - k - 1$ vertices in $f(S)$ for each v. But then the best we can show is $|f(S)| \geq 2k+2$, and in general if $|S| = k-j$ the best we can do is $|f(S)| \geq j(k+1)$; indeed, this is too weak since we only get a linear bound by repeatedly using the global fact that $f(v_1, \ldots, v_k) \geq 1$ in such a local setting, while almost ignoring the potential of our induction.

However, (*) fortunately does the trick. Indeed, taking a vertex in $f(S)$ of minimal degree, we have $(|f(S)|-1)/2 \geq k+1$ (if $|S| = k-2$), so $|f(S)| \geq 2k+3$. By induction, we can show that if $|S| = k-j$ (where $0 \leq j \leq k$), then $|f(S)| \geq 2^{j-1}(k+2) - 1$ (note that $f(\emptyset) = G$ from a bunch of vacuous statements; if this is uncomfortable, we can stop at $j = k-1$ and do the last step alone, noting that the degree of each vertex, particularly the minimal degree vertex, is at least $2^{k-2}(k+2) - 1$). For $j = k$, this is the desired bound, so we're done.

12. Let p, q be coprime positive integers. A subset S of the nonnegative integers is called ideal if $0 \in S$ and $n+p, n+q \in S$ for every $n \in S$. Determine the number of ideal subsets of the nonnegative integers.

    Solution. Define $[n]_q$ as the remainder when n is divided by q, and for $0 \le i \le q-1$, let a_i denote the smallest integer such that $qa_i + [pi]_q \in S$.

    Then it's clear that S is ideal iff $a_0 = 0$ and for $1 \le i \le q-1$, $0 \le a_i \le a_{i-1} + \frac{p+[p(i-1)]_q-[pi]_q}{q} = a_{i-1} + \left\lfloor \frac{pi}{q} \right\rfloor - \left\lfloor \frac{p(i-1)}{q} \right\rfloor$ (consider "jumpin" between the residue classes $p(i-1) \pmod q$ and $pi \pmod q$), i.e. if $b_i = a_i - \left\lfloor \frac{pi}{q} \right\rfloor$ for $0 \le i \le q-1$ with $b_0 = 0$, then there is a clear bijection between the ideal subsets and the nonincreasing lattice paths (each step of length 1) from $(0,0)$ to $(q,-p)$ that never drop below the line $px+qy=0$.

    Now take $t_i = p$ if the i^{th} step is rightward and $t_i = -q$ if the i^{th} step is downward so that $t_1 + \cdots + t_{p+q} = 0$, and consider the partial sums $s_i = t_1 + \cdots + t_i$ for $1 \le i \le p+q$. Since p, q are relatively prime, they are pairwise distinct. Notice that the index $1 \le m \le p+q$ that minimizes s_m is the only one that satisfies $s_{i+m} - s_m \ge 0$ for all $1 \le i \le p+q$ (indices taken $\pmod{p+q}$). But S is ideal iff $s_i \ge 0$ for all i, so exactly one cyclic shift of indices gives a working S, i.e. there are

    $$\frac{1}{p+q}\binom{p+q}{p}$$

    ideal subsets.

13. Prove that there exists a positive real number C with the following property: for any integer $n \ge 2$ and any subset X of the set $\{1, 2, \ldots, n\}$ such that $|X| \ge 2$, there exist $x, y, z, w \in X$(not necessarily distinct) such that

    $$0 < |xy - zw| < C\alpha^{-4}$$

    where $\alpha = \frac{|X|}{n}$.

    Solution. Nice problem! I think we can strengthen the bound to $\alpha^{-3} = n^3/k^3$ (stronger since $n/k \ge 1$)... does the following work?

    Let $k = |X|$, and go by contradiction (suppose that for every C, we can find a counterexample with some n and X).

    First, since $|X \cdot X| \ge k$, we have $n^2/k \ge n^2/|X \cdot X| \ge Cn^3/k^3$ by pigeonhole (since $\max X \cdot X \le n^2$), so $k^2 \ge Cn$.

    Now note that if some difference $d > 0$ occurs twice, say for $a, a+d$ and $b, b+d$ with $a \ne b$, then $a(b+d) - b(a+d) = d(a-b)$. (This is the key to the nontrivial part of the solution, motivated by extending the difference of squares factorization.)

    Let $D = \lfloor 5n/k \rfloor \ge 5n/k - 1 \ge 4n/k$; if P denotes the number of pairs $\{x, x+d\}$ with $1 \le d \le D$ and $x, x+d \in X$ and $t_i = |X \cap (D(i-1), Di]|$ for $1 \le i \le \lceil n/D \rceil$ (take $C \ge 8$ so that $k^2 \ge Cn = 8n \ge 16 \implies k \ge 4$, whence $\lceil n/D \rceil \le n/D + 1 \le k/4 + 1 \le k/2$), then by Jensen on $f(x) = x(x-1)/2$ (convex for $x \ge 0$),

    $$\begin{aligned} t_1 + \cdots + t_{\lceil n/D \rceil} = k \implies P \ge \binom{t_1}{2} + \cdots + \binom{t_{\lceil n/D \rceil}}{2} &\ge \lceil n/D \rceil \binom{k/\lceil n/D \rceil}{2} \\ &= \frac{k}{2}\left(\frac{k}{\lceil n/D \rceil} - 1\right) \\ &\ge \frac{k}{2}\left(\frac{k}{k/2} - 1\right) = \frac{k}{2}. \end{aligned}$$

    But then $P/D \ge (k/2)/(5n/k) = k^2/(10n)$, so by pigeonhole, there exists $1 \le d \le D$ such that there exist $\ell \ge k^2/(10n)$ elements $a_1 < \cdots < a_\ell$ with $a_i, a_i + d \in X$ for $1 \le i \le \ell$. We can take $C \ge 20$ so that $k^2 \ge Cn = 20n \implies \ell \ge k^2/(10n) \ge k^2/(20n) + 1$.

By pigeonhole, there exists $1 \le j \le \ell - 1$ such that $0 < a_{j+1} - a_j \le n/(\ell-1) \le 20n^2/k^2$. But then

$$0 \ne |a_j(a_{j+1}+d) - a_{j+1}(a_j+d)| = d(a_{j+1}-a_j) \le D\frac{20n^2}{k^2} \le \frac{100n^3}{k^3},$$

a contradiction for sufficiently large C.

Comment. Originally I set $D = \lfloor 5n^2/k^2 \rfloor$ to get the α^{-4} case (we cannot simply set $D = n$; this is too weak due to the scarcity of large differences), but later found this improvement while looking for optimal X (intuitively, it seems like $X = \{d, 2d, \ldots, \lfloor n/d \rfloor d\}$, which gets α^{-2}, should be close to the best). The current method loses a factor of α because for this construction, the only possible differences are multiples of d. Any ideas (for either direction)? I think the size of $|X \cdot X|$ may be an important consideration as well, although geometric progressions make the pigeonhole application $n^2/|X \cdot X|$ very weak.

14. Show that for two non-constant integer polynomials f, g, there exist infinitely many primes p such that there exist x, y with $p \mid f(x), g(y)$.

    Solution. The idea is to find $u(x)$ and $v(x)$ such that some non-constant polynomial $p(x)$ with integer coefficients divides $f(u(x))$ and $g(v(x))$. The corresponding problem for $p(x)$ (sometimes known as Schur's theorem) is easy: if $p(0) = 0$, obvious; if $p(0) = 1$, consider $p(p(1)p(2)\cdots p(n)) \equiv p(0) = 1 \pmod{p(1)p(2)\cdots p(n)}$ to generate infinitely many primes; if $p(0) \ne 0, 1$, then consider $q(x) = p(xp(0))/p(0)$ instead to reduce it to previous case.

    It will be simpler to work with rational polynomials instead (p, u, v rational coefficients); by easy scaling we can get integer polynomials later.

    WLOG f and g are irreducible and coprime (in $\mathbb{Q}$). It suffices to find an algebraic number r such that $u(r) = a$ and $v(r) = b$, where a is some root of f and b is some root of g, because if we let $p(x)$ be the minimal polynomial of r, then $p(x) \mid f(u(x)), g(v(x))$ (all in $\mathbb{Q}$).

    So this problem boils down to the classical fact that $\mathbb{Q}(a, b) = \mathbb{Q}(c)$ for some c. (field extension generated by finitely many elements is generated by a single element)

    For $\mathbb{Q}(c) \subseteq \mathbb{Q}(a, b)$, we'll just need $c = P(a, b)$ for some polynomial $P \in \mathbb{Q}[x]$.

    Let $a_1 = a, a_2, a_3, \ldots, a_m$ be the roots of f and $b_1 = b, b_2, b_3, \ldots, b_n$ be the roots of g. Then we need to show that $a, b \in \mathbb{Q}(c)$, or equivalently, that the minimal polynomials h_1, h_2 of a, b in $\mathbb{Q}(c)$ have degree 1. Of course, $h_1(x) \mid f(x)$ and $h_2(x) \mid g(x)$ (in $\mathbb{Q}(c)$). So to approach this, we want to find $c = P(a, b)$ such that there exist $F(x), G(x) \in \mathbb{Q}(c)[x]$ such that $F(a) = 0$ and $G(b) = 0$ but $\deg \gcd(f, F) = \deg \gcd(g, G) = 1$ (in $\mathbb{Q}(c)$). It's then natural to take $c = t_1 a + t_2 b$ for some nonzero $t_1, t_2 \in \mathbb{Q}$ such that $t_1 a_i + t_2 b_j$ are pairwise distinct for $1 \le i \le m$ and $1 \le j \le n$, because we can set $F(x) = g((c - t_1 x)/t_2) \in \mathbb{Q}(c)[x]$ and $G(x) = f((c - t_2 x)/t_1) \in \mathbb{Q}(c)[x]$. From the distinctness condition, it's then easy to check that $\gcd(f, F) = x - a$ and $\gcd(g, G) = x - b$, so we're done.

15. There are 100 apples on the table with total weight of 10 kg. Each apple weighs no less than 25 grams. The apples need to be cut for 100 children so that each of the children gets 100 grams. Prove that you can do it in such a way that each piece weighs no less than 25 grams.

    Solution. Divide everything by 25, so the weights are $1 \le b_1 \le \cdots \le b_n$, $b_1 + \cdots + b_n = 4n$, and we want to give a total weight of 4 to each of n children so that the weights of the pieces are all at least 1.

    We prove this by strong induction on n, where the base case $n = 1$ is obvious.

    Now suppose $n > 1$, and note that $b_n \ge 4$. If $b_1 \le 3$, then we can split b_n into $4 - b_1 \ge 1$ and $b_n + b_1 - 4 \ge b_n - 3 \ge 1$ and give $b_1, 4 - b_1$ to a child to reduce to the $n - 1$ case. (*)

    Otherwise, $3 < b_1 \le \cdots \le b_n$, and note that $s_i = b_1 + \cdots + b_i \le 4i$ ($s_0 = 0$) for all $0 \le i \le n$. We'll try to mimic the general idea of (*). In view of $s_1 > 3$, let $r \ge 1$ denote the largest index j such that $s_i > 4i - 1$ for $1 \le i \le j$.

    For $1 \le i \le r$, split b_i into $x_i = (4i - 3) - s_{i-1} \in [1, 2)$ (we have $x_1 = 1$) and $y_i = s_i - (4i - 3) \in (2, 3]$, and give x_{i+1}, y_i for $1 \le i \le r - 1$ to the first $r - 1$ children (since $x_{i+1} + y_i = 4$). If $r = n$, then we can give $x_1 = 1, y_r = 3$ to the last child.

Otherwise, $r < n$, so we can split b_{r+1} into $x_{r+1} = (4r+1) - s_r \in [1, 2)$ and $y_{r+1} = s_{r+1} - (4r+1) \in (1, 2]$, where we note that $s_{r+1} \le 4(r+1) - 1$ by the maximality of r (in particular, $r+1 < n$, since $s_n = 4n$) and $s_{r+1} = s_r + b_{r+1} \ge s_r + b_1 > s_r + 3 > (4r-1) + 3$. But then we can just give x_{r+1}, y_r to the r^{th} child and $x_1 = 1, x_{r+1}, 3 - x_{r+1}$ to the $(r+1)^{th}$ child, where the third piece is obtained by splitting b_n into $3 - x_{r+1} > 1$ and $b_n + x_{r+1} - 3 \ge 1 + x_{r+1} > 1$. We're done by the $n - (r+1) > 0$ case.

Comment. The same method shows the problem is true when 4 is replaced by any $c \ge 4$ (this is important for $y_{r+1} \ge 1$ and $3 - x_{r+1} \ge 1$).

16. Find all increasing $f : \mathbb{N} \to \mathbb{R}$ such that $f(ab) = f(a)f(b)$ whenever $\gcd(a, b) = 1$.

Solution. b) First $f(1)^2 = f(1) \implies f(1) \in \{0, 1\}$. The first case is trivial, so suppose that $f(1) = 1$, whence $f(n) \ge 1$ for all n. We'll prove that f is totally multiplicative, reducing this to the first part. It suffices to show that $f(p^r) = f(p)^r$ for all primes p and integers $r \ge 1$ since $f(n)$ is determined completely by the outputs of f at its maximal prime power divisors.

Note that for all integers $k, r \ge 1$ and primes p,

$$\frac{f(p^2k+1)}{f(pk+1)} \le \frac{f(p^r)}{f(p^{r-1})} \le \frac{f(p^2k-1)}{f(pk-1)}. \tag{1}$$

Multiplying (1) over $k = 1$ and $1 \le r \le s$, we have

$$\left(\frac{f(p^2+1)}{f(p+1)}\right)^r \le f(p^r) \le \left(\frac{f(p^2-1)}{f(p-1)}\right)^r.$$

Now suppose for the sake of contradiction that there exists a constant $c > 1$ such that $f(n+1) \ge cf(n)$ for all $n \ge 1$. Then multiplying this inequality over $1 \le n \le p^r - 1$, we have

$$c^{p^r-1} \le f(p^r) \le \left(\frac{f(p^2-1)}{f(p-1)}\right)^r,$$

a clear contradiction for sufficiently large r.

Thus for all $\epsilon > 0$, there exists a positive integer n such that $f(n+1) < (1+\epsilon)f(n)$. Hence for all sufficiently large $r \ge N$,

$$1 \le \frac{f(p^r n(n+1)+1)}{f(p^r n(n+1)-1)} \le \frac{f(n+1)}{f(n)} \le 1 + \epsilon.$$

Now taking $r = 1$ and $r = \ell \ge 1$ in (1) and dividing, we have

$$\frac{f(p^2k+1)}{f(pk+1)} \cdot \frac{f(pk-1)}{f(p^2k-1)} \le \frac{f(p^\ell)}{f(p^{\ell-1})} \cdot \frac{1}{f(p)} \le \frac{f(p^2k-1)}{f(pk-1)} \cdot \frac{f(pk+1)}{f(p^2k+1)}.$$

Plugging in $k = p^N n(n+1)$, we find that

$$\frac{1}{1+\epsilon} \le \frac{f(p^\ell)}{f(p)f(p^{\ell-1})} \le 1 + \epsilon.$$

Since this holds for all $\epsilon > 0$, we must in fact have $f(p^\ell) = f(p)f(p^{\ell-1})$ for all $\ell \ge 1$, i.e. $f(p^\ell) = f(p)^\ell$ for all $\ell \ge 1$ by induction, as desired.

17. Let $x \ne y$ be relatively prime natural numbers. Prove that for infinitely many primes p, the exponent of p in $x^{p-1} - y^{p-1}$ is odd.

Solution. Assume for the sake of contradiction that for all primes $p > N$ for some $N > xy(x-y)^2$, $v_p(x^{p-1} - y^{p-1}) \equiv 1 \pmod 2$.

First note that if $q | x^p - y^p$, $\gcd(q, xy) = 1$, and $q \equiv 1 \pmod p$ for some prime $q > p > N$, then by LTE $v_q(x^{q-1} - y^{q-1}) = v_q(x^p - y^p)$. Yet if $q \left| \frac{x^p - y^p}{x-y} \right.$, then either $q = p$ or $q \equiv 1 \pmod p$. But the former implies that $p | x^p - y^p \implies p | x - y$, contradicting the fact that $p > N$.

Thus for all $p > N$, $\frac{x^p-y^p}{x-y}$ is a perfect square. Now take a prime $r \equiv 3 \pmod 4$ dividing $4xy(x-y)^2-1$ (then $\gcd(r, xy(x-y)) = 1$). By assumption however, if we take a prime $p \equiv -1 \pmod{r-1}$ larger than N, then there exists z such that

$$z^2 = \frac{x^p - y^p}{x-y} \equiv \frac{\frac{1}{x} - \frac{1}{y}}{x-y} \equiv -\frac{1}{xy} \equiv -4(x-y)^2 \pmod r,$$

i.e. -1 is a quadratic residue $\pmod r$, contradiction.

Comment. There is another method using 2^s instead of p, which involves some basic diophantine equations.

18. Let $p \geq 13$ be a prime. Prove that for any integers a, b, c, d such that abc is not divisible by p and $(a+b+c)$ is divisible by p, there exist integers x, y, z belonging to the set $\{0, 1, 2, \ldots, \lfloor p/3 \rfloor\}$ such that $ax + by + cz + d$ is divisible by p.

Solution. Of course, the interesting part of the problem is when $t = 3$. As above, let $k = \lfloor p/3 \rfloor - 1$ (we have $3k + 4 \leq p \leq 3k + 5$), and set $S_\ell = \{0, 1, \ldots, \ell\}$ for every $\ell \geq 0$. Define $T_\ell = aS_\ell + bS_\ell + cS_\ell \pmod p$; we wish to show that $|T_k| = p$. However, note $a(k-x)+b(k-y)+c(k-z) \equiv -(ax+by+cz)$, so $r \in T_k$ iff $-r \in T_k$. Furthermore, $0 \equiv a + b + c \in T_k$, so it suffices to show that $|T_k| \geq p - 1$.

Case 1: $p \mid (a-b)(b-c)(c-a)$, WLOG $(a, b, c) = (1, 1, -2)$. Then it's easy to see that $aS+bS+cS = S + S - 2S = \{-2k, \ldots, 0, 1, \ldots, 2k\}$, so $|T| \geq \min(4k + 1, p) = p$ (this is true for $p \geq 13$).

Case 2: $p \nmid (a-b)(b-c)(c-a)$. It's easy to check that $|T_1| = |\{0, a, b, c, -a, -b, -c\}| = 7$ (since a, b, c are pairwise distinct and $a + b + c \equiv 0$). But $T_k = T_1 + T_{k-1}$, so by Cauchy-Davenport,

$$\begin{aligned} |T_k| \geq \min(|T_1| + |T_{k-1}| - 1, p) &= \min(6 + |aS_{k-1} + bS_{k-1} + cS_{k-1}|, p) \\ &\geq \min(6 + 3|S_{k-1}| - 2, p) = \min(3k + 4, p) \geq p - 1, \end{aligned}$$

as desired (I adapted this method from this thread).

Original Method: My (uglier) original proof (perhaps more motivated, though both of these give the extra boost to Cauchy-Davenport by using the intuition that aS_k, bS_k, cS_k are arithmetic progressions with pairwise distinct differences) uses Vosper's theorem, which shows that if $|A|, |B| \geq 2$, $|A + B| \leq p - 2$, and $|A + B| = |A| + |B| - 1$, then A, B are arithmetic progressions with the same difference. First, note that $a^2, b^2, c^2 \pmod p$ are pairwise distinct. WLOG set $a = 1$ by scaling.

Lemma. $|aS_k + bS_k| = |S_k + bS_k| \geq 2(k + 1) + 1$. If equality holds, then $aS_k + bS_k$ must be the union of two disjoint strings of consecutive residues, one of length $k + 1$ and the other of length $k + 2$.

Proof. Note that $k \geq 2 \implies |S_k| = k + 1 \geq 3$. Since $a = 1$, $b \not\equiv 0, \pm 1$. It's easy to show that there exists $1 \leq s \leq k$ such that $k + 2 \leq [bs]_p \leq p - (k + 2)$ by considering the three intervals $[0, k+1], [k+2, p-2-k], [p-(k+1), p]$ (and noting that $(p-2-k)-(k+2)+1 \geq (3k+4)-(2k+4)+1 = k+1$). Indeed, if $b \in [k+2, p-2-k]$ we're done, and otherwise by symmetry (negate b if necessary) we can assume $2 \leq b \leq k+1$ and note that $bk \geq k+2$ (so because $b \leq k+1$, $\{bi\}_{i=0}^k$ must hit the interval $[k+2, p-2-k]$, which has length $\geq k+1$, somewhere). So we already have $|S_k + \{0, bs\}| = 2(k+1)$; note that $S_k + 0$ and $S_k + bs$ are both consecutive strings of length $k + 1$, neither of which contains -1 or $k + 1$. But $|S_k| \geq 3$, so if we take any $s' \in S_k$ distinct from $0, s \pmod p$, $S_k + bs'$ must have an element neither in $S_k + 0$ nor $S_k + bs$, establishing the inequality.

If equality holds, then this last additional element must border either $S_k + 0$ or $S_k + bs$, since $S_k + bs'$ is itself a consecutive string of length $k + 1$ and there are "gap" between $S_k + 0$ and $S_k + bs$ at -1 and $k + 1$, so we're done (otherwise we would add at least two elements with $S_k + bs'$).■

Now assume for the sake of contradiction that $|T_k| \leq p - 2$. Let $U = aS_k + bS_k$; by the lemma, $|U| \geq 2k + 3$, so by Cauchy-Davenport,

$$p - 2 \geq |T_k| = |U + cS_k| \geq (2k + 3) + (k + 1) - 1 = 3k + 3 \geq p - 2.$$

Thus equality holds, so by Vosper's theorem, U and cS_k must be arithmetic progressions with the same difference in order for equality to hold. Because $|cS_k| = k + 1 \in [2, p - 2]$, it's easy to show that

cS_k can only be written as an arithmetic progression with difference $\pm c$, so U is also an arithmetic progression with difference $\pm c$. By the equality condition of the lemma, U is the union of two disjoint strings of consecutive residues, one of length $k+1$ (say $I_1 = [m_1, m_1 + k]$) and the other of length $k+2$ (say $I_2 = [m_2, m_2 + k + 1]$). By symmetry, suppose $[(m_1 - 1) - (m_2 + k + 1)]_p \geq 2$ (otherwise $2k + 5 = p \geq 3k + 4$). If I_1, I_2 are bordering, then $|U| = 2k + 3 \in [2, p - 2]$ gives a contradiction (in the same we show the progression cS_k must have difference d). Let $d \equiv \pm c \pmod p$ such that $2 \leq d \leq (p-1)/2$; clearly $m_2 + k + d, m_2 + k + 1 + d \notin I_2$ by simple bounding. But there's exactly one "end" of the arithmetic sequence U, so at least one of $m_2 + k + d, m_2 + k + 1 + d \in I_1$. Then it's easy to see there exists $x \in I_2$ such that $x + d \equiv m_1$; since there's at most one end to U, we must have $x \in \{m_2, m_2 + 1\}$ (since $m_1 - 1, m_1 - 2 \notin U$). If $m_2 \equiv m_1 + p - d$, then $m_2 + k + 1 + d \equiv m_1 + k + 1 \notin U$, so by discrete continuity (obviously $m_1 + k + d \notin I_1$, but it can't be the end of U) $I_1 + d \subseteq I_2 \implies d \geq [m_2 - m_1]_p = p - d$, contradiction, so $m_2 + 1 \equiv m_1 + p - d$. In this case, $m_2 + d \notin U$, so by discrete continuity $I_1 + d \subseteq I_2 \implies d \geq [m_2 - m_1]_p = p - 1 - d \implies d = (p-1)/2$. Thus $(a, b, c) \in \{(1, (p-3)/2, -(p-1)/2), (1, (p-1)/2, (p-1)/2)\}$. But these are equivalent to $(1, 2, -3)$ and $(1, 1, -2)$ by scaling, which we've already dealt with, contradiction (note that $a = 1$ is preserved, so we don't lose any generality from our earlier scaling).

Comment. The $T_k = T_1 + T_{k-1}$ method is much cleaner because it allows us to globally extend (using Cauchy-Davenport) the "local" idea of what $a + b + c \equiv 0 \pmod p$ does at a smaller scale (i.e. what it does to T_1), which is easier to understand. Nevertheless, I guess my original solution still has a few important ideas.

19. (Ehrenfucht) Suppose that $(\deg f, \deg g) = 1$; show that $f(x) - g(y)$ is irreducible.

Solution. It will be convenient in this solution to set $\deg 0 = 0$.

If $f(x, y) = cx^n + x^{n-1} f_1(y) + \cdots + x^0 f_n(y)$ for some polynomials $f_1, \ldots, f_n$ and positive integer n (call such a polynomial *good*), set $\alpha(f) = \max_{1 \leq i \leq n} \deg f_i / i$ (let $f_0 = 1$).

Lemma. If $f = gh$ for some nonconstant polynomials f, g, h (where f is good), then g, h are good as well and $\alpha(f) = \max(\alpha(g), \alpha(h))$. (I've seen this in some paper, but I think the authors' proof is kinda complicated.)

Proof. g, h are obviously good. WLOG $\alpha(g) \geq \alpha(h)$. Note that for all nonzero k, $\deg g_0 h_k / k = \deg h_k / k$ and $\deg g_k h_0 / k = \deg g_k / k$.

If $\alpha(g) > \alpha(h)$, then consider the smallest $u \geq 1$ such that $\deg g_u / u = \alpha(g)$; by the minimality of u,

$$\deg f_u / u = \deg g_u h_0 / u = \deg g_u / u = \alpha(g),$$

so we're done in this case ($g_0 h_u$ is not an issue if it exists).

Otherwise, $\alpha(g) = \alpha(h) = r$, so take the largest $u, v \geq 1$ such that $\deg g_u / u = \deg h_v / v = r$; by the maximality of u, v,

$$\deg f_{u+v} / (u + v) = \deg g_u h_v / (u + v) = r,$$

as desired (by maximality, $g_0 h_{u+v}, g_{u+v} h_0$ are not issues if they exist).

This is possibly more motivated if we assume WLOG f, g, h are all monic in x and write $f(x, y)/x^n = 1 + f_1(y)/x + \cdots + f_n(y)/x^n$. ■

Alternatively, choose z^n, z^m (possibly times some constant) to make sure the leading coefficient vanishes and use a degree (in z) argument.

The initial problem with $f(x, y) = x^m - y^n$ is now obvious: if $\deg_x g = a$ and $\deg_x h = b$, we have $\deg g_a / a, \deg h_b / b = \max(\alpha(g), \alpha(h)) \leq \alpha(f) = n/m$, but $(\deg g_a + \deg h_b)/(a + b) = n/m$, contradicting the fact that $a, b \geq 1$ (since $\gcd(m, n) = 1$). Of course, this generalizes just as easily to $f(x) - g(y)$.

