The Putnam Challenge

MATH 490, Texas A&M University

Taught by Prof. Sherry Gong

August 20, 2024 – November 26, 2024

Dates

1 August 20, 2024

Exercise 1

Show that if x is a rational number which is not an integer, then x^x is irrational.

Solution Let $x = \dfrac{m}{n}$ for $m,\ n \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and $n \neq 1$. For the sake of contradiction, suppose x^x is rational. Then

$$\left(\frac{m}{n}\right)^{\frac{m}{n}} = \frac{p}{q}$$

for some $p,\ q \in \mathbb{Z}$ with $\gcd(p, q) = 1$. Then

$$\left(\frac{m}{n}\right)^{m} = \left(\frac{p}{q}\right)^{n}$$

$$\frac{m^m}{n^m} = \frac{p^n}{q^n}$$

$$m^m \cdot q^n = p^n \cdot n^m$$

Since $m^m \mid m^m \cdot q^n = p^n \cdot n^m$ and $\gcd(m, n) = 1$, $m^m \mid p^n$. Similarly, since $p^n \mid p^n \cdot n^m = m^m \cdot q^n$ and $\gcd(p, q) = 1$, $p^n \mid m^m$. This gives $p^n = m^m$, and $q^n = n^m$.

Let m's prime factorization be $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then, since $p^n = m^m = p_1^{e_1 m} p_2^{e_2 m} \cdots p_k^{e_k m}$ and all p_is are prime, n should divide all exponents of p_is. That is, $n \mid e_i m$ for all i. Since $\gcd(m, n) = 1$, $n \mid e_i$ for all i. This gives $m = \alpha^n$ for some $\alpha \in \mathbb{Z}$. Similarly, $n = \beta^m$ for some $\beta \in \mathbb{Z}$. Here, $\beta \neq 1$ since n couldn't be 1. So $\beta \geq 2$, and $n \geq m$. However, we then have

$$m = \alpha^n \geq \alpha^m,$$

which forces $\alpha = 1$ and $m = 1$. This gives $p^n = 1^1 = 1$, so $p = 1$ and $n = 1$, which is a contradiction. Therefore, x^x is irrational.

Exercise 2

Show that no set of nine consecutive integers can be partitioned into two sets with the product of the elements of the first set equal to the product of the elements of the second set.

Solution For the sake of contradiction, suppose it is possible to partition nine consecutive sets with the same product of elements in each set, and let this product be n. Then the product of nine elements are n^2.

Claim. The prime factorization of n should be consisted of only 2, 3, 5, and 7.

Suppose $p \mid n$ for some $p \geq 11$. Then, the two sets should both contain a multiple of p, which is impossible because there are only nine consecutive elements.

Therefore, n is of the form $n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d$.

Claim. The exponents should satisfy:

$$4 \leq a \leq 7$$
$$b = 2$$
$$c = 1$$
$$d = 1.$$

Notice that $7 \mid n^2$ since n^2 is a product of nine numbers, which will always contain a multiple of 7. So $2d \geq 1$, so $d \geq 1$ since d is an integer. However, if $d \geq 2$, then $7^4 \mid n^2$, which is impossible unless one of the nine numbers is divisible by 7^3. In this case, it is impossible to partition the nine numbers with the same product of elements. Therefore $d = 1$. Similar argument holds for c.

For b, since consecutive nine numbers always contains three multiples of 3 and one multiple of 9, $2b \geq 4$. However, if $b \geq 3$, $3^6 \mid n^2$, which forces the multiple of 9 to be a multiple of 81 since the other two multiples of 3 couldn't be multiples of 9. If one of the nine number is a multiple of 81, then it is impossible to partition the nine numbers with the same product of elements. Therefore, $b = 2$.

For a, since consecutive nine numbers always contains four multiples of 2, two multiples of 4, and one multiple of 8, $2a \geq 7$. This gives $a \geq 4$. If $b \geq 8$, then $2^{16} \mid n^2$, which is only possible when one of the nine numbers is a multiple of 2^9. But if this is the case, it is impossible to partition the nine numbers with the same product of elements. Therefore $a \leq 7$.

We test the four cases: $n = 5040, 10080, 20160, 40320$. This gives

$$n^2 \leq (40320)^2 = 1,625,702,400 < \frac{15!}{6!} = 7 \cdot 8 \cdot \cdots \cdot 15,$$

so $n \leq 15$. Testing the numbers below or equal to 15, we see that it is impossible to partition consecutive nine numbers to have the same product of elements.

