Some 90 problems

Sepehr Hajebi*

Notes used for the Spring 2026 offering of CO 380 at the University of Waterloo

*Almost none of the problems in these notes is due to me. I came across and solved them over the years in various books, contests, conversations, etc., and wrote down the problems and solutions here from memory. Whenever I managed to track down the original source (or at least a source), I have cited it. If a problems is due to you and you would like to be credited, or you know the original source and want it to be mentioned, feel free to write to me.

Contents

1 Working backwards **1**

2 Proof by contradiction **3**

3 Tilings **6**

4 Invariants **8**

5 The Pigeonhole Principle **11**

6 Extremal arguments **14**

7 Induction **18**

8 Counting (and some graph theory) **23**

9 Number theory **31**

10 Geometry **44**

1 Working backwards

Sometimes, when a process is iterative and we want to understand its outcome at a given stage, it is helpful to *work backwards*: start from a possible outcome and analyze how earlier stages could have led to it. The following problems illustrate this approach.

Problem 1.

Andy and Mandy are walking down the street while Andy is carrying a bag of marbles. The bottom of the bag splits and all the marbles spill out. A third of the marbles roll down the slope too quickly to recover, and a sixth of the remaining marbles disappear into a rain-water drain. Andy and Mandy pick up all they can, but half of the marbles that remain nearby are picked up by other kids who run off. Andy gives a third of the rescued marbles to Mandy for helping, and he is left with 10 marbles. How many marbles were in Andy's bag before the bottom split?

Solution. Let's work backwards: Andy ends up with two-thirds of the rescued marbles, which is 10, so there were 15 rescued marbles in total. This is half of the marbles that survived the slope and the drain (the other half were taken by the kids), so there were 30 marbles before the kids got involved. These 30 marbles were five-sixths of the marbles that did not roll down the slope (the other sixth disappeared into the drain), so there were 36 marbles before the drain incident. Finally, these 36 marbles were two-thirds of the original total (the other third rolled down the slope), so Andy started with 54 marbles before things went downhill. ■

Problem 2.

There are five numbers arranged around a circle: four 1's and a 0. At each step, we replace them with another set of five numbers as follows: Write 1 between every two adjacent equal numbers, write 0 between every two adjacent distinct numbers; and then erase the original numbers. If this process is iterated indefinitely, will we ever get all five numbers to be equal to 1?

Solution. The answer is "no." Assume that we obtain five 1's around the circle. Consider the first time when this happens. Since 1's are placed only between adjacent equal numbers, the previous configuration must also have consisted of five equal numbers. So, this configuration must have been five 0's (because we just reached five 1's for the first time). Going one step further back: since 0's are placed only between adjacent distinct numbers, the configuration before five 0's must have alternated between 0 and 1. But this is impossible, as an alternating configuration requires an even number of entries around the circle, whereas 5 is odd. ■

Problem 3.

Let $n \in \mathbb{N}$. We create a partition (A, B) of $\{1, \ldots, n\}$ by starting with $A = B = \varnothing$ and placing the numbers one by one into either A or B. After each placement, we compare the sums of the elements currently in A and B: if the sum of A is larger, we record "A", and if the sum of B is larger, we record "B". This produces a string of length n over $\{A, B\}$ (written from left to right through the above process). Prove that for any given such string, there is an order of placements that produces it.

Solution. This becomes much easier if we work backwards. Let S be an A-B string of length n. First, partition $\{1, \ldots, n\}$ into two sets X_1, X_2, where one contains all even numbers and the other all odd numbers. Assume without loss of generality that $n \in X_1$. Then the sum of X_1 is larger than that of X_2 (why?). If the last (rightmost) letter of S is A, set $(A, B) = (X_1, X_2)$; otherwise set $(A, B) = (X_2, X_1)$. This is our final partition; and it matches the last recorded letter for S. Now, scan through S letter by letter from right to left. At each step:

- If the letter changes, remove the largest number currently in $A \cup B$ from whichever of A and B it belongs to.
- If the letter stays the same, remove the smallest number currently in $A \cup B$ from whichever of A and B it belongs to.

Observe that the first operation flips the inequality of the sums, while the second preserves it (why?). Finally, reverse the order in which we removed the numbers – this gives a sequence of insertions of $1, \ldots, n$ in A, B that exactly produces S.

Here is a demonstration for $n = 6$ and $S =$ ABBABA: Start with the partition $\{2, 4, 6\}$ and $\{1, 3, 5\}$ of $\{1, \ldots, 6\}$. Since $6 \in \{2, 4, 6\}$ and the last letter of S is A, we take $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$. Now, working backwards:

Step	Letter transition	Operation	Current A	Current B	Comparing sums
Initial	–	–	$\{2, 4, 6\}$	$\{1, 3, 5\}$	$A > B$
6	B $\leftarrow$ A	remove 6 from A	$\{2, 4\}$	$\{1, 3, 5\}$	$A < B$
5	A $\leftarrow$ B	remove 5 from B	$\{2, 4\}$	$\{1, 3\}$	$A > B$
4	B $\leftarrow$ A	remove 4 from A	$\{2\}$	$\{1, 3\}$	$A < B$
3	B $\leftarrow$ B	remove 1 from B	$\{2\}$	$\{3\}$	$A < B$
2	A $\leftarrow$ B	remove 3 from B	$\{2\}$	$\varnothing$	$A > B$
1	–	remove 2 from A	$\varnothing$	$\varnothing$	$A = B$

So, reversing the operations yields:

$$2 \text{ in } A, \quad 3 \text{ in } B, \quad 1 \text{ in } B, \quad 4 \text{ in } A, \quad 5 \text{ in } B, \quad 6 \text{ in } A.$$

Placing the numbers in this order produces the string ABBABA. ■

2 Proof by contradiction

You know the deal: the goal is to prove that a set of assumptions implies a conclusion. We do this by assuming the conclusion is false, adding this to our assumptions, and then using everything we know to derive a contradiction. Sometimes the contradiction is a blatant falsehood like "$0 > 1$". Sometimes it shows that one of our assumptions must be false (which is more in the spirit of "proof by contrapositive"). Here are some problems where this technique is particularly emphasized.

Problem 4.

Prove that among any three irrational numbers, there are two whose sum is also irrational.

Solution. Suppose not. Then there exist $x, y, z \in \mathbb{R} \setminus \mathbb{Q}$ such that $x+y, x+z, y+z \in \mathbb{Q}$. But now $x = \frac{1}{2}((x+y)+(x+z)-(y+z)) \in \mathbb{Q}$, a contradiction. ■

Problem 5.

Prove that there are no 20 consecutive positive integers whose sum is a perfect square.

Solution. Suppose not. Then for some $m, n \in \mathbb{N}$, we have $m+(m+1)+(m+2)+\cdots+(m+20) = n^2$. So, $12m + 210 = n^2$. It follows that n^2 is even, and thus n is even. Let $k \in \mathbb{N}$ such that $n = 2k$. Then $12m + 210 = 4k^2$, which implies that $6m - 2k^2 = 105$. But 105 is odd, a contradiction. ■

Problem 6.

Eleven officers and eleven criminals are sitting around a table. Prove that there exists a person who is sitting next to two officers.

Solution. Suppose not. By a *segment* we mean a maximal group of people with the same profession, sandwiched between two people of the other profession. Then each officer segment contains at most two officers, and each criminal segment contains at least two criminals. Therefore, there are at least 6 officer segments around the table, and so at least 6 criminal segments in between them. But now we have at least $2 \times 6 = 12$ criminals, a contradiction. ■

Problem 7.

Let $x_1, \ldots, x_n \in \mathbb{R}^3$, for $n \in \mathbb{N}$, be at unit distance from the origin. Let $M = \frac{1}{n}(x_1 + \cdots + x_n)$. Prove that there exists $i \in \{1, \ldots, n\}$ for which the distance between x_i and M is at most 1.

Solution. Suppose not. Let S be the unit sphere centered at the origin, and let S' be the unit sphere centered at M. Then $x_1, \ldots, x_n$ all lie on S, but outside S'. Note that by the triangle inequality, the distance between M and the origin is at most 1. It follows that S and S' intersect. Let H be the plane passing through the circle $S \cap S'$. Then $x_1, \ldots, x_n$ all lie strictly on one side of H, while M lies on the other side (or on H). Write the equation of H as $a \cdot x = c$, where $a \in \mathbb{R}^3$ is nonzero and $c \in \mathbb{R}$. Then we may assume that $a \cdot x_i > c$ for all $i \in \{1, \ldots, n\}$. But now $a \cdot M = \frac{1}{n}(a \cdot x_1 + \cdots + a \cdot x_n) > \frac{1}{n}(nc) = c$, and so M also lies strictly on the same side of H as the points $x_1, \ldots, x_n$, a contradiction. ■

Problem 8.

Let X be a set and let $\mathcal{S}$ be the set of all subsets of X. Prove that there is no surjective function $f : X \to \mathcal{S}$.

Solution. Suppose for a contradiction that there is a surjective function $f : X \to \mathcal{S}$. Let

$$S = \{x \in X : x \notin f(x)\} \subseteq X.$$

Then $S \in \mathcal{S}$. By surjectivity, there exists $s \in X$ with $f(s) = S$. Now ask: is $s \in S$ or $s \notin S$? ■

Problem 9.

Prove that for every $d \in \mathbb{R}$ and every partition (X, Y) of the interval $[0, 1]$, either there exists $x \in X$ such that $x + d \notin Y$ or there exists $y \in Y$ such that $y - d \notin X$.

Solution. Suppose not. Then there exist $d \in \mathbb{R}$ and a partition (X, Y) of $[0, 1]$ such that:

- for every $x \in X$, we have $x + d \in Y$; and
- for every $y \in Y$, we have $y - d \in X$.

Since $X \cap Y = \varnothing$, it follows that $d \neq 0$. Also, by swapping the roles of X and Y if needed, we may assume that $d > 0$.
By the above two bullets, $x \mapsto x + d$ is a surjection from X to Y, and it is clearly injective as well. Thus, $x \mapsto x + d$ is a bijection from X to Y. It follows in particular that $0 < d < 1$. (Why?)
Now, for each $a \geq 0$, let $A_a = \{a + nd : n \in \mathbb{N} \cup \{0\}\}$. Then $x \mapsto x + d$ is a bijection from $X \cap A_a$ to $Y \cap A_a$, so $|A_a \cap [0, 1]|$ is even. In particular, $|A_0 \cap [0, 1]|$ is even, and so there exists $k \in \mathbb{N}$ such that $0, d, 2d, \ldots, (2k-1)d \in [0, 1]$ and $dn > 1$ for all $n \geq 2k$. But then $A_d \cap [0, 1] = \{d, 2d, \ldots, (2k-1)d\}$, which means $|A_d \cap [0, 1]|$ is odd, a contradiction. ■

Problem 10.

Let $X_1, X_2, X_3 \subseteq \mathbb{R}^3$ be nonempty and pairwise disjoint with $X_1 \cup X_2 \cup X_3 = \mathbb{R}^3$. Prove that there exists $i \in \{1, 2, 3\}$ such that for every $d \geq 0$, there are two points in X_i at distance d.

Solution. Suppose not. Then for each $i \in \{1, 2, 3\}$, there exists $d_i > 0$ such that no two points in X_i are at distance exactly d_i. We may assume that $d_1 \geq d_2 \geq d_3$. Pick $x_1 \in X_1$ and let S_1 be the sphere centered at x_1 with radius d_1. Then $S_1 \cap X_1 = \varnothing$, so $S_1 \subseteq X_2 \cup X_3$.
Since $d_1 \geq d_3$, there are two points on S_1 at distance d_3, and so at least one of these points is not in X_3. Thus, we can choose a point $x_2 \in S_1 \cap X_2$. Let S_2 be the sphere centered at x_2 with radius d_2. Then $S_2 \cap X_2 = \varnothing$.
Let $C = S_1 \cap S_2$. Then C is a circle of diameter $\frac{d_2}{d_1}\sqrt{4d_1^2 - d_2^2}$ (why?). In fact, since $d_1 \geq d_2 \geq d_3$, this diameter is at least d_3 (why?). Moreover, $C \cap X_1 = \varnothing$ (because $C \subseteq S_1$) and $C \cap X_2 = \varnothing$ (because $C \subseteq S_2$). Hence, $C \subseteq X_3$. But now, since the diameter of C is at least d_3, there are two points on C, and hence in X_3, at distance exactly d_3, a contradiction. ■

Problem 11.

A function $f : \mathbb{N} \to \mathbb{N}$ is *multiplicative* if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$. Prove that if f is multiplicative and increasing, then $f(2) = 2^d$ for some integer $d \geq 0$.

Solution. Suppose for a contradiction that $f(2)$ is not a power of 2. First, we prove an auxiliary statement (all logarithms are base 2):

(1) *For all* $m, n \in \mathbb{N} \setminus \{1\}$, $f(m)^{\log n} = f(n)^{\log m}$.

Proof of (1). Let

$$r = \frac{\log m}{\log n} > 0.$$

Then, for each $k \in \mathbb{N}$, there exists $l \in \mathbb{N}$ with $kr \leq l \leq kr + 1$. So, $k \log m \leq l \log n \leq k \log m + 1$, which implies that $m^k = 2^{k \log m} \leq 2^{l \log n} \leq n^l$. Since f is multiplicative and increasing, it follows that

$$f(m)^k = f(m^k) \leq f(n^l) = f(n)^l \leq f(n)^{kr+1} \;\Rightarrow\; f(m) \leq f(n)^{r+\frac{1}{k}} = f(n)^{\left(\frac{\log m}{\log n}\right)+\frac{1}{k}}.$$

Since this holds for all $k \in \mathbb{N}$, we deduce that $f(m) \leq f(n)^{\frac{\log m}{\log n}}$, and thus $f(m)^{\log n} \leq f(n)^{\log m}$. A similar argument also shows that $f(n)^{\log m} \leq f(m)^{\log n}$. This proves (1). □

Now, from (1), it follows in particular that for all $m \in \mathbb{N} \setminus \{1\}$, we have

$$f(m) = f(2)^{\log m} = 2^{(\log m)(\log f(2))} = m^{\log f(2)}.$$

But $f(2)$ is not a power of 2, and so $\log f(2)$ is not an integer, which means $f(3) = 3^{\log f(2)}$ is not an integer, a contradiction. ■

Note. In Problem 11, in fact we proved that for every function $f : \mathbb{N} \to \mathbb{N}$ that is multiplicative and increasing, there is an integer $d \geq 0$ such that $f(n) = n^d$. (Why?)

3 Tilings

Tilings and tessellations look "recreational," but often have strong connections with other parts such as topology, geometry, dynamics, and combinatorics. The problems we will look at here are mostly combinatorial. A remarkable result on this front was proved in 1961 by M.E. Fisher, who showed that an 8×8 board can be tiled by dominoes in $16 \times 901^2 = 12988816$ different ways. The proof of this is rather difficult, but not all tiling results are as hard as this one. Sometimes, a quick "coloring argument" helps a lot.

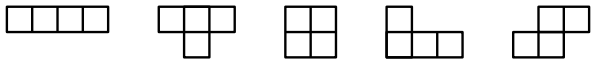
Problem 12.

Start with an 8×8 board and remove two opposite corners of the board. In how many ways can the resulting board be tiled by dominoes?

Solution. Zero! Suppose for a contradiction that a tiling exists. Then we have used exactly 31 dominoes. Now consider the 8×8 board colored in the standard black-and-white chessboard fashion. So, there are exactly 32 black cells and 32 white cells. Also, any two opposite corner cells have the same color; thus, once we remove them, the resulting board will have 32 cells of one color and 30 cells of the other color. But this contradicts the assumption that the board was tiled by 31 dominoes, because each domino covers exactly one black cell and one white cell. ■

Problem 13.

Can the following five tiles be put together to form a rectangle?



Solution. No. Suppose for a contradiction that the tiles put together form a rectangle. Then there are a total of 20 cells, and so the rectangle, no matter the dimensions, can be colored in the standard black-and-white chessboard fashion. There are now 10 cells of each color. Note also that each of our five tiles, except for the second from the left, covers two cells of each color. But the second tile from the left would cover 3 cells of one color and 1 cell of the other color, and so we would have 11 cells of one color and 9 of the other, a contradiction. ■

Problem 14.

One corner of a 51×51 board is removed. Clearly, the resulting board can be tiled with $\frac{1}{2}((51 \times 51) - 1) = 1300$ dominoes. But can this be done so that exactly 650 of the dominoes are horizontal?

Solution. No. Suppose for a contradiction that there is a tiling with exactly 650 horizontal dominoes. Color the board as follows: all cells in odd rows are black, and all cells in even rows are white. Then there are exactly $50 + (25 \times 51) = 1325$ black cells (note that row 1 has 50 cells). Recall that our tiling comprises exactly 650 horizontal dominoes and 650 vertical dominoes. Each horizontal domino covers either two black cells or two white cells. Therefore, the total number of black cells covered by the horizontal dominoes is even. Also, each vertical domino covers exactly one black cell, so the total number of black cells covered by the vertical dominoes is 650. But then the total number of black cells should be even, whereas 1325 is odd; a contradiction. ■

Problem 15.

Let R be a rectangle that can be tiled by finitely many rectangles each of which has at least one side of integer length. Prove that R also has at least one side of integer length.

First solution. Let $T_1, \ldots, T_n$, for $n \in \mathbb{N}$, be the rectangles that cover R, each with at least one integer side. We may assume that $R = [a_0, b_0] \times [c_0, d_0]$, where $a_0, b_0, c_0, d_0 > 0$ are real numbers with $a_0 < b_0$ and $c_0 < d_0$, and for each $i \in \{1, \ldots, n\}$, we may write $T_i = [a_i, b_i] \times [c_i, d_i]$, where $a_i, b_i, c_i, d_i > 0$ are real numbers with $a_0 \le a_i < b_i \le b_0$ and $c_0 \le c_i < d_i \le d_0$. In this language, we know that for each $i \in \{1, \ldots, n\}$, either $b_i - a_i$ or $d_i - c_i$ is an integer, and our goal is to show that $b_0 - a_0$ or $d_0 - c_0$ is an integer. Now, for $a, b, c, d \in \mathbb{R}$, define

$$I_{a,b} = \int_a^b e^{2\pi i x} dx \quad \text{and} \quad I_{a,b,c,d} = \int_a^b \int_c^d e^{2\pi i (x+y)} dx dy.$$

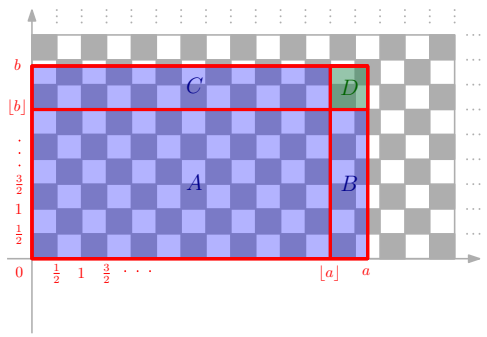
The trick lies in the following auxiliary statement:

(1) *For all $a, b, c, d \in \mathbb{R}$, we have $I_{a,b,c,d} = 0$ if and only if either $b - a \in \mathbb{Z}$ or $d - c \in \mathbb{Z}$.*

Proof of (1). Since $e^{2\pi i(x+y)} = e^{2\pi i x} e^{2\pi i y}$, we have $I_{a,b,c,c} = I_{a,b} \times I_{c,d}$. Also, note that for all $a, b \in \mathbb{R}$, we have $I_{a,b} = \frac{1}{2\pi i}\left(e^{2\pi i b} - e^{2\pi i a}\right) = \frac{e^{2\pi i a}}{2\pi i}\left(e^{2\pi i (b-a)} - 1\right)$, and so $I_{a,b} = 0$ if and only if $e^{2\pi i (b-a)} = 1$, which in turn holds if and only if $b - a \in \mathbb{Z}$. This proves (1). □

Now, for each $i \in \{1, \ldots, n\}$, since either $b_i - a_i \in \mathbb{Z}$ or $d_i - c_i \in \mathbb{Z}$, by (1), we have $I_{a_i,b_i,c_i,c_i} = 0$. Since $(T_1, \ldots, T_n)$ is a partition of R, by additivity of the integral, $I_{a_0,b_0,c_0,d_0} = \sum_{i=1}^n I_{a_i,b_i,c_i,c_i} = 0$. Hence, by (1), either $b_0 - a_0 \in \mathbb{Z}$ or $d_0 - c_0 \in \mathbb{Z}$, as desired. ■

Second solution. This time, let $R = [0, a] \times [0, b]$ with $a, b \in \mathbb{R}$ positive. Our goal is to show that a or b is an integer. Suppose not. Let $a = \lfloor a \rfloor + \alpha$ and $b = \lfloor b \rfloor + \beta$, where $0 < \alpha, \beta < 1$. Partition the entire first quadrant into $\frac{1}{2} \times \frac{1}{2}$ cells, and consider its chessboard coloring with $[0, \frac{1}{2}] \times [0, \frac{1}{2}]$ colored black. Since each rectangular tile has an integer side, the total black area and white area that it covers are equal. Thus, the total black area covered by R is equal to the total white area covered by R. Now, let



$$A = [0, \lfloor a \rfloor] \times [0, \lfloor b \rfloor], \quad B = [\lfloor a \rfloor, a] \times [0, \lfloor b \rfloor], \quad C = [0, \lfloor a \rfloor] \times [\lfloor b \rfloor, b], \quad D = [\lfloor a \rfloor, a] \times [\lfloor b \rfloor, b].$$

Then (A, B, C, D) is a partition of R, and for each of A, B and C, the covered black area and white area are equal. (Why?) It follows that the same should hold for D. Since the area of D is $\alpha\beta$, the total black area covered by D must be $\frac{\alpha\beta}{2}$. But the black area covered by D is equal to one of $\alpha\beta$, $\frac{\alpha}{2}$, $\frac{\beta}{2}$, or $\frac{1}{4} + (\alpha - \frac{1}{2})(\beta - \frac{1}{2})$ (why?), none of which is equal to $\frac{\alpha\beta}{2}$ (why?), a contradiction. ■

Note. Problem 15 is in fact a theorem of Nicolaas de Bruijn, and so not really a "problem." But comparing the two proofs (the first, by the way, is the original due to de Bruijn) is a perfect demonstration of how chessboard colorings can make our lives a lot easier.