20. Fix two positive integers $a, k \geq 2$. Suppose that there is a polynomial $f \in \mathbb{Z}[x]$ such that for all sufficiently large positive integers n, there exists a rational number x satisfying $f(x) = f(a^n)^k$. Prove that there exists a polynomial $g \in \mathbb{Q}[x]$ such that $f(g(x)) = f(x)^k$ for all real x.

Solution. Let $f(x_n) = f(a^n)^k$ for all $n \geq N$ (N such that the sign of $f(x)$ is determined from x and leading coefficient alone). If k is odd, replace f with $-f$ if necessary so that $f(x_n) > 0$ for all $n \geq N$; for k even this must be the case anyway.

Lemma. Suppose that $f(x) > 0$ for some x, $d = \deg f$, and $f(x) = c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0$. Then $f(x)^{1/d} = \pm a(x + b) + O(x^{-1})$, where $a = |c_d|^{1/d}$ and $b = c_{d-1}/(dc_d)$, and the $\pm$ sign is determined uniquely by the sign of x.

Proof. Well, this is a somewhat standard analytic problem, so I might as well post a solution.

By the problem condition, there exists a positive integer N (to be determined later) such that for every n, there exists $x_n \in \mathbb{Q}$ satisfying $f(x_n) = f(a^n)^k$. WLOG assume N is large enough so that $f(a^n)$ is nonzero with constant sign and $x_n \neq 0$ for $n \geq N$; then $f(x_n)$ must also have a fixed sign for $n \geq N$. By the rational root theorem, there exists a positive integer ℓ such that $x_n\ell \in \mathbb{Z}$ for all $n \geq N$.

Now suppose $d = \deg f > 0$, and fix two integers L, M (with $M > L, N$) to be determined later. By Van der Waerden's theorem, there exist positive integers $u, v \geq N$ such that the subsequence $\{x_{u+iv}\}_{i=0}^{M}$ has all terms of sign $\epsilon \in \{-1, 1\}$. Let $S = \{u + iv\}_{i=L}^{M}$ (note that we only consider $i \geq L$ here).

Lemma 1: There exist constants A, B, C with $A, C > 0$ and $A, B \in \mathbb{Q}$ such that

$$\left| |f(x)|^{1/d} - |Ax + B| \right| \leq C|x|^{-1}$$

for all $x \neq 0$.

Proof. Let $r = 1/d > 0$ and write $f(x) = cx^d(1 + F(x))$ (note that $F(x) = O(|x|^{-1})$ only contains the terms $x^{-1}, \ldots, x^{-d}$). We can absorb x with small absolute value into the constant C, so it suffices to prove the claim for sufficiently large $|x| \geq X$ satisfying $|F(x)| < 1/2$. Since $r > 0$, the binomial coefficients $\binom{r}{i}$ $(i \geq 0)$ are bounded in absolute value, so the binomial expansion

$$(1 + F(x))^r = 1 + \binom{r}{1}F(x) + \cdots + \binom{r}{\ell}F(x)^\ell + R_\ell(x)$$

for any $\ell \geq \lceil rd \rceil = 1$ establishes the claim. (Comparing to a geometric series in $F(x)$, we have

$$R_\ell(x) = O\left(\frac{F(x)^{\ell+1}}{1 - F(x)}\right) = O(F(x)^{\ell+1}) = O(|x|^{-\ell-1}),$$

as desired.)■

Corollary: There exists a constant $C' > 0$ and positive integer $N > 0$ such that for all $n \geq N$, $\left||f(x_n)|^{1/d} - |Ax_n + B|\right| \leq C'a^{-kn}$.

Proof. The relation $f(x_n) = f(a^n)^k$ implies that there exists a constant $C' > 0$ such that for sufficiently large n, $C|x_n|^{-1} \leq C'a^{-kn}$ for every $n \geq N$.■

Lemma 2: There exists a polynomial $h \in \mathbb{Q}[x]$ of degree k with positive leading coefficient and a constant $D > 0$ such that

$$\left||f(x)|^{k/d} - |h(x)|\right| \leq D|x|^{-1}$$

for all $x \neq 0$.

Proof. First we mimic the proof of lemma 1 (except with $r = k/d$ and $\ell \geq \lceil rd \rceil = k$) to get polynomial h (not necessarily with positive leading coefficient). If h has negative leading coefficient, however, we can just replace it with $-h$.■

First make L large enough so that $|Ax_n + B| = \epsilon(Ax_n + B)$ for all $n \in S$ (note that $A > 0$). Then by the corollary of lemma 1 (take N large enough),

$$\left||f(x_n)|^{1/d} - \epsilon(Ax_n + B)\right| \leq C'a^{-kn} \leq C'a^{-kLv} \leq C'a^{-Lv}$$

for all $n \in S$. If we also take L large enough so that $h(a^n) > 0$ for all $n \in S$ (note that h has positive leading coefficient), lemma 2 gives

$$\left||f(a^n)|^{k/d} - h(a^n)\right| = \left||f(a^n)|^{k/d} - |h(a^n)|\right| \leq D|a^n|^{-1} \leq Da^{-Lv}.$$

By the triangle inequality, we thus have

$$|\epsilon Ax_n + H(a^{iv})| = |\epsilon(Ax_n + B) - h(a^n)| \leq (C' + D)a^{-Lv}$$

for all $i \in [L, M]$ (where $n = u + iv$), where $H(x) = \epsilon B - h(a^u x) \in \mathbb{Q}[x]$ is a polynomial of degree k satisfying $\epsilon B - h(a^{u+iv}) = H(a^{iv})$ for all $i \in [L, M]$.

Now let $T : i \to i+1$ denote the shift operator and $U(x) = (x-a^0)(x-a^v)\cdots(x-a^{kv})$. Viewing $H(a^{iv})$ as a linear recurrence in $a^0, a^v, \ldots, a^{kv}$ indexed by i, we have $U(T)(H(a^{iv})) = 0$ for $i \in [L, M-k]$, so again by the triangle inequality,

$$\begin{aligned} |U(T)(\ell\ell' Ax_{i+uv})| &\leq \ell\ell'(C' + D)a^{-Lv}(a^0 + 1)(a^v + 1)\cdots(a^{kv} + 1) \\ &\leq \ell\ell'(C' + D)2^{k+1}a^{v(k(k+1)/2-L)}, \end{aligned}$$

where ℓ' is the smallest positive integer such that $\ell' A \in \mathbb{Z}$ (clearly ℓ' is independent of L, M).

Since ℓ, ℓ', C', D, k are all constants independent of L, M, we can choose L large enough so that the RHS is strictly less than 1, and then choose any $M \geq L + k + 2dk$. But then $|U(T)(\ell\ell' Ax_{i+uv})| \in \mathbb{Z}$ must in fact be zero, so there exists a polynomial $G \in \mathbb{Q}[x]$ of degree k (corresponding to a linear recurrence in $a^0, a^v, \ldots, a^{kv}$) such that $x_{u+iv} = G(a^{iv})$ for $i \in [L, M-k]$. Finally, if we take $g(x) = G(xa^{-u}) \in \mathbb{Q}[x]$, then $x_n = g(a^n)$ for $M - k - L + 1 \geq 2dk + 1$ values of n, whence $f(g(x)) - f(x)^k$ (which has degree $\leq dk$ yet vanishes for at least $2dk + 1$ values of x) must be identically zero, as desired.

Note. This is also true for integers $a \leq -2$, as we can just restrict ourselves to even n.

This also generalizes easily to the more natural statement: Fix two positive integers $a, k \geq 2$, and let $f, p \in \mathbb{Z}[x]$ be two nonconstant polynomials. Suppose that for all sufficiently large positive integers n, there exists a rational number x satisfying $f(x) = p(a^n)^k$. Prove that there exists a polynomial $g \in \mathbb{Q}[x]$ such that $f(g(x)) = p(x)^k$ for all real x.

21. Let n be an integer greater than 2, and $P_1, P_2, \ldots, P_n$ distinct points in the plane. Let $\mathcal{S}$ denote the union of all segments $P_1P_2, P_2P_3, \ldots, P_{n-1}P_n$. Determine if it is always possible to find points A and B in $\mathcal{S}$ such that $P_1P_n \parallel AB$ (segment AB can lie on line P_1P_n) and $P_1P_n = kAB$, where (1) $k = 2.5$; (2) $k = 3$.

Solution. If $k \geq 0$, this is always possible iff k is a nonnegative integer. If $k \leq 1$, this is all obvious; from now on, suppose that $k > 1$.

First suppose $k \notin \mathbb{Z}$, and let $m = \lceil k \rceil \geq 2$ so that $m - 1 < k < m$. For $1 \leq i \leq m - 1$, we take

$$\begin{aligned} &P_{8i-7} = (m(i-1), 0), P_{8i-6} = (m(i-1), m-i), P_{8i-5} = ((m-1)i, m-i), P_{8i-4} = ((m-1)i, 0), \\ &P_{8i-3} = ((m-1)i, 0), P_{8i-2} = ((m-1)i, -i), P_{8i-1} = (mi, -i), P_{8i} = (mi, 0), \end{aligned}$$

where the fact that $m(i-1) < (m-1)i < mi$ ensures that S is a simple curve (although the problem does not stipulate this, it's convenient for the construction). It's easy to see that $P_1 = (0, 0)$, $P_n = (m(m-1), 0)$, and the resulting figure S is symmetric about $(m(m-1)/2, 0)$.

Hence if we go by contradiction (i.e. assume we can find A, B such that $AB \in (m-1, m)$), we can WLOG work with A, B on or above the x-axis. Note that the region of S above the x-axis is a sequence of $m - 1$ disjoint squares (bottom sides missing) with decreasing height (from left to right), so we can assume that A lies on the i^{th} square and B lies on the j^{th}, where $1 \leq i < j \leq k - 1$. Since A, B have the same y-coordinate, the x-coordinate of A is either $m(i-1)$ or $(m-1)i$, and the x-coordinate of B lies in the closed interval $[m(j-1), (m-1)j]$. If $A_x = m(i-1)$, then $AB \geq m(j-1) - m(i-1) \geq m$, contradiction, so

$$A_x = (m-1)i \implies AB \in [m(j-1) - (m-1)i, (m-1)(j-i)].$$

But if $j = i + 1$, then $AB \leq m - 1$, and if $j \geq i + 2$, then $m(j-1) - (m-1)i \geq m(i+1) - (m-1)i = m + i \geq m$, contradiction.

It remains to show that when $k \geq 2$ is an integer, there exist $A, B \in S$ such that $P_1P_n = kAB$. Suppose otherwise; WLOG set $P_1 = (0, 0)$ and $P_n = (k, 0)$. For any curve C (possibly a point) and real r, let $C^{(r)} = C + (r, 0)$. By assumption, $C^{(r)}$ and $C^{(r+1)}$ are disjoint for all r. The key idea is to define "left/right" properly: take indices M and m such that the y-coordinates of P_M and P_m are maximal and minimal, respectively, and $|M - m|$ is as small as possible; WLOG $m < M$, and J is the region bounded by the two horizontal lines through P_M, P_m (inclusive); note that $y = 0$ lies in J. Let T denote the broken line $P_m P_{m+1} \dots P_M$, the exterior E be the set of points $X \neq P_M \in J$ such that there exists a continuous path from P_M to X intersecting T only at the beginning (at P_M), and the interior $I = J \setminus E$. Define the left L of T as the set of points $X \in J$ such that there exists a continuous path from $(-\infty, 0)$ to X that stays in J and never meets T; define the right R analogously (note that the points in I are in neither L nor R). Clearly $E = L \cup R$.

If $S^{(1)}$ intersects both I and E, then $S^{(1)}$ clearly hits T, contradiction, and if $S^{(1)}$ lies entirely in I, then the uppermost y-coordinate in $S^{(1)}$ is strictly less than that of I (since $S^{(1)}$ does not intersect T), contradicting the fact that $P_M^{(1)} \in S^{(1)}$. Hence $S^{(1)}$ lies entirely in either L or R (since $S^{(1)}$ never leaves J and never hits T). But it's not hard to show that $P_M^{(1)} \in R$, so $S^{(1)}$ lies entirely in R. In particular, $I^{(1)} \subset R$, so $R^{(1)} \subset R$ by the continuity of $I^{(1)}$ and R (in other words, a path staying in J from $(\infty, 0)$ to some $X \in R^{(1)}$ cannot meet I without first hitting $I^{(1)}$, since I and $I^{(1)}$ are disjoint). Hence $S^{(2)} \subset R^{(1)} \subset R$; by a simple induction, $S^{(i)}$ lies entirely in R for $i \geq 1$, and by symmetry, $S^{(-i)}$ lies entirely in L for $i \geq 1$. Thus $P_1^{(k-1)} \in R$ (recall that $k \geq 2$) and $P_n^{(-1)} \in L$, contradicting the fact that $P_1^{(k-1)} = P_n^{(-1)}$ and $L \cap R = \emptyset$.

22. In an acute-angled ABC, $\angle A > 60^\circ$, H is its orthocenter. M, N are two points on AB, AC respectively, such that $\angle HMB = \angle HNC = 60^\circ$. Let O be the circumcenter of triangle HMN. D is a point on the same side with A of BC such that $\triangle DBC$ is an equilateral triangle. Prove that H, O, D are collinear.

    Solution. The idea is duality/symmetry (helps to think of how one might prove it using complex numbers; then note that orientation almost certainly doesn't matter), or also cyclic quads/spiral similarity. We can also think of this as making everything completely symmetric to bring out patterns more easily. Let X, Y, Z be the feet of the altitudes, M' reflection of M over Z, N' reflection of N over Y, D' reflection of D over BC.

    First by standard spiral similarity results, $\triangle HM'N \sim \triangle HZY \sim \triangle HMN'$ (all same orientation), which are in turn similar to $\triangle HBC$ (opposite). It's then natural (using SAS similarity) to establish using rotation ($\triangle DCH$ toward CB) that $\triangle DHC \sim \triangle MNN'$ (opposite), so $\angle DHC = \angle MNN' = \angle MNH + 60^\circ = 150^\circ - \angle MHO = \angle OHC$, and we're done.

    Note that we have $\triangle D'HC \sim \triangle M'N'N$ as well, proven the same way, confirming our intuition at the beginning that the counterpart is also true by duality.

23. (China 2012) In some squares of a 2012×2012 grid there are some beetles, such that no square contain more than one beetle. At one moment, all the beetles fly off the grid and then land on the grid again, also satisfying the condition that there is at most one beetle standing in each square. The vector from the center of the square from which a beetle B flies to the center of the square on which it lands is called the translation vector of beetle B. For all possible starting and ending configurations, find the maximum length of the sum of the translation vectors of all beetles.

    Solution. Orient the grid in the lattice plane so that its center C is at $(0, 0)$ and the vertices are at $(\pm 1006, \pm 1006)$.

    If a beetle lies at (x, y) then we assign it the vector $\langle x, y \rangle$. Let H be the set of heads and T the set of tails; we want $\sum H - \sum T = \vec{V} = \langle X, Y \rangle$ as our final vector sum. We now make some simplifications, supposing our $|V|$ is maximal. First take out any overlaps in H and T. Suppose there are blank squares; since there is an even number of squares we have an even number of blank squares left, so consider two of them at a, b. But then $|V + b - a| + |V + a - b| \geq 2|V|$, so we can assume that all the squares are full (in fact this must be the case, but it doesn't matter since we only care about the maximum value itself). Now suppose we have $h \in H$ and $t \in T$; swapping h, t must have $|V - 2(h - t)| \leq |V|$, or equivalently, $|h - t|^2 \leq V \cdot (h - t)$, which means $V \cdot h > V \cdot t$. By our choice of C, there are p, q, p squares x with $V \cdot x$ positive, zero, and negative, respectively, for some $p, q \geq 0$. If there's a negative $V \cdot h$, then there must be a nonnegative $V \cdot t$, contradiction; similarly there's no positive $V \cdot t$. Thus the

q zeros are divided evenly among the $V \cdot h$'s and $V \cdot t$'s, so if $q > 0$ we get a contradiction; thus $q = 0$. Now draw the line perpendicular to CV; it must not hit any centers of the squares, and it divides the grid into two sides, one of all h's and one of all t's. Suppose the line intersects the top and bottom edges but not the left and right edges (note that the line can't pass through two opposite corners since $q = 0$). Further suppose it has positive slope; then suppose there are $1006 + x_i$ guys to the left of the i^{th} row for $1 \le i \le 1006$; by symmetry, the i^{th} row from the bottom has $1006 - x_i$ guys. It's easy to compute $|X| = \sum_{i=1}^{1006}(1006^2 - x_i^2)$ and $|Y| = \sum_{i=1}^{1006}(2i-1)x_{1007-i}$. We have $0 \le x_i \le 1006$ for each i; let $y_i = 1006x_{1007-i}$ $(0 \le y_i \le 1)$; then we need to show $n^2(\sum_{i=1}^{n}(1-y_i^2))^2 + (\sum_{i=1}^{n}(2i-1)y_i)^2 \le n^4$.

We'll generalize this to show that for all $x \in [0,1]^n$ and positive integers $n \ge 1$, $f = n^2(\sum_{i=1}^{n}(1 - x_i^2))^2 + (\sum_{i=1}^{n}(2i-1)x_i)^2 \le n^4$, where the base case $n = 1$ is obvious. We'll use the extreme value theorem of Karl Weierstrass, which states that every continuous real-valued function on a nonempty compact space attains a finite global maximum. Take some x that attains this maximum; obviously we have $0 \le x_1 \le \cdots \le x_n \le 1$ (note that $x_1^2 + \cdots + x_n^2$ stays fixed upon permutation of the x_i).

Consider some $1 \le i < j \le n$; then for fixed $x_i^2 + x_j^2 = k$, $(2i-1)x_i + (2j-1)x_j$ must be maximal. Note that $((2i-1)^2 + (2j-1)^2)k = ((2i-1)x_i + (2j-1)x_j)^2 + ((2j-1)x_i - (2i-1)x_j)^2$. If $\sqrt{k}(2j-1)/\sqrt{(2i-1)^2 + (2j-1)^2} \le 1$, then we must have $(2j-1)x_i - (2i-1)x_j$. Otherwise, this means $(2j-1)x_i - (2i-1)x_j > 0$, or else $x_j > 1$. (Note that we must have $k > 1$.) Thus the minimum of $((2j-1)x_i - (2i-1)x_j)^2$ occurs when $(2j-1)x_i - (2i-1)x_j$ is minimized. The latter is strictly increasing in x_i, however, so either $x_i = 0$ or $x_j = 1$ (since $x_i \le x_j$, or else swapping will increase $(2i-1)x_i + (2j-1)x_j$). If $x_i = 0$, then $1 < k \le x_j^2 \le 1$, contradiction, so $x_j = 1$ and $x_i = \sqrt{k-1}$.

If $x_1 = 1$, then $x_i = 1$ for all i and $f = n^4$, so suppose $x_1 < 1$. Then there exists $1 \le \ell \le n$ and $0 \le \lambda < 1/(2\ell-1)$ such that $x_i = \lambda(2i-1)$ for $1 \le i \le \ell$ and $x_i = 1$ for $\ell < i \le n$. It remains to show that

$$n^2(\sum_{i=1}^{\ell} 1 - \lambda^2(2i-1)^2)^2 + (\sum_{i=1}^{\ell} \lambda(2i-1)^2 + \sum_{i=\ell+1}^{n}(2i-1))^2 \le n^4,$$

or equivalently,

$$n^2(\ell - \lambda^2\ell(4\ell^2-1)/3)^2 + (\lambda\ell(4\ell^2-1)/3 + (n^2-\ell^2))^2 \le n^4.$$

The key is to note that this is equivalent to

$$n^2(\ell - \lambda^2\ell(4\ell^2-1)/3)^2 \le (\ell^2 - \lambda\ell(4\ell^2-1)/3)(2n^2 - \ell^2 + \lambda\ell(4\ell^2-1)/3).$$

Of course, $\ell^2 - \lambda\ell(4\ell^2-1)/3 \le n^2 < 2n^2$ and $\ell^2 - \lambda\ell(4\ell^2-1)/3 > \ell^2 - \ell(2\ell+1)/(3(2\ell-1)) \ge \ell^2 - \ell \ge 0$, so dividing both sides by n^2, it suffices to prove the inequality for $n = \ell$. Using DOS again, we rearrange this as

$$4n^2 - 1 \le 3n^2(2 - \lambda^2(4n^2-1)/3).$$

It suffices to prove this when $\lambda = 1/(2n-1)$, but this is just $4n^2 - 1 \le 6n^2 - n^2(2n+1)/(2n-1)$, or $(n-1)(2n^2 - n + 1) \ge 0$, so we're done.

In fact, when $x_n = 1$, we can use direct induction on the original inequality (when $\ell = n$, the other inequality is much easier to prove). Indeed, let $S = \sum_{i=1}^{n-1}(2i-1)x_i$; then it boils down to

$$\frac{n^2}{(n-1)^2}((n-1)^4 - S^2) + (S + (2n-1))^2 \le n^4,$$

where $0 \le S \le (n-1)^2$. By DOS, rearrange as

$$\frac{n^2}{(n-1)^2}((n-1)^2 - S)((n-1)^2 + S) \le ((n-1)^2 - S)(n^2 + 2n - 1 + S),$$

which is trivial if $S = (n-1)^2$; if $S < (n-1)^2$, then it boils down to $S \le (n-1)^2$ again, so we're done.

Comment. There's a much cleaner solution using induction in a more geometrically symmetric way: consider the inner $2(n-1) \times 2(n-1)$ grid; for the border we get $(2n-1)(2n-2) + x_1(2n-x_1) + (2n-x_1)x_1$

for x-coordinate and $(2n-1)(-x_1)+(2n-1)(2n-x_1)$ for y-coordinate. Let $t=(n-x_1)^2$ and observe that the resulting square magnitude of the vector is convex (positive quadratic) and thus maximized (we just have to be careful about the vertex, but the constant term is big enough) at boundary of t, which is either $x_1=0,2n$ or $x_1=n$. Anyway it's easy now by the triangle inequality.

24. Show that $x^x+y^y \geq x^y+y^x$ for positive reals x, y.

    Solution. If $x=y$, this is trivial, so suppose WLOG that $x>y>0$.

    If $x \geq 1$, then $x^x+y^y \geq x^y+y^x \iff x^y(x^{x-y}-1) \geq y^y(y^{x-y}-1)$ follows from the facts that $x^y \geq y^y$, $x^{x-y}-1 \geq y^{x-y}-1$, and $x^{x-y}-1 \geq 0$ (note that if $y<1$, the RHS is negative and the LHS is nonnegative).

    Otherwise, we must have $1>x>y>0$, so

    $$x^x+y^y \geq x^y+y^x \iff x^x-y^x \geq x^y-y^y \iff \int_y^x xt^{x-1}\,dt \geq \int_y^x yt^{y-1}\,dt,$$

    whence it's enough to show that $xt^{x-1} \geq yt^{y-1}$ for $y \leq t \leq x$, or equivalently, that $t^{x-y} \geq y/x$. Because $x-y>0$, the LHS is increasing in t and it suffices to show that $y^{x-y} \geq y/x$, or $x \geq y^{1-x+y}$. But $y-1>-1$ and $1-x+y=1-(x-y) \in (0,1]$, so by Bernoulli's inequality,

    $$y^{1-x+y}=(1+(y-1))^{1-x+y} \leq 1+(1-x+y)(y-1)=x+y^2-xy \leq x,$$

    as desired.

25. A piece begins at the origin of the coordinate plane. Two players, A and B, play the following game. In A's turn, A marks a lattice point in the first quadrant that the piece is not on. In B's turn, B moves the piece up to k times, where a move is defined as moving the piece from (x,y) to $(x+1,y)$ or $(x,y+1)$, as long as the lattice point that the piece moves onto is not marked. They then proceed to alternate turns, with A playing first. If B cannot move the piece, A wins. For what values of k can A win?

    Solution. This is a special case of Conway's Angel problem for which A (the devil) can always win.

    The idea is to reduce solution sets, where ultimately we'll need B to be at (x,y) while $(x+1,y)$ and $(x,y+1)$ are both unavailable. The "most obvious" way to guarantee this, i.e. to make sure that when B is at some (x,y), all of the $(x+i,y+j)$ are unavailable for $i,j \geq 0$ and $i+j=r$ (some $r \geq 1$), does not directly work if we try to get consecutive things on some fixed line $x+y=T$.

    The next dumbest thing, however, does work: we want to gradually narrow down the choices on this fixed line $x+y=T$ (call this L) depending on the remaining possible locations of B (note that if B is at (x,y), then it can only go to (x',y') later with $x' \geq x$ and $y' \geq y$). Hence we'll want to do this iteratively, checking at certain points where B is and letting A mark the remaining possible points between consecutive checks. The most natural way to do this is uniformly; for example, if we have m moves before the first check, then B can move up to the line $x+y=mk$ but no further, and we'll let A mark things at $(x,y) \in L$ with $x \equiv 0 \pmod{\lceil T/m \rceil}$. The idea is that we'll want to do $\lceil T/m \rceil$ checks to make sure B cannot get past L. Of course, if m is too small, our checking gets little done, and if m is too large, B will pass L before we even finish checking once (for instance, we need $m \leq T/k$ for the first time).

    Let $M=\lceil T/m \rceil$ and suppose that B is at $x_i+y_i=r_i$ at the i^{th} checkpoint ($i \geq 0$) and A responds by making $m_i \leq 2+(T-r_i)/M$ marks at the positions $(x,y) \in L$ with $x \equiv i \pmod M$ and $x \geq x_i$, $y \geq y_i$. Now suppose for contradiction that $r_n \geq T$ for n minimal; since we must not have finished marking all residues $\pmod M$ in order for B to have passed L between the $(n-1)^{th}$ and n^{th} checkpoints, we have $1 \leq n \leq M$ (otherwise, everything would've been marked between the 0^{th} and M^{th} checkpoints before B passed L). Since $r_i-r_{i-1} \leq km_{i-1} \leq 2k+k(T-r_{i-1})/M$ for $i \geq 1$ (note that $r_0=0$), this means that $r_{n-1}+2k+k(T-r_{n-1})/M \geq r_n \geq T$. Setting $c=k/M$ (let's choose M and T large enough so that $0<c<1$), we get $r_{n-1} \geq T-\frac{2k}{1-c}$, and by a simple induction with geometric series we get $0=r_0 \geq T-2k((1-c)^{-n}+\cdots+(1-c)^{-1})$, so fixing some $0<c<1$ and taking T sufficiently large, we get a contradiction.

26. (Aaron Pixton, MOP 2012) Let $n \geq 2$ be a positive integer; find the number $f(n)$ of $n \times n$ matrices of 0's and 1's with each row-sum and column-sum equal to 2. (http://oeis.org/A001499)

    Solution. One way is to view the rows as $\{1, 1, 2, 2, \ldots, n, n\}$ so that we want to pair these numbers with $1, 1, 2, 2, \ldots, n, n$ such that there are no double occurences of (i, j). Let $h(n) = 2^n f(n)$, so we have that "order" matters, i.e. $\{(i, j), (i, k)\}$ is not the same as $\{(i, k), (i, j)\}$. Then counting the number of "double fixed" points, we have
    $$\frac{(2n)!}{2^n} = \sum_{k=0}^{n} h(n-k)\binom{n}{k}^2 k!,$$
    from which we easily get the generating function (let $g(n) = f(n)/n!^2$)
    $$\sum_{n\geq 0} g(n)x^n = e^{-x/2}(1-x)^{-1/2}.$$
    As it turns out, the asymptotic formula is $(n!)^2/\sqrt{\pi e}\sqrt{n}$, and there is some connection to derangements.