> **Exercise 3**
>
> Consider a function $f : \mathbb{R}^3 \to \{0, 1, 2\}$. Show that there exists $i \in \{0, 1, 2\}$ such that for any $x \in \mathbb{R}_{>0}$, there exist points P, $Q \in f^{-1}(i)$ such that the Euclidean diatance between P and Q is x. That is, of the preimages of 0, 1, 2, one of these preimages attains all distances.

Solution We prove by contradiction. Suppose $\forall i \in \{0, 1, 2\}$ and for some $r \in \mathbb{R}_{>0}$, $\forall A$, $B \in f^{-1}(\{i\})$, $|A - B| \neq r$.

WLOG let $f\big((0, 0, 0)\big) = 0$. Then the sphere $x^2 + y^2 + z^2 = r^2$ should contain points mapping only to 1 or 2. WLOG let $f\big((0, 0, r)\big) = 1$. Then the circle

$$x^2 + y^2 = \frac{3}{4}r^2,\ z = \frac{r}{2}$$

should consist only points mapping to 2 since any point on this circle has distance r from both the origin and $(0, 0, r)$.

Now, take one point $P_0\left(x_0, y_0, \frac{r}{2}\right)$ with $x_0^2 + y_0^2 = \frac{3}{4}r^2$. Let Q_0 be the point $Q_0\left(x_0 \cdot e^{i\pi/3}, y_) \cdot e^{i\pi/3}, \frac{r}{2}\right)$. Then Q is on the circle defined above. Also, $PQ = r$ because the points P, Q, and $R(0, 0, r/2)$ form an equilateral triangle. This gives a contradiction and completes the proof.

Exercise 4

Show that there are no nonconstant functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ satisfying

$$xf(y) + yf(x) = (x+y)f(x^2+y^2).$$

Solution We prove by contradiction. Suppose there exists a function f. Take two positive integers a and b, and define a recursive sequence $\{b_n\}$ with $b_0 = b$ and $b_n = a^2 + b_{n-1}^2$ for $n \geq 1$. WLOG let $f(a) \leq f(b)$. If $f(a) \neq f(b)$, since

$$f(b_1) = f(a^2+b^2) = \frac{a}{a+b}f(b) + \frac{b}{a+b}f(a),$$

we have $f(a) < f(b_1) < f(b)$. We repeat the process and get

$$f(a) < \cdots < f(b_2) < f(b_1) < f(b).$$

However, repeating this $f(b) - f(a)$ times shows that it is impossible to have a function f since the range of f is positive integers, but more that $f(b) - f(a)$ positive integers fit in between $f(a)$ and $f(b)$. This gives $f(a) = f(b)$. Since a and b were chosen arbitrarily, this implies that f is a constant function, which is a contradiction.

2 August 27, 2024

Exercise 1

Show that $|\sin(nx)| \le n|\sin(x)|$ for any real number x and positive integer n.

Solution We use induction. The base case $n = 1$ obviously works.

Let $k \in \mathbb{N}$, and $|\sin(kx)| \le k|\sin(x)|$. We have

$$\begin{aligned}
\left|\sin\big((k+1)x\big)\right| &= |\sin(kx + x)| \\
&= |\sin(kx)\cos(x) + \cos(kx)\sin(x)| \\
&\le |\sin(kx)||\cos(x)| + |\cos(kx)||\sin(x)| \\
&\le |\sin(kx)| + |\sin(x)| \\
&\le k|\sin(x)| + |\sin(x)| \\
&= (k+1)|\sin(x)|
\end{aligned}$$

since the absolute value of the cosine function is bounded above by 1. Therefore, this completes the proof.

Exercise 2

Gina starts with a stack of n coins. On each of her turns, she selects one stack of coins that has at least two coins and splits it into two stacks, each with at least one coin. Her score for that turn is the product of the sizes of the two resulting stacks (for example, if she splits a stack of 5 coins into a stack of 3 coins and a stack of 2 coins, her score would be $3 \cdot 2 = 6$). She continues taking turns until all stacks have only one coin in them. Her score at the end is the sum of her scores in each turn. Prove that Gina's final score is the same no matter how she splits the stacks.

Solution We take a stronger claim. If Gina starts with i coins, let Gina's points be G_i.

Claim. $G_n = \dfrac{(n-1)n}{2}$.

If $n = 2$, then Gina's point is $1 \cdot 1 = 1$ since the only split possible is splitting to 1 and 1.