4 Invariants

This is a simple technique that can help with many seemingly impossible problems: *if there is an iterative process going on (in more technical terms, when there is a "dynamic"), look for an invariant that does not change throughout, or whose evolution can be tracked.* Here are a few problems where this approach is essentially all there is to the solution:

Problem 16.

The numbers $1, 2, \ldots, 100$ are written on the blackboard. At each step, we may remove two numbers m, n from the list, and add the number $|m - n|$ to the list (the list shrinks by one number). Is it possible to iterate this 99 times and be left with only the number 1 at the end?

Solution. No. The invariant we are interested in here is the "*parity of the sum of the remaining numbers.*" This stays the same after each iteration (why?). Initially, the total sum is $\frac{100\times 101}{2} = 5050$, which is even. So, it is impossible to end up with an odd number at the end. ■

Problem 17.

Given a square real matrix, at each step we may pick either a row, a column, or a slanted line parallel to a diagonal (including the diagonals themselves), and swap the signs of all the entries. Is it possible to transform the matrix A_1 below into the matrix A_2 below by an iterative sequence of such operations?

$$A_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Solution. No. For a ± 1-matrix $A = [a_{i,j}]_{4\times 4}$, let

$$M(A) = \{a_{12}, a_{13}, a_{42}, a_{43}, a_{21}, a_{31}, a_{24}, a_{34}\} \qquad A = \begin{pmatrix} a_{11} & \textcircled{a_{12}} & \textcircled{a_{13}} & a_{14} \\ \textcircled{a_{21}} & a_{22} & a_{23} & \textcircled{a_{24}} \\ \textcircled{a_{31}} & a_{32} & a_{33} & \textcircled{a_{34}} \\ a_{41} & \textcircled{a_{42}} & \textcircled{a_{43}} & a_{44} \end{pmatrix}$$

Note that each row, column, or slanted line parallel to a diagonal (including the diagonals) in A contains either 0 or 2 entries from $M(A)$. So the "*product of the entries in $M(A)$*" does not change (why?). But this product is -1 for A_1 and 1 for A_2. So, it is impossible to get from A_1 to A_2. ■

Problem 18.

Let $f(x)$ be a function. At each step, you may replace $f(x)$ by either

$$x^2 f\left(\frac{x+1}{x}\right) \quad \text{or} \quad (x-1)^2 f\left(\frac{1}{x-1}\right).$$

Could you apply a series of these operations starting at $x^2 + x + 1$ to obtain $x^2 + x - 1$?

Solution. No. One may check that none of the operations changes the "*discriminant*" of the polynomial (recall that the discriminant of ax^2+bx+c is b^2-4ac). So, it is impossible to get from x^2+x+1 with discriminant -3 to x^2+x-1 with discriminant 5. ■

Problem 19.

We start with $n \geq 3$ integers written around a circle. At each step, we may replace them with another set of n numbers as follows:

- For every adjacent pair x, y, write the number $\frac{x+y}{2}$ in between them.
- Erase the original numbers.

Prove that if there are at least three distinct numbers around the circle at first, then after sufficiently many iterations, we will see a number around the circle that is not an integer.

Solution. Suppose for a contradiction that all the numbers around the circle remain integers forever. The invariant that works here is the "*difference between the minimum and the maximum number around the circle.*" This time, the invariant does not remain constant; rather, as long as the numbers around the circle are not equal, the invariant strictly decreases (why?). On the other hand, since all the numbers are integers, this invariant is also an integer. Therefore, it must eventually become zero; that is, all the numbers become equal.
Let $m \geq 2$ such that the m^{th} iteration is the first at which all numbers are circle are equal. Let $a_1, \ldots, a_n$ be the numbers around the circle in clockwise order at iteration $m-1$. Then

$$\frac{a_1+a_2}{2} = \frac{a_2+a_3}{2} = \cdots = \frac{a_{n-1}+a_n}{2} = \frac{a_n+a_1}{2};$$

and so $a_1 = a_3 = a_5 = \cdots$ and $a_2 = a_4 = a_6 = \cdots$. Since not all of $a_1, \ldots, a_n$ are equal, it follows that $a_1 \neq a_2$, and thus n is even. Let $n = 2t$ for $t \geq 2$. Since there are only two distinct numbers at iteration $m-1$, we must have $m-1 > 1$ (because initially we had three distinct numbers).
Let $b_1, \ldots, b_n$ be the numbers around the circle at iteration $m-2$, in clockwise order, such that a_1 lies between b_1, b_2 and a_2 lies between b_2, b_3. Then

$$a_1 = \frac{b_1+b_2}{2} = \frac{b_3+b_4}{2} = \cdots = \frac{b_{2t-1}+b_{2t}}{2} \quad \text{and} \quad a_2 = \frac{b_2+b_3}{2} = \frac{b_4+b_5}{2} = \cdots = \frac{b_{2t}+b_1}{2}.$$

Adding the expressions on each side yields

$$ta_1 = \frac{1}{2}(b_1+b_2+\cdots+b_{2t}) \quad \text{and} \quad ta_2 = \frac{1}{2}(b_1+b_2+\cdots+b_{2t});$$

which means $a_1 = a_2$, a contradiction. ■

Problem 20.

We say that a set $S \subseteq \mathbb{R}^3$ is *cyclic* if for every $(a,b,c) \in S$, we have $(a-b, b-c, c-a) \in S$. Prove that if $S \subseteq \mathbb{R}^3$ is cyclic and has bounded diameter (meaning that there exists $d > 0$ such that the distance between every two points in S is less than d), then it is finite.

Solution. Let S be an infinite cyclic subset of $\mathbb{R}^3$. We prove that S has unbounded diameter. We consider two cases.

First, assume that S is a subset of the line L with equation $x = y = z$ (note that every subset of L containing the origin is cyclic). Clearly, every infinite subset of L has unbounded diameter.
Next, assume that S is not a subset of L. Then there exists $(a, b, c) \in S$ for which at least two of a, b, c are distinct. Define a sequence $\{X_n = (a_n, b_n, c_n) : n = 0, 1, 2, \ldots\}$ recursively as follows:

- Let $X_0 = (a_0, b_0, c_0) = (a, b, c)$.
- For every $n \geq 0$, let $X_{n+1} = (a_n - b_n, b_n - c_n, c_n - a_n)$.

Since S is cyclic and $X_0 \in S$, it follows that $X_n \in S$ for every $n \geq 0$. The invariant here is the "*distance of X_n from the origin*." We will show that this grows indefinitely.
Let $n \geq 1$. Then $a_n + b_n + c_n = 0$ (why?). Therefore,

$$0 = (a_n + b_n + c_n)^2 = a_n^2 + b_n^2 + c_n^2 + 2(a_n b_n + b_n c_n + c_n a_n) \Rightarrow a_n b_n + b_n c_n + c_n a_n \leq 0.$$

Moreover,

$$a_{n+1}^2 + b_{n+1}^2 + c_{n+1}^2 = (a_n - b_n)^2 + (b_n - c_n)^2 + (c_n - a_n)^2 = 2(a_n^2 + b_n^2 + c_n^2) - 2(a_n b_n + b_n c_n + c_n a_n);$$

and thus,

$$a_{n+1}^2 + b_{n+1}^2 + c_{n+1}^2 \geq 2(a_n^2 + b_n^2 + c_n^2).$$

It follows from a quick induction that for every $n \geq 1$,

$$a_n^2 + b_n^2 + c_n^2 \geq 2^{n-1}(a_1^2 + b_1^2 + c_1^2).$$

Now, recall that at least two of a_0, b_0, c_0 are distinct, and so $a_1^2 + b_1^2 + c_1^2 > 0$. We deduce that the distance of X_n from the origin can be arbitrarily large.
Now, S is a subset of $\mathbb{R}^3$ that contains points arbitrarily far from the origin. Of course, it cannot have bounded diameter. (Why?) ■

5 The Pigeonhole Principle

The *Pigeonhole Principle* (PP) says that if $n+1$ pigeons go into n pigeonholes, then at least two pigeons end up in the same pigeonhole. More generally, if m pigeons go into n pigeonholes, then at least $\lceil \frac{m}{n} \rceil$ pigeons end up in the same pigeonhole. This is quite useful in proving existential results: Out of every three integers, there are two with the same parity; Out of every eight people, there are two that were born on the same day of the week; The world's population is (roughly) 8.3 billion, and each day has 86.4 million milliseconds, so every day at least $\lceil \frac{8.3\times10^9}{8.64\times10^7} \rceil = 97$ people wake up at the exact same time up to milliseconds! Here are some more interesting examples:

Problem 21.

Prove that every set of $n \in \mathbb{N}$ integers has a subset whose elements add up to a multiple of n.

Solution. Let $S = \{a_1, \ldots, a_n\}$ be a set of n integers. For each $i \in \{1, \ldots, n\}$, let $s_i = a_1 + \cdots + a_i$. So, we have $s_1 = a_1$, $s_2 = a_1 + a_2$, $s_3 = a_1 + a_2 + a_3$, and so on. If there exists $i \in \{1, \ldots, n\}$ for which s_i is divisible by n, then we are done since $\{a_1, \ldots, a_i\}$ is the desired subset of S. Therefore, we may assume that none of $s_1, \ldots, s_n$ is divisible by n. Since there are only $n-1$ possible remainders modulo n other than zero, by PP, there exist $1 \leq i < j \leq n$ such that $s_i \equiv s_j \pmod{n}$. Thus, $n \mid s_j - s_i = a_{i+1} + \cdots + a_j$, and so $\{a_{i+1}, \ldots, a_j\}$ is the desired subset of S. ■

Problem 22.

Prove that there will be three problems on Assignment 2 such that either every two of those three problems are solved commonly by some student, or no two of those three problems are solved commonly by any student.

Solution. Let us say that a pair of problems is *blue* if at least one student solves them both, and *red* if no student solves both of them. Our goal is to prove that there are three problems such that either every two of them form a blue pair (which we call a *blue triple*), or every two of them form a red pair (which we call a *red triple*). Let $P_1, \ldots, P_6$ be the problems on Assignment 2. (Recall that we have six problems on each assignment!) Each of the five pairs $\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5\}, \{P_1, P_6\}$ is either blue or red. Thus, by PP, there are three pairs among these five that are all the same color. Without loss of generality, we may assume that $\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}$ are all blue. Now, if at least one of $\{P_2, P_3\}, \{P_3, P_4\}, \{P_2, P_4\}$ is blue, then that pair together with P_1 forms a blue triple. Otherwise, if all three of $\{P_2, P_3\}, \{P_3, P_4\}, \{P_2, P_4\}$ are red, then $\{P_2, P_3, P_4\}$ is a red triple. ■

Problem 23.

Prove that among any 5 points in $\mathbb{R}^2$ with integer coordinates, there exist two points such that the line segment joining them contains another point with integer coordinates (not necessarily one of the original 5 points).

Solution. Let $(x_1, y_1), \ldots, (x_5, y_5)$ be the five points. There are four possibilities for the parities of the coordinates of each point: (even, even), (even, odd), (odd, even), (odd, odd). So, by PP, there exist $1 \leq i < j \leq 5$ such that x_i, x_j have the same parity, and so do y_i, y_j. It follows that $x_i + x_j$ and $y_i + y_j$ are both even, and thus $(\frac{x_i+x_j}{2}, \frac{y_i+y_j}{2})$ has integer coordinates. But we are done already because $(\frac{x_i+x_j}{2}, \frac{y_i+y_j}{2})$ is the midpoint of the line segment joining (x_i, y_i) and (x_j, y_j). ■

Problem 24.

Prove that among any seven real numbers, there are two numbers x, x' such that

$$0 \leq \frac{x - x'}{1 + xx'} \leq \frac{\sqrt{3}}{3}.$$

Solution. Let $x_1 \leq \cdots \leq x_7$ be the numbers. Since every real number is the tangent of a unique angle in $(-\pi/2, \pi/2)$, and tangent is increasing on $(-\pi/2, \pi/2)$, it follows that there are angles $\theta_1 \leq \cdots \leq \theta_7$ in $(-\pi/2, \pi/2)$ such that for each $i \in \{1, \ldots, 7\}$, we have $x_i = \tan\theta_i$. Since $(-\pi/2, \pi/2)$ is an interval of length π, we may partition it into six intervals $I_1, \ldots, I_6$, each of length $\pi/6$. Since each of $\theta_1, \ldots, \theta_7$ belongs to one of $I_1, \ldots, I_6$, by PP, there exist $1 \leq i < j \leq 7$ such that θ_i, θ_j belong to the same interval. So, $0 \leq \theta_j - \theta_i \leq \pi/6$, and $0 \leq \tan(\theta_j - \theta_i) \leq \sqrt{3}/3$. But

$$\tan(\theta_j - \theta_i) = \frac{\tan(\theta_j) - \tan(\theta_i)}{1 + \tan(\theta_j)\tan(\theta_i)} = \frac{x_j - x_i}{1 + x_j x_i}. \quad \blacksquare$$

Problem 25.

Let $n \in \mathbb{N}$ and let $S \subseteq \{1, \ldots, 2n\}$ with $|S| = n + 1$.

(a) Prove that there exist $a, b, c \in S$ such that $a + b = c$. (We allow $a = b$.)

(b) Prove that there exist distinct $a, b \in S$ such that $a \mid b$.

Solution. Let $S = \{a_1, \ldots, a_{n+1}\}$ such that $a_1 < \cdots < a_{n+1}$. First, we prove (a). For each $i \in \{1, \ldots, n\}$, let $b_i = a_{n+1} - a_i$. Then $b_1 > \cdots > b_n$ are n elements in $\{1, \ldots, 2n\}$, all strictly smaller than a_{n+1}. Since the $2n+1$ numbers $a_1, \ldots, a_{n+1}, b_1, \ldots, b_n$ are all members of $\{1, \ldots, 2n\}$, by PP, two of them must be equal. Since $a_1, \cdots, a_{n+1}$ are pairwise distinct, and $b_1, \cdots, b_n, a_{n+1}$ are also pairwise distinct, it follows that there exist $i, j \in \{1, \ldots, n\}$ (possibly $i = j$) such that $a_i = b_j$. Therefore, we have $a_i = a_{n+1} - a_j$, and so $a_i + a_j = a_{n+1}$, as desired.

Next, we prove (b). By the prime factorization theorem, for each $i \in \{1, \ldots, n+1\}$, we may write $a_i = 2^{p_i} q_i$ where $p_i, q_i \geq 0$ are integers and q_i is odd. In particular, $q_1, \ldots, q_{n+1}$ are $n + 1$ odd numbers in $\{1, \ldots, 2n\}$. But there are only n odd numbers in $\{1, \ldots, 2n\}$; thus, by PP, there exist distinct $i, j \in \{1, \ldots, n+1\}$ such that $q_i = q_j$. Moreover, without loss of generality, we may assume that $p_i \leq p_j$. Hence, we have $a_i = 2^{p_i} q_i \mid 2^{p_j} q_i = 2^{p_j} q_j = a_j$, as desired. $\blacksquare$

Problem 26.

Define the sequence $\{a_n\}_{n \geq 1}$ recursively by $a_1 = 1, a_2 = 9, a_3 = 9, a_4 = 4$, and for every $n \geq 5$, a_n is the remainder of $a_{n-1} + a_{n-2} + a_{n-3} + a_{n-4}$ when divided by 10. Prove that at some point, $7, 5, 7, 4$ appear as four consecutive terms of this sequence.

Solution. Observe that *if any four consecutive terms of the sequence are given, then all the preceding terms are determined uniquely.* Now, note that there are only 10^4 quadruples of numbers in $\{0, 1, \ldots, 9\}$. Thus, by PP, there exist $1 \leq m < n \leq 10^4 + 1$ such that the quadruples $(a_m, a_{m+1}, a_{m+2}, a_{m+3})$ and $(a_n, a_{n+1}, a_{n+2}, a_{n+3})$ are the same. By the above observation, we have

$$a_{m-1} = a_{n-1},\ a_{m-2} = a_{n-2},\ \ldots,\ a_4 = a_{n-m+4},\ a_3 = a_{n-m+3},\ a_2 = a_{n-m+2},\ a_1 = a_{n-m+1}.$$

In particular, the first four terms $(a_1, a_2, a_3, a_4) = (1, 9, 9, 4)$ will reappear as four consecutive terms $(a_{n-m+1}, a_{n-m+2}, a_{n-m+3}, a_{n-m+4})$. Therefore, the first four terms will appear infinitely many times as four consecutive terms! But now deep enough into the sequence, we can work backwards from the terms $1, 9, 9, 4$ and obtain

$$0, 5, \mathbf{7,5,7,4}, 3, 9, 3, 9, 4, 5, 1, 9, 9, 4. \quad \blacksquare$$

Note. According to ChatGPT, the first time $7, 5, 7, 4$ appears is at $a_{1551}, a_{1552}, a_{1553}, a_{1554}$.

Problem 27.

For every $\alpha \in \mathbb{R}$, define $||\alpha||$ to be the minimum distance of α from an integer. For example,

$$||1.3|| = ||2.7|| = 0.3, \quad ||\pi|| = \pi - 3, \quad ||e|| = 3 - e.$$

Prove that for every $\alpha \in \mathbb{R}$, we have $\inf\{||n\alpha|| : n \in \mathbb{N}\} = 0$.

Solution. We write $\{x\}$ for the *fractional part* of x; that is, $\{x\} = x - \lfloor x \rfloor$. Note that $\{x\} \in [0, 1)$, and also $||x|| \in [0, 1)$. We need to prove that for every $\varepsilon \in (0, 1)$, there exists $n \in \mathbb{N}$ such that $||n\alpha|| < \varepsilon$. Let $\varepsilon \in (0, 1)$ be fixed and let $p = \lceil 1/\varepsilon \rceil$. Then, $p \in \mathbb{N}$ and $p \geq 2$. Consider the p intervals:

$$I_0 = \left[0, \frac{1}{p}\right), \quad I_1 = \left[\frac{1}{p}, \frac{2}{p}\right), \quad \cdots, \quad I_{p-1} = \left[\frac{p-1}{p}, 1\right).$$

Note that $(I_0, I_1, \ldots, I_{p-1})$ is a partition of $[0, 1)$.
Since the $p+1$ numbers $0, \{\alpha\}, \{2\alpha\}, \ldots, \{p\alpha\}$ belong to the interval $[0, 1)$, and since $(I_0, I_1, \ldots, I_{p-1})$ is a partition of $[0, 1)$ into p subintervals, by PP, at least two of $0, \{\alpha\}, \{2\alpha\}, \ldots, \{p\alpha\}$ belong to the same interval among $I_0, I_1, \ldots, I_{p-1}$; in particular, there exist distinct $i, j \in \{0, 1, 2, \ldots, p\}$ such that $0 \leq \{j\alpha\} - \{i\alpha\} < 1/p$. Since $1/p \leq 1/2$, it follow that $||\{j\alpha\} - \{i\alpha\}|| = \{j\alpha\} - \{i\alpha\}$. Thus, since $1/p \leq \varepsilon$, it follows that

$$||\{j\alpha\} - \{i\alpha\}|| < \varepsilon.$$

Now, let $n = |j - i|$. Then $n \in \mathbb{N}$, and we have $||n\alpha|| = ||(j - i)\alpha||$ (note that $||x|| = || - x||$ for every $x \in \mathbb{R}$). Therefore,

$$\begin{aligned}
||n\alpha|| &= ||(j-i)\alpha|| \\
&= ||j\alpha - i\alpha|| \\
&= ||(\lfloor j\alpha \rfloor + \{j\alpha\}) - (\lfloor i\alpha \rfloor + \{i\alpha\})|| \\
&= ||\underbrace{(\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor)}_{\text{integer}} + (\{j\alpha\} - \{i\alpha\})|| \\
&= ||\{j\alpha\} - \{i\alpha\}|| \\
&< \varepsilon.
\end{aligned}$$

$\blacksquare$

6 Extremal arguments

Your lesson here is: Look into the extremes; choose an example/counterexample that maximizes or minimizes some quantity, and analyze its behavior. This simple trick can be unexpectedly useful:

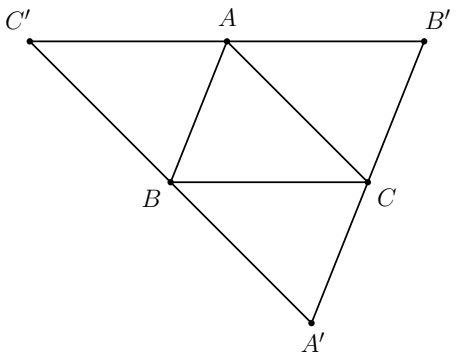
Problem 28.