    Another way is to look at cycles, where if for some $r \geq 2$ we have $(i_1, \ldots, i_r)$ and $(j_1, \ldots, j_r)$, we have the cycle $(i_1, j_1) \to (i_1, j_2) \to (i_2, j_2) \to \cdots$. WLOG assuming i_1 represents the smallest row remaining (if we want to recurse), this gets us (note that there are two ways to traverse a cycle, forward and backward)
    $$f(n) = \sum_{r=2}^{n} [\binom{n-1}{r-1}(r-1)!][\binom{n}{r}r!](1/2)f(n-r),$$
    or equivalently,
    $$g(n) = \frac{1}{2n}\sum_{k=0}^{n-2} g(k).$$
    Of course, we can rewrite this as $g(n+1)(2(n+1)) = g(n-1) + 2ng(n)$, and prove by induction that $g(n) \geq 1/4\sqrt{n}$ for $n \geq 2$.

27. If $a_1 \leq \cdots \leq a_n$ are positive integers such that $1/a_1 + \cdots + 1/a_n < 1$, show that $1/a_1 + \cdots + 1/a_n \leq 1/u_1 + \cdots + 1/u_n$, where $u_1 = 2$ and $u_{i+1} = u_i^2 - u_i + 1$ for $i \geq 1$.

    Solution. The idea is to induct and use the powerful identity $1/u_1 + \cdots + 1/u_n = 1 - 1/(u_1 \cdots u_n)$. Indeed, the base case $n = 1$ is obvious, and if we assume the result is true up to $n - 1$ for some $n \geq 2$, then going by contradiction, we have
    $$1 - \frac{1}{u_1 \cdots u_n} = \sum_{i=1}^{n} \frac{1}{u_i} < \sum_{i=1}^{n} \frac{1}{a_i} \leq 1 - \frac{1}{a_1 \cdots a_n},$$
    since $1/a_1 + \cdots + 1/a_n < 1$. But then setting $b_i = 1/a_i$ and $v_i = 1/u_i$, we have $b_1 \geq \cdots \geq b_n$, $v_1 \geq \cdots \geq v_n$, $v_1 + \cdots + v_m \geq b_1 + \cdots \geq b_m$ for $1 \leq m \leq n-1$, $v_1 + \cdots + v_n < b_1 + \cdots + b_n$, and $v_1 \cdots v_n > b_1 \cdots b_n$. But $\log x$ is concave, so letting $(w_1, w_2, \ldots, w_n) = (b_1 + \cdots + b_n - (v_2 + \cdots + v_n), v_2, \ldots, v_n)$ so that w majorizes b, we get
    $$w_1 \cdots w_n > v_1 \cdots v_n > b_1 \cdots b_n \geq w_1 \cdots w_n,$$
    contradiction.

28. (1999 C5, IMO 3) Let n be an even positive integer. We say that two different cells of a $n \times n$ board are neighboring if they have a common side. Find the minimal number of cells on the $n \times n$ board that must be marked so that any cell (marked or not marked) has a marked neighboring cell.

    Solution. Let $n = 2m$; after some small cases, we see the answer is $m(m+1)$.

    The dumb idea is to use the weak inequality $2c + 3e + 4i \geq 4m^2$, but this is insensitive to the fact that having too many things close to each other is bad, and we have issues around the borders. So we want to look at some trickier set of restrictions; looking at alternate odd-length black diagonals (chessboard), for instance, and noting that each white square covers at most 2 of them, we get the desired bound.

The more motivated way is to write out all the equations $a_{i-1,j} + a_{i+1,j} + a_{i,j-1} + a_{i,j+1} \geq 1$, where $1 \leq i, j \leq n$ and we extend $a_{i,j} = 0$ for $ij(n+1-i)(n+1-j) = 0$. We want to sum these over some subset S of squares so that each term $a_{i,j}$ ($1 \leq i, j \leq n$) appears the same number of times. Since corners have only two neighbors, we can either make this set 1- or 2-regular. After some small cases, we see that the easiest (probably only) way for 2-regularity is to take the "border", skip the next "layer", and alternate in this fashion. (This gets the desired bound.) Alternatively, we can get a 1-regular set from the class of good markings such that *every square has exactly one marked neighbor,* which is easy with some small cases.

29. (USAMO submission, 2002 from Gabriel Carroll MOP handout) Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that, for each n, $f(f(n))$ is the number of values of m such that $f(m) \leq n$. Prove that there are infinitely many values of n such that $f(f(n)) = n$.

    Solution. Observe that $f^2(m) = f^2(n) \implies f^3(m) = f^3(n)$ implies that $f(m) = f(n)$, so since $f^2(n)$ is nondecreasing, it's now easy to deduce the precise structure of f. Indeed, if $1 \leq x_1 < x_2 < x_3 < \cdots$ are the values such that $f(x) = f(x_i)$ for $x \in [x_i, x_{i+1})$, then it's not hard to show that the x_i form the range of $f(x)$ over all x (the only slightly different case is $x_1 = 1$, which is in the range since $f(f(1)) > 0$). Hence there exists a permutation π of the positive integers such that $f(x_i) = x_{\pi(i)}$ and $\pi^2(i)$ is increasing; but then $\pi^2(n) = n$ for all n, so $f^2(x_n) = x_n$ for all n, and we're done.

30. (MOP 2009) Prove that there exist infinitely many positive integers n such that every prime factor of $n^2 + 1$ is larger than $2009 \ln n$.

    Solution. Let $p_1 < \cdots < p_r$ be the first r primes (it will not make a significant difference to work only with primes 1 (mod 4)). By CRT, we can choose t_i such that $t_i \equiv 1 \pmod{p_i}$ and $t_i \equiv 0 \pmod{p_j}$ for $j \neq i$; then n of the form $\sum_{i=1}^{r} \epsilon_i t_i \pmod{p_1 \cdots p_r}$ have smallest prime divisor of $n^2 + 1$ at least p_{r+1}, as long as $\epsilon_k \not\equiv \pm i_{p_k} \pmod{p_k}$ for every k. On the other hand, for every odd prime p_k we can choose a set A_k (more precisely, an arithmetic progression) of size $(p-1)/2$ such that $A_k - A_k$ contains everything except $\pm i_{p_k} \pmod{p_k}$. (For p_1, just take $A_1 = \{0\}$.) By a simple pigeonhole argument, we can get $0 < n < \prod_{i=1}^{r} p_i/|A_i| < c^r$ for some $c > 1$, which works unless $p_{r+1} \leq 2009 \ln n = 2009 r \ln c$, which is false for sufficiently large r.

31. (IMO 2007) In a mathematical competition some competitors are friends. Friendship is always mutual. Call a group of competitors a clique if each two of them are friends. (In particular, any group of fewer than two competitiors is a clique.) The number of members of a clique is called its size.

    Given that, in this competition, the largest size of a clique is even, prove that the competitors can be arranged into two rooms such that the largest size of a clique contained in one room is the same as the largest size of a clique contained in the other room.

    Solution. Let $c(H)$ denote the clique number of a graph H.

    Suppose $c(G) = 2k$ and take a partition $G = A \cup B$ with $|c(A) - c(B)|$ minimal.

    Now let $r = c(A)$ and $s = c(B)$ and assume for the sake of contradiction that $r \neq s$; WLOG suppose that $r > s$ and $|A|$ is minimal, i.e. there doesn't exist a partition $G = X \cup Y$ with $|X| < |A|$, $r = c(X)$, and $s = c(Y)$.

    Fix some r-clique $\alpha \subseteq A$ and a vertex $v \in \alpha$. If $A' = A \setminus \{v\}$ and $B' = B \cup \{v\}$, then $c(A') \in \{r-1, r\}$ (because $\alpha \setminus \{v\}$ remains in A') and $c(B') \in \{s+1, s\}$ (or else B contains some K_{s+1}).

    By the minimality of $|A|$, we have $|c(A') - c(B')| \in \{|r-s-1|, |r-s-2|\}$, whence $r = s+1$, $|c(A') - c(B')| = |r-s-2|$ by the minimality of $r - s$. But then $c(A') = r-1$ and $c(B') = s+1$, so v must belong to every $K_r \subseteq A$ and there must exist a nonempty set $f(v)$ of s-cliques $\beta \subseteq B \cap N(v)$. Thus α is in fact the unique r-clique in A and $f(v)$ is nonempty for every $v \in \alpha$. (*)

    On the other hand, suppose there exists $v \in A \setminus \alpha$, and define A', B' as before. Then $c(A') = r$ since $v \notin \alpha$ and $c(B') \in \{s+1, s\}$, so by the minimality of $|A|$ we have $c(B') = s+1 \implies |c(A') - c(B')| = 0$, contradiction. Hence $A = \alpha$.

    Now fix a vertex $v \in A = \alpha$ and let $T(v) \subseteq B$ be a subset of G with $|T(v)|$ minimal such that $U(v) = T(v) \cup (A \setminus \{v\})$ contains a K_r (such a subset exists because $|A| \geq 2$ and for any $w \in A \setminus \{v\}$

and $\beta \in f(w) \neq \emptyset$, $w \cup \beta$ is a K_r). Since $|A \setminus \{v\}| = r - 1$, we clearly must have $|T(v)| > 0$; by minimality, $T(v)$ is a complete graph. Further suppose WLOG that $|T(v)|$ is minimal over all $v \in A$.

Case 1: There exists $\beta \in f(v)$ such that $T(v) \cap \beta = \emptyset$. Let A', B' be the sets obtained by swapping v and $T(v)$; then $c(A') = r$ by the definition of $T(v)$ and $c(B') = s + 1 = r$ by the definition of $f(v)$, contradiction.

Case 2: There exists $t \in T(v)$ such that $T'(v) \cap \beta \neq \emptyset$ for every $\beta \in f(v)$, where $T'(v) = T(v) \setminus \{t\}$. Let A', B' be the sets obtained by swapping v and $T'(v)$; by the minimality of $T(v)$, we have $c(A') = r - 1$, but because $T'(v)$ contains something from every β, we also have $c(B') = (s - 1) + 1 = s = r - 1$, contradiction.

Case 3: $T(v) \cap \beta \neq \emptyset$ for every $\beta \in f(v)$ but for every $t \in T(v)$, there exists a $\beta \in f(v)$ such that $t \in \beta$ but $t' \notin \beta$ for $t' \in T(v) \setminus \{t\}$. If $|T(v)| \geq 2$, then there exists $w \in A \setminus \{v\}$ such that $U(v) \setminus \{w\}$ contains a K_r, so $T(v) \subseteq N(v) \implies |T(w)| \leq |T(v)| - 1$, contradiction. Hence $|T(v)| = 1$, so...

Comments after fakesolving and reading Solution. this clearly is a dead end, however if we started with $A = K_{2k}$ and moved downward until $|A| = |B| + 1$, then this might be feasible; indeed, $T(v)$ can be any of $2k - r$ vertices part of some fixed K_{2k} containing A, so it's easy to show that if $t \notin \beta$ for some $\beta \subseteq f(v)$ then we can swap v and t to get a contradiction. but then if we move v to B (increasing clique number to $s + 1$) and just start removing stuff from the β's until clique number becomes s again (note clique number decreases by at most one at any point), then we cannot add new stuff to A's clique number or else we would get a larger maximum clique of G; this is useful since maximum clique of $2k$ is a global restriction while previous approach would at best give a local restriction using this method

key idea is that moving things doesn't change much about clique numbers, *especially* in certain cases, which we can utilize effectively using a maximal clique (not necessarily maximum, or maybe?)

analyze what i could've changed about my thought process to keep it simpler/ think it through more efficiently, since i wasn't really that far off

32. Let p be an odd prime. Determine the positive integers $x \leq y$ for which $\sqrt{2p} - \sqrt{x} - \sqrt{y}$ attains its minimum nonnegative value.

    Solution. In other words, maximize $x + y + 2\sqrt{xy}$ given that it's less than $2p$ (it clearly cannot equal $2p$). If $r = 1 + \lfloor 2\sqrt{xy} \rfloor$, then $r^2 \geq 4xy + 1$, $x + y \geq r \implies r \leq p$ (note $2p - x - y \geq r$), so by a simple computation we get that the minimum occurs when $r = p$ and $x = (p-1)/2$, $y = (p+1)/2$.

33. Find all $f : \mathbb{Q}^+ \to \mathbb{Q}^+$ such that $f(x) + f(1/x) = 1$ and $f(2x + 1) = f(x)/2$ for all x.

    Solution. If $g(x) = (x + 1)f(x)$, then we find $g(1) = 1$, $g(2x + 1) = g(x)$, and

    $$g(x) + xg(1/x) = x + 1 \implies g(1/x) = (x + 1 - g(x))/x$$

    for $x > 0$. Now consider induction on $p + q \geq 2$ where $\gcd(p, q) = 1$ and we want to show $g(p/q) = 1$. If $p > q$ and p, q have the same parity, then $g(p/q) = g((p - q)/2q)$ means that we can finish by induction (then $g(p/q) = 1$ means $g(q/p) = 1$ as well). On the other hand, if p, q are of opposite parity, then consider the operation taking $p/q \to q/p$ if $p < q$ and $p/q \to (p - q)/2q$ if $p > q$; as this operation preserves the sum of reduced numerator and denominator, which must be of opposite parity, this is reversible (for $x < 1$ with odd numerator and even denominator, we reverse to $2x + 1$, for $x > 1$ with odd denominator and even numerator, we reverse to $1/x$, and for $x > 1$ with even denominator and odd numerator, we reverse to $2x + 1$). Observe that this reversal is well-defined since if we start with $p > q$, we can never get to an $x < 1$ with odd denominator and even numerator. There are finitely many guys of fixed sum $p + q$, so as we cycle through equal g values (it might only change at $x \to 1/x$ locations), we have $x_1, \ldots, x_\ell > 1$ such that $g(x_i) = g(1/x_{i+1}) = (x_{i+1} + 1 - g(x_{i+1}))/x_{i+1}$ for $1 \leq i \leq \ell$. As $x_1 \cdots x_\ell > 1$, a solution to this system must be unique. But $g(x_i) = 1$ for all i is such a solution, so it must be the only solution. In particular, $g(p/q) = 1$ for any starting seed $p/q > 1$. But then $g(q/p) = 1$, so we're done.

34. Show that $l_b(n!) \geq \lfloor \log_b(n + 1) \rfloor$, where $l_b(n!)$ denotes the number of nonzero digits of $n!$ in base b.

    Solution. Let $m = \lfloor \log_b(n + 1) \rfloor$ so that $b^m - 1 \mid n!$. Then since the sum of digits is sub-additive, we have $s_b(n!) \geq (b - 1)m$, whence the result.

35. (Evan O'Dorney, ESL 2011) If $a+b+c=a^n+b^n+c^n=0$ for some positive integer n and complex a,b,c, show that two of a,b,c have the same magnitude.

    Solution. First get rid of nontrivial zero cases and stuff. Now if (by scaling) $abc=1$ and $x=-(ab+bc+ca)$, then $P_n(x)=xP_{n-2}(x)+P_{n-3}(x)$ with initial conditions $P_0=3$, $P_1=0$, $P_2=2x$. We want to show $P_n(x)$ has real roots times a third root of unity, modulo trivial cases.

    We first take out the 0 roots and do $x^3\to x$ to get new polynomials satisfying $Q_n=xQ_{n-2}+Q_{n-3}$ whenever $3\mid n$ and $Q_n=Q_{n-2}+Q_{n-3}$ otherwise (starting with $3,0,2$). We induct in groups of six to show that for all $m\ge 1$, the degrees for $Q_{6m},Q_{6m+2},\ldots,Q_{6m+5}$ are m and Q_{6m+1} has degree $m-1$, and ordering the roots from least to greatest (coefficients are all positive, so roots are clearly all negative), we have

    $$-\infty<r_{6m+2,1}<r_{6m,1}<r_{6m+1,1}<r_{6m+2,2}<\cdots<r_{6m+1,m-1}<r_{6m+2,m}<r_{6m,m}<0$$

    and

    $$-\infty<r_{6m+4,1}<r_{6m+5,1}<r_{6m+3,1}<r_{6m+4,2}<\cdots<r_{6m+3,m-1}<r_{6m+4,m}<r_{6m+5,m}<r_{6m+3,m}<0.$$

    For the first induction case, use IVT first for $6m+3,6m+4$ to get

    $$\begin{aligned}-\infty&<r_{6m+4,1}<r_{6m+2,1}<r_{6m,1}<r_{6m+3,1}<r_{6m+1,1}<r_{6m+4,2}<r_{6m+2,2}\\&<\cdots<r_{6m+1,m-1}<r_{6m+4,m}<r_{6m+2,m}<r_{6m,m}<r_{6m+3,m}<0.\end{aligned}$$

    Now we use $Q_{6m+5}=Q_{6m+3}+Q_{6m+2}$ to get $r_{6m+2,i}<r_{6m+5,i}<r_{6m+3,i}$ for all i, so

    $$\begin{aligned}-\infty&<r_{6m+4,1}<r_{6m+2,1}<r_{6m+5,1}<r_{6m+3,1}<r_{6m+1,1}<r_{6m+4,2}<r_{6m+2,2}\\&<\cdots<r_{6m+1,m-1}<r_{6m+4,m}<r_{6m+2,m}<r_{6m+5,m}<r_{6m+3,m}<0.\end{aligned}$$

    For the second induction case, use IVT first for $6m+6,6m+7$ to get

    $$\begin{aligned}-\infty&<r_{6m+6,1}<r_{6m+4,1}<r_{6m+7,1}<r_{6m+5,1}<r_{6m+3,1}<r_{6m+6,2}<r_{6m+4,2}\\&<\cdots<r_{6m+3,m-1}<r_{6m+6,m}<r_{6m+4,m}<r_{6m+7,m}<r_{6m+5,m}<r_{6m+3,m}<r_{6m+6,m+1}<0.\end{aligned}$$

    Now we use $Q_{6m+8}=Q_{6m+6}+Q_{6m+5}$ to get

    $$\begin{aligned}-\infty&<r_{6m+8,1}<r_{6m+6,1}<r_{6m+4,1}<r_{6m+7,1}<r_{6m+5,1}<r_{6m+8,2}<r_{6m+6,2}<r_{6m+4,2}\\&<\cdots<r_{6m+6,m}<r_{6m+4,m}<r_{6m+7,m}<r_{6m+5,m}<r_{6m+8,m+1}<r_{6m+6,m+1}<0,\end{aligned}$$

    completing the induction.

36. (MOP 1999) Given n points on the unit circle such that the product of the distances from any point on the circle to the given points does not exceed 2, prove that the points must be vertices of a regular n-gon.

    Solution. Discussion at AoPS and generalization at MO.

    One way is to sum over some suitable choice of roots of unity after scaling, using the triangle inequality. Another way to view this is by comparing to $g(x)=(x-1)(x-\omega)\cdots(x-\omega^{n-1})$, if $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ has $\alpha_1\cdots\alpha_n=1$. Then consider $\Re(g(x)-f(x))$, which must be greater than 0 at some vertices of regular polygon (arc midpoints of g's roots), which is a contradiction by summing over these special points.

    A dumb way to see this is by taking a_i to be the arguments of the vertices of f's roots, then set x as the varying argument; now if $t=\tan x/4$, $u_i=\cos a_i/2$, and $v_i=\sin a_i/2$, then we get a comparison between the new polynomial corresponding to f and the new polynomial corresponding to g (which will have to have the same leading coefficients), and use IVT and alternating root things to show that the modified polynomials (and thus originals) must be equal.

    This is a sort of analog of the Chebyshev polynomials problem of minimum deviation on $[-1,1]$.

37. (MOP 2007) Let a be a real number. Prove that $f(x) = x^{2n} + ax^{2n-1} + \cdots + ax + 1$ has at most 2 real roots and all nonreal roots on the unit circle.

    Solution. For the silly real zeros part, first write it as $z^{2n+1} + az^{2n} = az + 1$ and use Descartes rule of signs to show that there are at most 3 real roots (with multiplicity) in this modified polynomial and thus at most 2 in the original. Write $z = re^{i\theta}$ (for nonreal roots z); then to show that $|z| = 1$, it's enough to show $|\sin 2n\theta| < 2n|\sin\theta|$ if $\sin\theta \neq 0$, which can be proven a number of ways... (e.g. induction with sine addition formula).

    Alternatively, use the $x + 1/x$ trick and write in terms of Chebyshev polynomials (this is equivalent to the original solution, actually). Then use IVT by plugging in stuff to get $n - 1$ real roots to this modified equation, which translates to $2n - 2$ in the original.

38. (Descartes' rule of signs) Let $z(p)$ denote the number of positive zeros and $v(p)$ the number of sign changes; show that $z(p) \leq v(p)$ and $2 \mid z(p) - v(p)$.

    Solution. The parity part is easy, so we do the rest by induction.

    There are two clean ways of induction: one is first make sure the constant term is nonzero and then use Rolle's theorem to get $z(p') \geq z(p) - 1$ (there are two cases depending on whether the coefficients a_0, a_1 have opposite or same parity where a_1 is smallest nonzero coefficient after a_0).

    The other way is to show that $v((x - r)p(x)) \geq v(p(x))$ and then use the parity condition to finish by induction (r is a positive number).

39. (Putnam 2004) Let A be a set of positive integers and let $b_1 < b_2 < \cdots$ be the positive integers which can be written as a difference of two elements of A. If the sequences $b_{n+1} - b_n$ is unbounded, prove that A has density zero.

    Solution. In other words, we have arbitrarily long strings of unobtainable differences. Thus we can construct an increasing sequence of integers $0 = x_0 < x_1 < \cdots$ such that for every r, the sets $A + x_i$ are pairwise disjoint for $i \in [0, r]$. Indeed, the base case $r = 0$ is obvious, and once we find $x_1, \ldots, x_r$ for some $r \geq 0$, we just need to find $x_{r+1} > x_r$ such that $A + x_i \cap A + x_{r+1} = \emptyset$ for every $i \in [0, r]$, or equivalently, $A \cap A + x_{r+1} - x_i = \emptyset$, which is easy to find through any large sequence of $x_r + 5$ consecutive unobtainable differences.

    Taking r arbitrarily large shows that A has zero density.

40. (Miklos) Let f, g be two polynomials with real coefficients such that $f(\mathbb{Q}) = g(\mathbb{Q})$. Prove that there exist rational numbers a, b such that $f(x) = g(ax + b)$ for all x.

    Solution. Take a rational basis over the coefficients of f, g so that we can individually consider polynomials $f_i, g_i \in \mathbb{Q}[x]$ for $i \in [1, n]$ and then piece everything together. Indeed, if we show $f_i(x) = g_i(a_i x + b_i)$ for all x, i for some $a_i, b_i \in \mathbb{Q}$, then for every $x \in \mathbb{Q}$ there exists $t(x) \in \mathbb{Q}[x]$ such that $g_i(t(x)) = g_i(a_i x + b_i)$ for all i. By binomial expansion we can show via the rational root theorem that $|t(n)| = |a_i n + b_i|$ for all sufficiently large positive integers n. Hence there exist $a, b \in \mathbb{Q}$ such that $(a_i, b_i) = \pm(a, b)$ for every i, and WLOG $t(n) = an + b$ for infinitely many n. But then $f_i(x) = g_i(a_i x + b_i) = g_i(ax + b)$ for all i and x (nonzero polynomials have finitely many roots), as desired.

    So it's enough to solve the case in which $f, g \in \mathbb{Q}[x]$. But then we can define a sequence of rationals x_n with bounded denominators such that $f(x_n) = g(n)$ for every integer n; similarly define y_n. The rest is standard analytic fare: if $\deg g < \deg f$, for instance, we will eventually contradict the bounded denominators condition on x_n, so by symmetry $\deg f = \deg g$; now taking d^{th} roots of both sides and using Van der Waerden we're done.

41. (ISL 1990) Prove that every integer $k > 1$ has a multiple less than k^4 with at most four different digits.

    Solution. We can assume $k \geq 10^5$ or else the problem is obvious. Now consider all numbers with $\ell + 1$ digits, all in $\{0, 1\}$: it's enough to have $2^{\ell+1} \geq k$, where $\ell = \lfloor \log_{10} k^4 \rfloor - 1$; this is trivial.

42. (RMM 2010) Suppose $f \in \mathbb{Q}[x]$ has degree at least 2, and define the sets $f^0(\mathbb{Q}) = \mathbb{Q}$ and $f^n(\mathbb{Q}) = f(f^{n-1}(\mathbb{Q}))$. Show that $\cap_{n=0}^{\infty} f^n(\mathbb{Q})$ is a finite set.

    Solution. If some $a \in f^n(\mathbb{Q})$ for all $n \geq 0$, then by a simple induction there exists an infinite sequence $a_0 = a, a_1, a_2, \ldots$ such that $a_i = f(a_{i+1})$ for all $i \geq 0$. Clearly $|a|$ is bounded above, and because all we care about is proving we have a finite set, we can show that if a works, then $b_d a \in \mathbb{Z}$, where $f(x) = (b_d x^d + \cdots + b_0)/g$ for some $b_i, g \in \mathbb{Z}$ and $d \geq 2$. The idea is that if $v_p(a_{i+1}^{-1}) > v_p(b_d) \geq 0$ (we take $v_p(0) = \infty$), then

    $$v_p(a_i^{-1}) = v_p(g/b_d) + d v_p(a_{i+1}^{-1}) \geq v_p(g/b_d) + d + d v_p(b_d) = v_p(g) + (d-1) v_p(b_d) + d \geq v_p(b_d) + d.$$

    Hence the sequence $\{v_p(a_i^{-1})\}_{i \geq 0}$ is bounded above, so by the earlier size observation we know it must be eventually periodic and thus purely periodic (as $a_u = a_v$ means $a_{u-1} = a_{v-1}$). But then we must in fact have $v_p(a_i^{-1}) \leq v_p(b_d)$ for all $i \geq 0$, and we're done.

43. Do there exist positive integers $a < b$ (with $b - a > 1$) such that $\gcd(a, k) > 1$ or $\gcd(b, k) > 1$ whenever $k \in [a, b]$?

    Solution. Yes. If $b = a + r$, the condition boils down to $\gcd(i(r-i), a+i) > 1$ for all $i \in \{0, \ldots, r\}$. A good way to do this is to let p, q be primes with $q \equiv 1 \pmod{p}$ and $p^2 \geq p + q$ (for instance, the smallest pair is $(p, q) = (5, 11)$). Then take $r = p + q + 1$ and $a \equiv 0 \pmod{s}$ for every prime in $[1, r-1]$ except $s = p, q$, and let $a \equiv -q \pmod{p}$, $a \equiv -p \pmod{q}$. Then $a + i$ is satisfied whenever i is not $1, p, q$ (since $p^2 \geq p + q$). So $(a, b) = (2184, 2200)$ works.