We divide cases into odd and even. Assume that for $i = 2, 3, \ldots, 2k$, Gina's point is $\dfrac{(i-1)i}{2}$. Then,

$$\begin{aligned}
G_{2k+1} &= (1 \cdot 2k + G_1 + G_{2k}) + \cdots + \big(k \cdot (k+1) + G_k + G_{k+1}\big) \\
&= \sum_{j=1}^{k} \big(j \cdot (2k+1-j) + G_j + G_{2k+1-j}\big) \\
&= \sum_{j=1}^{k} \left((2k+1)j - j^2 + \frac{(j-1)j}{2} + \frac{(2k-j)(2k+1-j)}{2}\right) \\
&= \sum_{j=1}^{k} \frac{2k(2k+1)}{2} \\
&= \frac{2k(2k+1)}{2}.
\end{aligned}$$

Now, suppose that for $i = 2, 3, \ldots, 2k+1$, Gina's point is $\dfrac{(i-1)i}{2}$. Then,

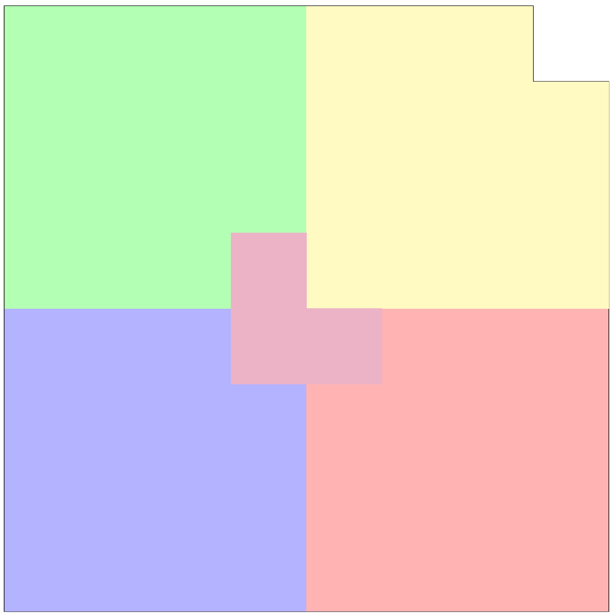
$$\begin{aligned}
G_{2k+2} &= \big(1 \cdot (2k+1) + G_1 + G_{2k+1}\big) + \cdots + \big((k+1)\cdot(k+1) + G_{k+1} + G_{k+1}\big) \\
&= \sum_{j=1}^{k+1} \big(j \cdot (2k+2-j) + G_j + G_{2k+2-j}\big) \\
&= \sum_{j=1}^{k+1} \left((2k+2)j - j^2 + \frac{(j-1)j}{2} + \frac{(2k+1-j)(2k+2-j)}{2}\right) \\
&= \frac{(2k+1)(2k+2)}{2}
\end{aligned}$$

This completes the proof by induction.

Exercise 3

Prove that for any $n \geq 1$ a $2^n \times 2^n$ checkerboard with 1×1 corner square removed can be tiled by pieces that are congruent to a 2×2 checkerboard with a 1×1 piece removed.

Solution We use induction. The base case $n = 1$ is obvious. Suppose that $n = k$ holds. That is, a $2^k \times 2^k$ checkerboard with 1×1 corner removed can be tilted by pieces that are congruent to a 2×2 checkerboard with a 1×1 piece removed. Then, we can fill in the $2^{k+1} \times 2^{k+1}$ checkerboard with 1×1 corner removed like in the figure below:

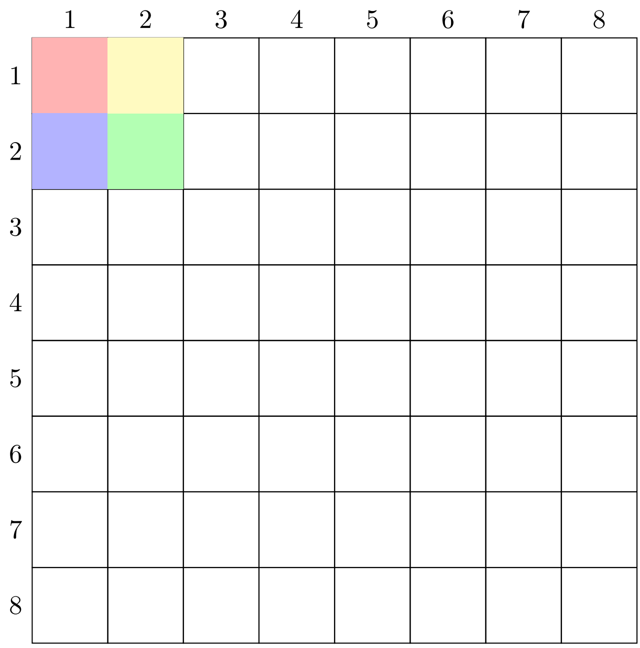


The blue, red, green, yellow figures are $2^k \times 2^k$ checkerboard with 1×1 corner removed, and the purple is 2×2 checkerboard with 1×1 corner removed. Since blue, red, green, and yellow figures can be filled up with 2×2 checkerboard with 1×1 corner removed, it is possible to fill a $2^{k+1} \times 2^{k+1}$ checkerboard with 1×1 corner removed. This completes the proof.