Let S be a finite set points in the plane such that every three of them form a triangle of area at most 1. Prove that S is contained in a triangle of area at most 4.

Solution. The case where S is contained in a line is easy. (Why?) So, assume that there are three points in S that form a triangle with nonzero area. The extremal trick is to:

Choose three points $A, B, C \in S$ such that the area of ΔABC is as large as possible.

Let ℓ_a be the line passing through A parallel to BC, let ℓ_b be the line passing through B parallel to AC, and let ℓ_c be the line passing through C parallel to AB. Let A', B', C' be the intersection points of ℓ_b, ℓ_c and ℓ_a, ℓ_c and ℓ_a, ℓ_b, respectively. Now, let X be a point in S other than A, B, C. Then X should lie either on ℓ_a or on the same side of ℓ_a as B, C, because otherwise ΔXBC would have larger area than ΔABC, contrary to the choice of A, B, C. Similarly, X should lie either on ℓ_b or on the same side of ℓ_b as A, C, and either on ℓ_c or on the same side of ℓ_c as A, B. It follows that X must lie on or inside the triangle $\Delta A'B'C'$. Since $X \in S$ was arbitrary, we deduce that all of S is contained in $\Delta A'B'C'$. Moreover, note that ΔABC, $\Delta A'BC$, $\Delta AB'C$, and $\Delta ABC'$ have the same area, and that ΔABC has area at most 1. So, the area of $\Delta A'B'C'$ is at most 4. ■



Problem 29.

Prove that the equation $a^2 + b^2 = 3(c^2 + d^2)$ has no solution in nonzero integers.

Solution. Suppose not. Here is the extremal trick:

Choose a solution (a, b, c, d) with $a^2 + b^2$ as small as possible.

Since $a^2 + b^2 = 3(c^2 + d^2)$, it follows that $3 \mid a^2 + b^2$, which means that $3 \mid a$ and $3 \mid b$ (why?). Let $a', b' \in \mathbb{Z}$ such that $a = 3a'$ and $b = 3b'$. Then

$$a^2 + b^2 = 3(c^2 + d^2) \Rightarrow 9(a'^2 + b'^2) = 3(c^2 + d^2) \Rightarrow c^2 + d^2 = 3(a'^2 + b'^2).$$

But now (c, d, a', b') is another solution with $c^2 + d^2 = \frac{1}{3}(a^2 + b^2) < a^2 + b^2$, contradiction to the choice of (a, b, c, d). ■

Note. We essentially proved that if there is one solution (a_0, b_0, c_0, d_0), then there are infinitely many solutions $(a_0, b_0, c_0, d_0), (a_1, b_1, c_1, d_1), (a_2, b_2, c_2, d_2), \cdots$ with $a_0^2+b_0^2 > a_1^2+b_1^2 > a_2^2+b_2^2 > \cdots$, and that would be impossible because *there is no infinite strictly decreasing sequence of positive integers*. This is sometimes called the method of *infinite descent*.

Problem 30.

Prove that there is no infinite arithmetic progression of integers whose terms are all perfect squares, unless all terms are equal.

Solution. Suppose for a contradiction that there is an infinite sequence $a_1 < a_2 < a_3 < \cdots$ of positive integers such that $a_1^2, a_2^2, a_3^2, \ldots$ is an arithmetic progression. Here is the extremal trick:

Choose this sequence with $a_2 - a_1$ as small as possible.

Since $a_1 < a_2 < a_3$, it follows that

$$a_2 + a_1 < a_3 + a_2.$$

Since a_1^2, a_2^2, a_3^2 is a (3-term) arithmetic progression, we have $a_3^2 - a_2^2 = a_2^2 - a_1^2$, and so

$$(a_3 + a_2)(a_3 - a_2) = (a_2 + a_1)(a_2 - a_1)$$

Therefore, $a_3 - a_2 < a_2 - a_1$. But now $a_2, a_3, a_4, \ldots$ is another sequence such that $a_2^2, a_3^2, a_4^2, \ldots$ is an arithmetic progression, and $a_3 - a_2 < a_2 - a_1$, contradiction to the choice of $a_1, a_2, a_3, \ldots$. ■

Note. Again, we are using infinite descent: if $a_1^2, a_2^2, a_3^2, \ldots$ is an arithmetic progression of integers with distinct terms, then

$$a_2 - a_1 > a_3 - a_2 > a_4 - a_3 > \cdots$$

which is impossible.

Problem 31.

"Air All Over" is an airline with remarkable coverage: between any two airports in the world, it has a direct flight in at least one direction. Prove that there is an airport that can be reached from any other airport via Air All Over flights either directly or with one stop.

Solution. For each airport a, let D_a be the set of all other airports with a direct Air All Over flight to a. Here is the extremal trick:

Choose an airport a with $|D_a|$ as large as possible.

We claim that a has the desired property. Let D' be the set of all airports in the world other than a and the airports in D_a. Then no airport in D' has a direct flight to a. We need to show that every airport in D' has a direct flight to some airport in D_a (because that would yield a one-stop flight to a). Suppose for a contradiction that some airport $a' \in D'$ has no direct flight to any airport in D_a. By the coverage property, it follows that every airport in D_a has a direct flight to a'. Also, recall that $a' \in D'$ has no direct flight to a, and again by the coverage property, there should be a direct AAO flight from a to a'. But now we have $D_a \cup \{a\} \subseteq D_{a'}$, and so

$$|D_{a'}| \geq |D_a \cup \{a\}| = |D_a| + 1 > |D_a|,$$

contradiction to the choice of a with $|D_a|$ maximum. ■

Problem 32.

In an event with $n \geq 4$ guests, among each four guests, there is at least one guest that shakes hands with the other three. Prove that some guest in this event shakes hands with everyone.

Solution. For each guest g, let S_g be the set of all other guests that shake hands with g. Here is the extremal trick:

Choose a guest g with $|S_g|$ as large as possible.

Since $n \geq 4$, applying the assumption to some four guests implies that there is a guest who shakes hands with at least three other guests. By the choice of g, it follows that $|S_g| \geq 3$.
We claim that g shakes hands with everyone else. Suppose not. Then there is a guest h in the event such that $h \notin S_g \cup \{g\}$. For every two guests $g_1, g_2 \in S_g$, one of the four guests g, g_1, g_2, h must shake hands with the other three. Since g, h do not shake hands, it follows that either g_1 or g_2 should shake hands with the other three. It follows that:

- Every two guests in S_g shake hands with each other; and
- At most one guest in S_g does not shake hands with h.

Since $|S_g| > 1$, by the second bullet, we may choose a guest $g' \in S_g$ that shakes hands with h. Note that g' also shakes hands with g (because $g' \in S_g$) and with everyone in $S_g \setminus \{g'\}$ (by the first bullet). But now $(S_g \setminus \{g'\}) \cup \{g, h\} \subseteq S_{g'}$, and thus

$$|S_{g'}| \geq |(S_g \setminus \{g'\}) \cup \{g, h\}| = |S_g| - 1 + 2 > |S_g|,$$

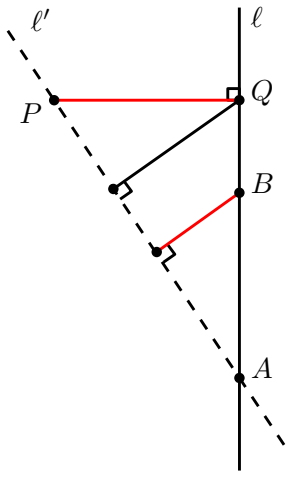
contradiction to the choice of g. ■

Problem 33.

Let S be a finite set of points in the plane, not all on the same line. Prove that there exists a line that passes through exactly two points in S.

Solution. Suppose not. Since S is not contained in a line, it follows that there are three points in S not on the same line. In particular, there is a line ℓ that passes through at least two points in S, as well as a point $P \in S$ not on ℓ. Here is the extremal trick:

Choose ℓ, P such that the orthogonal distance between P and ℓ is as small as possible.



Since ℓ passes through at least two points in S, but not exactly two points in S, it follows that there are three points $A, B, C \in S$ that lie on ℓ. Let Q be the foot of the perpendicular from P to ℓ. By the pigeonhole principle, two of A, B, C lie on the same side of Q; say, A, B, Q appear on ℓ in this order (where $B = Q$ is possible). Let ℓ' be the line passing through A, P. Then ℓ' is a line through two points in S (namely, A and P), and $B \in S$ is a point not on ℓ'. But the orthogonal distance between B and ℓ' is smaller than (or equal to) the orthogonal distance between Q and ℓ', which in turn is strictly smaller than the length of PQ, contradiction to the choice of ℓ, P. ■

Note. This is the *Sylvester-Gallai theorem*.

Problem 34.

Let $a, b \in \mathbb{N}$. Prove that if $\frac{a^2+b^2}{ab+1}$ is an integer, then it is a perfect square.

Solution. We may always assume that $a \geq b$. Suppose for a contradiction that for some pair (a, b) of positive integers, the number $\frac{a^2+b^2}{ab+1}$ is an integer but not a perfect square. Here is the extremal trick:

Choose such a pair (a, b) with a as small as possible.

Let $c = \frac{a^2+b^2}{ab+1}$. Note that $a^2 - (bc)a + (b^2 - c) = 0$, and so a is a solution to the equation

$$x^2 - (bc)x + (b^2 - c) = 0.$$

Let a' be the other solution. Then we have $a + a' = bc$ and $aa' = b^2 - c$. Since $a, b, c \in \mathbb{N}$, it follows that $a' = bc - a$ is an integer, and since c is not a perfect square, it follows that $a' = \frac{b^2-c}{a}$ is not zero. In fact, since $\frac{a'^2+b^2}{a'b+1} = c > 0$, it follows that $a'b + 1 > 0$, which in turn implies that $a' > 0$. Also, since $a \geq b$, it follows that

$$a' = \frac{b^2 - c}{a} < \frac{b^2}{a} \leq b \leq a.$$

But now (a', b) is another pair of positive integers for which $\frac{a'^2+b^2}{a'b+1} = c$ is an integer but not a perfect square, and yet $a' < a$, contradiction to the choice of (a, b). ■

Note. This is the infamous Problem 6 from IMO 1998. At the time, and for quite a while after, it was considered one of the hardest IMO problems ever.

Problem 35.

Let $m, n \in \mathbb{N}$. Prove that every sequence of $mn+1$ real numbers contains either an increasing subsequence with $m + 1$ terms or a decreasing subsequence with $n + 1$ terms.
(Here, a "subsequence" means a bunch of terms, in the same order as the original sequence, but not necessarily consecutive.)

Solution. Let $S = (a_1, \ldots, a_{mn+1})$ be the sequence. Here is the extremal trick:

For each $i \in \{1, \ldots, mn + 1\}$, let ℓ_i be the length (number of terms) of the longest increasing subsequence of S starting at a_i.

(Note that $\ell_i \geq 1$ because the single-term subsequence "a_i" is increasing on its own.)
If one of $\ell_1, \ldots, \ell_{mn+1}$ is at least $m + 1$, then we are done. Therefore, we may assume that $\ell_1, \ldots, \ell_{mn+1} \in \{1, \ldots, m\}$. By the pigeonhole principle, at least $\lfloor \frac{mn+1}{m} \rfloor + 1 \geq n+1$ numbers among $\ell_1, \ldots, \ell_{mn+1}$ are equal. Let $1 \leq i_1 < i_2 < \cdots < i_{n+1} \leq mn + 1$ such that $\ell_{i_1} = \ell_{i_2} = \cdots = \ell_{i_{n+1}}$.
We claim that $a_{i_1} > a_{i_2} > \cdots > a_{i_{n+1}}$. Suppose for contradiction that for some $j \in \{1, \ldots, n\}$, we have $a_{i_j} \leq a_{i_{j+1}}$. Let S' be the longest increasing subsequence of S starting at $a_{i_{j+1}}$. Then S' has $\ell_{i_{j+1}}$ terms. Since $a_{i_j} \leq a_{i_{j+1}}$, adding a_{i_j} to the left of S' yields an increasing subsequence S'' of S starting at a_{i_j} with $\ell_{i_{j+1}} + 1$ terms. But recall that $\ell_{i_{j+1}} = \ell_{i_j}$, and thus S'' has $\ell_{i_j} + 1$ terms, which is longer than the longest increasing subsequence of S starting at a_{i_j}, a contradiction.
From the above claim, it follows that $(a_{i_1}, a_{i_2}, \ldots, a_{i_{n+1}})$ is a decreasing subsequence of S with $n+1$ terms, as desired. ■

Note. This is the *Erdős-Szekeres theorem.*

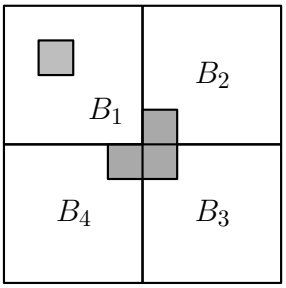
7 Induction

We all know about *induction* – arguably one of the most widely used proof techniques. There are many variants: the ordinary one ("assume for k, prove for $k+1$"), the *strong* one ("assume for all values $\leq k$, prove for $k+1$"), and some stranger versions (see Problems 42 and 43 below).

Problem 36.

Prove that for every $n \in \mathbb{N}$, a $2^n \times 2^n$ board with one cell removed can be tiled by 3-cell L-shaped tiles.

Solution. We proceed by induction on n. The base case $n = 1$ is immediate. Assume that the statement is true for some $n = k$, where $k \in \mathbb{N}$. Consider a $2^{k+1} \times 2^{k+1}$ board B. Break B into four $2^k \times 2^k$ boards B_1, B_2, B_3, B_4, where B_1 is the top left, B_2 is the top right, B_3 is the bottom right, and B_4 is the bottom left. Assume without loss of generality that the removed cell from B lies in B_1. Then, by the inductive hypothesis, the remainder of B_1 can be tiled. Also, the bottom left corner of B_2, the top left corner of B_3, and the top right corner of B_4 together can be tiled with one tile. Now, the remainder of B_2, B_3, B_4 can be tiled by the inductive hypothesis. ■



Problem 37.

Let $\alpha \in \mathbb{R} - \{0\}$ such that $\alpha + \alpha^{-1} \in \mathbb{Z}$. Prove that for every $n \in \mathbb{N} \cup \{0\}$, we have $\alpha^n + \alpha^{-n} \in \mathbb{Z}$.

Solution. We proceed by strong induction on n. The base cases $n = 0, 1$ are immediate. Assume that for some $k \in \mathbb{N}$, we have $\alpha^l + \alpha^{-l} \in \mathbb{Z}$ for every $0 \leq l \leq k$. Then

$$\alpha^{k+1} + \alpha^{-(k+1)} = \underbrace{\left(\alpha + \alpha^{-1}\right)}_{\in\mathbb{Z}} \underbrace{\left(\alpha^k + \alpha^{-k}\right)}_{\in\mathbb{Z}} - \underbrace{\left(\alpha^{k-1} + \alpha^{-(k-1)}\right)}_{\in\mathbb{Z}} \in \mathbb{Z}. \quad \blacksquare$$

Problem 38.

Recall the Fibonacci sequence $\{f_m\}_{m\geq 1}$, where $f_1 = 1, f_2 = 2$, and $f_m = f_{m-1} + f_{m-2}$ for all $m \geq 3$. Prove that every $n \in \mathbb{N}$ can be written as a sum of Fibonacci numbers no two of which are consecutive.

Solution. We proceed by strong induction on n. The base cases $n = 1, 2$ are clear. Assume that for some $k \geq 2$, every number in $\{1, \ldots, k\}$ can be written as a sum of Fibonacci numbers no two of which are consecutive. If $k+1$ is a Fibonacci number, then we are done. Therefore, since $\{f_m\}_{m\geq 1}$ is strictly increasing, we may assume that there exists $m \in \mathbb{N}$ such that $f_m < k+1 < f_{m+1}$. Note that $m \geq 3$ since $f_{m+1} > k+1 \geq 3$. Let

$$k' = (k+1) - f_m.$$

Since $f_m < k+1$, it follows that $1 \leq k'$, and since $k+1 < f_{m+1}$, it follows that $k' < f_{m+1} - f_m = f_{m-1}$. We deduce that

$$1 \leq k' < f_{m-1}.$$

In particular, since $f_{m-1} < f_m < k+1$, it follows that $k' \in \{1, \ldots, k\}$, and thus by the inductive hypothesis, k' can be written as a sum of Fibonacci numbers no two of which are consecutive. Moreover, since $k' < f_{m-1}$, each summand belongs to $\{f_1, \ldots, f_{m-2}\}$. But now $k+1 = k' + f_m$ can be written as a sum of Fibonacci numbers no two of which are consecutive; namely, the terms in the sum for k', together with f_m. This completes the inductive step. ■

Question. Can you find an $n \in \mathbb{N}$ that can be written as such a sum in two different ways?

Problem 39.

Prove that for every $n \in \mathbb{N} \cup \{0\}$, there is a partition (A, B) of $\{1, \ldots, 2^{n+1}\}$ such that for every $i \in \{0, 1, \ldots, n\}$, we have

$$\sum_{a \in A} a^i = \sum_{b \in B} b^i.$$

Solution. We proceed by ordinary induction on n. The base case $n = 0$ is immediate (choose $A = \{1\}$ and $B = \{2\}$). Assume that for some $k \in \mathbb{N}$, there is a partition (A, B) of $\{1, \ldots, 2^{k+1}\}$ such that for every $i \in \{0, 1, \ldots, k\}$, we have

$$\sum_{a \in A} a^i = \sum_{b \in B} b^i.$$

Let

$$C = A \cup \{b + 2^{k+1} : b \in B\} \quad \text{and} \quad D = B \cup \{a + 2^{k+1} : a \in A\}.$$

Then (C, D) is a partition of $\{1, \ldots, 2^{k+2}\}$. By the binomial theorem, for each $i \in \{0, 1, \ldots, k+1\}$, we have

$$\begin{aligned}
\sum_{c \in C} c^i - \sum_{d \in D} d^i &= \left(\sum_{a \in A} a^i + \sum_{b \in B} \left(b + 2^{k+1}\right)^i \right) - \left(\sum_{b \in B} b^i + \sum_{a \in A} \left(a + 2^{k+1}\right)^i \right) \\
&= \sum_{b \in B} \left(\left(b + 2^{k+1}\right)^i - b^i \right) - \sum_{a \in A} \left(\left(a + 2^{k+1}\right)^i - a^i \right) \\
&= \sum_{b \in B} \sum_{j=0}^{i-1} \binom{i}{j} b^j \left(2^{k+1}\right)^{i-j} - \sum_{a \in A} \sum_{j=0}^{i-1} \binom{i}{j} a^j \left(2^{k+1}\right)^{i-j} \\
&= \sum_{j=0}^{i-1} \binom{i}{j} \left(2^{k+1}\right)^{i-j} \left(\sum_{b \in B} b^j - \sum_{a \in A} a^j \right).
\end{aligned}$$

Since $i - 1 \leq k$, by the inductive hypothesis, for each $j \in \{0, \ldots, i-1\}$, we have $\sum_{a \in A} a^j = \sum_{b \in B} b^j$. Therefore,

$$\sum_{c \in C} c^i - \sum_{d \in D} d^i = \sum_{j=0}^{i-1} \binom{i}{j} \left(2^{k+1}\right)^{i-j} \left(\sum_{b \in B} b^j - \sum_{a \in A} a^j \right) = 0.$$

Hence, (C, D) is the desired partition of $\{1, \ldots, 2^{k+2}\}$. ■

Problems 40, 41, 42 each have a "moral."

Problem 40.

Prove that for every integer $n \geq 2$, we have $\sqrt{2\sqrt{3\sqrt{\cdots\sqrt{n}}}} < 3$.

Solution. The moral here is:

Sometimes you need to induct on a weird parameter that is not the first "obvious" choice.

For instance, inducting on n here is almost impossible (try it!). So we are going to prove a stronger statement, that for all $m, n \in \mathbb{N}$ with $m \leq n$, we have

$$\sqrt{m\sqrt{(m+1)\sqrt{\cdots\sqrt{n}}}} < m+1.$$

The proof of that is by induction on $d = n - m \geq 0$. The base case $d = n - m = 0$ is immediate: $\sqrt{m} < m+1$. Now, let $m < n$ (so $d = n - m > 0$). Since $n - (m+1) = d - 1 < d$, by the inductive hypothesis, we have

$$\sqrt{(m+1)\sqrt{(m+2)\sqrt{\cdots\sqrt{n}}}} < m+2.$$

Hence,

$$\sqrt{m\sqrt{(m+1)\sqrt{\cdots\sqrt{n}}}} < \sqrt{m(m+2)} = \sqrt{(m+1)^2 - 1} < \sqrt{(m+1)^2} = m+1. \quad \blacksquare$$

Problem 41.

Prove that every positive integer m can be written as $\pm 1^2 \pm 2^2 \pm \cdots \pm n^2$ for some $n \in \mathbb{N}$ and some choice of signs.

Solution. The moral here is:

Sometimes you need "wider" induction steps (and, as this necessitates, more base cases).

For this problem, the proof is by the following unusual version of induction on m:

- Base cases: $m = 1, 2, 3, 4$.
- Induction step: assume for $m = k$, prove for $m = k + 4$.