44. (Miklos) Let $F(n)$ be the number of functions $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ with the property that if i is in the range of f, then so is j for all $j \leq i$. Prove that

    $$F(n) = \sum_{k \geq 0} \frac{k^n}{2^{k+1}}.$$

    Solution. If we generalize this to $\{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ (say $F(m, n)$), where $m, n \geq 0$, then choosing the set of guys such that $f(k) = 1$ gives the recursion

    $$F(m, n) = \sum_{k=1}^{m} \binom{m}{k} F(m-k, n-1)$$

    whenever $m, n \geq 1$ (we have $F(0, n) = 1$ for $n \geq 0$ and $F(m, 0) = 0$ for $m \geq 1$). Computing $G(x, y) = \sum_{m,n \geq 0} F(m, n) \frac{x^m}{m!} y^n$ gives $G(x, y) = \frac{1}{(1-y)[1-y(e^x-1)]}$, so it's easy to find

    $$[x^n y^n] G(x, y) = [x^n](e^x - 1)^n + \cdots + (e^x - 1)^0 = [x^n] \frac{1}{1 - (e^x - 1)};$$

    the rest is obvious.

    We can also do this directly without generalizing: there is an obvious combinatorial interpretation for $(e^x - 1)^n$.

45. Find all positive integers n for which there exist four not necessarily distinct primitive n^{th} roots of unity adding up to 1.

    Solution. For $n = 10$, take the four roots of unity to be $-e^{2k\pi i/5}$ for $k = 1, 2, 3, 4$.

    Now we show $n = 10$; the condition implies $\Phi_n(x) \mid x^a + x^b + x^c + x^d - 1$ for some positive integers a, b, c, d coprime to n. Summing up $z^a + z^b + z^c + z^d = 1$ over all primitive roots of unity (use $x^m - 1 = \prod_{d|m} \Phi_d(x)$ and induction/Mobius inversion) we get $\phi(n) = 4\mu(n)$, whence n is squarefree and has an even number of prime factors. If n has at least three prime factors p, q, r, then $\phi(n) \geq (p-1)(q-1)(r-1) > 2 \cdot 2 \cdot 2 > 4$, so n must have exactly two prime factors p, q. Thus, $(p-1)(q-1) = 4pq \implies \{p, q\} = \{2, 5\} \implies n = 10$.

46. (Russia 2011) A 2010×2010 board is divided into L-trominos. Prove that it's possible to mark one cell in each L-tromino such that every row and each column has the number of marked cells.

Solution. We want to smooth in some way. The simplest way to do view this is to start with all the tromino corners marked, so we want to keep some guys the same, and move others in one of the two directions. Observe that every tromino belongs in exactly one pair of neighboring columns (and one pair of neighboring rows). In the original marking, let r_i be the number of marked cells in row i and define c_j similarly.

We first analyze what smoothing does to columns individually, for simplicity (although this is not guaranteed to work, it's a starting point and we have a lot of symmetry). There are four different kinds of trominos affecting column i: they can either lie in columns $i-1, i$ or $i, i+1$, and either have 1 or 2 squares in column i. But if we write out algebraic expressions for the changes in number of marked squares in column i, we see that we have a "telescoping" sum and it will be nicer to instead consider the changes in the quantities $R_i = r_1 + \cdots + r_i$ and $C_j = c_1 + \cdots + c_j$, because now there are only two different types of trominos that can change C_i.

Let a_i, b_i denote the number of trominos in columns $i, i+1$ with 2 cells in column i and 2 in column $i+1$, respectively. Clearly $C_i = \frac{2010i + a_i + 2b_i}{3} - b_i = 670i + \frac{a_i - b_i}{3}$. The key now is that $\Delta C_i = -(x_i - y_i)$, where x_i, y_i of horizontal moves of type-a_i, b_i trominos, respectively: it's *completely pointless* to operate to have both $x_i, y_i > 0$, since it can only help for the vertical row-changing operations later on. So we'll take $x_i = \max(0, \frac{a_i - b_i}{3}) \le \frac{a_i}{3}$ and $y_i = \max(0, \frac{b_i - a_i}{3}) \le \frac{b_i}{3}$ (note that $x_i y_i = 0$). Clearly we have no restrictions on the choice of which a_i, b_i-type trominos to operate on, as long as $x_i \le a_i$ and $y_i \le b_i$.

The rest is easy: take a bipartite graph $G = U \cup V$, where U has the 4020 vertices R_i, C_j for $1 \le i, j \le 2010$ and V has the trominos, and we draw edges from C_i (for fixed i) to the trominos of type a_i if $x_i > 0$ and the trominos of type b_i if $y_i > 0$. Then it's enough to find an edge-subgraph $H \subseteq G$ such that $\deg_H(u) \ge \frac{1}{3} \deg_G(u)$ for all $u \in U$ and $\deg_H(v) \le 1$ for all $v \in V$, because by construction we have $\deg_G(C_i) \ge 3|\frac{a_i - b_i}{3}|$. But $\deg_G(v) \le 2$ for all $v \in V$, so we get a union of pairwise edge-disjpoint paths and even cycles (in fact, cycle lengths must be multiples of 4), where every vertex $u \in U$ is an end of at most one (full) path. Now take every other edge of each full cycle and path in H (we can just do this arbitrarily), so that $\deg H(u) \ge \min(0, \frac{\deg_G(v) - 1}{2}) \ge \frac{1}{3} \deg_G(u)$ for every $u \in U$, as desired (if $\deg_G(u) > 0$, then it's at least 3 since $(a_i - b_i)/3$ is an integer for all i).

Observe that nothing in this solution was tricky, as every step simply rewords the problem in increasingly convenient fashions.

47. (Bondy's theorem) Let $A_1, \ldots, A_n$ be pairwise distinct subsets of $[n]$. Show that there exists an element x such that the $A_i \setminus \{x\}$ are also pairwise distinct.

Solution. An element x fails iff modulo 2, $A_i + A_j = \{x\}$ for some indices i, j. So go by contradiction and draw a graph with edges labeled with symmetric differences (and vertices the n sets). Now remove edges until we have exactly n remaining, one of each $\{x\}$ (by assumption). Then there must be a cycle, contradiction.

Another way to see this is if we let $A_{i(x)} + A_{j(x)} = \{x\}$ for some choice of $i(x), j(x)$ for every $x \in [n]$. But then we don't have any cycles, so in this way we can reverse-engineer the motivation for the graph.

48. (Classical) If $x^m + x^{-m}$ and $x^n + x^{-n}$ are both integers ($x > 1$ is a real number) and $\gcd(m, n) = 1$, show that $x + x^{-1}$ is also an integer.

Solution. First note that if $a = x^n + \frac{1}{x^n}$ is an integer, then so is $x^{kn} + \frac{1}{x^{kn}} = 2T_k\left(\frac{a}{2}\right)$ (since $2T_n\left(\frac{x}{2}\right) \in \mathbb{Z}[x]$), where $T_k(x)$ denotes the k^{th} Chebyshev polynomial of the first kind.

Since m, n are relatively prime, we can find integers such that $jm - kn = 1$, so WLOG $m = n + 1$. Then if $a = x^n + \frac{1}{x^n}$ and $b = x^{n+1} + \frac{1}{x^{n+1}}$, the quadratic formula yields (note that $a, b > 2$ are integers and $x > 1$)

$$x^n = \frac{a + \sqrt{a^2 - 4}}{2}, \quad x^{n+1} = \frac{b + \sqrt{b^2 - 4}}{2}.$$

It follows that

$$x + \frac{1}{x} = \frac{ab - \sqrt{(a^2-4)(b^2-4)}}{2}.$$

But $x, 1/x$ are clearly algebraic integers by the quadratic equations in x^n, x^{n+1}, so by the rational root theorem it suffices to show that $(a^2-4)(b^2-4)$ is a rational square. However, this follows trivially by equating the (nonzero) irrational terms in the equation

$$\left(\frac{a+\sqrt{a^2-4}}{2}\right)^{n+1} = \left(\frac{b+\sqrt{b^2-4}}{2}\right)^{n}.$$

Alternatively, consider the minimal polynomial of x (over $\mathbb{Q}$), which in particular divides $x^{2n} - ax^n + 1$ and $x^{2n+2} - bx^{n+1} + 1$, and so noting that we can generate all roots of these two polynomials by taking $xe^{2\pi i/n}$, for instance, it's not hard to show that their gcd must be quadratic and by Gauss's lemma, primitive and monic, as desired.

Of course, this is true for any complex number x.

49. (Colosimo Open 2011) Find all n such that there exists a permutation $(a_1, \dots, a_n)$ of $[n]$ with the $a_1 + \cdots + a_i \pmod n$ pairwise distinct.

    Solution. $n = 1$ and n even: for $n = 2m$, take $2m, 1, 2m-2, 3, 2m-4, 5, \dots, 2, 2m-1$, which can be found by small cases or guessing simple things. For n odd, note that $a_1 = n$ or else two consecutive sums will be equal somewhere, but also $n \mid 1 + \cdots + n = a_1 + \cdots + a_n$, contradiction.

50. (Russia 2011, 11.4) Ten cars, which do not necessarily start at the same place, are all going one way on a highway which does not loop around. The highway goes through several towns. Every car goes with some constant speed in those towns and with some other constant speed out of those towns. For different cards these speeds can be different. 2011 flags are put in different places next to the highway. Every car went by every flag, and no car passed another right next to any of the flags. Prove that there are at least two flags at which all cars went by in the same order.

    Solution. Let t_i denote the time it takes for car i to get to the first flag (choose a starting time arbitrarily). Suppose car i takes time per unit distance $0 < a_i, b_i < \infty$ when in and out of town, respectively; let $x_k, y_k \ge 0$ (not both zero) be the distances from flag 1 to flag k along in and out of town routes. Then car i takes $T_i(k) = t_i + a_i x_k + b_i y_k$ to get to flag k. If $t_i = t_j$ for some $i \ne j$, then we must have $T_i(k) = T_j(k)$ for all k (or else we violate the "no passing at flags" rule), whence car i is essentially a "clone" of car j. Since clones are ranked the same at each flag, we can remove all clones to get (WLOG) $1 \le m \le 10$ pairwise distinct cars (WLOG cars 1 through m). Then $T_i(k) \ne T_j(k)$ for all $1 \le k \le 2011$ and $1 \le i < j \le m$.

    Now note that for $i \ne j$, $T_i(k) > T_j(k)$ iff

    $$(x_k, y_k) \in S_{i,j} = \{(x,y) \mid L_{i,j}(x,y) = (a_i - a_j)x + (b_i - b_j)y + (t_i - t_j) > 0\},$$

    and $T_i(k) < T_j(k)$ iff $(x_k, y_k) \notin S_{i,j}$. Graphing $L_{i,j}(x,y) = 0$ in the Cartesian plane for $1 \le i < j \le m$ (note the symmetry between $L_{i,j}$ and $L_{j,i}$), we get at most $\binom{M}{2} + \binom{M}{1} + \binom{M}{0} \le 1036$ (where $M = \binom{m}{2}$ is the number of lines) distinct regions (well-known, e.g. this). But (x_r, y_r) and (x_s, y_s) are in the same region iff the orderings at flags r, s are equal, so we're done by pigeonhole.

    Comment. This is not ridiculous or anything, but doing the 1-d case helps a bit. Indeed, this generalizes to any number of dimensions, and the bound should be basically tight and not hard to find.

51. (Russia 2002, 11.8) Show that the numerator of H_n (in reduced form) is infinitely often not a prime power.

    Solution. Outline: Bound denominators using powers of 2 and primes from $n/2$ to n. Consider $p^k - 1$ for $k \ge 1$, and note that $v_p(H_{pn}) \ge v_p(H_n) - 1$, so consider $p^k - p$ as well. Subtracting dudes, get a contradiction.

52. (Sierpinski) Prove that for all N there exists a k such that more than N prime numbers can be written in the form $f(T)+k$ for some integer T, where $f \in \mathbb{Z}[x]$ is a nonconstant monic polynomial.

Solution. Let $d = \deg f$. For fixed k, let $g(k)$ denote the number of positive T such that $f(T)+k$ is prime, and suppose for the sake of contradiction that there exists some N such that $g(k) \le N$ for all $k \ge 1$. Fix a real $s > 1$; if $\mathbb{P}$ is the set of primes, then

$$\begin{aligned} N \sum_{k\ge 1} \frac{1}{k^s} &\ge \sum_{k \ge 1} \frac{g(k)}{k^s} \\ &= \sum_{p \in \mathbb{P}} \sum_{1 \le f(T) < p} \frac{1}{(p - f(T))^s} \ge \sum_{p\in\mathbb{P}} \frac{p^{1/d} - c}{p^s} \end{aligned}$$

for some c independent of p. Any $1 < s \le 1 + 1/d$ gives the desired contradiction, since the sum of the reciprocals of the primes diverges.

This is also not difficult using elementary forms of the PNT. Indeed, if we consider $f(1), \dots, f(n)$ for some fixed n and for every prime $p \le c_1 n^d$, take the smallest i such that $f(i) < p$ and consider $k = p - f(i)$, then by pigeonhole some $k \le c_2 n^{d-1}$ (the size of the largest "gap" between consecutive $f(i)$) will appear at least $cn/\log(n^d)$ times, which is unbounded.

53. (ROM TST 1996) Let $n \ge 3$ and consider a set S of $3n^2$ pairwise distinct positive integers smaller than or equal to n^3. Prove that one can find nine distinct numbers $a_1, \dots, a_9 \in S$ and three nonzero integers $x, y, z \in \mathbb{Z}$ such that $a_1x + a_2y + a_3z = 0$, $a_4x + a_5y + a_6z = 0$, and $a_7x + a_8y + a_9z = 0$.

Solution. The key is to realize that we probably want to use pigeonhole somehow (the $3n^2$ and n^3 are rather ugly for an inductive argument). But this is not really related to the geometry of numbers since we have at least as many equations as variables, so we want to "fix" some sort of vector (x, y, z) and then find the a_i's from there (the three vectors (a_1, a_2, a_3), etc. are orthogonal to (x, y, z)).

Now we want to get a feel of the most natural way to fix (x, y, z). Note that we can parameterize all solutions to $ax + by + cz = 0$ by

$$(x, y, z) = (sb - tc, rc - sa, ta - rb).$$

This gives us the idea of fixing r, s, t (all nonzero for pigeonhole to work out).

Intuitively, to get the best bounds for this simplest case, we want to take $r = s = t = 1$ (or all -1). (Furthermore, if we had, say, $s \ne t$, then it would be hard to control the requirement that x, y, z are all nonzero.) Luckily, the rest works out easily: to make x, y, z as small as possible (for pigeonhole to work optimally, since we know all the a_i are less than or equal to n^3), let the elements of S be $s_1 < s_2 < \cdots < s_{3n^2}$, and for the a_1, a_4, a_7, choose from the first set of n^2 indices, for a_2, a_5, a_8, choose from the second set of n^2 indices, and for a_3, a_6, a_9, choose from the last set of n^2 indices. We get a total of $N = (n^2)^3$ (optimal by AM-GM) (x, y, z) (note that $x + y + z = 0$ and $x, z < 0$), yet only $M = (n^3 - 1)(n^3 - 2)/2 < N/2$ triples with $x + y + z = 0$ and $x, z < 0$ are possible in the first place (to count all possible triples, we can assume the smallest number chosen is 1 and then choose two larger values in the range $[2, n^3]$), so by pigeonhole, some (x, y, z) must occur at least $\lceil N/M \rceil = 3$ times, as desired.

54. (USA TST 2003) For a pair a, b of integers with $0 < a < b < 1000$, a subset S of $\{1, 2, \dots, 2003\}$ is called a skipping set for (a, b) if $|s_1 - s_2| \notin \{a, b\}$ for any $(s_1, s_2) \in S^2$. Let $f(a, b)$ be the maximum size of a skipping set for (a, b). Determine the maximum and minimum values of f.

Solution. Let $T = \{1, 2, \dots, 2003\}$.

For the minimum, note that we can keep doing the following: take $\min T$, which kills at most two others in T ($\min T + a, \min T + b$ if they're in T), and repeat with the new set T'. Each time we remove at most 3 elements, so we end up with at least $\lceil 2003/3 \rceil = 668$ elements, which is realized for $(a, b) = (1, 2)$.

For the maximum, we first analyze the one variable case to gain some intuition: of course, for fixed a, we can just consider each residue modulo a separately (and it's just alternating in S, out S, etc. for a fixed residue), where the best ratio is around $(2/3)|T|$, achieved for $S = \{1, 2, \dots, j, k, \dots, 2003\}$ for $j, 2003 - k \approx 2003/3$.

With the proof and construction for the one variable case in mind, we suspect that $f(a, a + 1)$ for $a \approx 2003/3$ will give the maximum (we know it can't be far). Indeed, we can get $f(667, 668) \geq 1334$ with $S = \{1, 2, \dots, 667, 1337, 1338, \dots, 2003\}$.

It remains to show that $f(a, b) \leq 1334$ always. Assume for the sake of contradiction that $f(a, b) \geq 1335$ for some $0 < a < b < 1000$.

First we get some crude estimations from $f(a)$ alone: letting $2003 = qa + r = (q + 1)r + q(a - r)$ for $q = \lfloor 2003/a \rfloor$ and $0 \leq r < a$, we get

$$1335 \leq f(a, b) \leq f(a) = \lceil (q + 1)/2 \rceil r + \lceil q/2 \rceil (a - r).$$

If q is odd, this becomes $1335 \leq (qa + a)/2 \leq (2003 + a)/2 \implies a \geq 667$, and if q is even, then $1335 \leq qa/2 + r = (2003 + r)/2 \implies a > r \geq 667$.

Hence $a \geq 667$. If $a > 667$, then $a < 1000 \implies q = 2$, so $r = 2003 - 2a$ and from the previous paragraph, $1335 \leq a + r = 2003 - a \implies a \leq 668$. Thus $a = 668$, so because equality holds everywhere, we must have $S = \{1, 2, \dots, 668, \dots, 1337, 1338, \dots, 2003\}$, which contradicts $1000 > b \geq a + 1 = 669$.

Otherwise, if $a = 667$, then $q = 3$, so $1335 \leq (q + 1)a/2 = 2a \implies a \geq 667.5$, contradiction.

55. (Erdos and Selfridge) Find all positive integers $n > 1$ with the following property: for any real numbers $a_1, \dots, a_n$, knowing the numbers $a_i + a_j$, $i < j$, determines the values $a_1, \dots, a_n$ uniquely.

Solution. The property (say, *goodness*) holds iff for every two "polynomials" $f(x) = \sum_{i=1}^n x^{a_i}$ and $g(x) = \sum_{i=1}^n x^{b_i}$ (with real but not necessarily integer exponents), then $f(x)^2 - f(x^2) = g(x)^2 - g(x^2) \implies f(x) = g(x)$.

We'll show that n is good iff it's not a power of 2. To do this, we want to do some sort of bounding with values in $[0, 1]$ (maybe > 1), algebraic manipulation (especially either using $f(x)^2 - g(x)^2 = f(x^2) - g(x^2)$ to telescope products some way or differentiation), or just special values. Screwing around, it turns out differentiation is pretty helpful here.

If n is not a power of 2, then by the general Leibniz rule on $[f(x)f(x)]^{(m)}$ and the fact that

$$[f(x^2)]^{(m)} = (2x)^m f^{(m)}(x^2) + \sum_{j=0}^{m-1} P_{m,j}(x) f^{(j)}(x^2)$$

for some polynomials $P_{m,j}$ (both facts are easily proven by induction), we can show by induction on $m \geq 0$ (base case is just $f(1) = g(1) = n$) that (sorry for sloppiness, but this is assuming the strong inductive hypothesis for $\leq m - 1$)

$$2^m (f^{(m)}(1) - g^{(m)}(1)) = 2n[f^{(m)}(1) - g^{(m)}(1)],$$

which implies $f^{(m)}(1) = g^{(m)}(1)$ for all $m \geq 0$. Thus (by induction/Stirling numbers) $\sum a_i^r = \sum b_i^r$ for all integers $r \geq 0$, so by easy bounding considerations $f(x) = g(x)$.

Otherwise, let $n = 2^m$. For the construction, we take f, g to be actual polynomials (i.e. with integer exponents), so taking the induction from the previous paragraph up until m, we have that $f(x) - g(x) = (x-1)^{m+1} h(x)$ for some polynomial $h(x)$. Plugging this in, we have $f(x) + g(x) = (x+1)^{m+1} h(x^2)/h(x)$. We can just take $h(x) = 1$ (identically); then the sets of numbers corresponding to $f(x) = [(x+1)^{m+1} + (x-1)^{m+1}]/2$ and $g(x) = [(x+1)^{m+1} - (x-1)^{m+1}]/2$ suffice.

Edit: There's a cleaner way using rational approximation (assume all the guys are large integers). If 1 is a root of $f(x) - g(x)$ with multiplicity k, then $f(x) - g(x) = (x - 1)^k u(x)$ for some $u(1) \neq 0$. But then $f(x^2) - g(x^2) = (x - 1)^k (x + 1)^k u(x^2)$ means that $f(1) + g(1)$ is a power of 2, as desired.

56. (Brouwer-Schrijver) Prove that the minimal cardinality of a subset of $(\mathbb{Z}/p\mathbb{Z})^d$ that intersects all hyperplanes is $d(p - 1) + 1$.

Solution. Suppose by way of contradiction that there's a set S intersecting all hyperplanes with $|S| \le d(p-1)$. WLOG $(0,0,\dots,0) \in S$; now consider the polynomial (over $\mathbb{F}_p$)

$$f(x) = \prod_{s \in S' = S \setminus 0} (\langle x, s\rangle - 1) + C \prod_{i=1}^{d} \prod_{j=1}^{p-1} (x_i - j),$$

where $C \neq 0$ is taken so that $f(0) = 0$. Since $|S'| \le d(p-1)-1$, $\deg f = d(p-1)$. Since the coefficient of $x_1^{p-1} \cdots x_d^{p-1}$ in f is nonzero, CNS guarantees $y \in \mathbb{F}_p^d$ such that $f(y) \neq 0$ ($C \neq 0 \implies y \neq 0$), whence S does not intersect the plane $\langle y, t\rangle = 1$ (obviously $t = (0,0,\dots,0)$ does not belong to it, and because $y \neq 0$, the second part of f vanishes at y and so the first cannot, whence S' does not intersect the plane either), contradiction.

On the other hand, the construction for $d(p-1)+1$ is obvious: just take S the set of $(s_1, \dots, s_d)$ with at least $d-1$ of the s_i's zero (if a plane does not contain the origin, it's WLOG of the form $x_1 s_1 + \cdots + x_d s_d = 1$ with $x_1 \neq 0$, and so $(1/s_1, 0, \dots, 0)$ works).

Comment. This extends directly to any finite field $\mathbb{F}_q$.

57. (MOP 2007) In triangle ABC, point L lies on side BC. Extend segment AB through B to M such that $\angle ALC = 2\angle AMC$. Extend segment AC through C to N such that $\angle ALB = 2\angle ANB$. Let O be the circumcenter of triangle AMN. Prove that $OL \perp BC$.

    Solution. Extend MC and NB to hit (AMN) at M' and N', respectively. By easy angle chasing, $\angle N'MM' = 90°$, so O is the midpoint of $N'M'$; let L' denote the foot of the perpendicular from O to BC (we want to show $L = L'$). By Pascal's theorem on $AAMM'N'N$, there exists a point $X = AA \cap M'N' \cap BC$, so $XAOL'$ is cyclic. Thus

    $$\angle AL'B = \angle AL'X = \angle AOX = \angle AON' = 2\angle ANN' = 2\angle ANB$$

    and similarly $\angle AL'C = 2\angle AMC$, as desired.

    Alternatively, trig bash with POP to show that $OB^2 - OC^2 = LB^2 - LC^2$.

58. (MOP 2010) Fix n points in space in such a way that no four of them are in the same plane, and choose any $\lfloor n^2/4 \rfloor + 1$ segments determined by the given points. Determine the least number of points that are the vertices of a triangle formed by the chosen segments.

    Solution. Interpret this as a graph $G = G_1 \cup G_2$, where all $v \in G_1$ are *good* (i.e. belong to some triangle) and all $v \in G_2$ are *bad*. We induct on $n \ge 1$ to show that $|G_1| \ge 2 + \lfloor n/2 \rfloor$, where the base cases $n = 1, 2$ are vacuously true.

    Now suppose $n \ge 3$. By Turn's theorem, we have a triangle uvw. Suppose that $|G_1| \le 1 + \lfloor n/2 \rfloor$.

    If $\deg u + \deg v - 1 \le n - 1$, then removing u, v (and the edges incident to them) and noting that $n^2/4 = n - 1 + (n-2)^2/4$, the inductive hypothesis gives us at least

    $$2 + (2 + \lfloor (n-2)/2 \rfloor) = 3 + \lfloor n/2 \rfloor > 2 + \lfloor n/2 \rfloor$$

    vertices in G_1 (the 2 comes from u, v).

    Otherwise, if $\deg u + \deg v \ge n + 1$, then by pigeonhole, WLOG

    $$\deg u \ge \lceil (n+1)/2 \rceil = 1 + \lfloor n/2 \rfloor \ge |G_1|,$$

    so u is connected to some $x \in G_2$. Since $x \in G_2$, $\deg u + \deg x \le 1 + (n-2) = n - 1$, so removing u, x and applying the inductive hypothesis gives us

    $$|G_1| \ge 1 + (2 + \lfloor (n-2)/2 \rfloor) = 2 + \lfloor n/2 \rfloor,$$

    contradiction (the 1 comes from u).

59. (Bulgarian solitaire) Suppose we have $N = 1 + 2 + \cdots + n$ cards total among some number of stacks. In each move, Bob takes one card from each stack and forms a new stack with them. Show that Bob eventually ends up with $1, 2, \ldots, n$ in some order.

    Solution. We want to find some monovariant I. First, it's convenient to visualize the stacks as consecutive sets of lattice points in the first quadrant (e.g. lower left at $(1, 1)$).

    For simplicity, arrange the stacks in nonincreasing order (although it turns out this doesn't matter). Motivated by the final configuration, we take $I = \sum x + y$ over all points (x, y) corresponding to cards in our configuration. Suppose we have stacks of size $a_1 \geq \cdots \geq a_k \geq 1 > 0 = a_{k+1}$, and $1 \leq i \leq k + 1$ is the smallest index such that $a_i \leq k + 1$. Then to compute ΔI, visualize the process as reflecting the points on $y = 1$ over the line $y = x$, shifting the points with $y > 1$ via $(x, y) \mapsto (x + 1, y - 1)$ (up to this point, $\Delta \sum x + y = 0$), and then reordering the columns/stacks (here, $\Delta \sum x \leq 0$, with equality iff $i = 1$). Thus $\Delta I \leq 0$, with equality iff $a_1 \leq k + 1$. (*)

    There are finitely many configurations, so suppose we get into a loop with constant I. Then we cannot have any of the nontrivial "reordering" mentioned in (*), i.e. in any step, we have $(x, y) \mapsto (x+1, y-1)$ if $y \geq 2$ and $(x, y) \mapsto (y, x)$ if $y = 1$ (so $x + y$ is preserved for each card). In particular, for fixed $\ell \geq 2$, the points with coordinates summing up to ℓ "cycle" along the line $x + y = \ell$. Considering maximal ℓ, it's easy to see that because N is a triangular number, this final loop must be a constant loop with $k = n$ and $a_j = n + 1 - j$ for $1 \leq j \leq k$, as desired.