Exercise 4

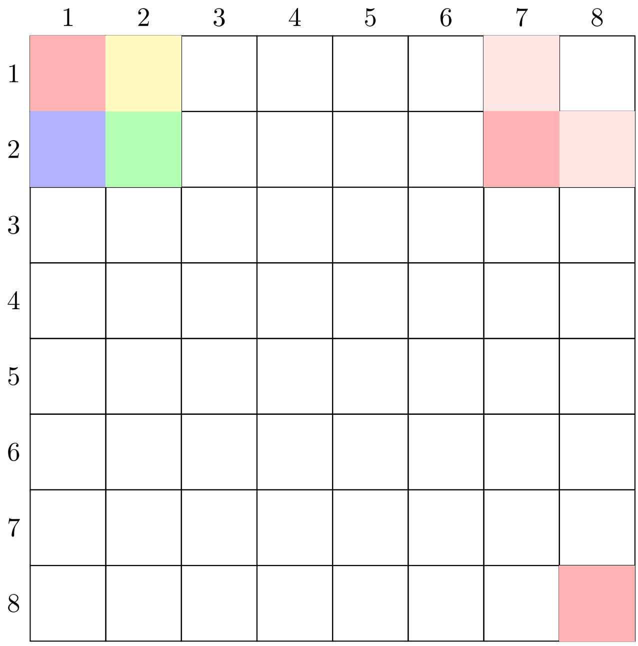
Let n be a positive integer. The cells of a $2n \times 2n$ grid are painted with one of four colors. Suppose that every 2×2 block of squares contains all four colors. Prove that the four corners of the chessboard are painted with different colors.

Solution Let the colors be red, green, blue, and yellow. We use induction. The base case $n = 1$ obviously works. Assume that the four corners should be different for $2k \times 2k$ grid. Below is a drawing for $k = 3$.



Let (m, n) be the cell at mth row and nth column. WLOG let $(1, 1)$ red, $(2, 1)$ blue, $(1, 2)$ yellow, and $(2, 2)$ green.

We have that one of $(1, 3)$ and $(2, 3)$ should be red, and the other should be blue. Then, one of $(1, 4)$ and $(2, 4)$ should be yellow, and the other should be green. Repeating this, if i is odd, then $(1, i)$ and $(2, i)$ should be red and blue, and if i is even, then $(1, i)$ and $(2, i)$ should be yellow and green. This gives that $(1, 2k + 2)$ can never be red since it is either yellow or green. Similarly, $(2k + 2, 1)$ can never be red.

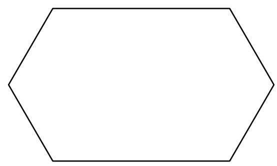


Suppose $(2k+2, 2k+2)$ is red. Then since $(2k+1, 2k+1)$ and $(2k+1, 2k+2)$ can't be red, either $(2k, 2k+1)$ or $(2k, 2k+2)$ should be red. Repeating this, we get either $(i, 2k+1)$ or $(i, 2k+2)$ should be red if and only if i is even. So one of $(2, 2k+1)$ and $(2, 2k+2)$ is red. We also had that one of $(1, 2k+1)$ and $(2, 2k+1)$ is red. However, if $(2, 2k+1)$ is not red, then $(1, 2k+1)$ and $(2, 2k+2)$ should both be red, which is impossible. Therefore, $(2, 2k+1)$ is red. Similarly, $(2k+1, 2)$ is red. However, this is a contradiction for the case $n = k$ since the $2k \times 2k$ tile in the middle has two red corners. This completes the proof.

Exercise 5

Show that for all $n > 3$ there exists an n-gon whose sides are not all equal and such that the sum of the distances from any interior point to each of the sides is constant.

Solution For n even, construct an n-gon by extending two parallel sides from a regular n-gon works. This works becase for any interior point, the sum of the distance to one side and the distance to the parallel opposite side is a constant. The figure below is an example of $n = 6$.



Claim. For $n > 3$ odd, note that for an regular n-gon, the distance from any interior point to each of the sides is constant.

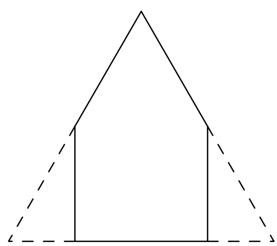
Let the distances be $d_1, d_2, \ldots, d_n$, and one side length r, a constant. Then the area of the regular n-gon is

$$S = n \cdot \frac{1}{2} \cdot r \cdot \left(\frac{1}{2} r \cdot \tan \left(90^\circ - \frac{180^\circ}{n} \right) \right),$$

which is a constant. Since we have

$$S = \frac{1}{2} r(d_1 + d_2 + \cdots + d_n),$$

$d_1 + d_2 + \cdots + d_n$ should be a constant. To construct an n-gon whose sides are not all equal, we cut out two small triangle by drawing two vertical lines at very right and very left. Below is a figure for the case $n = 5$.