For the base cases, note that

$$1 = 1^2, \quad 2 = -1^2 - 2^2 - 3^2 + 4^2, \quad 3 = -1^2 + 2^2, \quad 4 = -1^2 - 2^2 + 3^2.$$

Now, assume by the inductive hypothesis that for some $k \in \mathbb{N}$, we have $k = \pm 1^2 \pm 2^2 \pm \cdots \pm n^2$ for some $n \in \mathbb{N}$ and some choice of signs. Note that

$$(n+1)^2 + (n+4)^2 = 2n^2 + 10n + 17 \quad \text{and} \quad (n+2)^2 + (n+3)^2 = 2n^2 + 10n + 13.$$

Consequently, $(n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4)^2 = 4$, and thus

$$k + 4 = \pm 1^2 \pm 2^2 \pm \cdots \pm n^2 + (n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4)^2;$$

where the signs of the first n terms are the same as in the expression for k. $\blacksquare$

Problem 42.

For $n \in \mathbb{N}$, we say that a function $f : \mathbb{R} \to \mathbb{R}$ is *n-special* if for all $x_1, \ldots, x_n \in \mathbb{R}$, we have

$$f\left(\frac{x_1 + \cdots + x_n}{n}\right) = \frac{f(x_1) + \cdots + f(x_n)}{n}.$$

Prove that if $f : \mathbb{R} \to \mathbb{R}$ is 2-special, then f is n-special for every integer $n \geq 2$.

Solution. The moral here is:

Sometimes you need to induct backwards!

For this problem, the proof is by an even more unusual version of induction on n:

- Base case: $n = 2$.
- Induction step 1: assume for $n = k$, prove for $n = 2k$.
- Induction step 2: assume for $n = k + 1$, prove for $n = k$.

The base case $n = 2$ holds because f is 2-special. For induction step 1, assume that f is k-special for some $k \geq 2$. Then, for all $x_1, \ldots, x_{2k} \in \mathbb{R}$, we have

$$\begin{aligned}
f\left(\frac{x_1 + \cdots + x_{2k}}{2k}\right) &= f\left(\frac{\frac{x_1 + \cdots + x_k}{k} + \frac{x_{k+1} + \cdots + x_{2k}}{k}}{2}\right) \\
&= \frac{f\left(\frac{x_1 + \cdots + x_k}{k}\right) + f\left(\frac{x_{k+1} + \cdots + x_{2k}}{k}\right)}{2} && \text{Since } f \text{ is 2-special} \\
&= \frac{\frac{f(x_1) + \cdots + f(x_k)}{k} + \frac{f(x_{k+1}) + \cdots + f(x_{2k})}{k}}{2} && \text{Since } f \text{ is } k\text{-special} \\
&= \frac{f(x_1) + \cdots + f(x_{2k})}{2k}.
\end{aligned}$$

Thus, f is $2k$-special.
For induction step 2, assume that f is $(k+1)$-special for some $k \geq 2$. Then, for all $x_1, \ldots, x_k \in \mathbb{R}$, we have

$$\begin{aligned}
f\left(\frac{x_1 + \cdots + x_k}{k}\right) &= f\left(\frac{x_1 + \cdots + x_k + \left(\frac{x_1 + \cdots + x_k}{k}\right)}{k+1}\right) \\
&= \frac{f(x_1) + \cdots + f(x_k) + f\left(\frac{x_1 + \cdots + x_k}{k}\right)}{k+1} && \text{Since } f \text{ is } (k+1)\text{-special} \\
&\Rightarrow\ f\left(\frac{x_1 + \cdots + x_k}{k}\right) = \frac{f(x_1) + \cdots + f(x_k)}{k}.
\end{aligned}$$

Hence, f is k-special. ■

Problem 43.

Let $n \in \mathbb{N}$. Atlas is given a list of n pairwise distinct reals $x_1, \ldots, x_n > 0$. He is supposed to start from one end of a track of length $x_1 + \cdots + x_n$ and take n steps of lengths $x_1, \ldots, x_n$, in some order, to reach the other end. There are $n-1$ puddles along the track (no puddle at either end). Prove that the order can be chosen such that Atlas never steps into any puddle.

Solution. The proof is by strong induction on n. The base cases $n = 1, 2$ are easy to check. Assume that for some $k \geq 2$, the assertion holds for all $n \in \{1, \ldots, k\}$. We prove the case $n = k+1$. Without loss of generality, assume that $x_1 < \cdots < x_{k+1}$, and that Atlas starts at the left end of the track. From left to right, for each $i \in \{1, \ldots, k\}$, let y_i be the distance between the left end and the i-th puddle. Also, define $y_{k+1} = x_1 + \cdots + x_{k+1}$. There are three possibilities:

(i) Assume that $\{x_1, \ldots, x_{k+1}\} \not\subset (0, y_1] \cup \{y_2, \ldots, y_k\}$. Then $y_j < x_i < y_{j+1}$ for some $i \in \{1, \ldots, k+1\}$ and some $j \in \{1, \ldots, k\}$. In this case, Atlas first takes a step of length x_i, thereby passing over $j \geq 1$ puddles without stepping into any. From this point on, the number of remaining puddles is $k - j \leq k - 1$. So, by the inductive hypothesis (and by inserting $j-1$ "fake" puddles in the middle), he can take the remaining k steps in some order and make it to the right end without stepping into any puddle.

(ii) Assume that $\{x_1, \ldots, x_{k+1}\} \subset (0, y_1] \cup \{y_2, \ldots, y_k\}$ but $\{x_1, \ldots, x_{k+1}\} \not\subset (0, y_1]$. Then, for some $j \in \{2, \ldots, k\}$, we have $x_{k+1} = y_j$ and $\{x_1, \ldots, x_{k+1}\} \setminus (0, y_1) \subseteq \{y_1, \ldots, y_j\}$. It follows that $x_1, \ldots, x_{k+1-j} \in (0, y_1)$. Since $k+1-j > k-j$, there exists $\ell \in \{1, \ldots, k+1-j\}$ such that x_ℓ is distinct from each of $y_{j+1} - y_j, y_{j+2} - y_j, \ldots, y_k - y_j$. Now Atlas first takes a step of length $x_\ell < y_1$, which keeps him before the first puddle. Then he takes a step of length $x_{k+1} = y_j$, which takes him past the j-th puddle, but only by a distance of x_ℓ, which by the choice of x_ℓ does not land on any puddle after the j-th one. From this point on, there are at most $k - j \leq k - 2$ remaining puddles. So, by the inductive hypothesis (and by inserting $j-2$ "fake" puddles in the middle), he can take the remaining $k-1$ steps in some order and make it to the right end without stepping into any puddle.

(iii) Assume that $\{x_1, \ldots, x_{k+1}\} \subset (0, y_1]$. Then $0 < x_1 < \cdots < x_k < x_{k+1} \leq y_1$. Atlas first takes a step of length $z_0 = x_{k+1}$ – after which either he remains before the first puddle, or steps right into it. Ignore the first puddle for a moment. By the inductive hypothesis, there is a permutation $z_1, \ldots, z_k$ of $x_1, \ldots, x_k$ such that Atlas can start from *where he is now*, take k steps of lengths $z_1, \ldots, z_k$ in this order, and make it to the other end without ever stepping into any of the other $k-1$ puddles. Therefore, if he starts from the left end and takes $k+1$ steps of lengths $z_0, z_1, \ldots, z_k$ in this order (which is a permutation of $x_1, \ldots, x_{k+1}$), then he reaches the other end without ever stepping into any puddle except possibly the first one. If indeed he does not step into the first puddle either, then we are done. So we may assume that at some step, say right after the one of length z_i, where $i \in \{0, 1, \ldots, k\}$, he steps into the first puddle. Then $z_0 + \cdots + z_i = y_1$. Note that $i < k$ because no puddle is at the right end of the track; thus, the next step of length z_{i+1} exists. Now, since $z_{i+1} < x_{k+1} = z_0$, Atlas can avoid all puddles by only swapping the steps of lengths z_0 and z_{i+1}; so he takes $k+1$ steps of lengths $z_{i+1}, z_1, \ldots, z_i, z_0, z_{i+2}, \ldots, z_k$ in this order.

With all three cases handled, the induction is complete. ■

Note. This is Problem 6 from IMO 2009 (in disguise), which is to this day one of the hardest IMO problems ever. (This was my solution, which took me over 2 hours to figure out! You may find shorter/better solutions elsewhere.)

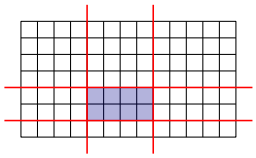
8 Counting (and some graph theory)

The purpose here is to discuss two counting techniques. First, counting the number of elements in a set X sometimes becomes easier if instead we find a set Y such that there is a bijection $f : X \to Y$, and then count the number of elements of Y. That is enough because *two finite sets X, Y have the same number of elements if and only if there exists a bijection between X and Y.* Here are some problems demonstrating this technique.

Problem 44.

For $m, n \in \mathbb{N}$, find the number of rectangles inside the $m \times n$ rectangular grid.

Solution. Each rectangle uniquely corresponds to a choice of two rows and two columns of the grid, which can be made in $\binom{m+1}{2}\binom{n+1}{2}$ ways. ■



Problem 45.

For $m, n \in \mathbb{N}$, find the number of non-decreasing functions $f : \{1, \ldots, m\} \to \{1, \ldots, n\}$.

Solution. It suffices to find the number of m-tuples $(a_1, \ldots, a_m)$ from the elements of $\{1, \ldots, n\}$ such that $a_1 \leq \cdots \leq a_m$ (why?). The set of all such m-tuples is in bijection with the set of all $0/1$ strings of length $m + n - 1$ with exactly m ones and $n - 1$ zeros, as follows: For each such m-tuple $(a_1, \ldots, a_m)$, let $k_i \geq 0$ be the number of i's among $a_1, \ldots, a_m$, where $i \in \{1, \ldots, n\}$. Then $k_1 + \cdots + k_n = m$. Now correspond the m-tuple to the following string with m ones and $n-1$ zeros:

$$\underbrace{1 \cdots 1}_{k_1}\ 0\ \underbrace{1 \cdots 1}_{k_2}\ 0\ \cdots\ 0\ \underbrace{1 \cdots 1}_{k_n}.$$

This is a bijection (why?), and so we need to count the number of $0/1$ strings with m ones and $n-1$ zeros. But that is easy: there are $m + n - 1$ spots in the string, and m spots should be chosen for the 1's (the rest are 0's), which can be done in $\binom{m+n-1}{m}$ ways. ■

Problem 46.

For $n \in \mathbb{N}$, find the number of ways to write n as a sum of positive integers. (The order matters: for instance, $1 + 1 + 2$ and $1 + 2 + 1$ are different sums amounting to 4.)

Solution. We count the number of all ordered tuples $(a_1, \ldots, a_k)$ in $\mathbb{N}$ such that $a_1 + \cdots + a_k = n$ (this automatically implies that $1 \leq k \leq n$). The set of all such ordered tuples is in bijection with the set of all $0/1$ strings with exactly n ones that start and end with a 1, and have no two consecutive 0's. For each such tuple $(a_1, \ldots, a_k)$, correspond it to the following string:

$$\underbrace{1 \cdots 1}_{a_1}\ 0\ \underbrace{1 \cdots 1}_{a_2}\ 0\ \cdots\ 0\ \underbrace{1 \cdots 1}_{a_k}.$$

This is a bijection (why?), and so the answer is equal to the number of $0/1$ strings with exactly n ones that start and end with a 1, and have no two consecutive 0's, which is 2^{n-1} (why?). ■

The second technique is *double-counting*: Start with a finite set X, and count the number of elements of X in two different ways. The results of the two enumerations must therefore be equal. This is extremely useful in proving (in)equalities that are algebraically painful (or nearly impossible) to prove. Here are a couple of problems demonstrating this:

Problem 47.

Prove that for every $n \in \mathbb{N}$,

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}.$$

Solution. Here, the algebraic proof is not that bad: Note that for all $n \geq k \geq 1$,

$$k\binom{n}{k} = k \times \frac{n!}{k!(n-k)!} = \frac{n!}{(k-1)!(n-k)!} = n \times \frac{(n-1)!}{(k-1)!(n-k)!} = n\binom{n-1}{k-1}.$$

Therefore,

$$\sum_{k=1}^{n} k\binom{n}{k} = \sum_{k=1}^{n} n\binom{n-1}{k-1} = n \times \underbrace{\sum_{l=0}^{n-1} \binom{n-1}{l}}_{2^{n-1}} = n2^{n-1}.$$

But here is an easier proof: Consider the set of all subsets of $\{1, \ldots, n\}$ with one element marked as special:

$$X = \{(S, a) : \ S \subseteq \{1, \ldots, n\}, \ a \in S\}.$$

We count $|X|$ in two ways:

- **Enumeration 1:** First, we choose $S \subseteq \{1, \ldots, n\}$. If S has k elements (where $1 \leq k \leq n$), then we can choose S in $\binom{n}{k}$ ways, and then choose $a \in S$ in k ways. It follows that the number of ways to construct the pair (S, a) with $|S| = k$ is $k\binom{n}{k}$. Since k could be any number in $\{1, \ldots, n\}$, we have
$$|X| = \sum_{k=1}^{n} k\binom{n}{k}.$$
- **Enumeration 2:** First, we choose a. This can be done in n ways (because $a \in \{1, \ldots, n\}$). Now, we choose S. Note that $a \in S$ already holds, so we only need to choose $S \setminus \{a\}$, which is simply a subset of $\{1, \ldots, n\} \setminus \{a\}$. This can be done in 2^{n-1} ways. Hence,
$$|X| = n2^{n-1}.$$

Equating the above counts yields a proof of the identity. ■

Problem 48.

Prove that for every $n \in \mathbb{N}$,

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

Solution. We use double-counting. (Try proving it algebraically!) Consider this situation: We want to select a committee with n members from n professors and n students. The committee must include at least one professor. We also need to choose a president and a vice-president for the committee from the professor members (but the two can be the same individual).

In how many ways can this be done? Here are two different ways to count:

- **Enumeration 1:** Let $1 \leq k \leq n$ be the number of professors on the committee. They can be selected in $\binom{n}{k}$ ways. Then we need $n-k$ students, who can be chosen in $\binom{n}{n-k}$ ways. Finally, we need to choose a president and a vice-president from the k chosen professors on the committee, which can be done in k^2 ways. Since $\binom{n}{k} = \binom{n}{n-k}$, it follows that the total number of ways the committee can be selected is

$$\sum_{k=1}^{n} k^2 \binom{n}{k}\binom{n}{n-k} = \sum_{k=1}^{n} k^2 \binom{n}{k}^2.$$

- **Enumeration 2:** First, we choose a president and a vice-president, and then we choose the other members. There are two cases: If the president and the vice-president are the same individual, that individual can be chosen in n ways from the n professors, and the rest of the committee can be selected in $\binom{2n-1}{n-1}$ ways. If the president and the vice-president are different individuals, then the president can be chosen in n ways, and the vice-president can be chosen in $n-1$ ways. The rest of the committee can then be chosen in $\binom{2n-2}{n-2}$ ways. Hence, the total number of ways to form the committee is

$$n\binom{2n-1}{n-1} + (n^2-n)\binom{2n-2}{n-2}.$$

Equating the above counts yields the identity. ■

Problem 49.

For $n \in \mathbb{N}$, let $\tau(n)$ be the number of divisors of n, and let $\overline{\tau}(n)$ be the average of $\tau(1), \ldots, \tau(n)$. (So, $\tau(7) = 2$, and $\overline{\tau}(7) = 16/7$.) Prove that for every $n \in \mathbb{N}$, we have $\overline{\tau}(n) \leq 1 + \frac{1}{2} + \cdots + \frac{1}{n}$.

Solution. Let $X = \{(a,b) : a, b \in \{1, \ldots, n\},\ a \mid b\}$. We count $|X|$ in two ways. For each $b \in \{1, \ldots, n\}$, the number of valid choices of a is $\tau(b)$; thus, $|X| = \tau(1) + \cdots + \tau(n)$. On the other hand, for each $a \in \{1, \ldots, n\}$, the number of valid choices of b is $\lfloor n/a \rfloor$; therefore, $|X| = \lceil n/1 \rceil + \cdots + \lceil n/n \rceil$. Equating the two counts yields:

$$\tau(1) + \cdots + \tau(n) = \left\lfloor \frac{n}{1} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor \leq \frac{n}{1} + \cdots + \frac{n}{n}$$

and so

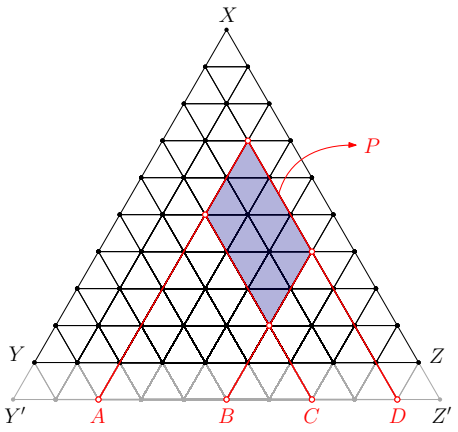
$$\overline{\tau}(n) = \frac{1}{n}(\tau(1) + \cdots + \tau(n)) \leq \frac{1}{n}\left(\frac{n}{1} + \cdots + \frac{n}{n}\right) = 1 + \frac{1}{2} + \cdots + \frac{1}{n}. \quad ■$$

Here are a few more problems illustrating these techniques:

Problem 50.

What is the number of parallelograms inside the $n \times n \times n$ triangular grid (with $n+1$ points on each side)?

Solution. The answer is $3\binom{n+2}{4}$. There are three types of parallelograms, depending on which two sides of the grid their sides are parallel to. Let us count the parallelograms with sides parallel to XY, XZ. Let P be such a parallelogram. Extend the grid along XY, XZ by one row; the side $Y'Z'$ now has $n+2$ points on it. Extend the sides of P, and let A, B, C, D be the intersection points of the extended sides of P with $Y'Z'$ (appearing from Y' to Z' in this order). These four points uniquely determine P (why?), and thus there is a bijection between the parallelograms with sides parallel to XY, XZ, and the 4-subsets of the points on $Y'Z'$, which can be chosen in $\binom{n+2}{4}$ ways. ■



Problem 51.

For an integer $n \geq 2$, an arithmetic progression in $\{1, \ldots, n\}$ is *maximal* if it has at least two terms and cannot be extended to a longer progression *with the same common difference*. Prove that the number of maximal arithmetic progressions in $\{1, \ldots, n\}$ is $\lfloor n^2/4 \rfloor$.

Solution. Each maximal progression in $\{1, \ldots, n\}$ is uniquely determined by the pair (a, d), where a is the first term and d is the common difference; by maximality, we should start at a and continue adding d until we fall out of $\{1, \ldots, n\}$. There are two constraints:

- The progression cannot be extended from below, which means $a \leq d$. (Why?)
- The progression has at least two terms, which means $a \leq n - d$. (Why?)

We deduce that there is a bijection between the set of maximal arithmetic progressions and

$$N = \{(a, d) : \ a, d \in \{1, \ldots, n\}, \ a \leq \min\{d, n-d\}\}.$$

It remains to count $|N|$, which we do in two cases:

(i) Assume that n is even; say, $n = 2t$ for $t \in \mathbb{N}$. If $d \in \{1, \ldots, t\}$, then $\min\{d, n-d\} = d$, and so the valid choices of a are $1, \ldots, d$. If $d \in \{t+1, \ldots, 2t\}$, then $\min\{d, n-d\} = n - d = 2t - d$, and so the valid choices of a are $1, \ldots, 2t - d$. Therefore,

$$|N| = \sum_{d=1}^{t} d \ + \ \sum_{d=t+1}^{2t} (2t - d) = \sum_{d=1}^{t} d \ + \ \sum_{d'=0}^{t-1} d' = \frac{t(t+1)}{2} + \frac{t(t-1)}{2} = t^2 = \left\lfloor \frac{n^2}{4} \right\rfloor.$$

(ii) Assume that n is odd; say, $n = 2t+1$ for $t \in \mathbb{N}$. If $d \in \{1, \ldots, t\}$, then $\min\{d, n-d\} = d$, and so the valid choices of a are $1, \ldots, d$. If $d \in \{t+1, \ldots, 2t+1\}$, then $\min\{d, n-d\} = n - d = 2t + 1 - d$, and so the valid choices of a are $1, \ldots, 2t + 1 - d$. Therefore,

$$|N| = \sum_{d=1}^{t} d \ + \ \sum_{d=t+1}^{2t+1} (2t + 1 - d) = \sum_{d=1}^{t} d \ + \ \sum_{d'=0}^{t} d' = t(t+1) = \left\lfloor \frac{n^2}{4} \right\rfloor. \quad ■$$

Problem 52.

Let $n \geq r \geq 1$ be integers. For each r-subset of $\{1, \ldots, n\}$, consider its smallest element. Prove that the average of all these smallest elements is equal to $\frac{n+1}{r+1}$.