    Note that this method also determines the possible final states for N not necessarily triangular.

60. (Russia 2003, 11.4) Ana and Bora start with the letters A and B, respectively. Every minute, one of them either prepends or appends to his/her own word the other person's word (not necessarily operating one after another). Prove that Ana's word can always be partitioned into two palindromes.

    Solution. Call a word *good* if it can be partitioned into two palindromes.

    The possible operations are $\{X, Y\} \mapsto \{X, XY\}, \{X, Y X\}, \{Y, XY\}, \{Y, Y X\}$.

    So there are basically two ways to look at the process: we can either think of it as directly showing XY and YX are good given X, Y, or we can think of it as "preserving" goodness through $X \mapsto XY$, etc. (basically stupid, forward induction vs. "reverse" induction).

    The first way gets too messy quickly, so we focus on the more natural second way, i.e. by induction, it suffices to show that goodness is preserved by any of the substitutions $A \mapsto AB$, $A \mapsto BA$, $B \mapsto AB$, and $B \mapsto BA$.

    Hence we consider what $A \mapsto AB$ does to a palindrome P (the other cases are analogous); it's easy to show (by comparing the left-to-right and right-to-left orientations) that if $P \mapsto P'$, then BP' and P'/B (sorry for terrible notation) are palindromes.

    Therefore if $P \mapsto P'$ and $Q \mapsto Q'$ for palindromes P, Q, then

    $$P'Q' = (P'/B)(BQ'),$$

    as desired.

61. (Motzkin-Rabin) Let $\mathcal{S}$ be a finite set of points in the plane (not all collinear), each colored red or blue. Show that there exists a monochromatic line passing through at least two points of $\mathcal{S}$.

    Solution. After playing around with this setup a bit (with contradiction), we see that the most annoying issue is "betweenness", which screws up a lot of positioning by forcing a lot of cases on us.

    So we prove the projective dual instead, since lines are generally much more flexible with positioning: for a finite set $\mathcal{S}$ of lines in the projective plane (not all concurrent), each colored red or blue, we prove that there exists a monochromatic point belonging to at least two lines of $\mathcal{S}$.

    Indeed, suppose the contrary (WLOG, we work in the Euclidean plane by taking a suitable projection to ensure that no two lines intersect at infinity). Clearly, the blue lines are not all concurrent (same for the red lines).

Consider two lines ℓ_1, ℓ_2 of the same color α passing through point A. Then there exists a line ℓ_3 of the other color β passing through A as well. Since not all lines of color β pass through A, there exists a line ℓ_4 of color β passing through a point $B \in \ell_3 \setminus \{A\}$. Let $C = \ell_4 \cap \ell_1$ and $D = \ell_4 \cap \ell_2$.

The rest is easy: taking such a configuration with minimal area $[ACBD]$, B must be monochromatic (color β), or else there exists a line through B of color α, and we get a smaller configuration (the line must intersect either segment AC or segment AD).

62. (KMaL) Let k be an integer and $a_1, a_2, \ldots, a_n$ be integers that give at least $k+1$ distinct remainders when divided by $n+k$. Prove that some of these n numbers add up to a multiple of $n+k$.

    Solution. Assume for the sake of contradiction that no nonempty zero-sum subset exists.

    To use pigeonhole modulo $n+k$ (which is really the only reasonable way), we need to get both k and n involved. The easiest way to do this is to WLOG let $a_1, \ldots, a_{k+1} \pmod{n+k}$ be pairwise distinct (we know such numbers exist by the problem hypothesis) and consider the partial sums $s_{k+1} = a_1 + \cdots + a_{k+1}, \ldots, s_n = a_1 + \cdots + a_n \pmod{n+k}$ (which are pairwise distinct and nonzero by our assumption; we start at the $(k+1)^{th}$ partial sum so that when we subtract elements from $\{a_1, \ldots, a_{k+1}\}$ we still have a sum of distinct a_i).

    Now we need another set of at least $(n+k) - (k+1) - (n-k) = k-1$ nonzero elements for pigeonhole to work; something like $\{-a_1, \ldots, -a_{k+1}\}$ quickly comes to mind (since the a_i are distinct, at most one of them can satisfy $a_i \equiv -a_i \pmod{n+k}$, and we can afford to lose a few), provided we make it compatible with $\{s_{k+1}, \ldots, s_n\}$. But this is easy, since adding s_{k+1} to every entry to get $\{s_{k+1} - a_1, \ldots, s_{k+1} - a_{k+1}\}$ does not make it less compatible with $\{a_1, \ldots, a_{k+1}\}$.

    WLOG $a_i \not\equiv s_{k+1} - a_i \pmod{n+k}$ for $1 \le i \le k-1$ (we can assign the roles to $i = k$ and $i = k+1$ if necessary); then the sets $\{a_1, \ldots, a_{k+1}\}$, $\{s_{k+1} - a_1, \ldots, s_{k+1} - a_{k-1}\}$, and $\{s_{k+1}, \ldots, s_n\}$ each contain pairwise distinct nonzero elements modulo $n+k$. But they have $(k+1)+(k-1)+(n-k) = n+k$ elements in all, so by pigeonhole some two sets must intersect (we are only dealing with the $n+k-1$ nonzero elements). If the third set intersects with either the first or the second, we obviously get a nonempty zero-sum subset; otherwise, if the first two sets intersect, then we must have $k-1 \ge 1 \implies k \ge 2$ and $s_{k+1} - a_i - a_j \equiv 0 \pmod{n+k}$ for some $i \ne j$, which also gets a nonempty zero-sum subset since $s_{k+1} - a_i - a_j$ contains at least $(k+1) - 2 = k-1 \ge 1$ terms.

63. (AMM) Let $P_0, P_1, \ldots, P_{n-1}$ be some points on the unit circle. Also let $A_1A_2 \cdots A_n$ be a regular polygon inscribed on this circle. Fix an integer k with $1 \le k \le n/2$. Prove that one can find i, j such that $A_iA_j \ge A_1A_k \ge P_iP_j$.

    Solution. For a real number x, let $|x|_n = d(x, n\mathbb{Z})$ denote how far x is from its closest integer multiple of n (i.e. absolute value $\pmod{n}$). If we go by contradiction, then we have that $|p_i - p_j|_n \le k-1 \implies |i-j|_n \le k-2$, where $p_0, \ldots, p_{n-1} \in \mathbb{R}$ represent the positions of $P_0, \ldots, P_{n-1}$ on an angular scale. To utilize this local information (which restricts what points can be close to each other) in the context of our global situation of n reals spread out $\pmod{n}$, we want to get a lot of the p_i in some interval $[r, r+k-1] \pmod{n}$.

    On average, $[r, r+k-1] \pmod{n}$ contains $n \cdot (k-1)/n = k-1$ of the p_i. If some $[r, r+k-1] \pmod{n}$ contains k or more of the p_i, then two of the indices u, v must satisfy $|u-v|_n \ge k-1$, contradiction. Otherwise, the interval $[r, r+k-1] \pmod{n}$ contains *exactly* $k-1$ of the p_i for almost all r (except for a set of zero density), which is impossible as we consider $r \in [p_m - \epsilon, p_m + \epsilon]$ for any m and sufficiently small $\epsilon > 0$ unless $p_{i_m} = p_m + k - 1$ for some i_m; but then we get k or more p_i in $[p_m, p_m + k - 1] \pmod{n}$.

64. (1998 C1) A rectangular array of numbers is given. In each row and each column, the sum of all numbers is an integer. Prove that each nonintegral number x in the array can be changed into either $\lceil x \rceil$ or $\lfloor x \rfloor$ so that the row-sums and column-sums remain unchanged. (Note that $\lceil x \rceil$ is the least integer greater than or equal to x, while $\lfloor x \rfloor$ is the greatest integer less than or equal to x.)

    Solution. We want to reduce the number of non-integers while preserving row and column sums. Intuitively, if we change x to $\lfloor x \rfloor$, then if we can increase by $\{x\}$ something else in the same row or column and keep alternately increasing/decreasing stuff, we'll eventually have to "cycle" back to x (and the cycle must have even length, since we switch between modifying in the same row and modifying in the same column).

This motivates us to take a bipartite graph $R \cup C$ where R is the set of rows, C is the set of columns, and the grid numbers are written on corresponding edges. Furthermore, we can take out all edges with integer labels; we want to get down to zero edges. Because all rows and columns have integer sums, each vertex has degree at least 2, and so we can find an (even) cycle. Then the rest is clear: taking an edge label x in the cycle that minimizes $|[x] - x|$ (where $[x]$ denotes the nearest integer function), we can proceed as described in the first paragraph.

65. (2003 HMMT Guts) A teacher must divide a apples evenly among b students, where $a \le b$. What is the minimal number of pieces into which she must cut the apples? (A whole uncut apple counts as one piece.)

    Solution. Trying some small cases really helps to find this crucial lemma...

    Lemma. If $\gcd(p, q) = 1$ and $p \le q$, then the teacher can divide p apples evenly among q students with just $p + q - 1$ pieces in all.

    Proof. One way is just inducting on $p+q$. Otherwise, motivated by the previous problem, we interpret this as a bipartite graph $G = A \cup S$ the edges represent the portions of apple students in S get from the vertices in A. At first, label each edge with $1/q$. We want to reduce to $p + q - 1$ edges (i.e. a tree) by modifying edges and deleting the zero labels. To this end, suppose we have a cycle C, which must be even since G is bipartite. If the edge label $0 \le x \le p/q$ minimizes $\epsilon = \min\{x, p/q - x\}$ in the cycle, then change x to 0 or p/q accordingly and alternately modify the other edges in the cycle by $\pm\epsilon$, preserving both the sum of edges emanating from vertices in A (which must be 1) and the sum of edges emanating from vertices in S (which must be p/q), as well as the positiveness of the edge labels. If we change x to 0 in the process, then we lose at least one edge; otherwise, if we change it to p/q, then the vertex in S belonging to it goes from ≥ 2 edges (necessary to participate in the cycle) to exactly 1 edge (since all its other edges must become 0), and we still lose at least one edge. Clearly this process terminates when we reach a tree of $p + q - 1$ vertices, as desired.■

    Let $(a, b) = (gp, gq)$ for $g = \gcd(a, b)$, so $\gcd(p, q) = 1$. The bipartite graph $G = A \cup S$ only has connected components with u vertices in A and v vertices in S with $u = (p/q)v$ and thus at least $pr + qr - 1$ edges for some $r \ge 1$. Since the sum of all such r is g, there are at most g components and thus at least $pg + qg - g = a + b - \gcd(a, b)$ edges, with equality achievable by the lemma.

66. (2009 AMP Team Contest) Given a set of positive integers ranging from 1 to n with sum no less than $2n!$, show that there exists a subset of them summing up to exactly $n!$.

    Solution. Induction is clearly the most natural path, as long as we find a reasonable way to go down from $[1, n]$ and $n!$ to $[1, n-1]$ and $(n-1)!$.

    Lemma. Given $\ge n$ integers, we can find $\le n$ of them with sum divisible by n.

    Proof. Well-known pigeonhole on partial sums $\pmod n$.■

    Directly using this lemma and inducting does not work, because we can be left with $n - 1$ numbers in $[1, n-1]$. However, $(n-1) \cdot (n-1)$ is quadratic, so with a little fiddling we weaken the hypothesis to "$\ge 2n! - n$", with the base case $n = 1$ being clear. Now it works smoothly, since if we use the lemma to break our set into groups of $\le n$ numbers with sum both divisible by n and at most $n(n-1)$ (first we put the n's in their own groups, and then just work with the numbers in $[1, n-1]$), then dividing each of these groups' sums by n, we have a new sum at least

    $$\left\lceil \frac{2n! - n - (n-1)^2}{n} \right\rceil = 2(n-1)! - (n-1),$$

    for $n \ge 2$, as desired.

    Alternative method by Palmer: Induct. $n = 1$ is obvious.

    First of all, given the problem statement is true for n, we easily generalize it to the following: Given a sequence for which the sum is at least $k \cdot n!$, we can find $k - 1$ pairwise disjoint subsequences each of which sum to $n!$. Given all up to n, consider the sum of all terms in the sequence equal to n. If it as at least $n!$, then we just pick them. If it is less than $n! - (n-1)!$, then the sequence formed of the terms from $1, 2, \dots, n-1$ has sum at least $n! + (n-1)! = (n+1)(n-1)!$ so we use the generalization above to get n sequences summing to $(n-1)!$ and we just combine them.

So if the sum of ns in the sequence is s_n, we have $n! - (n-1)! < s_n < n!$. In particular the sum of all of the terms not equal to n is greater than $n!$. So that means we can find $n-1$ disjoint subsequences that sum to $(n-1)!$, and we will still have at least one term left over. Pick one of those terms and let it be m. Consider the sequence $(n-1)!, 2(n-1)!, \dots, (n-1)(n-1)!$. Either one of these is divisible by n or all of the residues are distinct mod n. In the first case, take the term divisible by n and include as many terms equal to n as needed to get the sum to $n!$. This is possible since $s_n > n! - (n-1)!$. In the second case, we cover all nonzero residues. Find the one with residue $-m$ and include it with m. Now we have a sum divisible by n that is at least $(n-1)!$, so proceed as in the previous case.

This bound can probably be brought way lower, but I didn't feel like analyzing the case where was prime in that much detail, which is when case (ii) occurs.

67. (China 2007) Prove that for any given positive integer n, there exists a unique polynomial $f(x)$ of degree n with integer coefficients such that $f(0) = 1$ and $(x+1)f(x)^2 - 1$ is odd.

Solution. We will show that up to sign, there is in fact a unique polynomial in $\mathbb{R}[x]$. Let $f(x) = p(x^2) + xq(x^2)$, so $(x+1)f(x)^2 - 1 = -[(-x+1)f(-x)^2 - 1]$ rewrites as $x[p(x)+q(x)]^2 + (1-x)p(x)^2 = 1$. (*)

Let $r(x) = p(x) + q(x)$. Differentiating both sides, we have

$$r(x)[r(x) + 2xr'(x)] = p(x)[p(x) + 2(x-1)p'(x)].$$

Clearly $\deg p = \deg r$ or else (*) can't hold (the leading coefficients must be the same up to sign), so because $\gcd(p(x), r(x)) = 1$, $p(x)$ must divide $r(x) + 2xr'(x)$ and so there exists a constant c such that $p(x) = c[r(x) + 2xr'(x)]$. Plugging this into (*), we get the differential equation

$$1 = [x + c^2(1-x)]r(x)^2 + 4c^2x(1-x)r'(x)r(x) + 4c^2x^2(1-x)r'(x)^2.$$

From the quadratic formula, we find

$$r'(x) = -\frac{c(x-1)r(x) \pm \sqrt{(x-1)[xr(x)^2 - 1]}}{2cx(x-1)},$$

or letting $s(x) = r(x)\sqrt{x}$ so that $2xr'(x)\sqrt{x} = 2xs'(x) - s(x)$ and simplifying,

$$\frac{2cs'(x)}{\sqrt{s(x)^2 - 1}} = \sqrt{\frac{1}{(2x-1)^2 - 1}},$$

where WLOG $\lim_{x\to\infty} s(x) = \infty$. Anyway, it's easy to find that

$$\int \frac{1}{\sqrt{x^2 - 1}}\, dx = \ln(x + \sqrt{x^2 - 1}) + C,$$

so for some constant C_0 we have

$$c \ln(s(x) + \sqrt{s(x)^2 - 1}) = \ln(\sqrt{x} + \sqrt{x-1}) + C_0,$$

i.e.

$$\frac{1}{s(x) - \sqrt{s(x)^2 - 1}} = s(x) + \sqrt{s(x)^2 - 1} = e^{C_0/c}(\sqrt{x} + \sqrt{x-1})^{1/c},$$

so there exist constants C_1, C_2 such that

$$r(x) = \frac{e^{C_1}(\sqrt{x} + \sqrt{x-1})^{C_2} + e^{-C_1}(\sqrt{x} - \sqrt{x-1})^{C_2}}{2\sqrt{x}}.$$

Since r is a polynomial, we clearly have $C_2 \in \mathbb{Z}$ and thus $C_1 = 0$. Now we can easily compute $f(x) = (1-x)p(x^2) + xr(x^2) = T_{n+1}(x) - (x-1)U_n(x)$ (up to sign of course).

Note that (*) rearranges to the Pell equation $u(x)^2 - (x^2-1)v(x)^2 = 1$ upon the substitutions $u(x) = xr(x^2)$, $v(x) = p(x^2)$.

As for actually using Chebyshev polynomials in number theory... well it turns out that $\frac{T_{2n+1}(x)}{x}$ is almost never a perfect square for integers x, n.

68. (Albania 2009) Find all differentiable functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = f(x/2) + (x/2)f'(x)$ for all $x \in \mathbb{R}$.

    Solution. First we show that f' is continuous everywhere. For $x \neq 0$, this is obvious by the continuity of f (of course, f' is in fact differentiable at x). To show f' is continuous at 0, we find by the definition of $f'(0)$ that $f(x) = xf'(0) + f(0) + o(x)$ and observe that

    $$\lim_{x\to 0} f'(x) = \lim_{x\to 0} \frac{f(x) - f(x/2)}{x/2} = \lim_{x\to 0} f'(0) + o(1) = f'(0),$$

    as desired.

    Now observe that for any $x \neq 0$, there exists x' strictly between $x/2$ and x satisfying $f'(x') = f'(x)$ (by the mean value theorem). (*) Assume for the sake of contradiction that some $y \neq f'(0)$ lies in the range of f', and take the infimum $m \geq 0$ of $S = \{|x| : f'(x) = y\}$. By (*), S has an infinite subsequence of decreasing absolute value tending to $\pm m$ (for a fixed sign), whence $m \in S$ by continuity and $m \neq 0$ by assumption. Then if we take x_0 of absolute value m such that $f'(x_0) = y$, there exists (again by (*)) x_0' strictly between $x_0/2$ and x_0 satisfying $f'(x_0') = f'(x_0) = y$, contradicting the definition of m.

    Thus $f'(x)$ is constant, so $f(x) = ax + b$ for some reals a, b; this clearly works.

69. (St. Petersburg) Is it possible to partition the set of all 12-digit numbers into groups of four numbers such that the numbers in each group have the same digits in 11 places and four consecutive digits in the remaining place?

    Solution. We show that even the weakening to sums of digits does not allow such a partition. Indeed, depending on interpretation, this would require

    $$\sum x^{s_i}(1 + x + x^2 + x^3) \in \{(x + \cdots + x^9)(1 + \cdots + x^9)^{11}, (1 + \cdots + x^9)^{12},$$

    whence reducing modulo $1 + x + x^2 + x^3$, we must have either $(1+x)^{11}$ or $(1+x)^{12}$ divisible by $1 + x + x^2 + x^3$. Taking $x = i$, for instance, shows this is not possible.

70. (St. Petersburg 2003) Let p be a prime and let $n \geq p$ and $a_1, \ldots, a_n$ be integers. Define $f_0 = 1$ and f_k the number of subsets $B \subseteq \{1, 2, \ldots, n\}$ having k elements such that $p \mid \sum_{i\in B} a_i$. Show that p divides $f_0 - f_1 \pm \cdots + (-1)^n f_n$.

    Solution. If $F(x, y) = \prod_{i=1}^n (1 + x^{a_i} y)$, then we just need to show that $x^p - 1 \mid F(x, -1)$ in $\mathbb{F}_p$, which is easy since $n \geq p$ means $(x-1)^p \mid F(x, -1)$.

    Alternatively, we can get a bit of a strenghtening for $n \geq 2p$ by considering extensions of v_p (working in $\mathbb{Q}_p$ instead?) to things like $v_p(1 - \omega^k)$, where ω is a primitive p^{th} root of unity.

71. (M. Haiman, D. Richman, AMM 6458) Let x, y be noncommutative variables. Express in terms of n the constant term of the expression $(x + y + x^{-1} + y^{-1})^n$.

    Solution. I think it is actually A035610. (The proof also works for "the number of length $2n$ words over an alphabet of size 4 that can be built by repeatedly inserting doublets into the initially empty word". A direct bijection shouldn't be hard to find, although it seems a bit annoying to describe explicitly.)

    Let $f(n)$ (for $n \geq 0$) be the constant term of $(x + y + x^{-1} + y^{-1})^{2n}$ (of course, the answer is 0 for odd exponents), or equivalently, the number of expressions $w_1 w_2 \cdots w_{2n}$ evaluating to 1 in the free group generated by x, y, x^{-1}, y^{-1} (call these *n-words*). In the same vein as the Catalan left/right parentheses bijection (where we match the leftmost parenthesis with its partner to get a recursion), it will be convenient to define $g(n)$ (for $n \geq 1$) as the number of *primitive n-words* $w_1 w_2 \cdots w_{2n}$ evaluating to 1 such that there does not exist $m \in (0, 2n)$ satisfying $w_1 w_2 \cdots w_m = 1$ (of course, m would have to be even for this to happen).

Clearly $f(0) = 1$ and $g(1) = 4$, and considering the smallest index m such that $w_1 w_2 \cdots w_{2m} = 1$ given an n-word $w_1 w_2 \cdots w_{2n}$, we find

$$f(n) = g(n)f(0) + g(n-1)f(1) + \cdots + g(1)f(n-1)$$

for $n \geq 1$.

It remains to compute $g(n)$. First we prove by a simple induction on $m \geq 1$ that a primitive m-word $w_1 w_2 \cdots w_{2m}$ must have $w_1 w_{2m} = 1$: the claim is obvious for $m = 1$ and for $m \geq 2$, there exists an index $i \in [1, 2m+1]$ such that $w_i w_{i+1} = 1$, where by primitiveness $i \in (1, 2m+1)$; now by the inductive hypothesis on $w_1 \cdots w_{i-1} w_{i+2} \cdots w_{2m}$ the claim follows. (*)

Now it is not too difficult to find a recursion for $g(n)$ (although it is trickier than the Catalan case), as an n-word $W = w_1 \cdots w_{2n}$ is primitive iff it's of the form $wU_1 U_2 \cdots U_r w^{-1}$ for some letter w and non-empty primitive words $U_1, U_2, \ldots, U_r$ ($r \geq 0$) that do not start with w^{-1}. Indeed, if W is a primitive n-word then by (*) $w_1 w_{2n} = 1$, so expressing the $n-1$-word $w_2 \cdots w_{2n-2}$ as a product of non-empty primitive words $U_1 \cdots U_r$ for some $r \geq 0$ and noting that $wU_1 \cdots U_k w^{-1} = 1$ for all $k \in [0, r]$, we see that no U_i can start with w^{-1}.

On the other hand, if W is of the form $wU_1 U_2 \cdots U_r w^{-1}$ but not primitive, then take the smallest m such that $w_1 \cdots w_{2m} = 1$ (which must be a primitive m-word), so $w_1 w_{2m} = 1$. But the U_i are all primitive, so $w_2 \cdots w_{2m-1} = 1$ is of the form $U_1 \cdots U_k$ for some $k \in (0, r)$, contradicting the fact that by construction, U_{k+1} (which must start with $w_{2m} = w_1^{-1}$) does not start with w^{-1}.

Thus

$$g(n) = \sum \left(\frac{3}{4} g(\ell_1)\right) \left(\frac{3}{4} g(\ell_2)\right) \cdots \left(\frac{3}{4} g(\ell_r)\right),$$

where the sum runs over all r-tuples of positive integers satisfying $\ell_1 + \cdots + \ell_r = n - 1$. Equivalently by induction (we can also get this directly by noting that $wU_2 U_3 \cdots U_r w^{-1}$ is also primitive),

$$g(n) = \frac{3}{4} \sum_{k=1}^{n-1} g(k) g(n-k),$$

whence

$$G(x) = \sum_{n \geq 1} g(n) x^n = 4x + \frac{3}{4} G(x)^2.$$

From earlier, we have

$$F(x) = \sum_{n \geq 0} f(n) x^n = 1 + F(x) G(x),$$

so now we can solve to get

$$G(x) = \frac{2}{3}(1 - \sqrt{1 - 12x}) = \sum_{n \geq 1} 4 \cdot 3^n C_{n-1} x^n$$

and

$$F(x) = \frac{1}{1 - G(x)} = \sum_{n \geq 0} (16x)^n \left(1 - \sum_{r=1}^{n} \left(\frac{3}{16}\right)^r C_{r-1}\right),$$

where C_n denotes the n^{th} Catalan number.

Comment. There is also a more visual block walking proof (Mark Sellke showed me this). Start from the origin in the Cartesian plane (we will always stay on or above the x-axis). At the k^{th} step ($k \geq 1$), suppose we're at $(k-1, t)$, and move up by $(+1, +1)$ if there exists $j \in [1, k-1]$ such that

$w_j w_{j+1} \cdots w_k = 1$; otherwise move down by $(+1, -1)$. It's not hard to show that we always stay above the y-axis, so using a similar notion to the primitiveness described earlier, we can directly find the continued fraction of $F(x)$, i.e.

$$\cfrac{1}{1 - \cfrac{4x}{1 - \cfrac{3x}{1 - \cfrac{3x}{1 - \cfrac{3x}{1 - \ddots}}}}},$$

from which it's standard to derive a closed form for F (we get a quadratic equation, as above).

72. Generating functions for Catalan numbers modulo p: from $(1-4x)^{-1/2} = \sum_{n\ge 0} \binom{2n}{n} x^n$, we have $(1-4x)^{(p-1)/2} = \sum_{n=0}^{p-1} \binom{2n}{n} x^n$ in $\mathbb{F}_p$. "Integrating," we can get a nice expression for the Catalan generating function as well.

73. Show that $\sum_{k=1}^{p-1} \binom{2k}{k} \frac{1}{k} \equiv 0 \pmod p$ for $p > 3$ prime.

    Solution. Converting to mod p^2 in the standard way, we just need to show that $\sum_{k=1}^{p-1} (-1)^k \binom{p}{k} \binom{2k}{k} \equiv 0 \pmod{p^2}$. Observe that $\binom{2p-k}{p} \equiv 1 \pmod p$ for $k \in (0, p)$. So it's enough to show that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{2n-k}{n} \binom{2k}{k} = 0$$

    whenever $3 \nmid n$. relevant paper

74. Let a, b, c be positive real numbers such that $3 + 1/a + 1/b + 1/c \le 2(a + b + c)$. Prove that $\sum_{cyc} 1/\sqrt{a + b^3 + c^5} \le 3/\sqrt{a + b + c}$.