This 5-gon is generated by cutting off the sides of an equilateral triangle. Let the distances to two new sides be d_{n+1} and d_{n+2}. Then for any interior point, $d_1 + d_2 + \cdots + d_n$ is a constant, and $d_{n+1} + d_{n+2}$ is a constant, so the sum of the distances is equal. This completes the proof.

3 September 3, 2024

Exercise 1

In a group of six people, show that there are either three people any two of whom aren't friends, or three people any two of whom are friends.

Solution Define the graph with six vertices by A, B, $\ldots$, F. Let e_{AB} be the edge connecting A and B, and so on. Color the edges to red if the two people connecting are friends, and blue if they're not. Then the problem changes to

> **Claim.** Prove that there is a triangle of three vertices which sides are all the same color.

In A's point of view, there are five edges connecting A and some other vertex. Then, at least three of them should be the same color. WLOG let this color be red, and let the three edge be e_{AB}, e_{AC}, and e_{AD}.

Consider the three edges e_{BC}, e_{CD}, e_{DB}. If any of these are red, then there is a triangle of all sides having red color (for example, if e_{BC} is red, then triangle ABC has all sides of red color). If none of these are red, then triangle BCD has all sides of blue color. This completes the proof.

Exercise 2

Given nine points inside a unit square, show that some three of them form a triangle whose area does not exceed 1/8.

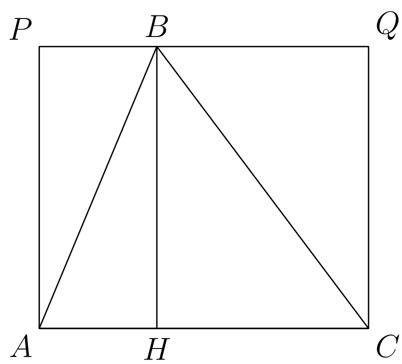
Solution Divide the unit square to four congruent squares with side lengths 1/2. Then in one of them, three points should be inside. This square has area 1/4.

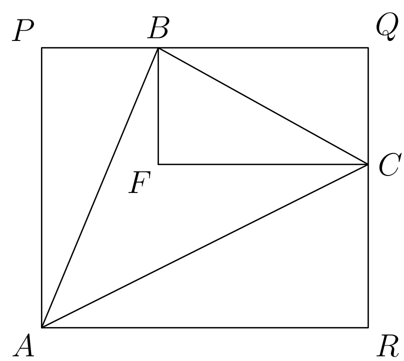
For any triangle, construct a smallest rectangle, whose sides are parallel to the axes, containing the triangle. This can be done in two ways:

1. If one of the sides are parallel to the axes, make the side coincide with one side of the rectangle and the opposite point lie on the opposite side of the square

2. If none of the sides are parallel to the axes, make one vertex coincide with one vertex of the square and the other two vertices of the two triangles lie on the edges of the square not containing the first vertex of the triangle.

The diagram for the two cases are below.





Claim. The area of the triangle is at most half of the area of the rectangle.

For the first case, let H be the feet of altitude from B to AC. Then since

$$S_{ABH} = S_{ABP} \text{ and } S_{CBH} = S_{CBQ},$$

we have $S_{ABC} = \dfrac{1}{2} S_{APQC}$.

For the second case, let F be the intersection of two lines: one passing B and parallel to AP, and one passing C and parallel to AR. Then we have

$$S_{QBC} = S_{FBC}$$

$$S_{ABP} + S_{ACR} \geq S_{ABFC}$$

so $S_{APQR} \geq 2S_{ABC}$.

Therefore, in the small square containing three points, the triangle constructed by these three points should have area at most the half of the area of the small square, which is $\frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$. This completes the proof.

Exercise 3

A chess player trains by playing at least one game per day, but, to avoid exhaustion, no more than 12 games a week. Prove that there is a group of consecutive days in which he plays exactly 20 games.

Solution Let a_n be the number of games played on days 1 to n. Then

$$\begin{aligned} a_7 &\leq 12 \\ a_{14} - a_7 &\leq 12 \\ &\vdots \\ a_{77} - a_{70} &\leq 12. \end{aligned}$$

Adding up all these gives $a_{77} \leq 132$.

Claim. There exists i, $j \in \mathbb{Z}^+$ such that $a_{i+j} = a_i + 20$.