Solution. Let $\mathcal{S}$ be the set of all r-subsets of $\{1, \ldots, n\}$. We would like to prove that

$$\frac{1}{\binom{n}{r}} \sum_{S \in \mathcal{S}} \min S = \frac{n+1}{r+1}.$$

For each $S \in \mathcal{S}$, we have $\min S \in \{1, \ldots, n-r+1\}$ (because there should be room for choosing the other $r-1$ elements of S). Also, for each $k \in \{1, \ldots, n-r+1\}$, there are exactly $\binom{n-k}{r-1}$ sets $S \in \mathcal{S}$ with $\min S = k$. Thus,

$$\sum_{S \in \mathcal{S}} \min S = \sum_{k=1}^{n-r+1} k \binom{n-k}{r-1}.$$

On the other hand,

$$\binom{n}{r} \times \frac{n+1}{r+1} = \frac{n!}{r!(n-r)!} \times \frac{n+1}{r+1} = \frac{(n+1)!}{(r+1)!((n+1)-(r+1))!} = \binom{n+1}{r+1}.$$

So, it suffices to show that

$$\sum_{k=1}^{n-r+1} k \binom{n-k}{r-1} = \binom{n+1}{r+1}.$$

To that end, let $\mathcal{S}^+$ be the set of all $(r+1)$-subsets of $\{0, 1, \ldots, n\}$. Clearly,

$$|\mathcal{S}^+| = \binom{n+1}{r+1}.$$

We now count $|\mathcal{S}^+|$ in a different way. Since $r+1 \geq 2$, each set $S \in \mathcal{S}^+$ has a second smallest element, and that element lies in $\{1, \ldots, n-r+1\}$ (since we need room for choosing the smallest element before it, and the other $r-1$ elements after it). For each $k \in \{1, \ldots, n-r+1\}$, let $\mathcal{S}_k$ be the set of all $S \in \mathcal{S}^+$ whose second smallest element is k. Then $\mathcal{S}_1, \ldots, \mathcal{S}_{n-r+1}$ partition $\mathcal{S}^+$, and so $|\mathcal{S}^+| = |\mathcal{S}_1| + \cdots + |\mathcal{S}_{n-r+1}|$. Moreover, we may count $|\mathcal{S}_k|$ as follows: For each $S \in \mathcal{S}_k$, the smallest element of S should be chosen from $\{0, \ldots, k-1\}$, which can be done in k ways. The second smallest element is k, and the remaining $r-1$ elements must be chosen from $\{k+1, \ldots, n\}$, which can be done in $\binom{n-k}{r-1}$ ways. Hence,

$$|\mathcal{S}_k| = k \binom{n-k}{r-1} \;\Rightarrow\; |\mathcal{S}^+| = \sum_{k=1}^{n-r+1} |\mathcal{S}_k| = \sum_{k=1}^{n-r+1} k \binom{n-k}{r-1}. \quad \blacksquare$$

Note. This is Problem 2 from IMO 1981.

Problem 53.

Prove that for every $n \in \mathbb{N}$

$$\sum_{k=0}^{n} 2^{-k} \binom{n+k}{k} = 2^n.$$

Solution. Instead, we will show that:

$$\sum_{k=0}^{n} 2^{n+2-k}\binom{n+k}{k} = 2^{2n+2}.$$

Let X be the set of all 0/1 strings of length $2n+2$. Clearly,

$$|X| = 2^{2n+2}.$$

We now count $|X|$ in a different way. Note that for every string $s \in X$, by the pigeonhole principle, there are at least $n+1$ identical characters among the first $2n+1$ characters of s. Now, for each $s \in X$, let $f(s)$ be the minimum i such that among the first i characters of s, there are $n+1$ identical characters (0 or 1; it does not matter). For instance, when $n = 2$, we have

$$f(\underline{1011}01) = 4 \quad \text{and} \quad f(\underline{0011}01) = 5.$$

It follows that f is well-defined, and $n+1 \le f(s) \le 2n+1$ for every $s \in X$. Therefore, we can group the strings in X according to the value of f: For each $k \in \{0, 1, \ldots, n\}$, let

$$X_k = \{s \in X : \ f(s) = n+k+1\}.$$

Then $X_0, X_1, \ldots, X_n$ partition X, and so $|X| = |X_0| + |X_1| + \cdots + |X_n|$. Moreover, we may count $|X_k|$ as follows: Let $s = c_1 c_2 \cdots c_{2n+2} \in X_k$. Since $f(s) = n+k+1$, among $c_1, c_2, \ldots, c_{n+k+1}$, there are $n+1$ identical characters; say, they are equal to $c \in \{0,1\}$. There are two possibilities for c. By the minimality of $f(s) = n+k+1$, we have $c_{n+k+1} = c$, and among $c_1, \ldots, c_{n+k}$, there are exactly n characters equal to c. So, the first $n+k$ characters can be chosen in $\binom{n+k}{n}$ ways. The remaining $n+1-k$ characters of s (coming after c_{n+k+1}) each have two possibilities, giving rise to a count of 2^{n+1-k}. Hence,

$$|X_k| = 2 \times \binom{n+k}{n} \times 2^{n+1-k} = 2^{n+2-k}\binom{n+k}{k} \ \Rightarrow \ |X| = \sum_{k=0}^{n} |X_k| = \sum_{k=0}^{n} 2^{n+2-k}\binom{n+k}{k}. \quad \blacksquare$$

Sometimes, counting arguments, especially double-counting, work more efficiently in conjunction with a graph-theoretic interpretation. Recall, for instance, that the hand-shaking lemma is nothing but double-counting the set

$$\{(v, e) \in V(G) \times E(G) : v \text{ is incident with } e\}$$

in a graph G. Below are some examples geared toward this approach. But let us first awaken our graph theory mode with quick warm-up problem:

Problem 54.

In a country with serious traffic issues, the government plans to make all roads one-way. To avoid congestion, the goal is that at each city, the numbers of incoming and outgoing roads differ by at most 1. Show that this is possible.

Solution. The graph-theoretic statement says that, "*For every graph G, the edges of G can be oriented such that the in-degree and out-degree of each vertex in the resulting digraph differ by at most* 1." We prove this by induction on $|V(G)| + |E(G)|$.

If G has no edge, then we are done. So we may assume that G has at least one edge. Assume that G has a cycle. Then we can orient the edges of the cycle in, say, the clockwise direction, remove those edges, and win by the inductive hypothesis. Therefore, we may assume that G has no cycle and so (each component of) G is a tree. Since G has at least one edge, it follows that G has a vertex of degree exactly 1. Let x be such a vertex in G, and let y be the unique neighbor of x. Remove x (and the edge xy) from G. By the inductive hypothesis, the resulting graph G' admits a desired orientation. Let d_{in} and d_{out} be the in-degree and out-degree of y in the orientation of G'. It follows that either $d_{in} = d_{out}$, or $d_{in} - d_{out} = 1$, or $d_{out} - d_{in} = 1$. Now put back x, joining it to y via the edge xy. If either $d_{in} = d_{out}$ or $d_{in} - d_{out} = 1$, orient the edge xy from y to x, and if $d_{out} - d_{in} = 1$, orient the edge xy from x to y. This yields a winning orientation for G. ■

The next three problems focus on counting:

Problem 55.

A group of students and a group of professors have some 1-on-1 meetings, each between a student and a professor.

(a) Assume that all individuals have had the same number of meetings. Prove that the number of students equals the number of professors.

(b) Assume that each individual goes to at least one meeting, and every two individuals who meet have the same number of meetings. Prove that the number of students equals the number of professors.

Solution. For (a), the graph-theoretic statement says that, "*If G is a bipartite graph with bipartition (A, B) and all degrees equal, then $|A| = |B|$.*" Suppose that for every $v \in V(G)$, we have $d_G(v) = d \geq 0$. We double-count $|E(G)|$: Each edge has exactly one end in A and one end in B; thus,

$$|E(G)| = \sum_{v \in A} d_G(v) = \sum_{v \in B} d_G(v) \ \rightarrow \ d|A| = d|B| \ \Rightarrow \ |A| = |B|.$$

Part (b) is subtly different from part (a) – the graph-theoretic statement says that, "*If G is a bipartite graph with bipartition (A, B), where no vertex has degree zero, and every two adjacent vertices have equal degrees, then $|A| = |B|$.*" The key is to look at the *connected components* of G: Since G has no degree-zero vertex, each component C of G has at least one edge, and since C is connected, all vertices in $V(C)$ have equal degrees (why?). Therefore, by (a), we have $|A \cap V(C)| = |B \cap V(C)|$ for each component C of G, and therefore $|A| = |B|$. ■

Problem 56.

Let $n \geq 4$. Consider a convex n-gon with all diagonals drawn such that no three diagonals pass through the same point. What is the total number of segments created on the diagonals?

Solution. First, we need to count the number of intersection points: Note that each intersection point corresponds uniquely to a choice of four vertices of the n-gon. Thus, the number of intersection points is $\binom{n}{4}$. Now, consider a graph whose vertices are the vertices of the n-gon along with the intersection points, and whose edges are the segments created on the diagonals. In this graph, the degree of each of the n vertices of the n-gon is $n - 3$, and the degree of each intersection point is 4. Hence, by the hand-shaking lemma, the total number of segments is equal to $2\binom{n}{4} + \frac{n(n-3)}{2}$. ■

Problem 57.

We wish to divide $m \in \mathbb{N}$ identical snickers bars equally among $n \in \mathbb{N}$ students. Prove that:

(a) This can be done by dividing the bars into a total of $m + n - \gcd(m, n)$ pieces.

(b) It is impossible to do so by dividing the bars into fewer than $m + n - \gcd(m, n)$ pieces.

Solution. Throughout, let

$$d = \gcd(m, n), \quad l = \operatorname{lcm}(m, n), \quad m' = \frac{m}{d}, \quad n' = \frac{n}{d}.$$

Then $\gcd(m', n') = 1$ and $l = \frac{mn}{d} = mn' = nm' = m'n'd$. By rescaling our units of measurement, we may assume that each bar has length n'.

For (a), no graph theory is needed. Glue all the bars together along a circle to obtain one giant snickers ring of perimeter $mn' = l$. We can cut this into n equal pieces, each of length $l/n = m'$ for a student. Call these cuts of *type 1*. Also, we need to cut the ring back into the original m bars, each of length n'. Call these cuts of *type 2*. There is a total of $m+n$ cuts; however, some type-1 cuts overlap with type-2 cuts, hence being counted twice. Note that the length of each segment between two consecutive overlapping cuts is the least common multiple of the lengths of a type-1 segment and a type-2 segment; that is, $\operatorname{lcm}(m', n')$. But $\gcd(m', n') = 1$, and so $\operatorname{lcm}(m', n') = m'n'$. Therefore, the number of overlapping cuts is $l/m'n' = d$, and so the actual number of cuts is $m + n - d$.

We do need some graph theory for (b). Suppose that the fair division has been done using p pieces. Our goal is to show that $p \geq m + n - d$. Make a bipartite graph G with parts M and N, such that M is the set of all m bars, N is the set of all n students, and there is an edge between a bar and a student if and only if the student has received a piece from the bar. Observe that $p = |E(G)|$. So, we need to prove that $|E(G)| \geq m + n - d$.
Let k be the number of components of G; say, $G_1, \ldots, G_k$. For each $i \in \{1, \ldots, k\}$, since G_i is connected, it has a spanning tree, and so $|E(G_i)| \geq |V(G_i)| - 1$. It follows that

$$|E(G)| = \sum_{i=1}^{k} |E(G_i)| \geq \sum_{i=1}^{k} (|V(G_i)| - 1) = |V(G)| - k = m + n - k.$$

Now, it suffices to show that $k \leq d$. For each $i \in \{1, \ldots, k\}$, let $M_i = V(G_i) \cap M$ and let $N_i = V(G_i) \cap N$. Then G_i is bipartite with bipartition (M_i, N_i). Since $|M_1| + \cdots + |M_k| = |M| = m$, it follows that there exists $j \in \{1, \ldots, k\}$ such that $|M_j| \leq m/k$. Let us double-count the total length of bars in M_j. On one hand, since each bar has length n', the total length of the bars in M_j is $n'|M_j|$. On the other hand, the bars in M_j are exactly those divided among the students in N_j, and each student receives the same total length m'. Therefore, the total length of the bars in M_j is also equal to $m' \cdot |N_j|$. We deduce that

$$n'|M_j| = m'|N_j|$$

and thus $m' \mid n'|M_j|$. Since $\gcd(m', n') = 1$, it follows that $m' \mid |M_j|$, and so $m' \leq |M_j|$. But recall that $|M_j| \leq m/k$. Hence

$$m' \leq \frac{m}{k} \;\Rightarrow\; k \leq \frac{m}{m'} = d. \quad \blacksquare$$

9 Number theory

We start with four problems that, although interesting, only concern (very) basic number theory: divisibility, primes and gcd, congruences, etc.

Problem 58.

Find all $x \in \mathbb{N}$ such that x^2 is the product of four positive consecutive integers.

Solution. Suppose that $x, y \in \mathbb{N}$ such that $x^2 = y(y+1)(y+2)(y+3)$. Let $z = y(y+3)$. Then z is even; say, $z = 2t$ for some $t \in \mathbb{N}$. Moreover,

$$x^2 = y(y+3)(y^2+3y+2) = z(z+2) = 2t(2t+2) = 4t(t+1).$$

Since x^2 and 4 are both perfect squares, it follows that $t(t+1)$ is a perfect square. But then since $\gcd(t, t+1) = 1$, it follows that both t and $t+1$ must be perfect squares, which is impossible. Hence, no such $x \in \mathbb{N}$ exists. ■

Problem 59.

Find all $x \in \mathbb{N}$ such that $x^4 + 4^x$ is prime.

Solution. Note that for all $x, y \in \mathbb{N}$, we have

$$x^4 + 4y^4 = (x^2+2y^2)^2 - (2xy)^2 = (x^2+2y^2-2xy)(x^2+2y^2+2xy).$$

This is called the *Sophie Germain's identity*.
Now, assume that $x \in \mathbb{N}$ with $x > 1$. If x is even, then $x^4 + 4^x \geq 32$ is even, and not a prime. If x is odd, then $x = 2k+1$ for some $k \in \mathbb{N}$. Let $y = 2^k$. Then, $4^x = 4 \cdot 4^{2k} = 4 \cdot 2^{4k} = 4(2^k)^4 = 4y^4$, and by Sophie Germain's identity, we have:

$$x^4 + 4^x = x^4 + 4y^4 = (x^2+2y^2-2xy)(x^2+2y^2+2xy).$$

which is not a prime. So $x = 1$ is the only value for which $x^4 + 4^x = 5$ is a prime. ■

Problem 60.

Find all coprime $x, y \in \mathbb{N}$ such that $y/x = x.y$. (For example, we have $5/2 = 2.5$.)

Solution. Assume that y has $k \in \mathbb{N}$ digits. Then

$$\frac{y}{x} = x.y = x + \frac{y}{10^k} \;\Rightarrow\; 10^k y = 10^k x^2 + xy.$$

Since $xy = 10^k(y - x^2)$, it follows that

$$10^k \mid xy.$$

Since $10^k y = x(10^k x + y)$, it follows that $x \mid 10^k y$, which combined with $\gcd(x, y) = 1$ implies that $x \mid 10^k$. Also, since $10^k x^2 = y(10^k - x)$, it follows that $y \mid 10^k x^2$. Therefore, since $\gcd(x^2, y) = \gcd(x, y) = 1$, we deduce that $y \mid 10^k$. Now, from $x \mid 10^k$, $y \mid 10^k$, and $\gcd(x, y) = 1$, it follows that:

$$xy \mid 10^k.$$

We deduce that $xy = 10^k$, which combined with $\gcd(x, y) = 1$ yields

$$(x, y) \in \{(1, 10^k), (10^k, 1), (2^k, 5^k), (5^k, 2^k)\}.$$

Moreover, note that $y \geq y/x = x.y > x$. So there are two cases: $(x, y) = (1, 10^k)$ or $(x, y) = (2^k, 5^k)$. The former is impossible because y has k digits (not $k + 1$). For $(x, y) = (2^k, 5^k)$, if $k \geq 2$, then

$$y = 5^k = 5^{k-1}(4+1) > 4^{k-1}(4+1) = 4^k + 4^{k-1} = 4^k + 2^{2k-2} \geq 4^k + 2^k = 2^k(2^k+1) = x(x+1) > x(x.y)$$

and so $y/x > x.y$. Hence $k = 1$, and $(x, y) = (2, 5)$ is the only solution. ■

Problem 61.

(a) Prove that $\underbrace{333\cdots3}_{330 \text{ digits}}$ is divisible by 331.

(b) We say that a sequence $\{x_n\}_{n\geq 1}$ of positive integers is *digital* if, for every $n > 1$, x_n is by attaching a digit other than 9 to the right of x_{n-1}. Prove that every digital sequence contains infinitely many composite numbers.

Solution. For (a), note that

$$\underbrace{333\cdots3}_{330 \text{ digits}} = \frac{10^{330} - 1}{3}.$$

Also, 331 is a prime and $\gcd(10, 331) = 1$. Thus, by Fermat's little theorem, $10^{330} \equiv 1 \pmod{331}$, and so $331 \mid 10^{330} - 1$. Since $\gcd(3, 331) = 1$, it follows that

$$331 \,\Big|\, \frac{10^{330} - 1}{3}.$$

In fact, we proved more generally that $\underbrace{333\cdots3}_{p-1 \text{ digits}}$ is divisible by p for every prime $p \neq 2, 5$.

For (b), suppose for a contradiction that there is a digital sequence $\{x_n\}_{n\geq 1}$ for which there exists $N \in \mathbb{N}$ such that x_n is prime for every $n > N$. Since $\{x_n\}_{n\geq 1}$ is digital, for every $n > 1$, there exist $y_n \in \{0, 1, \ldots, 8\}$ such that $x_n = 10x_{n-1} + y_n$. It follows that for every $n > 1$, we have $x_n \equiv x_{n-1} + y_n \pmod 3$, and so for all $n_2 > n_1 \geq 1$, we have

$$x_{n_2} \equiv x_{n_1} + \sum_{m=n_1+1}^{n_2} y_m \pmod 3.$$

For every $n > N \geq 1$, since x_n is a prime with at least $n \geq 2$ digits, it follows that x_n is not divisible by any of $2, 3$, and 5. In particular,

$$y_n \in \{1, 3, 7\}.$$

We claim further that there are at most two values of $n > N$ for which $y_n \in \{1, 7\}$. Suppose for a contradiction that there exist $n_3 > n_2 > n_1 > N$ such that $y_{n_1}, y_{n_2}, y_{n_3} \in \{1, 7\}$ and $y_m = 3$ for every m with $n_1 < m < n_2$ or $n_2 < m < n_3$. Note that

$$x_{n_3} \equiv x_{n_2} + \sum_{m=n_2+1}^{n_3} y_m \equiv x_{n_2} + y_{n_3} \pmod 3$$

and

$$x_{n_2} \equiv x_{n_1} + \sum_{m=n_1+1}^{n_2} y_m \equiv x_{n_1} + y_{n_2} \pmod 3.$$

Also, $y_{n_1}, y_{n_2}, y_{n_3} \equiv 1 \pmod 3$. Since x_{n_1} is prime and not divisible by 3, it follows that $x_{n_1} \equiv 1$ or 2. If $x_{n_1} \equiv 1 \pmod 3$, then

$$x_{n_3} \equiv x_{n_2} + y_{n_3} \equiv x_{n_1} + y_{n_2} + y_{n_3} \equiv 1 + 1 + 1 \equiv 0 \pmod 3;$$

which is a contradiction because $3 \nmid x_{n_3}$. Likewise, if $x_{n_1} \equiv 2 \pmod 3$, then

$$x_{n_2} \equiv x_{n_1} + y_{n_2} \equiv 2 + 1 \equiv 0 \pmod 3;$$

again a contradiction because $3 \nmid x_{n_2}$. This proves the claim.

From the claim, we deduce that there exists $M > N$ such that for every $n > M$, we have $y_n = 3$. Let $p = x_M$ and let $n = M + p - 1$. Then $n > M$, and so

$$x_n = x_{M+p-1} = 10^{p-1}x_M + \underbrace{333\cdots3}_{p-1 \text{ digits}} = 10^{p-1}p + \underbrace{333\cdots3}_{p-1 \text{ digits}}.$$

Note that $p \mid 10^{p-1}p$. Recall also that p is a prime and $p \neq 2, 5$, and so by (the extended version of) part (a), we have

$$p \,\Big|\, \underbrace{333\cdots3}_{p-1 \text{ digits}}.$$

Now $p \mid x_n$, whereas $x_n > p$ because $p = x_M$ and $n > M$, contrary to x_n being prime. ■

Note. If we also allow the digit 9 to be appended to the right, the same problem is open!

The next four problems are on *functional equations*. The first (in two parts) is fairly easy:

Problem 62.

(a) Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $x + f(y) \,\big|\, f(x) + y$ for all $x, y \in \mathbb{N}$.

(b) Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $x^2 + yf(y) \,\big|\, xf(x) + y^2$ for all $x, y \in \mathbb{N}$.