    Solution. The denominators are ugly, and stuff is in the wrong direction for Holder/Cauchy in the usual way, so we just kill the denominators. This is easy:

$$(a + b^3 + c^5)(a + 1 + 1/c)(a + 1 + 1/c) \ge (a + b + c)^3 \implies \sqrt{\frac{a+b+c}{a+b^3+c^5}} \le \frac{a+1+1/c}{a+b+c},$$

    so we're done by summing up.

75. For a positive integer n with prime factorization $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ (where $p_1 < \cdots < p_k$), define $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$ and let $d_1 < \cdots < d_{d(n)}$ be the divisors of n. For a fixed positive integer $j < d(n)$, let t be the smallest integer such that $\prod_{i=1}^{t} (\alpha_i + 1) \nmid j$. Prove that $d_{j+1}/d_j \le p_t$.

    Solution. We need an extra condition like $p_1 < \cdots < p_k$, or else $n = 5 \cdot 2 \cdot q_1 \cdot q_2 \cdots$ is a counterexample for sufficiently large primes q_i. Indeed, $\alpha_i = 1$ for all i, so taking $j = 2$, we have $t = 2$. But $d_3/d_2 = 5/2 > p_t = 2$, contradiction. (This can be easily generalized, especially when all the $\alpha_i = 1$ for all i, as then we would need $d_{j+1}/d_j \le 2$ for all j by taking suitable permutations of the p_i but in general $2^{d(n)} < n$.)

    Suppose $d_{j+1} > d_j p_t > d_j$ for contradiction. Then we can prove that for any $i \in (0, j)$ such that $\gcd(d_i, p_1 \cdots p_t) = 1$, $d_i p_1^{\alpha_1} \cdots p_t^{\alpha_t} \le d_j$. Indeed, $d_i < d_j$ implies there is a largest M with prime factors among $p_1, \ldots, p_t$ such that $d_i M \le d_j$, and if there exists $l \in [1, t]$ such that $v_{p_l}(M) < \alpha_l$, $d_i M p_l \in (d_j, d_j p_t]$ by maximality and the fact that $p_l \le p_t$, contradicting the fact that $d_{j+1} > d_j p_t$ (since $d_i M p_l \mid n$). On the other hand, we can divide out some powers of $p_1, \ldots, p_t$ from any $d_r < d_j$ to get such a d_i, so $\prod_{i=1}^{t} (\alpha_i + 1) \mid j$, contradiction.

76. On some planet, there are 2^N countries, where $N \ge 4$. Each country has a flag N units wide and one unit high composed of N fields of size 1×1, each field being either yellow or blue. No two countries have the same flag. We say that a set of N flags is diverse if these flags can be arranged into an $N \times N$

square so that all N fields on its main diagonal will have the same color. Determine the smallest positive integer M such that among any M distinct flags, there exist N flags forming a diverse set.

Solution. By taking the set of guys starting with 10, we have $f(n) \geq 2^{n-2} + 1$ for $n \geq 2$. We now show that $f(n) \leq 2^{n-2} + 1$ for $n \geq 4$.

One way is induction, where the base case $n = 4$ can be done by analyzing the left and right halves of strings separately and combining things together (it's slightly tedious though). For $n \geq 5$, if we assume the induction hypothesis, then consider a set S of $2^{n-2}+1$ n-flags. Now take a non-monochrome column, say the first, and say there are at least $2^{n-3}+1$ 1s in this column by pigeonhole. Now removing the first column the rest follows easily by induction (since we chose a non-monochrome column, we have both 0s and 1s left to satisfy the top left corner).

A cleaner, more insightful way is via Hall. We can construct two bipartite graphs G_0, G_1 in the obvious ways, letting F denote the set of flags and C the set of columns, drawing an edge between f and c if f has a 0 in column c for G_0 and similar for G_1. Suppose a set $D = \{c_1, \ldots, c_k\}$ of columns fails the hall condition in G_0: then $F \setminus N(S)$ has all 1s in columns c_1 through c_k, so $2^{n-2}+1 = |F| \leq |N(S)|+2^{n-k} \leq k-1+2^{n-k}$, so $k-2 \geq 2^{k-2}-1$ (since $n \geq k$), which means $k \leq 3$. But if $k = 3$, then $n \geq 4$ screws things up, so $k \leq 2$. The case $k = 1$ corresponds to $|N(S)| = 0$, i.e. a monochrome column of 1s. On the other hand, the case $k = 2$ corresponds to $|N(S)| = 1$ and $2^{n-2} = |F \setminus N(S)|$ (since equality must hold), in which case $F \setminus N(S)$ contains every flag starting with 11 and since $2^{n-2} \geq n$ (since $n \geq 4$), we can take the $n-2$ flags $1110\ldots$, $11110\ldots$, $111110\ldots$, etc. in addition to any two remaining flags starting with 11. So we only need to consider the case $k = 1$: since there's at most one monochrome column, we're done. (The official solution doesn't do this explicitly, instead just taking a failing set of columns from each of the graphs and getting a contradiction.)

77. Given $2n+1$ points, no four concyclic and no three collinear, show that exactly n^2 distinct circles pass through three of them and contain $n-1$ points inside and $n-1$ outside.

Solution. The most natural way is smoothing and induction. Say we have $P_1, \ldots, P_{2n+1}$ and we want to show that moving P_1 to Q_1 doesn't change the number of halving circles. It's enough to prove this when P_1Q_1 is a line crossing only one boundary determined by $P_2, \ldots, P_{2n+1}$ (circumcircles through any three and lines through any two), because the only way the number of halving circles can change is if P_1 changes position relative to some $(P_iP_jP_k)$ (with $i, j, k \neq 1$) or some P_i changes position relative to $(P_1P_jP_k), (Q_1P_jP_k)$ $(j, k \neq 1)$, and this can only happen if P_1Q_1 (the segment) intersects the boundary of some $(P_iP_jP_k)$ or some line P_jP_k (the latter only in the second case). Now it's easy to see that only crossing a line P_iP_k does nothing except swap outside and inside points of $(P_1P_iP_k)$ and $(Q_1P_iP_k)$ (which preserves halving property), so we just have to deal with the case when we cross WLOG arc P_iP_k not containing P_j of $(P_iP_jP_k)$, and further WLOG P_1 moves out (as long as we show P_1 and Q_1 are "exchangeable" we can reverse if necessary). By the minimality assumption (that we only cross one boundary), $P_1P_iP_kP_j$ is convex, so it is easy to then show (using minimality more) that $(P_1P_iP_k), (P_jP_iP_k)$ are of type (a, b) and change to type $(a-1, b+1)$ (we lose P_j) and $(P_1P_jP_i), (P_1P_jP_k)$ are of type $(a-1, b+1)$ and change to type (a, b) (we gain P_k, P_i respectively), where (u, v) means u on inside and v on outside.

So it's enough to construct one example (and we can also exploit inductive hypothesis). So we want to use symmetry, starting with an approximately regular $(2n-1)$-gon and letting another point O be its center (which is contained in all circumcircles from the regular polygon). Now the simplest way to finish is if we can add a point T such that the remaining $2n-1$ halving circles are of the form (TP_iO) for $1 \leq i \leq 2n-1$. This is easy if we let T be a point outside of all circles determined by the other $2n$ points. By construction, (TXY) is a halving circle iff XY is a halving line of the $2n$ points not equal to T.

For the sake of completeness, I'll mention two solutions to the generalized problem with a set S of $2n+1$ points $(n \geq 1)$.

The first is Federico Ardila's smoothing argument, which someone linked to in another thread.

The second (which is not as motivated, but perhaps more beautiful) is based on ideas from a paper on the connection between balancing lines and halving triangles (in particular, Theorem 2.2 from here, which is essentially a subtler application of the invariant used in IMO 2011.2).

Here we use (a special case of) the inverted form of Theorem 2.2, i.e. the fact that for a fixed point $P \in S$ and circle C passing through P but no other points of S, there are exactly $\min(m, 2n-m)$ ordered pairs of points $(Q, R) \in S^2$ with (PQR) a separator of S, Q inside C, and R outside C, where m is the number of points in S lying inside C.

Take a point O such that $OP \neq OQ$ for any two distinct points $P, Q \in S$, and label the points P_i $(1 \leq i \leq 2n+1)$ of S so that $OP_1 < \cdots OP_{2n+1}$ (this may be more natural with stereographic projection, interpreting this as "decreasing z-coordinates" instead); let C_i denote the circle centered at O passing through P_i. Then we can identify each separator $(P_iP_jP_k)$ (where $i < j < k$) with C_j, the unique circle C_l passing through one of P_i, P_j, P_k and "separating" the other two. Furthermore, C_i contains exactly $i-1$ points in its interior for every i, so by the previous paragraph, there must be exactly

$$\sum_{i=1}^{2n+1} \min(i-1, 2n-i+1) = n^2$$

separators, as desired.

And as noted in Ardila's paper, we can just as easily count the total number of separators of type (a, b) *or* (b, a) (where there are either exactly a inside and b outside or a outside and b inside) whenever $a + b = 2n - 2$ (the original problem is just $(n-1, n-1)$). But the *general* inverted form of Theorem 2.2 still applies, except we have to sum up $2\min(i-1, 2n-i+1, a+1, b+1)$ instead of $\min(i, 2n-i)$, where the extra factor of 2 accounts for our inability (with this method) to distinguish between types (a, b) and (b, a) whenever $a \neq b$.

78. Let $z_1, \ldots, z_n$ be the roots of $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_i \in \mathbb{C}$. Show that $\frac{1}{n}\sum |z_k|^2 < 1 + \max_{0 \leq k \leq n-1} |a_k|^2$.

Solution. Go by contradiction. Then by the classical Mahler measure bound,

$$\sum_{k=1}^{n} |z_k|^2 \geq n + |a_0|^2 + \cdots + |a_{n-1}|^2 \geq (n-1) + \prod_{k=1}^{n} \max(1, |z_k|^2).$$

If some $z_i \leq 1$, then subtracting 1 from both sides we can just WLOG remove it (the corresponding $n-1$ inequality then still holds), so suppose $z_k > 1$ for all k WLOG. But by induction or smoothing we can show that $x_1 \cdots x_n + n - 1 > x_1 + \cdots + x_n$ whenever $x_1, \ldots, x_n > 1$.

79. (Finite projective planes) Let $G = P \cup L$ be a bipartite graph (with $|P|, |L| \geq 2$) such that $|N(P_i) \cap N(P_j)| = 1$ and $|N(L_i) \cap N(L_j)| = 1$ for distinct i, j. Characterize all such non-regular graphs.

Solution. If $N(l) = P$ for some $l \in L$, then since $|L| > 1$, we see that there must exist a point $p \in P$ such that $N(l') = \{p\}$ for all $l' \neq l$ in L: this is one "degenerate" case. Of course, there is also the case with L, P swapped: but this is equivalent. Now suppose neither of these is the case; there is only one more degenerate case. (*)

Now we show everything has degree at least 2. Since $|P|, |L| > 1$, everything has degree at least 1, so suppose $N(l) = \{p\}$ for some $l \in L$; then $p \in N(l')$ for all $l' \neq l$ in L, contradicting (*).

The key idea is this: if we fix $L_1 \in L$ with neighbors $P_1, \ldots, P_r$ ($r \geq 2$ by the previous paragraph), then any two of P_i, P_j with $i, j \leq r$ share only the neighbor L_1. Thus for any $p \notin \{P_1, \ldots, P_r\}$, the $N(p) \cap N(P_i)$ are distinct. On the other hand, every $l \in L$ shares a neighbor with L_1, so $|N(p)| = |N(L_1)|$. So whenever $p_1 \neq p_2$ are in P and $|N(p_1) \cup N(p_2)| < |L|$, $|N(p_1)| = |N(p_2)|$.

However, if $|N(p_1) \cup N(p_2)| = |L|$, then $l = N(p_1) \cap N(p_2)$ has degree exactly 2 (as each of $N(l)$'s neighbors only share l as a common neighbor, and we need $N(p_1) \cup N(p_2) = L$). So $|N(p)| = |N(l)| = 2$ whenever $p \neq p_1, p_2$ (since then p is not adjacent to l). On the other hand, if $l' = N(p) \cap N(p_2)$ and $\deg l' = 2$, then $\deg p_1 = 2$. But if $\deg l' > 2$, then since $l' \neq l$ we must have $P = N(l') \cup N(l)$ (or else $2 < |N(l')| = |N(l)| = 2$), and by dual logic we know $N(l') \cap N(l) = p_2$ must have degree exactly 2.

So if such l' doesn't exist, we must have $\deg p_t = 2$ for all $p_t \in P$ in this case, whence $|L| = 3$. Summing up degrees, we have $|P| = 3$ and G isomorphic to C_6.)But this is regular anyway.)

In the more interesting case where such l' exists, then $N(p_1) \cup N(p_2) = L$ and $N(l') \cup N(l) = P$, so by our above logic we know all $p \neq p_1$ have degree 2 and (similarly) all $l_i \neq l'$ have degree 2. So we essentially have $p_1, \ldots, p_r$ for P and $l_1, \ldots, l_s$ for L, where $N(p_1) = \{l_2, \ldots, l_s\}$, $N(l_1) = \{p_2, \ldots, p_r\}$. But $\deg p_i = \deg l_j = 2$ for $i, j \neq 1$, so it's easy to see $r = s$ and WLOG we have $N(p_i) = \{l_1, l_i\}$, $N(l_i) = \{p_1, p_i\}$ for $i = 2, \ldots, r$. This is the other degenerate case.

Otherwise, if $|N(p_1) \cup N(p_2)| < |L|$ and $|N(l_1) \cup N(l_2)| < |P|$ always, then $N(p)$ is constant for $p \in P$ and also equal to some $N(l_p)$; but $N(l)$ must also be constant, so we conclude that G is regular and $|L| = |P|$. Suppose it is d-regular ($d > 1$); then considering $N(l)$ for $l \in N(p)$ for a fixed p, we conclude that $|L| = |P| = 1 + (d-1)d$.

80. Show that we can fill a $p^2 + p + 1 \times p^2 + p + 1$ board with 0s and 1s such that every row and column has exactly $p + 1$ 1s and if the centers of four unit squares form a rectangle whose edges are parallel to the edges of the board, at least one of these squares contains a 0.

Solution. This is the incidence matrix of the finite projective plane of order p!

We can in fact prove it has to be this up to ordering. Label the rows $P_1, \ldots, P_n$ and the columns $L_1, \ldots, L_n$ ($n = p^2 + p + 1$), where (i, j) has a 1 iff $P_i \in L_j$. Then the conditions force $|L_i \cap L_j| \leq 1$ for distinct i, j, so summing up and using regularity we get $n\binom{p+1}{2} = \sum |L_i \cap L_j| \leq \binom{n}{2}$. But equality must hold, so in fact $|L_i \cap L_j| = 1$ for all $i \neq j$. Considering the dual sets $P_1, \ldots, P_n$ (abuse of notation here), we can also get $|P_i \cap P_j| = 1$ for all $i \neq j$, which along with regularity implies that we must have a projective plane.

We base the construction on $\mathbb{F}_p$. Take the points to be of the form $p = (a, b, c) \in \mathbb{F}_p^3$, where not all a, b, c are zero and (x, y, z) is considered the same as (tx, ty, tz) for any $t \neq 0$. Then considering the first nonzero coordinate we see we have n points. On the other hand, we can just take the line corresponding to $l = (a, b, c)$ to consist of the points (x, y, z) such that $ax + by + cz = 0$. Then it is easy to verify that every two lines intersect in a unique point up to scaling and every two points determine a unique line, as desired. (It is easy to see that every line contains $\frac{p^2-1}{p-1} = p + 1$ points, and every point lies on $\frac{p^2-1}{p-1} = p + 1$ lines by duality/symmetry.)

81. (AoPS) Consider the sequence defined by $x_1 = 1$ and $x_{n+1} = 1 + \frac{n}{x_n}$. Find all n such that x_n is an integer.

Solution. Let $a_n = x_1 \cdots x_n$ for $n \geq 0$ (where $a_0 = 1$ is the empty product) so that the recurrence becomes the more wieldy $a_{n+1} = a_n + na_{n-1}$ (for $n \geq 1$). Rewriting the recurrence as $\frac{a_{n+1}}{n!} = \frac{a_n}{n!} + \frac{a_{n-1}}{(n-1)!}$ and letting $f(x) = \sum_{n \geq 0} \frac{a_n}{n!} x^n$ denote the exponential generating function of (a_n), we have

$$\begin{aligned} f'(x) = \sum_{n \geq 1} \frac{a_n}{(n-1)!} x^{n-1} &= \frac{a_1}{0!} + \sum_{n \geq 1} \frac{a_{n+1}}{n!} x^n \\ &= \frac{a_1}{0!} + \sum_{n \geq 1} \frac{a_n}{n!} x^n + \sum_{n \geq 1} \frac{a_{n-1}}{(n-1)!} x^n \\ &= a_1 + (1 + x) f(x) - a_0 = (1 + x) f(x). \end{aligned}$$

But $f(0) = 1$, so dividing both sides by $f(x)$ and integrating we get $\log f(x) = x + x^2/2$ and

$$f(x) = \exp\left(x + \frac{x^2}{2}\right) = \sum_{n \geq 0} \frac{1}{n!} \left(x + \frac{x^2}{2}\right)^n = \sum_{n \geq 0} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} \left(\frac{x^2}{2}\right)^k x^{n-k},$$

from which we can easily find

$$a_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (2k)!!.$$

(Note that we can also directly use the recurrence relation and induction to show that a_n is the number of ways to partition $[n]$ into sets of size 1 or 2, by considering the size of the set $n + 1$ belongs to.)

For odd primes p it directly follows that $a_{np} \equiv 1 \pmod p$ for $n \geq 0$ (for $n \geq 1$, observe that the $(2k)!!$ terms vanish modulo p for $k \geq (p+1)/2$, and $\binom{np}{2k} = \frac{np}{2k}\binom{np-1}{2k-1}$ for $k \geq 1$). Now suppose for contradiction that $p \mid a_{n_0}, a_{n_0+1}$ with $n_0 \geq 0$ minimal; then $a_0 = a_1 = 1 \implies n_0 \geq 2$. But we know $p \nmid n_0$, so $a_{n_0+1} = a_{n_0} + n a_{n_0-1}$ implies $p \mid a_{n_0-1}, a_{n_0}$, contradicting the minimality of n_0.

Thus $a_n \mid a_{n+1}$ can only occur if a_n is a power of 2. But it's easy to show by induction that $\ell_n = \min(v_2(a_n), v_2(a_{n+1})) \leq v_2(n!)$ for $n \geq 1$, as

$$2^{\ell_{n+1}} \mid (p_{n+1}, p_{n+2}) = (p_{n+1}, (n+1)p_n) \mid (n+1)(p_{n+1}, p_n)$$

(we can also find the exact value of $v_2(a_n)$ as **Rust** did, but this is unnecessary). So if $a_n \mid a_{n+1}$ for some $n > 3$, then

$$2^{n-1} \geq 2^{v_2(n!)} \geq 2^{\ell_n} = a_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}(2k)!! > \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = 2^{n-1},$$

which is absurd. But $a_3 = 4 \nmid 10 = a_4$, so we see that only $n = 0, 1, 2$ work, corresponding to $x_1, x_2, x_3 \in \mathbb{Z}$ in the original sequence.

82. (generatingfunctionology) Show that $\sum_{k=0}^{2n}(-1)^{n-k}\binom{2n}{k}^2 = \binom{2n}{n}$.

    Solution. We use DIE (Description, Involution, Exception). The LHS is an alternating sum of the number of ways to choose k elements of $\{1, \ldots, 2n\}$ and k of $\{2n+1, \ldots, 4n\}$, so consider the pairs $\{i, 2n+i\}$. If we toggle (i.e. symmetric difference operate) the first pair with an even number of elements chosen (i.e. 0 or 2), then we have an involution with things canceling out, except when every pair has exactly 1 element chosen. In this case, we have $k = n$, corresponding to a leftover contribution of $(-1)^{n-n}\binom{2n}{n}$, so we're done.

    We can also generalize the identity and use snake oil (as is, there are too many ns, making it hard to do directly). Doing $\binom{n}{k}\binom{m}{k}$ doesn't help much, but rewriting one of the coefficients as $\binom{n}{n-k}$ and replacing the bottom n with m does: we get

$$\sum_{m,n,k \geq 0} (-1)^k \binom{n}{k}\binom{n}{m-k} x^m y^n = \frac{1}{1 - y(1-x^2)},$$

    from which the rest is obvious.

83. (David Yang) Find the smallest positive integer k such that for any simple directed graph G (with 2-cycles permitted, but not 1-cycles) with all out-degrees equal to 2, we can assign one of k colors to each of its vertices so that no vertex $v \in V(G)$ has the same color as both of its out-neighbors.

    Solution. The answer is 3. First we show $k = 2$ doesn't work: suppose it does (let our color sets be A, B) for G defined by $V(G) = \mathbb{Z}/7\mathbb{Z}$ and $(u, v) \in E(G)$ iff $v - u \in \{1, 3\}$. As 7 is odd, there exist two neighboring residues of the same color, say $C(0) = C(1) = A$. Then $(0,1), (0,3) \in E(G) \implies C(3) = B$. If $C(2) = A$, then $(1,2), (1,4) \implies C(4) = B$, so $(3,4), (3,6) \implies C(6) = A$, whence $(6,0), (6,2) \in E(A)$, contradiction. Thus $C(2) = B$, so $C(2) = C(3) = B \implies C(5) = A$. Now $(4,5), (4,0) \implies C(4) = B$, and $(5,6), (5,1) \implies C(6) = B$. But then $C(3) = C(4) = C(6) = B$, contradicting $(3,4), (3,6)$.

    Now we show $k = 3$ works, by inducting on the obvious generalization to $\deg^+(v) \leq 2$ always, with the base case vacuously true.

    First suppose there exists $v \in G$ with $\deg^-(v) \leq 1$, and find a good 3-coloring in A, B, C for $G \setminus \{v\}$. Suppose for contradiction that we cannot place v in any subset without violating the conditions. But we only violate a fixed S if $u, w \in S$ and $(u, v), (u, w) \in E(G)$ or if $N(v) \subseteq S$, contradicting (by pigeonhole) the fact that $\deg^-(v) \leq 1$ implies there's at most one violation of the first type and (obviously) at most one of the second type.

    The only case remaining is $\deg^-(v) \geq 2$ for all v: but summing up and using $\deg^+(v) \leq 2$ always, we get that in fact $\deg^+(v) = \deg^-(v) = 2$ for all $v \in V(G)$. So take a partition $A \cup B \cup C$ maximizing the number of edges between vertices of distinct subsets (i.e. total between A, B, B, C, C, A), and suppose for contradiction that there exist $u, v, w \in A$ with $(u, v), (u, w) \in E(G)$. As $\deg^-(u) = 2$, we can WLOG $|N^-(u) \cap B| \leq 1$. Then moving u to B gives a net contribution of at least $+2 - 1 > 0$, contradiction.

84. (China 2010) Given a positive integer n, find the largest real number $\lambda = \lambda(n)$ such that for any degree n polynomial with complex coefficients $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and any permutation $x_0, x_1, \ldots, x_n$ of $0, 1, \ldots, n$, the following inequality holds: $\sum_{k=0}^{n} |f(x_k) - f(x_{k+1})| \geq \lambda |a_n|$, where $x_{n+1} = x_0$.

Solution. I think the answer is $\lambda(n) = \frac{n!}{2^{n-2}}$.

Let $f(k) = t_k$ for $k = 0, 1, \ldots, n$ so matching leading coefficients from Lagrange interpolation (note that $\deg f < n + 1$) we have

$$f(x) = \sum_{k=0}^{n} t_k \prod_{j \neq k} \frac{x - j}{k - j} \implies a_n = \sum_{k=0}^{n} \frac{t_k(-1)^{n-k}}{k!(n-k)!}.$$

(Clearly $\deg f = n$ iff $a_n \neq 0$.) This gives us our equality case easily: letting $t_k = (-1)^k$ and

$$(x_0, \ldots, x_n) = (0, 2, \ldots, 2\lfloor n/2 \rfloor, 1, 3, \ldots, 2\lfloor (n-1)/2 \rfloor + 1),$$

we have

$$\frac{\sum_{k=0}^{n} |f(x_k) - f(x_{k+1})|}{|a_n|} = \frac{\sum_{k=0}^{n} |t_{x_k} - t_{x_{k+1}}|}{|\sum_{k=0}^{n} \frac{t_k(-1)^{n-k}}{k!(n-k)!}|} = \frac{2|1 - (-1)|n!}{2^n} = \frac{n!}{2^{n-2}},$$

where we note that $a_n = \pm 2^n \neq 0$. So it remains to show that

$$\sum_{k=0}^{n} 2^{n-2} |t_{x_k} - t_{x_{k+1}}| \geq \left| \sum_{k=0}^{n} t_k (-1)^k \binom{n}{k} \right|$$

always holds. By the triangle inequality, it suffices to show that there exist reals $\alpha_0, \ldots, \alpha_n$ such that $|\alpha_k| \leq 2^{n-2}$ and $\alpha_k - \alpha_{k-1} = (-1)^{x_k}\binom{n}{x_k}$ for all k. Indeed, we would then have

$$\sum_{k=0}^{n} t_{x_k}(-1)^{x_k}\binom{n}{x_k} = \sum_{k=0}^{n} t_{x_k}(\alpha_k - \alpha_{k-1}) = \sum_{k=0}^{n} \alpha_k (t_{x_k} - t_{x_{k+1}}).$$

But this is easy: let $m = \min_{0 \leq k \leq n} \sum_{i=1}^{k} (-1)^{x_i}\binom{n}{x_i}$ and $M = \max_{0 \leq k \leq n} \sum_{i=1}^{k} (-1)^{x_i}\binom{n}{x_i}$, and observe that $0 \leq M - m \leq 2^{n-1}$. So taking

$$\alpha_k = \frac{-m - M}{2} + \sum_{i=1}^{k} (-1)^{x_i}\binom{n}{x_i}$$

for all k, we get $\alpha_k - \alpha_{k-1} = (-1)^{x_k}\binom{n}{x_k}$ and

$$-2^{n-2} \leq \frac{m - M}{2} \leq \frac{-m - M}{2} + m \leq \alpha_k \leq \frac{-m - M}{2} + M = \frac{M - m}{2} \leq 2^{n-2},$$

as desired.

85. (MOP 2008) Let $\mathcal{F}$ be a collection of 2^{n-1} subsets $A_1, A_2, \ldots$ of $\{1, 2, \ldots, n\}$ such that any three subsets have nonempty intersection. Prove that there is a common element x contained in every A_i.