Consider the set $A = \{a_i \mid 1 \leq 1 \leq 77\}$. Then $A \subset \{1, 2, \ldots, 132\}$. Now, construct the set $B = A + 20 = \{a_i + 20 \mid 1 \leq i \leq 77\}$. Then $B \subset \{21, 22, \ldots, 152\}$. Now,

$$|A \cup B| = |A| + |B| - |A \cap B| = 77 + 77 - |A \cap B| = 154 - |A \cap B|,$$

but since

$$A \cup B \subset \{1, 2, \ldots, 132\} \cup \{21, 22, \ldots, 152\} = \{1, 2, \ldots, 152\},$$

$|A \cup B| \leq 152$. Therefore $154 - |A \cap B| \leq 152$, so $|A \cap B| \geq 2$, which means that there is a common element in both A and B. Let this value be k, where

$$\begin{aligned} k &= a_m \text{ for some } 1 \leq m \leq 77 \\ &= a_i + 20 \text{ for some } 1 \leq i \leq 77. \end{aligned}$$

Let $m = i + j$. (Note that we can do this since $\{a_n\}$ is strictly increasing and $a_i < a_m$, so $i < m$.) Then $a_{i+j} = a_i + 20$. This completes the proof.

Exercise 4 (Putnam 1990)

Prove that any convex pentagon whose vertices (no three of which are collinear) have integer coordinates must have area greater than or equal to $5/2$.

Lemma : Pick's Theorem

A polygon whose vertices have integer coordinates has area

$$I + \frac{B}{2} - 1$$

where I is the number of lattice points in the interior and B is the number of lattice points on the boundary.

Solution Since $B \geq 5$, it suffices to prove that $I \geq 1$ or $B \geq 7$.

Claim. Any convex pentagon whose vertices have integer coordinates contain at least one interior lattice point or has at least 7 lattice points on the boundary.

Lattice points (a, b) can be divided to four kinds: either a is odd or even, and either b is odd or even. By Pigeonhole, there exists at least two lattice points of the same parity. WLOG let these lattice points A and B be the form $(\text{even}, \text{even})$.

We divide cases by the following:

1. The other three points has different parities besides $(\text{even}, \text{even})$.
2. Some of the other two points have the same parity.

For the first case, we first can find another lattice point on the boundary, the midpoint of AB. Call this point M.

- If M has parity $(\text{even}, \text{even})$, then the midpoints of AM and BM are also on the boundary, so $B \geq 8$.
- If M has parity other that $(\text{even}, \text{even})$, then the midpoint of M and the point on the boundary that has same parity with M is inside the pentagon, so $I \geq 1$.

For the second case, let the two points (other than A and B) that have the same parity be C and D. Then the midpoint of AB and the midpoint of CD are both on the boundary, so $B \geq 7$.

This completes the proof.

Exercise 5 (Putnam 1994)

Let A and B be 2×2 matrices with integer entries such that A, $A+B$, $A+2B$, $A+3B$, and $A+4B$ are all invertible matrices whose inverses have integer entries. Show that $A+5B$ is invertible and that its inverse has integer entries.

Solution We first start with a claim.

Claim. $\det(A)$ is either 1 or -1.

Since A has integer matrices, $\det(A)$ is an integer. Since A^{-1} also has integer matrices, $\det(A^{-1}) = 1/\det(A)$ is also an integer. Therefore $\det(A)$ should be either 1 or -1.

Similarly, $\det(A)$, $\det(A+B)$, $\dots$, $\det(A+4B)$ are all 1 or -1. By Pigeonhole, at least three of these should have the same value. Let this value be $k \in \{-1, 1\}$. Let

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \text{ and } B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

Then, for $n \in \mathbb{Z}^+$,

$$\det(A+nB) = \begin{vmatrix} a_1 + nb_1 & a_2 + nb_2 \\ a_3 + nb_3 & a_4 + nb_4 \end{vmatrix} = an^2 + bn + c$$

for some integer constants a, b, and c. Then the quadratic equation

$$an^2 + bn + c = k$$

has three distinct integer roots (from $\{0, 1, 2, 3, 4\}$). However, a quadratic equation can have at most two distinct roots, this gives $a = b = 0$ and $c = k$. Therefore, this equation has infinitely many roots (i.e. all integers), and $\det(A+5B) = k$. Since k is either -1 or 1, $A+5B$ is invertible and that its inverse has integer entries.