Solution. For (a), we can swap x and y: For all $x, y \in \mathbb{N}$, we have $x + f(y) \mid f(x) + y$ and also $y + f(x) \mid f(y) + x$; therefore, $x + f(y) = y + f(x)$. Applying this to $y = 1$, it follows that for every $x \in \mathbb{N}$, we have $f(x) = x + f(1) - 1$. So, f satisfies the condition if and only if $f(x) = x + b$ for some fixed integer $b \geq 0$.
For (b), again, we can swap x and y: For all $x, y \in \mathbb{N}$, we have $x^2 + yf(y) \mid xf(x) + y^2$ and also $y^2 + xf(x) \mid yf(y) + x^2$; therefore, $x^2 + yf(y) = y^2 + xf(x)$. Applying this to $y = 1$, it follows that for every $x \in \mathbb{N}$, we have $f(x) = x + \frac{f(1)-1}{x}$. Since $f(x)$ is an integer for every $x \in \mathbb{N}$, it follows that $f(1) - 1$ is divisible by every $x \in \mathbb{N}$. Consequently, $f(1) - 1 = 0$, and so $f(x) = x$. ■

The third one is a "mix" of the previous two, and somewhat harder.

Problem 63.

Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $x^2 + f(y) \mid xf(x) + y$ for all $x, y \in \mathbb{N}$.

Solution. Let $a = f(1)$. Applying $x^2 + f(y) \mid xf(x) + y$ with $x = 1$, it follows that for every $y \in \mathbb{N}$, we have $1 + f(y) \mid a + y$, and so

$$f(y) \leq y + a - 1 \quad \text{for all } y \in \mathbb{N}.$$

In particular, for all $x \geq a$, we have $xf(x) + 1 \leq x(x + a - 1) + 1 < x(x + x) + 2a = 2(x^2 + a)$. On the other hand, applying $x^2 + f(y) \mid xf(x) + y$ with $y = 1$, it follows that for every $x \in \mathbb{N}$, we have

$$x^2 + a \mid xf(x) + 1 \quad \text{for all } x \in \mathbb{N}.$$

Consequently, for every $x \geq a$, since $xf(x) + 1 < 2(x^2 + a)$, it follows that $xf(x) + 1 = x^2 + a$. We deduce that $f(x) = x + \frac{a-1}{x}$ for all $x \geq a$. Similar to part (b) from the previous problem, this implies that $a - 1 = 0$, and so $a = 1$. Now, on one hand, for every $y \in \mathbb{N}$, we have

$$f(y) \leq y + a - 1 = y$$

and on the other hand, for every $x \in \mathbb{N}$, we have

$$x^2 + a \mid xf(x) + 1 \;\Rightarrow\; xf(x) + 1 \geq x^2 + a = x^2 + 1 \;\Rightarrow\; f(x) \geq x.$$

Hence, $f(x) = x$. ■

The next two are substantially harder to solve (although the equations look simpler).

Problem 64.

Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(x) + f(y) \mid x + y$ for all $x, y \in \mathbb{N}$.

Solution. Applying $f(x)+f(y) \mid x+y$ with $x = y$, it follows that for every $x \in \mathbb{N}$, we have $f(x) \mid x$, and so $f(x) \leq x$. In particular, $f(1) = 1$. Now, assume that $f(x) \neq x$ for some integer $x \geq 2$. Let $t \geq 2$ be minimum such that $f(t) \neq t$. Let

$$f(t) = d.$$

Since $d \mid t$, it follows that there is an integer $k \geq 2$ such that

$$t = kd.$$

Since $(k - 1)d < kd = t$, by the minimality of t, we have

$$f((k - 1)d) = (k - 1)d.$$

Applying $f(x) + f(y) \mid x + y$ with $x = (k - 1)d$ and $y = t$, it follows that

$$f((k-1)d) + f(t) \mid (k-1)d + t \;\Rightarrow\; (k-1)d + d \mid (k-1)d + kd \;\Rightarrow\; k \mid 2k - 1 \;\Rightarrow\; k \mid 1;$$

a contradiction to $k \geq 2$. Hence $f(x) = x$. ■

Problem 65.

Let $f : \mathbb{N} \to \mathbb{N}$ be an increasing function such that for all $x, y \in \mathbb{N}$, there exists $z \in \mathbb{N}$ that satisfies $f(x) + f(y) = f(z)$. Prove that there exist integers $a > 0$ and $b, N \geq 0$ such that for every integer $x > N$, we have $f(x) = a(x + b)$.

Solution. For each $i \in \mathbb{N}$, let $s_i = f(i)$. Then $s_1 < s_2 < s_3 < \cdots$. Let $S = \{s_1, s_2, s_3, \ldots\}$. Then, S is closed under addition; that is, if $s, s' \in S$, we have $s + s' \in S$. Consider the following statement:

$$(*)\ \textit{There exist } a, t \in \mathbb{N} \textit{ such that } S \setminus \{1, \ldots, at\} = \{ak : k \in \mathbb{N},\ k > t\}.$$

We claim that $(*)$ implies that there exist integers $a > 0$ and $b, N \geq 0$ such that for every integer $x > N$, we have $f(x) = a(x + b)$. Assume that $(*)$ holds. Let $S \cap \{1, \ldots, at\} = \{s_1, \ldots, s_N\}$ where $N \geq 0$ is an integer (and $N = 0$ if and only if $S \cap \{1, \ldots, at\} = \varnothing$). Let $b = t - N$. Since $S \setminus \{1, \ldots, at\} = \{s_{N+1}, s_{N+2}, \ldots\} = \{a(t+1), a(t+2), \ldots\}$ with $s_{N+1} < s_{N+2} < \cdots$, it follows that $f(x) = a(x + t - N) = a(x + b)$ for every integer $x > N$. Moreover, since S is closed under addition and every element of $S \setminus \{1, \ldots, at\}$ is divisible by a, it follows that every element of $S \cap \{1, \ldots, at\}$ is also divisible by a, and so $N = |S \cap \{1, \ldots, at\}| \leq t$. Therefore, $b = t - N \geq 0$, as desired.

It remains to prove $(*)$. Let

$$a = \min\{s_{i+1} - s_i : i \in \mathbb{N}\}.$$

Then $a > 0$ and there exists $s \in S$ such that $a + s \in S$. We need the following auxiliary statement:

(1) *For all $k \in \mathbb{N}$ with $k \geq s^2$, we have $ak \in S$.*

Proof of (1). Write $k = sq + r$ for integers $q, r \geq 0$ with $r < s$. Then, $s^2 < k = sq + r < s(q + 1)$, and so $q \geq s$, which in turn implies that $aq - r \geq q - r \geq s - r > 0$. But now since $s, a + s \in S$, it follows that

$$ak = a(sq + r) = (aq - r)(s) + (r)(a + s) \in S.$$

This proves (1). □

Now, we prove that $(*)$ holds for the above choice of a, and $t = s^2$. Note that by (1), for every integer $k > t = s^2$, we have $ak \in S$; therefore, $\{ak : k \in \mathbb{N},\ k > t\} \subseteq S \setminus \{1, \ldots, at\}$. For the reverse inclusion, suppose for a contradiction that there exists $x \in S$ with $x > at$ such that $a \nmid x$. Then $x = aq' + r'$ for integers $q' \geq 0$ and $0 < r' < a$. In particular, $as^2 = at < x = aq' + r' < a(q' + 1)$, and so $q' \geq s^2$. Consequently, by (1), we have $aq' \in S$. But recall that $x \in S$, and now $r' = x - aq'$ is the difference between two elements of S, whereas $0 < r' < a$, contrary to the choice of a. ■

We all know Euclid's theorem: there are infinitely many prime numbers. For composite numbers, there is even more to be said: There are arbitrarily long intervals of consecutive positive integers that are all composite numbers. To see this, let $t \in \mathbb{N}$, and for each $k \in \{1, \ldots, t\}$, let

$$x_k = (t + 1)! + k + 1.$$

Then $x_1, \ldots, x_t$ are consecutive positive integers, and for each $k \in \{1, \ldots, t\}$, we have $k + 1 \mid x_k$. In fact, even more can be said about composite numbers:

Problem 66.

Prove that in every infinite arithmetic progression of (distinct) positive integers, there are arbitrarily long intervals of consecutive terms that are all composite numbers.

Solution. Let $a, b \in \mathbb{N}$ be the first term and the common difference. Let $t \in \mathbb{N}$. The goal is to prove that the progression $\{a + bk : k \geq 0\}$ has t consecutive terms that are all composite.
Choose t pairwise distinct primes $p_1, \ldots, p_t$, none of which divides b. (This is possible because there are infinitely many primes!) It suffices to find $x \in \mathbb{N}$ such that for every $i \in \{1, \ldots, t\}$, we have $a + b(x + i) \equiv 0 \pmod{p_i}$. For each $i \in \{1, \ldots, t\}$, since $\gcd(b, p_i) = 1$, there exists $c_i \in \mathbb{N}$ such that $bc_i \equiv 1 \pmod{p_i}$. Therefore,

$$a + b(x + i) \equiv 0 \pmod{p_i} \iff x + i \equiv -ac_i \pmod{p_i} \iff x \equiv -ac_i - i \pmod{p_i}.$$

But now, since $p_1, \ldots, p_t$ are pairwise distinct primes, the Chinese remainder theorem guarantees that there exists $x \in \mathbb{N}$ such that $x \equiv -ac_i - i \pmod{p_i}$ for all $i \in \{1, \ldots, t\}$. ■

What about prime numbers in arithmetic progressions? Can we extend Euclid's theorem? Not always – For instance, $\{3k + 6 : k \geq 0\}$ contains no primes at all. More generally, if we want the progression $\{a + bk : k \geq 0\}$ to contain even one prime, we had better ask for $\gcd(a, b) = 1$. Also, we may assume that $a \in \{1, \ldots, b - 1\}$ (why?). So, the question is:

For $a, b \in \mathbb{N}$ with $a \in \{1, \ldots, b - 1\}$, does $\{a + bk : k \geq 0\}$ contain infinitely many primes?

For $b = 1, 2$, this is Euclid's theorem. Here is (a twisted version of) the proof for $b = 2$ and $a = 1$:

Step 1. *Suppose that there are just $t \in \mathbb{N}$ primes $p_1, \ldots, p_t$ that are 1 mod 2. Let $m = 2p_1 \cdots p_t$.*

For Step 2, we consider the number $m + 1$. Since $m + 1 > 1$, it has a prime divisor q. Note that q is a prime divisor of $m + 1$ if and only if $q \mid m^2 - 1$ and $q \nmid m - 1$ (why?). Also, observe that $q \nmid m$, because otherwise $q \mid m^2$, which, combined with $q \mid m^2 - 1$, yields $q \mid 1$. Thus, we may write:

Step 2. *Find a prime q such that $q \mid m^2 - 1$, and $q \nmid m - 1$. In particular, $q \nmid m$.*

Then, since $q \nmid m$, it follows in particular that $q \neq 2$, and so q is odd. In other words,

Step 3. *Deduce, from $q \nmid m$, that $2 \mid q - 1$.*

But now $q \in \{p_1, \ldots, p_t\}$, which is a contradiction to $q \nmid m$.

Could the same recipe work for larger values of b and $a = 1$? Let's try the case $b = 3$:

Problem 67.

There are infinitely many primes that are 1 mod 3.

Solution. For Step 1, we suppose for a contradiction that

There are only $t \in \mathbb{N}$ primes $p_1, \ldots, p_t$ that are 1 mod 3. Let $m = 3p_1p_2 \cdots p_t$.

For Step 2, we need to prove that

There is a prime q such that $q \mid m^3 - 1$ and $q \nmid m^r - 1$ for all $1 \leq r < 3$. In particular, $q \nmid m$.

To see this, let q be a prime divisor of $m^2+m+1>1$. Then

$$q \mid m^2+m+1 \;\Rightarrow\; q \mid (m^2+m+1)(m-1) = m^3-1.$$

Also, note that $q \nmid m$, because otherwise $q \mid m^3$, which, combined with $q \mid m^3-1$ implies that $q \mid 1$, which is impossible. It remains to show that $q \nmid m^2-1$ and $q \nmid m-1$. We only need to prove the former (why?). Suppose that $q \mid m^2-1$. Since $q \mid m^2+m+1$, it follows that $q \mid \gcd(m^2+m+1, m^2-1)$. On the other hand,

$$\begin{aligned}
&\gcd(m^2+m+1, m^2-1)\\
=&\gcd(m^2+m+1-(m^2-1), m^2-1)\\
=&\gcd(m+2, m^2-1)\\
=&\gcd(m+2, m^2-1-m(m+2))\\
=&\gcd(m+2, -1-2m)\\
=&\gcd(m+2, -1-2m+2(m+2))\\
=&\gcd(m+2, 3)\\
=&\gcd(m+2-3(p_1p_2\cdots p_t), 3)\\
=&\gcd(2,3)=1.
\end{aligned}$$

But now $q \mid 1$, a contradiction. This completes Step 2.

For Step 3, we need to prove that

$$3 \mid q-1.$$

Suppose not. Then $q-1 = 3s+r$ for some integers $s \geq 0$ and $r \in \{1,2\}$. It follows that $m^{q-1} = (m^3)^s \times m^r$. Recall also from Step 2 that $m^3 \equiv 1 \pmod q$. Thus, we have $m^{q-1} \equiv m^r \pmod q$. Since $q \nmid m$, by Fermat's little theorem, we have $m^{q-1} \equiv 1 \pmod q$, and so $m^r \equiv 1 \pmod q$. But now $q \mid m^r-1$ for some $r \in \{1,2\}$, contrary to what we proved in Step 2. This completes Step 3.

Now, as proved in Step 3, q is a prime that is 1 mod 3. So, $q \in \{p_1, \ldots, p_t\}$. But then $q \nmid m$, a contradiction. ■

What about larger values of b? Step 2 becomes rather tricky, so we handle it separately.

Problem 68.

Let $b, m \geq 2$ be integers such that $b \mid m$. Then there exists $M \in \mathbb{N}$ with $m \mid M$ for which there is a prime q such that $q \mid M^b-1$ and $q \nmid M^r-1$ for all $1 \leq r < b$. In particular, $q \nmid M$.

Solution. Recall that for every $n \in \mathbb{N}$, the polynomial x^n-1 has n complex roots $\zeta_n, \zeta_n^2, \ldots, \zeta_n^n$, where $\zeta_n = e^{2\pi i/n}$; in particular, $\zeta_n^n = 1$.
For every $n \in \mathbb{N}$, define

$$\Phi_n(x) = \prod_{\substack{1 \leq j \leq n \\ \gcd(j,n)=1}} (x-\zeta_n^j).$$

Then $\Phi_n(x)$ is a polynomial in $\mathbb{C}[x]$, called the n^{th} *cyclotomic polynomial*.
In fact, $\Phi_n(x)$ always has integer coefficients, but to see that, we first need to prove a well-known recursion:

(1) *For every* $n \in \mathbb{N}$, *we have* $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proof of (1). Observe that

$$k \to \left(\frac{k}{\gcd(k,n)}, \frac{n}{\gcd(k,n)} \right)$$

is a bijection from $\{1, \ldots, n\}$ to $\{(j,d) : \ d \mid n, \ 1 \le j \le d, \ \gcd(j,d) = 1\}$. Thus,

$$x^n - 1 = \prod_{k=1}^{n} \left(x - e^{2\pi i \left(\frac{k}{n}\right)} \right) = \prod_{k=1}^{n} \left(x - e^{2\pi i \left(\frac{k/\gcd(k,n)}{n/\gcd(k,n)}\right)} \right) = \prod_{d|n} \prod_{\substack{1 \le j \le d \\ \gcd(j,d)=1}} \left(x - e^{2\pi i \left(\frac{j}{d}\right)} \right) = \prod_{d|n} \Phi_d(x).$$

This proves (1). □

(2) *For every* $n \in \mathbb{N}$, $\Phi_n(x)$ *is monic and* $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof of (2). We proceed by induction on n. Note that $\Phi_1(x) = x - 1$. Assume that $n \ge 2$. Let $\Phi_n(x) = a_k x^k + \cdots + a_1 x + a_0$, where $k \in \mathbb{N}$ is the degree of $\Phi_n(x)$, and $a_0, a_1, \ldots, a_k \in \mathbb{C}$. By the inductive hypothesis, for every $d \mid n$ with $d < n$, $\Phi_d(x)$ is monic with integer coefficients. So the product of all these polynomials is also monic with integer coefficients, and we may write

$$\prod_{\substack{d|n \\ d<n}} \Phi_d(x) = x^l + b_{l-1} x^{l-1} + \cdots + b_1 x + b_0,$$

where $l \in \mathbb{N}$ is the degree, and $b_0, \ldots, b_{l-1} \in \mathbb{Z}$. Now, by (1), we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \times \prod_{\substack{d|n \\ d<n}} \Phi_d(x) = (a_k x^k + \cdots + a_1 x + a_0)(x^l + b_{l-1} x^{l-1} + \cdots + b_1 x + b_0).$$

It follows that $k + l = n$ and $a_k = 1$; so, $\Phi_n(x)$ is monic. Now, suppose that $\Phi_n(x) \notin \mathbb{Z}[x]$, and let $i \in \{0, 1, \ldots, k-1\}$ be maximum with $a_i \notin \mathbb{Z}$. On the LHS, the coefficient of x^{i+l} is zero because $0 < l \le i + l < n$. On the RHS, the coefficient of x^{i+l} is $a_i + (a_{i+1} b_{l-1} + a_{i+2} b_{l-2} + \cdots)$. Thus, $a_i + (a_{i+1} b_{l-1} + a_{i+2} b_{l-2} + \cdots) = 0$. Recall that $b_0, \ldots, b_{l-1} \in \mathbb{Z}$, and also by the choice of i, we have $a_{i+1}, a_{i+2}, \ldots \in \mathbb{Z}$. But now $a_i \in \mathbb{Z}$, a contradiction. This proves (2). □

We shall also use the following:

(3) *We have* $\Phi_1(0) = -1$ *and* $\Phi_n(0) = 1$ *for all* $n \ge 2$.

Proof of (3). The first assertion is immediate since $\Phi_1(x) = x - 1$. We prove the second assertion by induction on $n \ge 2$. For $n = 2$, by (1), we have $\Phi_2(x) = (x^2 - 1)/\Phi_1(x) = x + 1$, and so $\Phi_2(0) = 1$. Assume that $n \ge 3$. By the inductive hypothesis, we have

$$\prod_{\substack{d|n \\ 1<d<n}} \Phi_d(0) = 1.$$

Therefore, by (1) and since $\Phi_1(0) = -1$, we have

$$-1 = \prod_{d|n} \Phi_d(0) = \Phi_1(0) \times \Phi_n(0) \times \prod_{\substack{d|n \\ 1<d<n}} \Phi_d(0) \ \Rightarrow \ \Phi_n(0) = 1.$$

This proves (3). □

Back to the problem, recall that we have integers $b, m \geq 2$ with $b \mid m$. By (2), $\Phi_b(x)$ is monic, and so $\lim_{x\to\infty} \Phi_b(x) = \infty$. Therefore, there is a large enough multiple $M \in \mathbb{N}$ of m such that $\Phi_b(M) > 1$. Moreover, by (2), $\Phi_b(x) \in \mathbb{Z}[x]$, and so $\Phi_b(M) \in \mathbb{N}$. It follows that there is a prime q such that $q \mid \Phi_b(M)$.
By (1), $\Phi_b(M) \mid M^b - 1$, and so $q \mid M^b - 1$. Also, note that $\Phi_b(M) \equiv \Phi_b(0) \pmod{M}$, and so by (3), we have $\Phi_b(M) \equiv 1 \pmod{M}$; that is, $M \mid \Phi_b(M) - 1$. If $q \mid M$, then combined with $M \mid \Phi_b(M) - 1$, this yields $q \mid \Phi_b(M) - 1$, contrary to the fact that $q \mid \Phi_b(M)$. We deduce that

$$q \nmid M.$$

In particular, since $b \mid m$ and $m \mid M$, it follows that $q \nmid b$. It remains to show that $q \nmid M^r - 1$ for all $1 \leq r < b$. Suppose for a contradiction that $q \mid M^r - 1$ for some $r \in \{1, \ldots, b-1\}$. Let

$$G(x) = \prod_{\substack{d \mid b \\ d < b \\ d \nmid r}} \Phi_d(x).$$

Then, by (1), we have

$$x^b - 1 = \prod_{d \mid b} \Phi_d(x) = \Phi_b(x) \times G(x) \times \prod_{d \mid r} \Phi_d(x) = \Phi_b(x) \times G(x) \times (x^r - 1).$$

By taking the derivative of both sides and setting $x = M$, we obtain

$$bM^{b-1} = \Phi_b(M)G(M)(rM^{r-1}) + \Phi_b(M)G'(M)(M^r - 1) + \Phi_b'(M)G(M)(M^r - 1).$$

Since $q \mid \Phi_b(M)$ and $q \mid M^r - 1$, it follows that the RHS is divisible by q, and so $q \mid bM^{b-1}$. But now $q \mid b$ or $q \mid M$, a contradiction. ■

Now we handle the case $a = 1$ for general b:

Problem 69.

For every $b \in \mathbb{N}$, there are infinitely many primes that are 1 mod b.

Solution. We may assume that $b \geq 2$. For Step 1, we suppose for a contradiction that

There are only $t \in \mathbb{N}$ primes $p_1, \ldots, p_t$ that are 1 mod b. Let $m = bp_1p_2 \cdots p_t$.

For Step 2, we use the previous problem. Since $b, m \geq 2$ and $b \mid m$, it follows that for some $M \in \mathbb{N}$ with $m \mid M$, we have

There is a prime q such that, $q \mid M^b - 1$ and $q \nmid M^r - 1$ for all $1 \leq r < b$. In particular, $q \nmid M$.