Solution. As there are 2^{n-1} subsets, we must have exactly one of each complementary pair of sets. If $\{i\} \in \mathcal{F}$ for some i, then we're done, so suppose otherwise. Then $[n] \setminus \{1\}, \ldots \in \mathcal{F}$. But $\{i, j\} \cap [n] \setminus \{i\} \cap [n] \setminus \{j\} = \emptyset$, so $[n] \setminus \{i, j\} \in \mathcal{F}$ always. Continuing, we have $\{i, j, k\} \cap [n] \setminus \{i, j\} \cap [n] \setminus \{k\} = \emptyset$, so $[n] \setminus \{i, j, k\} \in \mathcal{F}$ but $\{i, j, k\} \notin \mathcal{F}$, etc. so by induction $\{1, 2, \ldots, n - 1\} \notin \mathcal{F}$, contradiction.

86. (MOP 2011, Ricky Liu) Let k be a positive integer, and divide the region R between the parallel lines $x = 0$ and $x = 2k$ in the Cartesian plane into $2k$ stripes of equal width, alternately colored white and black. Consider a convex polygon P lying completely inside R with at least one vertex on each of the lines $x = 0$, $x = 2k$. Prove that at least $\frac{2k-1}{4k}$ of P's interior must be black.

    Solution. We prove a slight generalization by induction: for every positive integer $m \geq 0$, if we divide the region R between the parallel lines $x = 0$ and $x = m$ into m strips of equal width and the first strip is black, then at least $\frac{m-1}{2m}$ of P's interior is white.

    Lemma. For $m \geq 2$, any triangle with its vertices on $x = 0$, $x = m - 1$, and $x = m$ is half white and half black.

    Proof. Induction, where we note that by symmetry we can generalize this statement to when the region between $x = 0$ and $x = 1$ is white as well. For $m = 2$ this is obvious. Suppose A, B, C are the vertices from left to right, and let AC intersect $x = 1$ at T. Then split into ATB and BTC.■

    For $m = 1$ this is obvious, so suppose $m > 1$ and assume the result for $m - 1$. Suppose the boundary of P intersects the lines $x = i$ for $i = 0, 1, \ldots, m$ such that the upper half of intersection points forms a convex polygon $Q_0Q_1 \ldots Q_m$ and the lower half forms $R_0R_1 \ldots R_m$ (where Q_i, R_i lie on $x = i$). Then it's not hard to show that the polygon P' formed by the sides

$$R_0Q_0, Q_1Q_2, Q_3Q_4, \ldots, Q_{2\lfloor m/2\rfloor-1}Q_{2\lfloor m/2\rfloor}, Q_mR_m, R_{2\lfloor m/2\rfloor}R_{2\lfloor m/2\rfloor-1}, \ldots, R_4R_3, R_2R_1$$

    is convex, has black area at most that of P, and white area at least that of P (e.g. by definition of Q_{2i-1}, Q_{2i}, every point of P lies above $Q_{2i-1}Q_{2i}$ between $x = 2i - 1$ and $x = 2i$ or below $Q_{2i-1}Q_{2i}$, proving the relevant area increases and decreases; we have convexity since $R_0Q_0Q_1 \ldots Q_mR_m \ldots R_1$ is convex, and we are just "extending" every other side to form P').

    So it's enough to prove the claim for polygons of the form P' with extreme vertices (i.e. actual ones not on edges) on $x = 0$, $x = m$, or in between $x = 2i - 1$ and $x = 2i$ for some i. Suppose such P' intersects the lines $x = i$ at A_i and B_i with $y(A_i) \geq y(B_i)$ (for $i \in \{0, m\}$, we might have $A_i = B_i$). Then it's enough to show that the regions $A_0A_mB_mB_0$, the part of P' above A_0A_m, and the part of P' below B_0B_m are each at least $\frac{m-1}{2m}$ white. Now observe that no vertex T of P' lies above $B_{m-1}B_m$ in the region between $x = m - 1$ and $x = m$: if it's colored white, then this true by construction (i.e. the smoothing), and if it's colored black, then the intersection of $B_{m-1}T$ and $x = m$ is a vertex of P' by construction, contradicting the fact that T is above $B_{m-1}B_m$. By convexity, the part of P' above A_0A_m is thus bounded by the lines A_0A_m, $x = 0$, and $A_{m-1}A_m$, so by the inductive hypothesis (consider the part of P' above A_0A_{m-1} bounded by $x = 0$ and $x = m - 1$) we have a white density of at least

$$\frac{m-1}{m}\frac{(m-1)-1}{2(m-1)} + \frac{1}{m}\frac{1}{2} = \frac{m-1}{2m},$$

    where we use the lemma to deal with $\triangle A_0A_{m-1}A_m$. By symmetry, this also works for the part below $B_{m-1}B_m$. We can just compute $A_0A_mB_mB_0$'s density directly: if m is odd, we get

$$\frac{[(a+d)+(a+2d)]+\cdots+[(a+(m-2)d)+(a+(m-1)d)]}{m(a+(a+md))} = \frac{m-1}{2m}$$

    by a symmetry argument, and if m is even we get

$$\frac{[(a+d)+(a+2d)]+\cdots+[(a+(m-1)d)+(a+md)]}{m(a+(a+md))} = \frac{1+\frac{d}{2a+md}}{2} \geq \frac{m-1}{2m},$$

    where we use the fact that $a, a + md \geq 0$.

    Equality cases are isosceles trapezoid for m odd and isosceles triangle for m even.

87. (WOOT 2013) Given that $f(x, y)$ is a polynomial in x for any fixed real number y, and $f(x, y)$ is a polynomial in y for each fixed real number x, must $f(x, y)$ be a polynomial in x and y?

    Solution. If we restrict ourselves to real inputs, then yes (otherwise $f(x, y) = [x \in \mathbb{C}]$ is an obvious counterexample).

By the problem conditions there exist functions $g_n(y)$ and $h_m(x)$ such that

$$f(x,y) = \sum_{n\ge 0} \binom{x}{n} g_n(y) = \sum_{m\ge 0} \binom{y}{m} h_m(x),$$

where for fixed (real) y we have $g_n(y) = 0$ for all $n > N(y)$ (where $N(y) = \deg_x f(x,y)$) and for fixed (real) x we have $h_m(x) = 0$ for all $m > M(x)$ (where $M(x) = \deg_y f(x,y)$).

But if we fix y to be a nonnegative integer u, then

$$\sum_{n=0}^{N(u)} \binom{x}{n} g_n(u) = \sum_{m=0}^{u} \binom{u}{m} h_m(x)$$

for all (real) x, whence $h_u(x)$ is a polynomial in x for all $u \ge 0$ by induction. (Similarly, we can show $g_v(y)$ is a polynomial in y for all $v \ge 0$, but this is unnecessary.)

Finally, because the reals are uncountable, there exists a nonnegative integer M such that $M(x) = M$ for infinitely many (real) x, whence for every $m > M(x)$, the polynomial $h_m(x)$ has infinitely many zeros and is thus identically zero, so we're done.

88. (WOOT Practice Olympiad) Let $\mathcal{P}$ be a convex polygon with n vertices, such that no four vertices are concyclic. If A, B, and C are three vertices of $\mathcal{P}$ such that the remaining $n-3$ vertices of $\mathcal{P}$ lie in the interior of the circumcircle of triangle ABC, then triangle ABC is said to be a *covering triangle* of polygon $\mathcal{P}$.

    Show that $\mathcal{P}$ has exactly $n-2$ covering triangles.

    Solution. The idea is just to characterize covering triangles ABC: if X is opposite BC of A, then $\angle BYC + \angle BXC > 180^\circ$ for any Y on the same side of BC as A, so we can call all such segments BC *major*. This condition holds vacuously for sides of $\mathcal{P}$, and we see that every covering triangle consists of major segments (and any triangle with major segments is covering). It's easy to see no two major segments intersect (except possibly at endpoints). Furthermore, every major side belongs to exactly one covering triangle and every major diagonal belongs to exactly two covering triangles, so pushing these facts forward we see that the major segments form a triangulation of $\mathcal{P}$.

    More generally, there are $f_n(k) = (k+1)((n-3-k)+1)$ triangles covering all but k points: induct with the double-counting relation $(n+1)f_n(k) = ((n+1-3)-k)f_{n+1}(k) + (k+1)f_{n+1}(k+1)$.

89. (RMM 2011) The cells of a square 2011×2011 array are labelled with the integers $1, 2, \dots, 2011^2$, in such a way that every label is used exactly once. We then identify the left-hand and right-hand edges, and then the top and bottom, in the normal way to form a torus (the surface of a doughnut). Determine the largest positive integer M such that, no matter which labelling we choose, there exist two neighbouring cells with the difference of their labels at least M. (Cells with coordinates (x,y) and (x',y') are considered to be neighbours if $x = x'$ and $y - y' \equiv \pm 1 \pmod{2011}$, or if $y = y'$ and $x - x' \equiv \pm 1 \pmod{2011}$.)

    Solution. After trying small cases we conjecture an answer of $2N-1$ for $N \ge 3$ (for $N = 2$ everything only has two instead of four neighbors). Inspired by the classical problem where the board doesn't wrap around, we try to find k such that when 1 through k are filled in, there are at least $2N-1$ "border" squares (filled squares that are next to an unfilled square). (In a sense, a suitable isoperimetric inequality.)

    The most obvious thing (which works for the classical version) to try is to go up to the smallest k for which every row and column has at least one filled square, or its dual (the first time some row or column is completely filled). This doesn't work for the new toroidal version, though, because we might only be able to get one "border" square if, in the first method, we last filled a row and end up with a column with only one filled square.

    Instead, we go until all rows have at least 2 filled in *or* all columns have at least 2. (Actually, this works for the original too, if we wait for 1 instead of 2.) If this happens for rows, then at most one row is completely filled in (or else either the rows or columns would've been satisfied before, depending on whether k is in or out of one of the complete rows). Now we can easily finish: the potential filled row will get at least 1 and the others at least 2 "border" squares—note that the "boundary" that exists in the classical version would've prevented this from working there.

For the construction just do a spiral after experimenting small cases.

90. (Engel NT, also http://oeis.org/A121319) Prove that 2^n has decimal representation ending in n infinitely often.

    Solution. $2^{36} \equiv 736 \pmod{10^3}$. Now it's enough to show that if $10^k < n < 10^{k+1}$ ($k \geq 1$) and $2^n \equiv 10^{k+1}d + n \pmod{10^{k+2}}$ for some $d \in [0, 9]$, then $2^{10^{k+1}d+n} \equiv 10^{k+1}d + n \pmod{10^{k+2}}$.

    By CRT, there are two obvious things: (1) $\phi(5^{k+2}) = 4 \cdot 5^{k+1} \mid 10^{k+1}d$, so $2^{10^{k+1}d+n} \equiv 2^n \pmod{10^{k+2}}$; and (2) $2^n > 10^{k+1} > 2^{k+1} \implies n \geq k+2$, so $2^{10^{k+1}d+n} \equiv 2^n \equiv 0 \pmod{2^{k+2}}$.

    But we also need to make sure the "lifting" gives us an infinite sequence since $d = 0$ could mess things up. So we actually want to write $2^n - n = 10^{k+1+\ell}(d + 10m)$ where $\ell \geq 0$ and d is a nonzero digit. Let $n' = 10^{k+1+\ell}d + n$; then $2^n \equiv n' \pmod{10^{k+2+\ell}}$, so as above we just need to verify that $2^{k+2+\ell}$ and $5^{k+2+\ell}$ both divide $2^n(2^{10^{k+1+\ell}d} - 1)$, which just follows from $2^n > 10^{k+1+\ell}$ and $\phi(5^{k+2+\ell}) = 4 \cdot 5^{k+1+\ell}$.

    Actually, if we increase k by 1 even if $d = 0$, we don't need the second case.

91. (IMO 2007) Consider five points A, B, C, D, and E such that $ABCD$ is a parallelogram and $BCED$ is a cyclic quadrilateral. Let ℓ be a line passing through A. Suppose that ℓ intersects the interior of the segment DC at F and intersects line BC at G. Suppose also that $EF = EG = EC$. Prove that ℓ is the bisector of angle DAB.

    Solution. This is equivalent to $CF = CG$, $AB = BG$, and finally $AD = DF$.

    Either angle chasing to get $\angle BDE = \angle ECG$ and $\angle DBE = \angle DCE$, or noting that $AD = BC$ means it's basically equivalent (by acute/obtuseness) for spiral similarity, we need to show $ED = EB$, our most natural condition yet.

    One way to finish is to use the E-Simson line of $\triangle BCD$. Alternatively, phantom point the spiral center taking DFC to BCG.

    We can also use complex numbers centered at unit circle (CFG).

    The converse is also true, if we set the phantom point E' the midpoint of arc BCD.

92. Form a $m \times n$ screen with unit screens. Initially, there are at least $(m-1)(n-1)+1$ unit screens turned on. In any 2×2 screen, as soon as there are 3 unit screens that are turned off, the 4th screen turns off automatically. Prove that the whole screen can never be totally off.

    Solution. Perimeter invariant isn't enough. But analyzing some small cases it's easy to come up with the following invariant: if we construct the bipartite graph $R \cup C$ with an edge iff (r, c) is off, then the set of connected components remains the same. If it's completely off eventually we need the whole graph to be connected, which is impossible unless there are at least $m + n - 1$ edges in the original.

93. Let $S(f)$ be the set of roots (without multiplicity) of a polynomial $f \in \mathbb{C}[x]$. Are there two distinct polynomials $P, Q \in \mathbb{C}[x]$ such that $S(P) = S(Q)$ and $S(P+1) = S(Q+1)$.

    Solution. No. Go by contradiction and suppose for disjoint sets of roots $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$,

    $$1 = [P(x)+1] - P(x) = c(x-a_1)^{r_1} \cdots (x-a_m)^{r_m} - c(x-b_1)^{s_1} \cdots (x-b_n)^{s_n}$$

    and

    $$1 = [Q(x)+1] - Q(x) = d(x-a_1)^{t_1} \cdots (x-a_m)^{t_m} - d(x-b_1)^{u_1} \cdots (x-b_n)^{u_n}.$$

    By differentiating, we get

    $$2\deg(P) - m - n = (r_1 - 1) + \cdots + (r_m - 1) + (s_1 - 1) + \cdots + (s_n - 1) \leq \deg(P) - 1,$$

whence $\deg(P) \le m+n-1$ and similarly, $\deg Q \le m+n-1$. Then we have

$$(x-b_1)\cdots(x-b_n) \mid c(x-a_1)^{r_1-1}\cdots(x-a_m)^{r_m-1} - d(x-a_1)^{t_1-1}\cdots(x-a_m)^{t_m-1} \neq 0,$$

so $n \le \max(\deg P - m, \deg Q - m) \le n-1$, contradiction.

Equivalent wording by Alex Zhu: Let S and T be the sets of roots of P and $P+1$, respectively, and let $\deg P = n \ge \deg Q$. Then P' has at least $n-|S|$ roots from S and at least $n-|T|$ from T, so $n-|S|+n-|T| \le \deg P'$, so $|S|+|T| \le n-1$. On the other hand, all elements of S and T are also roots of $P-Q=(P+1)-(Q+1)$, so $|S|+|T| \ge n$, contradiction.

94. For a function $f:\mathbb{R}\to\mathbb{R}$, not necessarily continuous, we say f is periodic if there exists a nonzero real number t such that $f(x)=f(x+t)$ for all reals x. Let P be a polynomial of degree n with real coefficients. Show that P cannot be written as the sum of n periodic functions.

    Solution. Induction and finite differences.

95. 3-D proofs for Brianchon and Pascal.

    Solution. This proof only works for non-degenerate cases (for Brianchon, $ABCDEF$ all distinct points on opposite sides; for Pascal, no two opposite sides parallel)

    $ABCDEF$ circumscribes the circle with tangency points $PQRSTU$ (P on AB, Q on BC, etc.)

    lift stuff alternately by constant angles so that A' is above, B' is below B, etc. so that $A'B'D'E'$ is a plane, etc.

    now we get three planes of the form $A'B'D'E'$, $B'C'E'F'$, etc. that are not the same, but have pairwise intersections exactly equal to lines $A'D'$, $B'E'$, $C'F'$, which means that the three planes must intersect in a point, which must lie on all three lines; now project everything onto the plane of $ABCDEF$ to get a proof of brianchon

    for pascal, note that PQ, A_1B_1, B_1C_1 are coplanar, so PQ and ST intersect at a point on the line equal to the intersection of planes $A'B'C'$ and $D'E'F'$, which also contains $A'B'\cap D'E'$ and $B'C'\cap E'F'$

    if $L=A'B'\cap D'E'$, $M=B'C'\cap E'F'$, $N=C'D'\cap F'A'$, then the plane LMN (possibly degenerate, but then the result's obvious) intersects plane $ABCDEF$ at a line containing $PQ\cap ST$, $QR\cap TU$, $RS\cap UP$, so we're done

96. No $4\times n$ closed knight's tour for $n\ge 1$.

    Solution. The intuition is that we have to use the middle two rows to transport most of the time, yet the boundary rows have the same number of squares as the middle two. If we color rows 1 and 4 A and rows 2 and 3 B, then each A must be followed by a B in a knight's tour, whence the tour must take the form $(AB)^{2n}$ (indeed, we require a B after each of $2n$ occurences of A, so there can't be any others stuck in between two consecutive AB's). But then the standard chessboard coloring yields a contradiction.

97. Let $a_1,a_2,\ldots,a_n$ be positive rational numbers and let $k_1,k_2,\ldots,k_n$ be integers greater than 1. If $\sum_{i=1}^n \sqrt[k_i]{a_i}\in\mathbb{Q}$, show that $\sqrt[k_i]{a_i}\in\mathbb{Q}$ for all i.

    Solution. Let $S=\sum_{i=1}^n a_i^{1/k_i}$ and go by contradiction. For motivation we look at the $n=2$ case. WLOG k_1,k_2 are "minimal" in the sense that $a_i^{j/k_i}\notin\mathbb{Q}$ for $j=1,2,\ldots,k_i-1$. Then our assumption is equivalent to $k_i>1$ for all i.

    Note that $x^{k_1}-a_1$ is the minimal polynomial of a_1^{1/k_1} over the rationals, so $x_{k_1}-a_1 \mid (S-x)^{k_2}-a_2$. But then $k_2\ge k_1$; by symmetry $k_1\le k_2$ and we can easily get a contradiction by considering the $[x^{k_1-1}]$ coefficients.

    In a similar vein,

$$x^{k_1}-a_1 \mid \prod_{\omega_i^{k_i}=1, 2\le i\le n} \left(S-x-\sum_{i=1}^n \omega_i a_i^{1/k_i}\right)\in\mathbb{Q}[x],$$

so for some choice of k_ith roots of unity ω_i and (any) nontrivial k_1th root of unity ω_1, we have $S = \omega_1 a_1^{1/k_1} + \sum_{i=2}^n \omega_i a_i^{1/k_i}$. But then

$$0 = \Re(S - S) = \Re(a_1^{1/k_1}(1 - \omega_1)) + \sum_{i=2}^{n} \Re((1 - \omega_i)a_i^{1/k_i}) > \sum_{i=2}^{n} \Re((1 - \omega_i)a_i^{1/k_i}) \geq 0,$$

contradiction. (We can also take magnitudes and use the triangle inequality: for equality, the ω_i must be in the same positive direction since the a_i are all positive, but then S would be in $\mathbb{R}\omega_1 \cap \mathbb{R} = \emptyset$.)

Comment. By induction we can show $\sum_{i=1}^n \pm\sqrt{a_i} \in \mathbb{Q}$ iff $\sqrt{a_i} \in \mathbb{Q}$ for all i, but this doesn't work as well when $k_i > 2$.

98. (Russia 1998) Each square of a $2^n - 1 \times 2^n - 1$ square board contains either $+1$ or -1. Such an arrangement is deemed successful if each number is the product of its neighbors. Find the number of successful arrangements.

Solution. For $n = 1$ there are two; we restrict our attention to $n \geq 2$. Let $N = 2^n - 1$. Take the $\log_{-1}$ of each entry so we're working in $\mathbb{F}_2$ instead; we're choosing some of the N^2 entires to be 1. Viewing this as the equation $a_{i,j} = a_{i-1,j} + a_{i+1,j} + a_{i,j-1} + a_{i,j+1}$ (where boundary cases are 0 for convenience), we can set up a matrix equation $Av = 0$ where $A_{i,j} = 1$ iff entries i and j (there are $(N)^2$ total) are neighboring, and $v \in \mathbb{F}_2^{N^2}$ has a 1 for each entry i we include in the successful arrangement.

We show by induction on $n \geq 1$ that $\det A = 1$ (whence v must be the all-zero vector and there's exactly one solution)—note that for $n = 1$ the matrix equation doesn't actually correspond to the original problem, but this is not an issue. To do this, observe that $\det A = \sum_\pi A_{1,\pi(1)} \cdots A_{N^2,\pi(N^2)}$ (as we're working $\mathbb{F}_2$). Now for a fixed permutation π that contributes 1 to the sum (i.e. doesn't vanish), draw an arrow from i to $\pi(i)$ for each i; we get a partition of the original $N \times N$ board into disjoint directed cycles of size 1 or $2k$ for some $k \geq 1$ (arrows connect neighboring elements—these directed cycles correspond to permutation cycles). These cycles are nontrivially "reversible" iff $k \geq 2$, so pairing up the permutations with their reversals (this corresponds to π^{-1}), we're left (mod 2, of course) with the number of tilings of the $N \times N$ grid using 1×2, 2×1, and 1×1 tiles. Reflecting over the horizontal axis we're left with horizontally symmetric tilings; now reflecting over the vertical axis we're left with tilings that are both horizontally and vertically symmetric.

For odd N it's easy to check that $x_N \equiv x_{\frac{N-1}{2}} F^2_{1+\frac{N-1}{2}}$ where $F_0 = 0$, $F_1 = 1$, $F_m = F_{m-1} + F_{m-2}$ is Fibonacci, as all dominoes intersecting one of two axes must lie within the axes (by symmetry). By induction we get $\det A = x_N = 1$.

Comment. We can use this kind of symmetry argument directly on the original problem (e.g. consider the product of a successful arrangement with its vertical reflection, which results in another successful arrangement), which is slightly weaker but still works for the particular problem (we don't immediately get $3 \mid N+1 \implies x_N \equiv 0 \pmod 2$), but the linear algebra setting is perhaps more motivated. It may be possible to do nontrivial general analysis on $m \times n$ boards using the same recursive linear algebra ideas, but when both of m, n are even it seems hard to reduce the problem.

99. (Putnam 2011 A2) Induct and notice the general form of the numerator is something like $\frac{1}{2}(\prod(x_i+2) - \prod x_i)/\prod(x_i + 2)$ (when expanded). Alternatively, divide the recursion $b_n = a_n b_{n-1} - 2$ by $a_1 \cdots a_n$; this is not as versatile a stragey though. Maybe guess the answer is the same regardless of x_i, as it would likely be ugly otherwise (especially with only the "bounded" restraint a nice closed form's unlikely).

100. (Putnam 2011 A3) Find a real number c and a positive number L for which

$$\lim_{r\to\infty} \frac{r^c \int_0^{\pi/2} x^r \sin x \, dx}{\int_0^{\pi/2} x^r \cos x \, dx} = L.$$

Solution. If this were discrete then obviously we would focus on the largest exponential/base power in each sum.

It turns out the same intuition works here (consider, for instance, multiplying the integral by $(2/\pi)^r$): we focus on the sin integral since x^r and sin are both increasing. Integration by parts deals with the cos part. So the estimation $\frac{2}{\pi}x \le \sin x \le 1$ on $[0, \pi/2]$ suffices. We could also use $1 - \frac{(\pi/2-x)^2}{2} \le \sin x \le 1$ and beta function: $\int_0^{\frac{\pi}{2}} x^r \left(\frac{\pi}{2} - x\right)^2 \, dx = \frac{2}{(r+1)(r+2)(r+3)} \left(\frac{\pi}{2}\right)^{r+3}$. The point is to deal with the small error terms in a simple way as the details don't matter so much.

Note. (mavropnevma) In some circles, it is common knowledge that for an elementary function f, one has $\lim_{r\to\infty} \int_0^1 x^r f(x)\, dx = 0$, and $\lim_{r\to\infty} r \int_0^1 x^r f(x)\, dx = f(1)$; typically this is done by breaking the interval $[0, 1]$ into $[0, 1 - \delta]$ and $[1 - \delta, 1]$, with δ as close to 0 as needed.

101. (Russia 2010) Let G be a connected graph disconnected by the removal of (all of the edges of) any odd cycle. Prove that G is 4-partite.

Solution. Since we need to find a 4-(vertex)-coloring, the following lemma will help:

Lemma. Let $m, n \ge 2$ be two positive integers. A graph $G(V, E)$ is mn-colorable iff there exists an edge partition $E = E_1 \cup E_2$ such that $G_1 = G(V, E_1)$ and $G_2 = G(V, E_2)$ are m- and n-colorable, respectively.

Proof. Just use product coloring for the "if" direction: we can assign the color (c_1, c_2) to a vertex colored c_1, c_2 in G_1, G_2, respectively.

Conversely, if G is mn-colorable, then split the graph into m sets $A_1, \ldots, A_m$, each containing the vertices of exactly n colors; we can then take G_1, G_2 defined by $E_1 = \{xy \in E : x \in A_i, y \in A_j, i \ne j\}$ and $E_2 = \{xy \in E : x, y \in A_i\} = E \setminus E_1$, which are m- and n-colorable, respectively. Alternatively, label the mn colors (i, j) for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$ and define E_1, E_2 by the first and second coordinates, respectively—the induced subgraphs G_1, G_2 are clearly m- and n-colorable, and we can then remove duplicate edges from E_1, E_2 until we get an edge partition. (The idea is that independent sets behave like single vertices, and K_{mn} can easily be split in the desired form.) ■

In view of the lemma, we try to find an edge partition such that G_1 and G_2 are both bipartite.

Let $G_1 = G(V, E_1)$ be a maximal bipartite subgraph; then we can't add any more edges to E_1 without inducing an odd cycle. Now assume for the sake of contradiction that $G_2 = G(V, E_2)$ (where $E_2 = E \setminus E_1$) has an odd cycle $C = v_1 v_2 \ldots v_\ell v_1$, $\ell \ge 3$. By the maximality of G_1, v_i and v_{i+1} (indices modulo ℓ) are connected by a (simple) path of even length in G_1 (i.e. with edges in E_1) for all i, so in particular v_i, v_j are connected in $G' = G(V, E \setminus E(C))$ for all $i \ne j$. Then since G is connected, every vertex $v \notin C$ is connected in G' to at least one vertex of C, whence G' must be connected as well, contradicting the problem hypothesis. Hence G_2 must be bipartite and since G_1 is bipartite by construction, we're done by the lemma.

Comment. In fact, we could've taken G_1 to be a maximal forest (any spanning tree) instead of a maximal bipartite graph.

102. (USAMTS 2012 Year 24) Let $P, Q \in \mathbb{R}[x]$ be two polynomials of degree greater than 1 such that $P(Q(x)) = P(P(x)) + P(x)$. Prove that $P(-x) = P(x) + x$.