Exercise 6 (Putnam 2006)

Prove that, for every set $X = \{x_1, x_2, \dots, x_n\}$ of n real numbers, there exists a non-empty subset S of X and an integer m such that

$$\left| m + \sum_{s \in S} s \right| \le \frac{1}{n+1}.$$

Solution The problem is equivalent to proving that $\sum_{s \in S} s$ has distance at most $1/(n+1)$ from its closest integer. Define a sequence $\{a_n\}$ by $a_k = \sum_{i=1}^{k} x_i$ for $k = 1$, 2, ..., n, and define the sequence $\{I_n\}$ by the union of intervals

$$I_l = \bigcup_{p \in \mathbb{Z}} \left[p + \frac{l-1}{n+1}, p + \frac{l}{n+1} \right) \quad l = 1, 2, \dots, n+1.$$

If $a_k \in I_1$ or I_{n+1} for some k, then we are done. Suppose none of the a_ks are in I_1 or I_{n+1}. Then since a_1, ..., a_n should be in I_2, ..., I_n, by Pigeonhole, at least two of a_ks should be in the same union of intervals. That is, there exists i and $j \in \{1, 2, \dots, n\}$ such that $a_i \in I_q$ and $a_j \in I_q$ for some $q \in \{1, 2, \dots, n+1\}$. WLOG let $i > j$. Then

$$\{a_i - a_j\} = \{a_{j+1} + a_{j+2} + \cdots + a_i\} \le \frac{1}{n+1}$$

where $\{x\} = x - \lfloor x \rfloor$ indicates the fractional part of $x \in \mathbb{R}$. Since $\{a_{j+1}, a_{j+2}, \dots, a_i\}$ is nonempty and is a subset of X, there exists a nonempty subset S of X such that

$$\left\{ \sum_{s \in S} s \right\} \le \frac{1}{n+1},$$

which is equivalent to

$$\left| m + \sum_{s \in S} s \right| \le \frac{1}{n+1}$$

for some integer m.

4 September 10, 2024

Exercise 1

Find all real polynomials P satisfying

$$(x+1)P(x) = (x-10)P(x+1)$$

for all x.

Solution Substituting $x = -1$ gives $0 = -9P(0)$, so $P(0) = 0$, and substituting $x = 10$ gives $11P(10) = 0$, so $P(10) = 0$.

Claim. All integers between 0 and 10 are also roots.

Substitute $x = 1$. Then $2P(1) = -9P(2)$, but since $P(1) = 0$, $P(2) = 0$. Now, substituting $x = 2$ gives $3P(2) = -8P(3)$, so $P(3) = 0$. Repeating this until $x = 9$ gives

$$P(0) = P(1) = \cdots = P(9) = P(10) = 0.$$

Claim. Integers from 0 to 10 are the only roots.

Suppose there exists a root $a \in \mathbb{C}$ such that $a \notin \{0, 1, \ldots, 10\}$. Then substituting $x = a$ gives

$$\begin{aligned}(a+1)P(a) &= (a-10)P(a+1) \\ &= 0 \\ P(a+1) &= 0.\end{aligned}$$

Repeating this process gives infinitely many roots, namely a, $a+1$, $a+2$, ... This is a contradiction, so there does not exist a root $a \in \mathbb{C}$ such that $a \notin \{0, 1, \ldots, 10\}$.

Let

$$P(x) = x^{e_0}(x-1)^{e_1} \cdots (x-10)^{e_{10}}.$$

Then

$$\begin{aligned}(x+1)P(x) &= (x+1)x^{e_0}(x-1)^{e_1} \cdots (x-10)^{e_{10}} \\ (x-10)P(x+1) &= (x+1)^{e_0}x^{e_1} \cdots (x-9)^{e_{10}}(x-10).\end{aligned}$$

Comparing the exponents gives $1 = e_0 = e_1 = \cdots = e_9 = e_{10} = 1$. Therefore,

$$P(x) = cx(x-1)\cdots(x-10).$$

where c is a constant.

Exercise 2 (Putnam 2010)
Find all pairs of polynomials $p(x)$ and $q(x)$ with real coefficients that satisfy

$$p(x)q(x+1) - p(x+1)q(x) = 1$$

for all x.

Solution Substituting $x-1$ gives

$$\begin{aligned} p(x)q(x+1) - p(x+1)q(x) &= 1 \\ p(x-1)q(x) - p(x)q(x-1) &= 1. \end{aligned}$$

Subtracting the second from the first, we get

$$p(x)q(x+1) - p(x+1)q(x) - p(x-1)q(x) + p(x)q(x-1) = 0.$$

So

$$\begin{aligned} p(x)q(x+1) + p(x)q(x-1) &= p(x+1)q(x) + p(x-1)q(x) \\ p(x)\big(q(x+1) + q(x-1)\big) &= q(x)\big(p(x+1) + p(x-1)\big). \end{aligned}$$

Claim. $\gcd\big(p(x), q(x)\big) = 1.$

Suppose by contradiction, $\gcd\big(p(x), q(x)\big) \neq 1$. Then there exists some linear factor $x-a$ both dividing $p(x)$ and $q(x)$, where $a \in \mathbb{C}$. However, then

$$x - a \mid p(x)q(x+1) - p(x+1)q(x) = 1,$$

which is a contradiction. So $\gcd\big(p(x), q(x)\big) = 1$.