For Step 3, we need to prove that $b \mid q - 1$. Suppose not. Then $q - 1 = bs + r$ for some integer $s \geq 0$ and $r \in \{1, \ldots, b-1\}$. It follows that $M^{q-1} = (M^b)^s \times M^r$. Recall also from Step 2 that $M^b \equiv 1 \pmod{q}$. Thus, we have $M^{q-1} \equiv M^r \pmod{q}$. Since $q \nmid M$ (from Step 2), by Fermat's little theorem, we have $M^{q-1} \equiv 1 \pmod{q}$, and therefore $M^r \equiv 1 \pmod{q}$. But now $q \mid M^r - 1$ for some $1 \leq r < b$, contrary to Step 2.

Now, as proved in the third step, q is a prime that is 1 mod b. So, $q \in \{p_1, \ldots, p_t\}$. But then $q \mid m$, and hence $q \mid M$, a contradiction. ■

Indeed, it is true in general that

For all $a, b \in \mathbb{N}$ with $a < b$ and $\gcd(a, b) = 1$, there are infinitely many primes that are a mod b.

This is *Dirichlet's Theorem*. We saw a proof for the case $a = 1$. The general case does not have an "easy" proof. (But it does have an "elementary" proof – meaning that it is comprehensible to anyone with fair knowledge of calculus.) Even the case $a = b - 1$ does not have an easy proof that works for all b, but some special values are easy, such as $b = 3$:

Problem 70.

There are infinitely many primes that are 2 mod 3.

Solution. Suppose for a contradiction that for some $t \in \mathbb{N}$, there are only t primes $p_1, \ldots, p_t$ that are 2 mod 3. Let

$$m = 3p_1p_2 \cdots p_t.$$

Then $m - 1 > 1$ has a prime divisor of q. Note that $q \nmid m$, since otherwise it follows from $q \mid m - 1$ that $q \mid 1$, which is impossible. In particular, $q \neq 3$ and $q \notin \{p_1, \ldots, p_t\}$. Thus, $q \equiv 1 \pmod 3$. We deduce that all prime divisors of $m-1$ are 1 mod 3. But then $m-1$ is also 1 mod 3, a contradiction because in fact $m - 1 \equiv 2 \pmod 3$. ■

We mentioned before that there are arbitrarily large intervals of consecutive composite numbers. In other words, the gap between a prime p and the next one can be arbitrarily large. The first question we are interested in here is: *Is there at least some control over this gap in terms of p?* The answer is yes: the next prime is no larger than $p!$, and that is easy to prove.

Problem 71.

Prove that for every integer $n > 2$, there is a prime p such that $n < p < n!$.

Solution. Note that $n! - 1 > 1$ has a prime divisor p. In particular, $p \leq n! - 1$. Also, if $p \leq n$, then $p \mid n!$, which along with $p \mid n! - 1$ yields $p \mid 1$, a contradiction. Therefore, $p > n$. ■

The second question we ask is: *How good a control do we have over the gap between a prime p and the next one?* It turns out that the next prime is smaller than $2p$. This is *Chebyshev's theorem*:

For every integer $n > 1$, there is a prime p such that $n < p < 2n$.

The original proof by Chebyshev is rather involved. Later, Erdős found an outstandingly simple proof that we will work out here.

First, we need a well-known result due to Legendre. Throughout, for $n \in \mathbb{N}$ and prime p, we denote by $v_p(n)$ the power of p in the prime factorization of n. (So, if $p \nmid n$, then $v_p(n) = 0$.)

Problem 72.

For all $n \in \mathbb{N}$ and every prime p, we have $v_p(n!) = \displaystyle\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$.

Solution. Note that

$$v_p(n!) = \sum_{m=1}^{n} v_p(m).$$

Now, we double count the set $X = \{(i,m) : \ i \in \mathbb{N},\ m \in \{1,\ldots,n\},\ p^i \mid m\}$. On one hand, for each $m \in \{1,\ldots,n\}$, we have $|\{i \in \mathbb{N} : \ (i,m) \in X\}| = |\{i \in \mathbb{N} : \ p^i \mid m\}| = v_p(m)$, and so

$$|X| = \sum_{m=1}^{n} |\{i \in \mathbb{N} : \ (i,m) \in X\}| = \sum_{m=1}^{n} v_p(m) = v_p(n!).$$

On the other hand, for each $i \in \mathbb{N}$, we have

$$|\{m \in \{1,\ldots,n\} : \ (i,m) \in X\}| = |\{m \in \{1,\ldots,n\} : \ p^i \mid m\}| = \left\lfloor \frac{n}{p^i} \right\rfloor,$$

and thus

$$|X| = \sum_{i=1}^{\infty} |\{m \in \{1,\ldots,n\} : \ (i,m) \in X\}| = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor. \quad \blacksquare$$

Erdős's proof of Chebyshev's theorem builds on an analysis of the prime factorization of the central binomial coefficient $\binom{2n}{n}$. Specifically, the key step is to show that for every prime p, the power of p in the prime factorization of $\binom{2n}{n}$ is at most the largest $\alpha \geq 0$ for which $p^\alpha \leq 2n$.

Problem 73.

Let $n \in \mathbb{N}$ with $n \geq 2$, let p be a prime, and let $t \in \mathbb{N} \cup \{0\}$ with $p^t \leq 2n < p^{t+1}$. Then

$$v_p\left(\binom{2n}{n}\right) \leq t.$$

Solution. For each $i \in \mathbb{N}$, let $f_i = 2n/p^i$. Note that if $i > t$, then $p^i > 2n$, and so $0 < f_i < 1$, which in turn yields $\lfloor f_i \rfloor = \lfloor f_i/2 \rfloor = 0$. Since $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, it follows from Problem 72 that

$$v_p\left(\binom{2n}{n}\right) = v_p((2n)!) - 2v_p(n!) = \sum_{i=1}^{\infty}(\lfloor f_i \rfloor - 2\lfloor f_i/2 \rfloor) = \sum_{i=1}^{t}(\lfloor f_i \rfloor - 2\lfloor f_i/2 \rfloor).$$

Also, recall that for every $x \in \mathbb{R}$, either $\lfloor 2x \rfloor = 2\lfloor x \rfloor$ or $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$, and so $\lfloor f_i \rfloor - 2\lfloor f_i/2 \rfloor \in \{0,1\}$ for all $i \in \mathbb{N}$. Hence,

$$v_p\left(\binom{2n}{n}\right) = \sum_{i=1}^{t}(\lfloor f_i \rfloor - 2\lfloor f_i/2 \rfloor) \leq t. \quad \blacksquare$$

Another important ingredient of the proof is the following beautiful inequality:

Problem 74.

For $n \in \mathbb{N}$ with $n \geq 2$, we have $\displaystyle\prod_{\substack{p:\ \text{prime} \\ p \leq n}} p < 4^{n-1}$.

Solution. For each $n \in \mathbb{N}$ with $n \geq 2$, let

$$P(n) = \prod_{\substack{p\text{: prime} \\ p \leq n}} p.$$

We prove by induction n that $P(n) < 4^{n-1}$. The case $n = 2$ is trivial. Assume that $k \geq 3$ and $P(k) < 4^{k-1}$ for all $k \in \{1, \ldots, n-1\}$. If n is even, $P(n) = P(n-1) \leq 4^{n-2} < 4^{n-1}$. So we may assume that $n = 2t+1$ for some $t \in \mathbb{N}$. By the inductive hypothesis, we have $P(t+1) < 4^t$. Also, for prime p with $t+1 < p \leq 2t+1$, we have $p \mid (2t+1)!$ but $p \nmid (t+1)!$, and in particular, $p \nmid t!$; thus, $p \mid \binom{2t+1}{t}$. Let Q be the product of all primes p with $t+1 < p \leq 2t+1$. It follows that $Q \mid \binom{2t+1}{t}$, and so $Q \leq \binom{2t+1}{t}$. Moreover,

$$\binom{2t+1}{t} = \frac{1}{2}\left(\binom{2t+1}{t} + \binom{2t+1}{t+1}\right) \leq \frac{1}{2}\sum_{i=0}^{2t+1}\binom{2t+1}{i} = \frac{2^{2t+1}}{2} = 4^t.$$

We deduce that $Q < 4^t$. Hence, $P(n) = P(t+1) \times Q < 4^t \times 4^t = 4^{n-1}$. ■

The last ingredients is a fairly easy lower bound for the central binomial coefficient:

Problem 75.

For every $n \in \mathbb{N}$, we have $\binom{2n}{n} \geq \dfrac{2^{2n-1}}{2n}$.

Solution. Recall that $\binom{2n}{n}$ is the largest among $\binom{2n}{0}, \binom{2n}{1}, \ldots, \binom{2n}{n}$. Therefore,

$$2^{2n} = \sum_{i=0}^{2n}\binom{2n}{i} \leq (2n+1)\binom{2n}{n} < 2(2n)\binom{2n}{n} \;\Rightarrow\; \binom{2n}{n} \geq \frac{2^{2n-1}}{2n}. \quad ■$$

We can now complete the proof:

Problem 76.

For every integer $n > 1$, there is a prime p such that $n < p < 2n$.

Solution. ... Suppose not. Then, for some $n \geq 3$, there is no prime p with $n < p \leq 2n$ (because $2 < 3 < 4$, and $2n$ is surely not a prime anyway). Let's have a close look at the prime factorization of $\binom{2n}{n}$. For each prime p, let $t_p \geq 0$ be the integer such that $p^{t_p} \leq 2n < p^{t_p+1}$. We break the set of all primes into five sets:

- Let S_1 be the set of all primes $p \leq \sqrt{2n}$. Then, since $p^{t_p} \leq 2n$ for every prime p, it follows from Problem 73 that
$$\prod_{p \in S_1} p^{v_p\left(\binom{2n}{n}\right)} \leq \prod_{p \in S_1} p^{t_p} \leq (2n)^{\sqrt{2n}}.$$
- Let S_2 be the set of all primes p with $\sqrt{2n} < p \leq 2n/3$. Then, for every $p \in S_2$, we have $t_p \leq 1$. Therefore, by Problems 73 and 74, we have
$$\prod_{p \in S_2} p^{v_p\left(\binom{2n}{n}\right)} \leq \prod_{p \in S_2} p^{t_p} \leq \prod_{p \in S_2} p \leq \prod_{\substack{p\text{: prime} \\ p \leq \lfloor 2n/3 \rfloor}} p < 4^{\lfloor 2n/3 \rfloor - 1} \leq 4^{\frac{2n}{3}-1} = 2^{\frac{4n}{3}-2} < 2^{\frac{4n}{3}-1}.$$

- Let S_3 be the set of all primes p with $\frac{2n}{3} < p \leq n$. For every $p \in S_3$, since $p \leq n$, it follows that $p, 2p \in \{1, \ldots, 2n\}$, and since $2n < 3p$, it follows that $p, 2p$ are in fact the only multiples of p that belong to $\{1, \ldots, 2n\}$. In particular, $v_p((2n)!) = 2$ (note that $p > 2n/3 \geq 2$ as $n \geq 3$). Also, since $p \leq n$, it follows that $v_p(n!) \geq 1$. Therefore, $v_p\left(\binom{2n}{n}\right) = v_p((2n)!) - 2v_p(n!) \leq 0$ for all $p \in S_3$, and so
$$\prod_{p \in S_3} p^{v_p\left(\binom{2n}{n}\right)} = 1.$$

- Let S_4 be the set of all primes p with $n < p \leq 2n$. We started with the assumption that $S_4 = \varnothing$!

- Let S_5 be the set of all primes $p > 2n$. Then, for every $p \in S_5$, we have $t_p = 0$, and so by Problem 73, we have
$$\prod_{p \in S_5} p^{v_p\left(\binom{2n}{n}\right)} \leq \prod_{p \in S_5} p^{t_p} = 1.$$

We deduce that
$$\binom{2n}{n} = \prod_{p \in S_1 \cup \cdots \cup S_5} p^{v_p\left(\binom{2n}{n}\right)} \leq (2n)^{\sqrt{2n}} \times 2^{\frac{4n}{3}-1}.$$

Recall also that by Problem 75, we have $\binom{2n}{n} \geq \frac{2^{2n-1}}{2n}$. Consequently,
$$2^{2n/3} \leq (2n)^{\sqrt{2n}+1}.$$

Now, let $m = \sqrt{2n}$. Then
$$2^{2n/3} \leq (2n)^{\sqrt{2n}+1} \;\Rightarrow\; 2^{m^2/3} \leq m^{2(m+1)} = 2^{2(m+1)\log m} \;\Rightarrow\; m^2 \leq 6(m+1)\log m.$$

This cannot be true if m is large enough. To see this, consider the function $f(x) = x^2 - 6(x+1)\log x$. Then $f(m) \leq 0$ and $f(32) = 1024 - (6 \times 33 \times 5) > 0$. Also, $f'(x) = 2x - 6\log x - 6\left(1 + \frac{1}{x}\right)\log e$. Since $\log e < 2$, it follows that for every $x > 12$, we have $6\left(1 + \frac{1}{x}\right)\log e < 13$, and so
$$f'(x) > 2x - 6\log x - 13; \quad \forall x > 12.$$

Next, consider the function $g(x) = x - 3\log x$. Then, since $\log 22 < 5$, it follows that $g(22) > 22 - 15 = 7$. Also, $g'(x) = 1 - \frac{3\log e}{x}$. Since $\log e < 2$, it follows that
$$g'(x) > 0; \quad \forall x > 6.$$

Thus, g is increasing on $(6, \infty)$. Since $g(22) > 7$, it follows that $g(x) > 7$ for all $x \geq 22$. This, combined with $f'(x) > 2x - 6\log x - 13$ for all $x > 12$, implies that
$$f'(x) > 2g(x) - 13 > 0; \quad \forall x > 22.$$

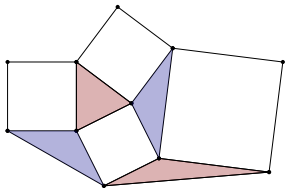
In particular, f is increasing on $(22, \infty)$. Therefore, since $f(32) > 0$, it follows that $f(x) > 0$ for all $x \geq 32$. We deduce that $m < 32$, and so $n < 512$. But this is a contradiction to the assumption that there is no prime p with $n < p < 2n$, because
$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$
are all primes, each smaller than twice the preceding one, and so one of them falls between n and $2n$ (because $n < 512$). ■

10 Geometry

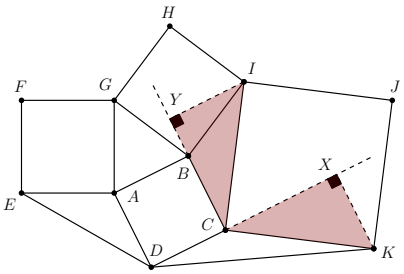
Let us start with some puzzle-looking problems. Throughout, for a polygon P, we use $[\mathsf{P}]$ to denote the area of P.

Problem 77.

In this figure, all four quadrilaterals are squares, and the total area shaded in blue is equal to 1. Find the total area shaded in red.

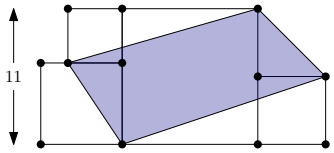


Solution. The answer is 1. Let X be the foot of the perpendicular from K to (the extension of) CD. Let Y be the foot of the perpendicular from I to (the extension of) BC. Then ΔKXC and ΔIYC are congruent (why?). In particular, $KX = IY$. So, $[\Delta CDK] = (KX \times CD)/2 = (IY \times BC)/2 = [\Delta BCI]$. Similarly, we can show that $[\Delta BCI] = [\Delta ABG] = [\Delta ADE]$. ■



Problem 78.

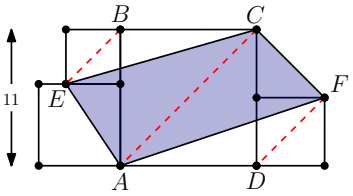
In this figure, all four quadrilaterals are squares. Find the shaded area.



Solution. Note that $AC \parallel BE$, and so

$$[\Delta AEC] = [\Delta ABC].$$

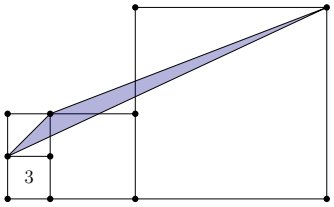
Likewise, $AC \parallel DF$, and so $[\Delta AFC] = [\Delta ADC]$.



Therefore, $[AECF] = [\Delta AEC] + [\Delta AFC] = [\Delta ABC] + [\Delta ADC] = [ABCD] = 121$. ■

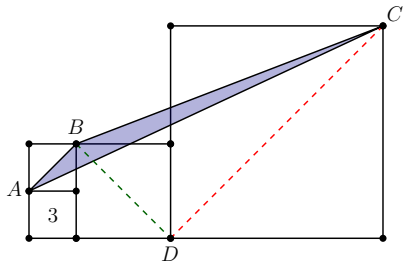
Problem 79.

In this figure, all four quadrilaterals are squares, and the bottom left square has area 3. Find the shaded area.



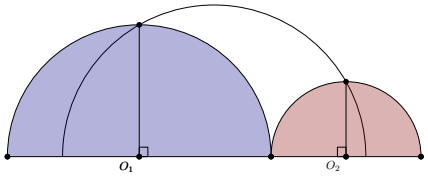
Solution. Since $\angle ABD = \angle BDC = 90°$, it follows that $AB \parallel CD$, and so $[\Delta ABC] = [\Delta ABD]$. Moreover, note that $AB = \sqrt{6}$ and $BD = \sqrt{24}$. (Why?) Therefore, since $\angle ABD = 90°$, it follows that

$$[\Delta ABC] = [\Delta ABD] = \frac{AB \times BD}{2} = \frac{\sqrt{6} \times \sqrt{24}}{2} = 6. \quad \blacksquare$$



Problem 80.

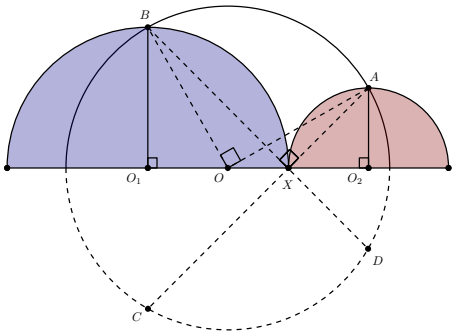
In this figure, O_1 is the center of the blue semicircle, O_2 is the center of the red semicircle, and the sum of the areas of the blue and red semicircles is equal to 1. Find the area of the third semicircle.



Solution. Let O be the center of the third semicircle and let R_1, R_2, R be the radii of the blue semicircle, the red semicircle, and the third one, respectively. Note that we have $\angle AXO_2 = \angle BXO_1 = 45°$, and so $\angle AXB = 90°$. It follows that $AB^2 = AX^2 + BX^2 = 2R_1^2 + 2R_2^2$. Also, in the circle with center O, the following hold (why?):

$$\overset{\frown}{AB} = \overset{\frown}{CD}; \quad \overset{\frown}{AD} = 2 \times \angle ABD; \quad \overset{\frown}{BC} = 2 \times \angle BAC.$$

Since $\angle ABD + \angle BAC = 180° - \angle AXB = 90°$, it follows that $\angle AOB = \overset{\frown}{AB} = 90°$, and so $AB^2 = AO^2 + BO^2 = 2R^2$. But now, $R^2 = R_1^2 + R_2^2$; hence, the area of the third semicircle is equal to the sum of the areas shaded in blue and red, which is 1. $\blacksquare$



The next four problems on angles and triangles are somewhat more challenging:

Problem 81.

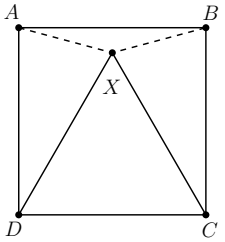
(a) Let X be a point on the diagonal AC of a square $ABCD$ such that $AX + BX = CX$. Find the angle $\angle BXC$.

(a) Let X be the point inside a square $ABCD$ such that $\angle XAB = \angle XBA = 15°$. Prove that ΔXCD is equilateral.

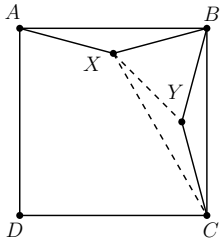
Solution. For (a), choose the point Y on CX such that $CY = AX$. Then

$$XY = CX - CY = CX - AX = BX.$$

Also, note that $AX = CY$, $AB = CB$, and $\angle XAB = \angle YCB = 45°$. Therefore, ΔXAB and ΔYCB are congruent, and so $BX = BY$. It follows that ΔBXY is equilateral. Hence $\angle BXC = 60°$.



For (b), let Y be the point inside $ABCD$ with $\angle YBC = \angle YCB = 15°$. Then ΔXAB and ΔYBC are congruent, and so $BX = BY$. Moreover, $\angle XBY = 90° - (2 \times 15°) = 60°$. Thus, ΔBXY is equilateral; in particular, $BY = XY$ and $\angle BYX = 60°$. Also, $\angle BYC = 180° - (2 \times 15°) = 150°$, and so $\angle XYC = 360° - 150° - 60° = 150°$. Now, since $BY = XY$ and $\angle BYC = \angle XYC$, it follows that ΔBYC and ΔXYC are congruent; hence, $XC = BC$. Likewise, one may show that $DX = DA$. ■

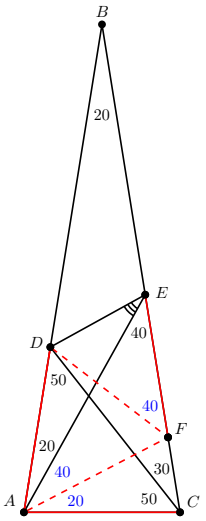


Problem 82.