Solution. Let $P(x) = \sum a_k x^k$ and $Q(x) = \sum b_k x^k$, and expanding out (comparing coefficients), note that $\deg P(x)^n - Q(x)^n \le n(n-1)$. But using $\omega = e^{2\pi i/n}$ factorization the rest is clear.

103. (consistency of Thurston's height function) A domino tiling of a simple lattice polygon with all sides parallel to the x- and y-axes can be split into two smaller simply connected tilings.

Solution. Consider a domino D sharing a side with the boundary/perimeter of the polygon P. If we treat the dominos as vertices of a graph adjacent iff they share a side (not just a corner), then removing D divides the polygon into at most 3 connected components (a fairly clean way to conceptualize this is by tracing the boundary of P and looking at its intersections with D—there are at most 3 disjoint intersections since the path repeats no points or sides). If there's 1 then we can remove D and we're fine. If there's at least two we can remove one of them to get a simply connected tiling.

Why do we need to take a domino sharing a side with P? This guarantees that the regions left when D is removed are simple. (Again, a good way to rigorize this is by visualizing the boundary of P.)

104. Let a, b, c, d be positive reals such that $a+b+c+d=4$. Show that $\frac{4}{abcd} \geq \sum \frac{a}{b}$.

Solution. Rearrangement. Equality occurs when all are equal, or if we allow zeros and multiply both sides by $abcd$, also cyclic permutations of $(0, 1, 1, 2)$.

105. (Putnam 1999) Let S be a finite set of positive integers greater than 1 such that for any positive integer n, there exists some $s \in S$ such that either $s \mid n$ or $s \perp n$. Prove that there exist two elements of S (possibly the same) whose greatest common divisor is prime.

Solution. A helpful observation is that we only need to work with squarefree n in the condition.

So to start we note that if there's a prime in S then we're done, and there must exist $s \in S$ dividing $\operatorname{rad} S$. Thus there exists a maximal squarefree n such that $s \nmid n$ for all $s \in S$ (and $n > 1$). Then we must be able to find $t \in S$ such that $t \perp n$, so if we take a prime $p \mid t$ then by the maximality of n, there exists $u \in S$ dividing np (note that $p \nmid n$, so pn is squarefree). But if $p \perp u$, then $u \mid n$, contradicting the definition of n, so $p \mid u$ forces $\gcd(t, u) = p(t/p, u/p)$. Yet $(t/p, u/p) \mid (t, n) = 1$, so $\gcd(t, u) = p$ and we're done.

Alternatively, we can look at this from the "dual" perspective (this may not be accurate strictly speaking, but intuitively we have a minimal "cover" of S here and a maximal "anti-cover" of S previously). Indeed, if we take the smallest n such that $\gcd(s, n) > 1$ for all $s \in S$ (note $\operatorname{rad}(S)$ works, so a minimal element exists), then there exists $t \in S$ such that $t \mid n$. If $p \mid n$ (clearly n is squarefree), then there exists $u \in S$ such that $u \perp n/p$; yet $(u, n) > 1$ by definition, so $p \mid u$ and $\gcd(t, u) = p$.

Comment. Observe that $p \mid t$ (by construction) in the first method while $p \mid u$ (by deduction) in the second. In any case, the concept of minimality/maximality is key.

106. (2012 Winter OMO Problem 50) $SABC$ tetrahedron

Solution. Let $r = 35$, I, ω, u, O, and Ω be the inradius, incenter (given), insphere, circumradius, circumcenter, and circumsphere of $SABC$, respectively. Let $s = SI = 125$; Q be the reflection of S over O; F be the foot from S to plane ABC; $h = SF$ be the length of the S-altitude; I_A, I_B, I_C be the feet from I to SBC, SCA, SAB, respectively; O_A, O_B, O_C, O_S be the circumcenters of triangles SAB, SBC, SCA, ABC, respectively; and $a = 108$ be the common circumradius of triangles SAB, SBC, SCA. For convenience, define $v = SI_A = SI_B = SI_C = \sqrt{s^2 - r^2} = 120$.

First, we note that $OO_A^2 = OO_B^2 = OO_C^2 = u^2 - a^2$ by the Pythagorean theorem, so O is equidistant from the three planes SAB, SBC, SCA.

Taking the cross section formed by $\triangle OO_BO_C$, we see that O lies on one of the two planes bisecting the angle formed by planes SAB and SAC: either the *interior* one or the *exterior* one (these correspond naturally to the two-dimensional interior and exterior angle bisectors). Now assume for the sake of contradiction that O lies on the exterior bisector (which is perpendicular to the interior one), and WLOG suppose plane SAB separates O and C. Since O is the center of $\Omega = (SABC)$, we then have $a = R_{SAC} < R_{SAB} = a$, a contradiction. Thus O must lie on the interior angle bisector P_A of $\angle(SAB, SAC)$.

If we similarly define P_B, P_C, then $S, O, I \in P_A \cap P_B \cap P_C$ (as I lies completely inside $PABC$). But the intersection of three distinct planes can only form a point, a line, or the empty set, so S, O, I must be collinear. Let ϵ equal $+1$ if O, S are on the same side of plane ABC and -1 otherwise. Clearly O cannot be higher than S (relative to plane ABC), since the line $SI = SO$ intersects the interior of $\triangle ABC$. In particular, S and Q must lie on opposite sides of ABC. (*) Using similar triangles and the Pythagorean theorem, we get

$$\frac{h - \epsilon OO_S}{h - r} = \frac{SO}{SI} = \frac{SO_A}{SI_A} \implies \frac{h - \epsilon\sqrt{u^2 - R^2}}{h - r} = \frac{u}{s} = \frac{a}{v}. \tag{1}$$

It immediately follows that $u = as/v = 225/2$.

We will now compute h using inversion (this is natural because several circles and spheres in our diagram pass through S, and when we invert about X, the circumcenter of $\triangle XYZ$ is simply mapped to the reflection of X over $Y'Z'$). Invert about S with radius α, and let J_A, J_B, J_C be the midpoints of

I'_A, I'_B, I'_C, respectively. Observe that SQ is a diameter of Ω, so $\angle SQ'A' = \angle SQ'B' = \angle SQ'C' = 90°$, whence Q' is the foot from S to $A'B'C'$ (the spheres with diameters SA', SB', SC' intersect at S and its reflection over the plane formed by their centers). But J_A is the foot from S to $B'C'$, so $Q'P$ is minimized over $P \in B'C'$ at $P = J_A$ (by the Pythagorean theorem) and J_A is the foot from Q' to $B'C'$. On the other hand, $SJ_A = SJ_B = SJ_C = \frac{\alpha^2}{2SI_A}$ implies $Q'J_A = Q'J_B = Q'J_C$, whence $\triangle A'B'C'$ has incircle $(J_AJ_BJ_C)$ and inradius

$$t = Q'J_A = \sqrt{\left(\frac{\alpha^2}{2SI_A}\right)^2 - \left(\frac{\alpha^2}{2SO}\right)^2} = \frac{\alpha^2}{2}\sqrt{\frac{1}{a^2} - \frac{1}{u^2}} = \frac{\alpha^2}{2}\frac{r}{as}. \tag{2}$$

(Indeed, according to (*), Q' cannot be an excenter of $\triangle A'B'C'$, since Q' lies on the same side of planes $SB'C' = SBC, SC'A' = SCA, SA'B' = SAB$ as A', B', C', respectively.)

It remains to analyze F'. $\angle SA'F' = \angle SB'F' = \angle SC'F' = 90°$, so A', B', C' lie on the sphere Γ with diameter SF'. Let K be the midpoint of SF' and L be the foot from K to $A'B'C'$; then K is the center of Γ and L is the circumcenter of $\triangle A'B'C'$. If $x = SK$ denotes the radius of Γ, then $2x = SF' = \alpha^2/SF = \alpha^2/h$.

Fortunately, Q', the foot of S, lies in the interior of $\triangle A'B'C'$, so K cannot be higher than S (relative to plane $A'B'C'$); hence T lies on ray $\overrightarrow{SQ'}$. Since the (acute) angle θ between lines $SF' = SF$ and $SQ' = SQ$ is fixed under inversion, we get

$$\frac{Q'L}{x} = \frac{TK}{SK} = \sin\theta = \frac{\sqrt{SI^2 - (h-r)^2}}{SI} = \frac{\sqrt{s^2 - (h-r)^2}}{s}$$

and

$$KL = TQ' = |SQ' - ST| = \left|\frac{\alpha^2}{2u} - SK\cos\theta\right| = \left|\frac{xh}{u} - x\frac{h-r}{SI}\right| = x\left|\frac{h}{u} - \frac{h-r}{s}\right|.$$

Plugging the previous two equations and (2) into Euler's formula (for $\triangle A'B'C'$) yields

$$\begin{aligned}
x^2 - x^2\frac{(h-r)^2}{s^2} = x^2\frac{s^2-(h-r)^2}{s^2} = Q'L^2 &= R_{A'B'C'}^2 - 2tR_{A'B'C'} \\
&= (x^2 - KL^2) - \alpha^2\frac{r}{as}\sqrt{x^2 - KL^2} \\
&= x^2 - x^2\left(\frac{h}{u} - \frac{h-r}{s}\right)^2 - 2xh\frac{r}{as}x\sqrt{1 - \left(\frac{h}{u} - \frac{h-r}{s}\right)^2}.
\end{aligned}$$

Adding $-x^2$ to both sides, substituting $as = uv$, and multiplying both sides by $-x^{-2}u^2s^2$, we get

$$\begin{aligned}
u^2(h-r)^2 &= (sh - u(h-r))^2 + \frac{2hrs}{v}\sqrt{u^2s^2 - (sh-u(h-r))^2} \\
-s^2h^2 + 2shu(h-r) &= \frac{2hrs}{v}\sqrt{u^2s^2 - (sh-u(h-r))^2} \\
v(-sh + 2u(h-r)) &= 2r\sqrt{u^2s^2 - (sh-u(h-r))^2} \\
(s^2-r^2)[h^2(2u-s)^2 - 4h(2u-s)ur + 4u^2r^2] &= 4r^2[-h^2(s-u)^2 - 2h(s-u)ur - u^2(r^2-s^2)] \\
v^2[h(2u-s)^2 - 4(2u-s)ur] &= 4r^2[-h(s-u)^2 - 2(s-u)ur],
\end{aligned}$$

whence

$$\begin{aligned}
h = 4ur\frac{v^2(2u-s) - 2r^2(s-u)}{v^2(2u-s)^2 + 4r^2(s-u)^2} &= 4\frac{225}{2}35\frac{120^2(225-125) - (35)^2(2\cdot 125 - 225)}{120^2(225-125)^2 + (35)^2(2\cdot 125-225)^2} \\
&= 70\cdot 15^2\frac{120^2\cdot 10^2 - 35^2\cdot 5^2}{120^2\cdot 10^4 + 35^2\cdot 5^4} \\
&= 70\cdot 3^2\frac{24^2\cdot 2^2 - 7^2}{24^2\cdot 2^4 + 7^2} \\
&= \frac{284130}{1853}.
\end{aligned}$$

We can find ϵ now (actually, $h > u$, so we trivially have $\epsilon = +1$), but this is unnecessary: plugging h into (1) yields

$$\begin{aligned}
R^2 &= u^2 - \left(h - \frac{a}{v}(h-r)\right)^2 \\
&= \frac{225^2}{2^2} - \left(\frac{284130}{1853}\left(1 - \frac{108}{120}\right) + \frac{108 \cdot 35}{120}\right)^2 \\
&= \frac{9^2 \cdot 25^2}{2^2} - \left(\frac{28413}{1853} + \frac{9 \cdot 7}{2}\right)^2 \\
&= \frac{9^2 \cdot 25^2}{2^2} - \left(\frac{28413}{1853} + \frac{9 \cdot 7}{2}\right)^2 \\
&= \left(9^2 - \frac{28413}{1853}\right)\left(9 \cdot 16 + \frac{28413}{1853}\right) \\
&= \frac{121680 \cdot 295245}{1853^2} \\
&= \frac{35925411600}{3433609}.
\end{aligned}$$

Thus the answer is $35925411600 + 3433609 = 35928845209$.

(Sketch of Existence.) For existence, we work with the S-inverted form. If we start with a triangle $A'B'C'$ satisfying $R_{A'B'C'} = \frac{234}{78925}\alpha^2$ ($\sqrt{x^2 - KL^2}$, where x, KL are as defined above; $x = \frac{1853}{568260}\alpha^2 = \frac{\alpha^2}{2h}$ and $KL = \frac{551}{405900}\alpha^2$) and $r_{A'B'C'} = \frac{7}{5400}\alpha^2$ ($t = (\alpha^2/2)(r/as)$), and then take S so that the S-altitude of $SA'B'C'$ (SQ' in the above notation) passes through the incenter of $\triangle A'B'C'$ and has length $\frac{1}{225}\alpha^2$ ($\alpha^2/2u$), then it is not difficult to show that $SI = 125$, $r_{SABC} = 35$, and $R_{SAB} = R_{SBC} = R_{SCA} = 108$ (this is mostly just running the solution's arguments in reverse). It's nicer to do everything in terms of $r = 35$, $a = 108$, $s = 125$, but since this is just a sketch it's easier to include the worked out values.

107. (Russia 1999) If $x, y > 0$ satisfy $x^2 + y^3 \ge x^3 + y^4$, show that $x^3 + y^3 \le 2$.

Solution. By AM-GM, $x^2 - x^3 \ge y^3 - y^4 \ge y^3 - y^2$ (alternate motivation: want to get $x^3 + y^3$ on lesser side). The rest follows by homogenization. In fact, the stronger result $x^5 + y^5 \le 2$ also follows.

108. (Aaron Pixton, MOP 2012) good sets $3n$, $3n+1$

Solution. Interpret as a pair of matchings on K_{2n} for the $3n$ one, one with As on the left and Bs on the right and the other with Bs on the left and Cs on the right: As correspond to smallest elements of sets, Bs middle, Cs largest. This gets $((2n-1)!!)^2$ for the first one.

for the second one it's the same thing, but we have an additional "space" denoted by X. in both cases we can interpret the X as an unmatched B, so we have n As and $n+1$ Bs. we want the Xs to have the same index among Bs in the two matchings. note however the orientation of the two matchings is B, so if we fix an orientation (say the BC one) and let u_i be the number of ways to get X in the ith position among Bs, then $u_k = 2^{n+2-2k} n! \binom{2k-2}{k-1}$. the answer is thus $\sum_{i=1}^{n+1} u_i u_{n+2-i} = 2^{(n+2)-2(n+2)} n!^2 4^n = ((2n)!!)^2$, where we use the classical $\binom{2k}{k}$ convolution thing. note that we can interpret this as number of good sets of $3n+3$ where one of the sets has smallest element 1 and largest element $3n+3$

109. (MOP 2004/2005?) Let n be an integer greater than 1. Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be nonnegative real numbers with $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_n$, $b_1 + b_2 + \cdots + b_n = 1$, and

$$\sum_{1 \le i < j \le n} |a_i - a_j| \le \sum_{1 \le i < j \le n} |b_i - b_j|.$$

Determine the maximum value of $a_1 + a_2 + \cdots + a_n$.

Solution. Small cases are very helpful for realizing what kinds of bounding to do. $n = 2$ is not particularly helpful, but $n = 3$ is already very messy without the "right" idea (to use AM-GM to get rid of the weird product condition when the a_i are all positive). $n=4$ checks our intuition for $n=3$ after that.

Equality is for $(0,1,\ldots,1)$ and $(0,\ldots,0,1)$ for a,b, respectively (we get $n-1$). Order $a_1\le\cdots\le a_n$ and $b_1\le\cdots\le b_n$. If $x_1+\cdots+x_m=1$ for nonnegative x_i, we can prove $\sum|x_i-x_j|\le m-1$, e.g. by looking at $|x_{j+1}-x_j|+\cdots+|x_m-x_j|$ (which has an obvious upper bound of $1-(x_1+\cdots+x_j)$, even though we can do better). Actually, $m-1-\sum|x_i-x_j|=\sum_{i=1}^{m-1}2(m-i)x_i$, although we can get away without the factor of 2.

This works directly when $a_1=0$, and if $a_1,b_1>0$, we just use $na_1\ge\sum_{i=1}^n a_i-\sum|a_i-a_j|$ (motivation: $n=3$ and $n=4$ cases. The factor of 1 is mostly so we can get rid of the $n-1$ on the RHS of $a_1+\cdots+a_n>n-1$, but this really mostly based on aesthetics and small cases as well). Then just $a_n>(n-1)/n$ to get a contradiction (if we assume $a_1+\cdots+a_n>n-1$). Use $b_1b_2\cdots b_{n-1}=(a_1a_2\cdots a_n)/b_n\ge a_1a_2\cdots a_{n-1}(n-1)/n$ to finish.

110. (ISL 2010 C7) Let $P_1,\ldots,P_s$ be s arithmetic progressions of integers such that (a) each integer belongs to at least one progression; (b) each progression contains a number which does not belong to any other progression. Denote by n the least common multiple of the differences of these progressions; let $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ be its prime factorization. Prove that

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

Solution. For the sake of completeness, here's a (IMO) somewhat simplified version of Simpson's proof, with a little motivation. I meant to post a while ago but got caught up in some things (also this is really annoying to write up...).

Define $f(n)=\sum_{i=1}^k\alpha_i(p_i-1)$ ($f(1)=0$ for convenience), $S=\{P_i\}$, and suppose $P_i=a_i \pmod{d_i}$ for $i=1,2,\ldots,s$. For a set of indices A, let $L(A)=\operatorname{lcm}_{i\in A}(d_i)$, so we want to show $|S|\ge 1+f(L(S))$. Note that $f(mn)=f(m)+f(n)$ for positive integers m,n. For $i=0,1,\ldots,p_1-1$, let S_i be the set of indices of a **minimal** cover of the residues $i \pmod{p_1}$. Clearly $S=\bigcup_{i=0}^{p_1-1}S_i$ and by (ii), each S_i contains j with $p_1\mid d_j$ (which of course requires $a_j\equiv i \pmod{p_1}$). Similarly, S_i,S_j can only intersect at indices l with $p_1\nmid l$. Furthermore, for fixed j, there must exist i such that $p_j^{\alpha_j}\mid L(S_i)$.

When $k=1$, it's obvious how to proceed: WLOG $L(S_0)=p_1^{\alpha_1}$; then noting that $P_j\cap 0 \pmod{p_1}$ is an AP with step divisible by p_1, we get

$$\begin{aligned}|S|&\ge|S_0|+|S_1\setminus S_0|+\cdots+|S_{p_1-1}\setminus S_0,\ldots,S_{p_1-2}|\\&\ge 1+f(L(S_0)/p_1)+p-1=1+f(L(S))\end{aligned}$$

by the inductive hypothesis (base case is trivial), as desired.

For $k>1$, we'll need something a bit stronger, but it's natural to conjecture something like $|S_i\setminus T_{i-1}|\ge 1+f\left(\frac{L(T_i)}{L(T_{i-1})}\right)$ for $i\ge1$, where $T_i=\bigcup_{j=0}^i S_j$ (which clearly suffices). Thus we try to prove the following: If S is a minimal covering set of the integers with $n=L(S)$, then for any $m\mid n$ with $m<n$, S has at least $1+f(n/m)$ progressions $P_j=a_j \pmod{d_j}$ with $d_j\nmid m$. Equality holds, for instance, when S consists of $0 \pmod n$ and for each i, $jp_i^{\ell-1} \pmod{p_i^\ell}$ for $j=1,2,\ldots,p_i-1$, $\ell=1,2,\ldots,k$.

To set an inductive proof (on n) up, let $M=\{j:d_j\mid m\}$. WLOG $p_1\mid n/m$ (since $m<n$) and $p_1^{\alpha_1}\mid L(S_0)$. Fix i; for $P_j\in S_i$, define $P_j^{(i)}=a_j^{(i)} \pmod{d_j^{(i)}}$ so that $P_j\cap i \pmod{p_1}=p_1P_j^{(i)}$. Note that $d_j^{(i)}=\frac{d_j}{\gcd(p_1,d_j)}$ and $S_i^{(i)}$ (slight abuse of notation here) must be a minimal cover of the integers (since S_i is a minimal cover of $i \pmod{p_1}$). Observe that $L(S_i^{(i)})=L(S_i)/p_1$ and for any positive integer t, $d_j^{(i)}\nmid\frac{t}{(t,p_1)}\implies d_j\nmid t$. (*)

First we consider $S_0\setminus M$. If $L(S_0)/p_1=(m,L(S_0))/(m,L(S_0),p_1)$, this is obvious from $p_1^{\alpha_1}\mid L(S_0)$. Otherwise, $d_j\mid m$ iff $d_j\mid(m,L(S_0))$, so by (*), $|S_0\setminus M|$ is at least the number of $j\in S_0$ such that

$d_j^{(0)} \nmid (m, L(S_0))/(m, L(S_0), p_1)$, which is at least

$$1 + f\left(\frac{|S_0^{(0)}|}{(m, L(S_0))/(m, L(S_0), p_1)}\right) = 1 + f\left(\frac{L(S_0)/p_1}{(m, L(S_0))/(m, L(S_0), p_1)}\right)$$
$$= 1 + f\left(\frac{(m, L(S_0), p_1)}{p_1}\frac{\operatorname{lcm}(m, L(S_0))}{m}\right)$$

by the inductive hypothesis, since $(m, L(S_0)) \mid L(S_0)$ forces $(m, L(S_0))/(m, L(S_0), p_1) \mid L(S_0)/p_1$.

For $i \geq 1$, $S_i \setminus M, T_{i-1}$ contains all $j \in S_i$ such that $d_j \nmid m$ and $d_j \nmid L(T_{i-1})$, and thus all j with $d_j \nmid \operatorname{lcm}(m, L(T_{i-1}))$ (although this is a weaker condition), or equivalently, $d_j \nmid (L(S_i), \operatorname{lcm}(m, L(T_{i-1})))$. Using (*) as in the previous paragraph, $|S_i \setminus M, T_{i-1}|$ is at least the number of $j \in S_i$ such that $d_j^{(i)} \nmid (L(S_i), \operatorname{lcm}(m, L(T_{i-1})))/p_1 = L(S_i)\operatorname{lcm}(m, L(T_{i-1}))/p_1 \operatorname{lcm}(m, L(T_i))$ (note $p_1 \mid T_0 \mid L(T_{i-1})$ and of course $p_1 \mid L(S_i)$). If $L(S_i)/p_1 > (L(S_i), \operatorname{lcm}(m, L(T_{i-1})))/p_1$, we get a lower bound of

$$1 + f\left(\frac{L(S_i)/p_1}{L(S_i)\operatorname{lcm}(m, L(T_{i-1}))/p_1 \operatorname{lcm}(m, L(T_i))}\right) = 1 + f\left(\frac{\operatorname{lcm}(m, L(T_i))}{\operatorname{lcm}(m, L(T_{i-1}))}\right).$$

Otherwise, if $\operatorname{lcm}(m, L(T_i)) = \operatorname{lcm}(m, L(T_{i-1}))$, we get a lower bound of $\geq 1 = 1 + f\left(\frac{\operatorname{lcm}(m,L(T_i))}{\operatorname{lcm}(m,L(T_{i-1}))}\right)$ when $p_1 \nmid m$ (as S_i has at least one j with $p_1 \mid d_j$, which clearly must be unique to S_i) and obviously $\geq 0 = f\left(\frac{\operatorname{lcm}(m,L(T_i))}{\operatorname{lcm}(m,L(T_{i-1}))}\right)$ when $p_1 \mid m$.

Case 1. $p_1 \nmid m$. Then $S \setminus M$ has at least $p_1 + f\left(\frac{(m,L(S_0),p_1)}{p_1}\frac{\operatorname{lcm}(m,L(T_{p_1-1}))}{m}\right) = 1 + f\left(\frac{n}{m}\right)$ elements, as desired.

Case 2. $p_1 \mid m$. Then $S \setminus M$ has at least $1 + f\left(\frac{(m,L(S_0),p_1)}{p_1}\frac{\operatorname{lcm}(m,L(T_{p_1-1}))}{m}\right) = 1 + f\left(\frac{n}{m}\right)$ elements, so we're done in this case too.

111. Suppose n coins have been placed in piles on the integers on the real line. (A pile may contain zero coins.) Let T denote the following sequence of operations.

(a) Move piles $0, 1, 2, \ldots$ to $1, 2, 3 \ldots$, respectively.

(b) Remove one coin from each nonempty pile from among piles $1, 2, 3, \ldots$, then place the removed coins in pile 0.

(c) Swap piles i and $-i$ for $i = 1, 2, 3, \ldots$.

Prove that successive applications of T from any starting position eventually lead to some sequence of positions being repeated, and describe all possible positions that can occur in such a sequence.

Solution. First, since we expect coins to gravitate towards the origin, we note that $\sum |x| + |y|$ over all coins decreases by $\sum a_i - (i - 1)$

112. (related to Putnam 2000 B6) Let n be a positive integer and $m \in \{1, 2, \ldots, 2^n\}$. Prove that there exists a 2^n-coloring $f : \{0,1\}^{2^n} \to \{1, 2, \ldots, 2^n\}$ such that for any $v \in \{0,1\}^{2^n}$, there exists $u \in \{0,1\}^{2^n}$ with $d(u, v) = 1$ (exactly one bit different) such that $f(u) = m$.

tenuously related problem (trivial): Find $g : \{0,1\}^n \to \{0,1\}^n$ such that for any $v \in \{0,1\}^n$, exists $u \in \{0,1\}^n$ with $d(u, v) = 1$ and $g(u) = v$.

Solution. Let $e_1, \ldots, e_{2^n}$ be the unit vectors in coordinates $1, 2, \ldots, 2^n$. Then we want f such that $f(v + e_1 \pmod 2), \ldots, f(v + e_{2^n} \pmod 2)$ (input vector addition modulo 2) is a permutation of the colors $1, 2, \ldots, 2^n$. For simplicity, we take $f(a_1 e_1 + \cdots + a_{2^n} e_{2^n})$ of the form $f_1(a_1) + \cdots + f_{2^n}(a_{2^n})$ (in some group G—probably abelian—of size 2^n).

In view of the natural modulo 2 definition of $d(u, v) = 1$ in coordinate i ($u \equiv v + e_i \pmod 2$)—we would like the result of changing $0 \to 1$ to be the same as that of $1 \to 0$—we take $G = (\mathbb{Z}/2\mathbb{Z})^n$, with $f_i(0) = \vec{0}$ and $f_i(1)$ equal to the vector corresponding to i's binary representation. Now we can finish by arbitrarily ordering the elements of G from 1 to 2^n.

Solution. For the tenuously related problem, we need a vertex-partition of the unit graph into cycles (allowing 2-cycles). But then we can just set $f(v) = v + e_1 \pmod 2$.

We can also overkill using Hall's marriage lemma, since our graph is clearly a n-regular bipartite graph (based on parity of coordinate sum). So we can partition into n matchings, any two of which induce the desired cycle structure. (Note that if we use the same two matchings, we just get a bunch of 2-cycles).