Let ΔABC be a triangle with $AB = BC$ and $\angle ABC = 20°$. Let D, E be points on AB, BC, respectively, such that $\angle DAE = 20°$ and $\angle DCE = 30°$. Find $\angle DEA$.

Solution. First, note that $\angle ACD = \angle ADC = 50°$, and so $AC = AD$. Also, $\angle AEC = 40°$.
Choose the point F on EC such that $\angle CAF = 20°$. Then $\angle EAF = 40°$, and $\angle AFC = \angle ACF = 80°$, which in turn yields $AC = AF$. It follows that $AD = AF$, which, along with $\angle DAF = \angle DAE + \angle EAF = 60°$, implies that ΔADF is equilateral. In particular, we have $AF = FD$.
Now, since $\angle EAF = \angle AEF = 40°$, we have $AF = FE$. Therefore, $FD = FE$. Moreover, since $\angle AFC = 80°$ and $\angle AFD = 60°$ (because ΔADF is equilateral), it follows that $\angle DFE = 40°$. Therefore, $\angle DEF = \angle EDF = 70°$, and so

$$\angle DEA = \angle DEF - \angle AEF = 70° - 40° = 30°. \quad ■$$

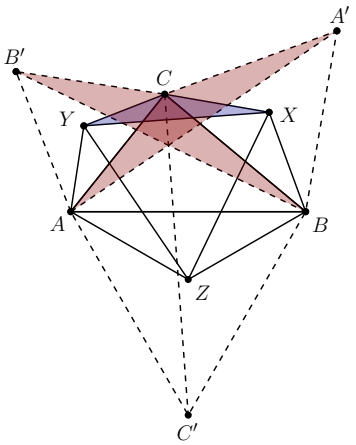


Note. This is the so-called *adventitious angles puzzle* (quite fittingly; it does feel rather random!).

Problem 83.

Let ΔABC be a triangle. Let X be the point outside ΔABC such that $\angle XBC = \angle XCB = 30°$, let Y be the point outside ΔABC such that $\angle YAC = \angle YCA = 30°$, and let Z be the point outside ΔABC such that $\angle ZAB = \angle ZBA = 30°$. Prove that ΔXYZ is equilateral.

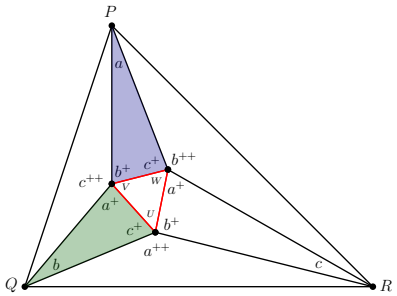
Solution. Let A' be the point on the same side of BC as X such that $\Delta A'BC$ is equilateral, let B' be the point on the same side of CA as Y such that $\Delta AB'C$ is equilateral, and let C' be the point on the same side of AB as Z such that $\Delta ABC'$ is equilateral. Since $CA = CB'$, $A'C = BC$, and $\angle A'CA = \angle B'CB = \angle BCA + 60°$, it follows that $\Delta A'CA$ and $\Delta BCB'$ are congruent, and so $AA' = BB'$. Likewise, we can show that $BB' = CC'$. Thus, $AA' = BB' = CC'$. Now, note that $CY/CA = CX/CA' = (\sec 30°)/2 = 1/\sqrt{3}$. Also, $\angle XCY = \angle A'CA = \angle BCA + 60°$. Hence, ΔXCY and $\Delta A'CA$ are similar, and so $XY/AA' = 1/\sqrt{3}$. Likewise, we may show that $YZ/BB' = ZA/CC' = 1/\sqrt{3}$. ■



Problem 84.

Let ΔABC be a triangle. Let A_1, A_2 be points on BC (with A_1 between B and A_2) such that AA_1, AA_2 trisect the angle $\angle CAB$, let B_1, B_2 be points on CA (with B_1 between C and B_2) such that BB_1, BB_2 trisect the angle $\angle ABC$, and let C_1, C_2 be points on AB (with C_1 between A and C_2) such that CC_1, CC_2 trisect the angle $\angle BCA$. Let X be the intersection point of AA_1 and BB_2, let Y be the intersection point of BB_1 and CC_2, and let Z be the intersection point of CC_1 and AA_2. Prove that ΔXYZ is equilateral.

Solution. Let us call ΔXYZ the *Morley triangle* of ΔABC. We prove that for every three angles a, b, c with $a + b + c = 60°$, there is a triangle with angles $3a, 3b, 3c$ whose Morley triangle is equilateral. This implies that there is a triangle similar to our ΔABC whose Morley triangle is equilateral, which in turn implies that the Morley triangle ΔXYZ of ΔABC is equilateral. (Why?)



Suppose a, b, c are angles with $a + b + c = 60°$. Throughout, for an angle x, we write $x^+ = x + 60°$ (and so $x^{++} = x + 120°$). Start with an equilateral triangle ΔUVW with side length 1. Let P be the point on the opposite side of VW from U such that $\angle PVW = b^+$ and $\angle PWV = c^+$. (Convince yourself that there is exactly one such point P.) Likewise, let Q be the point on the opposite side of UV from W such that $\angle QUV = c^+$ and $\angle QVU = a^+$, and let R be the point on the opposite side of WU from V such that $\angle RWU = a^+$ and $\angle RUW = b^+$. (Again, the choice of Q, R is unique.) We claim that

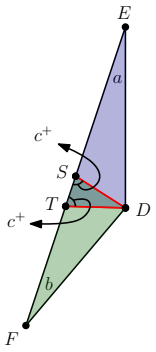
$$\angle VPQ = a \text{ and } \angle VQP = b; \quad \angle UQR = b \text{ and } \angle URW = c; \quad \angle WRP = c \text{ and } \angle WPR = a.$$

This shows that $\Delta U'V'W'$ has angles $3a, 3b, 3c$, and so ΔUVW is the Morley triangle of $\Delta U'V'W'$. We only prove that $\angle VPQ = a$ and $\angle VQP = b$; the other four equalities can be proved similarly.

Let ΔDEF be the triangle with the following specifications:

- $\angle DEF = a$ and $\angle DFE = b$.
- Let S, T be the two points on EF such that $\angle DTE = \angle DSF = c^+$ (and so $DS = DT$). Then we have $DS = DT = 1$.

(Convince yourself that such a triangle exists and is unique. In particular, the points S, T always exist.)



It follows that $VW = DT = 1$ and $\angle PWV = \angle ETD = c^+$. Also, recall that $\angle PVW = b^+$, and note that $\angle EDT = 180° - \angle DEF - \angle ETD = 180° - a - c^+ = b^+$. Therefore, the triangles ΔEDT and ΔPVW are congruent, and so $DE = VP$. Likewise, the triangles ΔFDS and ΔQVU are congruent, and so $DF = VQ$. Moreover, note that

$$\angle EDF = 180° - \angle DEF - \angle DFE = 180° - a - b = c^{++};$$

$$\angle PVQ = 360° - \angle PVW - \angle UVW - \angle QVU = 360° - b^+ - 60° - a^+ = 180° - b - a = c^{++}.$$

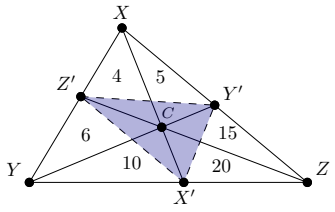
From $DE = VP$, $DF = VQ$, and $\angle EDF = \angle PVQ$, we deduce that the triangles ΔDEF and ΔVPQ are congruent, and so $\angle VPQ = \angle DEF = a$ and $\angle VQP = \angle DFE = b$, as desired. ■

Note. This is *Morley's Theorem*. It has several proofs, most of which are rather technical. The above marvelous proof is due to Conway.

In a triangle ΔABC, a *cevian* is a line segment joining a vertex of the triangle to some point in the interior of the opposite side.

Problem 85.

The cevians XX', YY', ZZ' in a triangle ΔXYZ are concurrent at a point C. The areas of the triangles $\Delta XZ'C, \Delta YZ'C, \Delta YX'C, \Delta ZX'C, \Delta ZY'C, \Delta XY'C$ are, respectively, equal to $4, 6, 10, 20, 15, 5$. Find the area of the triangle $\Delta X'Y'Z'$.



Solution. Here is a useful trick (convince yourself why this holds): If AD is a cevian in a triangle ΔABC, then

$$\frac{[\Delta ABD]}{[\Delta ACD]} = \frac{BD}{CD}.$$

Applying the above to our problem, we deduce that

$$\frac{[\Delta X'Y'C]}{[\Delta X'YC]} = \frac{Y'C}{YC} = \frac{[\Delta XY'C]}{[\Delta XYC]} = \frac{[\Delta XY'C]}{[\Delta XZ'C] + [\Delta YZ'C]} \Rightarrow [\Delta X'Y'C] = \frac{10 \times 5}{4+6} = 5.$$

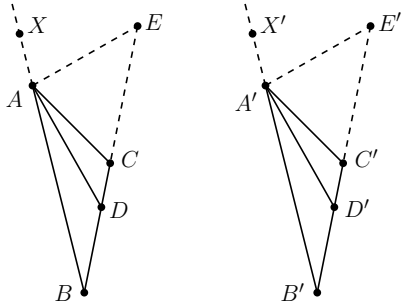
Likewise, $[\Delta Y'Z'C] = \dfrac{6 \times 15}{10+20} = 3$ and $[\Delta Z'X'C] = \dfrac{4 \times 20}{15+5} = 4$. Hence, $[\Delta X'Y'Z'] = 12$. ■

Here is another application of the "area trick" from Problem 85:

Problem 86.

Let ΔABC and $\Delta A'B'C'$ be triangles such that $\frac{AB}{AC} = \frac{A'B'}{A'C'}$, $BC = B'C'$, and the length of the bisector of $\angle BAC$ is equal to the length of the bisector of $\angle B'A'C'$. Prove that ΔABC and $\Delta A'B'C'$ are congruent.

Solution. Let AD and $A'D'$ be the bisectors of $\angle BAC$ and $\angle B'A'C'$. Let $a = \angle BAC/2$ and let $a' = \angle B'A'C'/2$. The length of the altitude in ΔABD from D is $AD \sin a$, and so $[\Delta ABD] = (AB \cdot AD \cdot \sin a)/2$. Similarly, we have $[\Delta ACD] = (AC \cdot AD \cdot \sin a)/2$. It follows that $\frac{BD}{CD} = \frac{[\Delta ABD]}{[\Delta ACD]} = \frac{AB}{AC}$, and likewise, $\frac{B'D'}{C'D'} = \frac{A'B'}{A'C'}$. We deduce that $BD = B'D'$ and $CD = C'D'$.



Now, if $a = 45°$ or $a' = 45°$, then we are done. (Why?) So we may assume that, for points X, X' on the extensions of $AB, A'B'$ beyond A, A', respectively, the bisectors of $\angle XAC$ and $\angle X'A'C'$ intersect the extensions of $BC, B'C'$ beyond C, C' at points E, E', respectively.

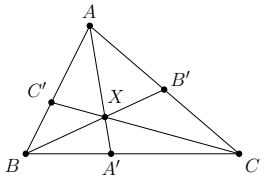
An argument similar to the one above shows that $BE = B'E'$, which, combined with $BD = B'D'$, yields $DE = D'E'$. Also, note that $\angle EAD = \angle E'A'D' = 90°$, and recall that $AD = A'D'$.

Therefore, ΔDAE and $\Delta D'A'E'$ are congruent, and so $\angle ADC = \angle A'D'C'$. This, combined with $AD = A'D'$ and $CD = C'D'$, implies that ΔDAC and $\Delta D'A'C'$ are also congruent, and so $AC = A'C'$. Likewise, from $\angle ADC = \angle A'D'C'$, it follows that $\angle ADB = \angle A'D'B'$. This, combined with $AD = A'D'$ and $BD = B'D'$, implies that ΔDAB and $\Delta D'A'B'$ are congruent, and so $AB = A'B'$. Hence, ΔABC and $\Delta A'B'C'$ have the same side lengths. ■

The "area trick" from Problem 85 can be used to prove *Ceva's Theorem* (Ceva was an Italian mathematician, and the name "cevian" also comes from his name):

Problem 87.

Prove that the cevians AA', BB', CC' in a triangle ΔABC are concurrent if and only if $\frac{AC'}{C'B} \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = 1$.



Solution. First, assume that the cevians AA', BB', CC' are concurrent at a point X. Note that if two fractions $\frac{a}{b}$ and $\frac{c}{d}$ are equal, then they are both equal to $\frac{a-c}{b-d}$. Therefore,

$$\frac{AC'}{C'B} = \frac{[\Delta ACC']}{[\Delta CBC']} = \frac{[\Delta XAC']}{[\Delta XBC']} = \frac{[\Delta ACC'] - [\Delta XAC']}{[\Delta CBC'] - [\Delta XBC']} = \frac{[\Delta CXA]}{[\Delta BXC]}.$$

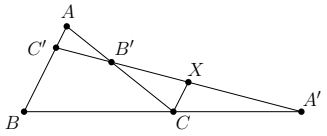
Similarly, $\frac{BA'}{A'C} = \frac{[\Delta AXB]}{[\Delta CXA]}$ and $\frac{CB'}{B'A} = \frac{[\Delta BXC]}{[\Delta AXB]}$. Therefore, $\frac{AC'}{C'B} \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = 1$.

Conversely, assume that $\frac{AC'}{C'B} \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = 1$. Let X be the intersection point of AA' and BB', and let C'' be the intersection point of AB and the extension of CX beyond X. Then, the cevians AA', BB', CC'' are concurrent, and so $\frac{AC''}{C''B} \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = 1$. Therefore, $\frac{AC''}{C''B} = \frac{AC'}{C'B}$, and $C' = C''$, meaning that CC' passes through X in the first place. ■

Ceva's theorem has a "dual" that deals with collinearity, known as *Menelaus's Theorem*.

Problem 88.

Let ΔABC be a triangle and let A', B', C' be points on the lines containing BC, CA, AB. Prove that A', B', C' are collinear if and only if $\frac{AC'}{C'B} \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = 1$.



Solution. Assume that A', B', C' are collinear. Assume that A' lies on the extension of BC beyond C, B' lies on CA, and C' lies on AB. (The other cases are similar.) Choose $X \in A'B'$ such that AB and CX are parallel. Then $\Delta AC'B'$ and $\Delta CXB'$ are similar, and so $\frac{AC'}{CX} = \frac{B'A}{CB'}$. Also, $\Delta A'BC'$ and $\Delta A'CX$ are similar, and so $\frac{CX}{C'B} = \frac{A'C}{BA'}$. Therefore,

$$\frac{AC'}{C'B} \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = \left(\frac{AC'}{CX} \times \frac{CX}{C'B}\right) \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = \left(\frac{B'A}{CB'} \times \frac{A'C}{BA'}\right) \times \frac{BA'}{A'C} \times \frac{CB'}{B'A} = 1.$$

The converse can be proved by an argument similar to the second direction of Ceva's theorem. ■

There are several instances of concurrency that occur in a triangle ΔABC, including:

- The perpendicular bisectors of the sides are concurrent at the *circumcenter*, often denoted by O. This is the center of the *circumcircle* of ΔABC – the unique circle passing through A, B, C.
- The medians are concurrent at the *centroid* (also called the *center of mass*), often denoted by G.
- The altitudes are concurrent at the *orthocenter*, often denoted by H.
- The internal bisectors of the angles are concurrent at the *incenter*, often denoted by I. This is the center of the incircle of ΔABC, the unique circle that is tangent to the three sides.

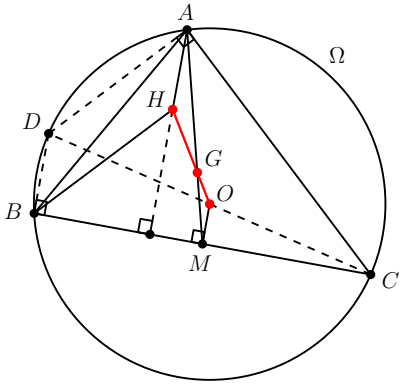
The first is fairly easy to see; the other three can be proved using Ceva's theorem (with some extra work following techniques we saw in previous problems – you should try these as exercises).

There are also several instances of collinearity. Here is a particularly nice one.

Problem 89.

Prove that in a triangle ΔABC, the circumcenter O, the centroid G, and the orthocenter H are collinear (in this order).

Solution. Let M be the midpoint of BC. First, we show that $AH = 2OM$. Let Ω be the circumcircle of ΔABC. Extend CO beyond O to hit Ω at D. Then $\angle DAC = \angle DBC = 90^\circ$ (because CD is the diameter of Ω). Since $DA \perp CA$ and $BH \perp CA$, it follows that $DA \parallel BH$, and since $DB \perp BC$ and $AH \perp BC$, it follows that $DB \parallel AH$. Therefore, $ADBH$ is a parallelogram, and so $AH = DB$. Moreover, since $DB \perp BC$ and $OM \perp BC$, it follows that $DB \parallel OM$, which, combined with $BM = CM$, implies that $DB = 2OM$. We deduce that $AH = 2OM$.



Next, we show that $AG = 2GM$. There are several ways to do this – here is one using Menelaus's theorem. Let P be the midpoint of AB. Then P, G, C are collinear, and so by Menelaus's theorem applied to ΔABM and points P, C, G, we have:

$$\frac{AP}{PB} \times \frac{BC}{MC} \times \frac{MG}{GA} = 1 \Rightarrow 1 \times 2 \times \frac{MG}{GA} = 1 \Rightarrow AG = 2GM.$$

Now, since $AH \perp BC$ and $OM \perp BC$, it follows that $AH \parallel OM$, and so $\angle GMO = \angle GAH$. This, combined with $AH = 2OM$ and $AG = 2GM$, implies that ΔAHG and ΔMOG are similar. In particular, $\angle AGH = \angle MGO$. Hence, O, G, H are collinear because A, G, M are. ■

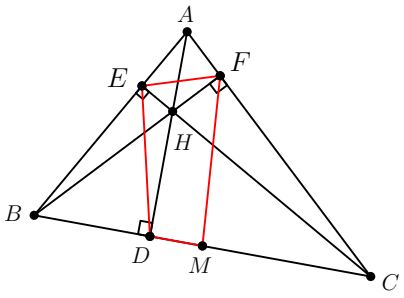
Note. The line passing through O, G, H is called the *Euler line of* ΔABC, and has several interesting properties. Note, for instance, that we also proved that $GH = 2OG$.

There are also some nice instances of "concyclicity" – a fancy word for points lying on the same circle. Here is a famous one, which is somewhat wild – you get nine points on the same circle!

Problem 90.

Let ΔABC be a triangle, let D, E, F be the feet of the altitudes from A, B, C, and let H be the orthocenter of ΔABC. Prove that D, E, F, the midpoints of AB, BC, CA, and the midpoints of AH, BH, CH, are all concyclic.

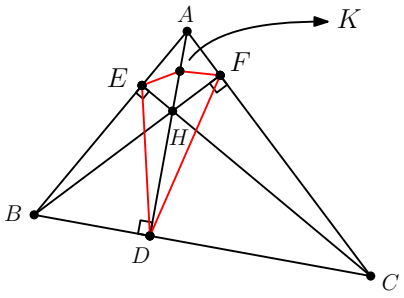
Solution. First, we prove that the midpoint M of BC is concyclic with D, E, F (and the same can be proved for the midpoints of AB and AC with a similar argument). Since $\angle AFH = \angle AEH = 90°$, it follows that A, F, H, E are concyclic, and so $\angle EFH = \angle EAH = 90° - \angle BCA$. Likewise, we have $\angle DFH = \angle DBH = 90° - \angle BCA$. Thus, $\angle EFD = \angle EFH + \angle DFH = 180° - 2\angle BCA$. Moreover, since $\angle BEC = 90°$ and $BM = CM$, it follows that M is the circumcenter of ΔBCE, and so $ME = MC$, which in turn implies that $\angle MEC = \angle MCE = \angle BCA$. Consequently, $\angle EMD = \angle MEC + \angle MCE = 2\angle BCA$. Now,



$$\angle EFD + \angle EMD = 180° - 2\angle BCA + 2\angle BCA = 180°.$$

Therefore, D, E, F, M are concyclic.

Next, we prove that the midpoint K of AH is concyclic with D, E, F (and the same can be proved for the midpoints of BH and CH with a similar argument). Recall that since $\angle AFH = \angle AEH = 90°$, the four points A, F, H, E are concyclic; in fact, AH is the diameter of the circle passing through A, F, H, E, and so K is the center of that circle. It follows that $\angle EKF = 2\angle EAF = 2\angle BAC$. Recall also that, as shown above, $\angle EFD = 180° - 2\angle BCA$. A similar argument proves that $\angle EDF = 180° - 2\angle ABC$. Now,



$$\angle EKF + \angle EFD = 2\angle BAC + 180° - 2\angle BAC = 180°.$$

Therefore, D, E, F, K are concyclic. ■

Note. This circle is called the *nine-point circle of* ΔABC, and has several fascinating properties.