Claim. $p(x)$ and $q(x)$ are linear.

We have

$$p(x) \mid p(x)\big(q(x+1) + q(x-1)\big) = q(x)\big(p(x+1) + p(x-1)\big).$$

Since $\gcd\big(p(x), q(x)\big) = 1$, $p(x) \mid \big(p(x+1) + p(x-1)\big)$. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then

$$\frac{p(x+1) + p(x-1)}{p(x)} = \frac{2a_n x^n + \cdots}{a_n x^n + \cdots}.$$

Since this value should be a polynomial, it is 2. So $p(x+1) + p(x-1) = 2p(x)$. Rearranging gives

$$p(x+1) - p(x) = p(x) - p(x-1)$$

for all x. Therefore, $p(x+1) - p(x)$ is a constant, and $p(x)$ is linear. Similarly, $q(x)$ is also linear.

Let $p(x) = ax + b$ and $q(x) = cx + d$. Plugging in to the original formula gives

$$\begin{aligned} p(x)q(x+1) - p(x+1)q(x) &= (ax+b)(cx+c+d) - (ax+a+b)(cx+d) \\ &= bc + bd - ad - bd \\ &= bc - ad \\ &= 1. \end{aligned}$$

Therefore, the pairs of polynomials that satisfy the equation is $(ax + b, cx + d)$, where $bc - ad = 1$.

Exercise 3 (Putnam 2003)

Let $f(z) = ax^4 + bz^3 + cz^2 + dz + e = a(z - r_1)(z - r_2)(z - r_3)(z - r_4)$ where a, b, c, d, e are integers, $a \neq 0$. Show that if $r_1 + r_2$ is a rational number and $r_1 + r_2 \neq r_3 + r_4$, then $r_1 r_2$ is a rational number.

Solution By Vieta,

$$r_1 + r_2 + r_3 + r_4 = -\frac{b}{a},$$

which is rational. So $r_3 + r_4$ is rational. Then,

$$r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 = \frac{c}{a}$$

is rational by Vieta again. So

$$r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 - (r_1 + r_2)(r_3r_4) = r_1r_2 + r_3r_4$$

is also rational. Let this value be k. Now, we have

$$-\frac{d}{a} = r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4 = r_1r_2(r_1 + r_2) + r_3r_4(r_3 + r_4)$$

also rational. Then,

$$\begin{aligned} -\frac{d}{a} - (r_3 + r_4)k &= r_1r_2(r_1 + r_2) + r_3r_4(r_3 + r_4) - (r_3 + r_4)(r_1r_2 + r_3r_4) \\ &= r_1r_2(r_1 + r_2 - r_3 - r_4) \end{aligned}$$

is rational. Since both $r_1 + r_2$ and $r_3 + r_4$ are rational, $r_1 + r_2 - r_3 - r_4$ are rational, and this gives $r_1 r_2$ rational. This completes the proof.

Exercise 4 (Putnam 2018)

Let n be a positive integer, and let $f_n(z) = n+(n-1)z+(n-2)z^2+\cdots+z^{n-1}$. Prove that f_n has no roots in the closed unit disk $\{z \in \mathbb{C} : |z| \leq 1\}$.

Solution Note that $(z-1)f_n(z) = z^n + z^{n-1} + \cdots + z - n$. Suppose f_n has a root $|z|$ such that $|z| \leq 1$. Then $z^n + z^{n-1} + \cdots + z - n = 0$. We have

$$\begin{aligned} |z^n + z^{n-1} + \cdots + z| &\leq |z^n| + |z^{n-1}| + \cdots + |z| \\ &\leq n \end{aligned}$$

by the triangular inequality. Equality occurs when $z = 1$. However, since $f_n(1) \neq 0$, f_n has no roots in the closed unit disk.

5 September 17, 2024

Useful Results

Theorem : Eisenstein's Criterion

Let $a_0,\ a_1,\ \ldots,\ a_n$ be integers and p be a prime. Then the polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ cannot be factored into the product of two non-constant polynomials if p divides each of $a_0,\ a_1,\ \ldots,\ a_{n-1}$, p does not divide a_n and p^2 does not divide a_0.

Theorem : Hensel's Lemma

Let $f(x)$ be a polynomial with integer coefficients, and let $m \leq k$ be integers. If r is an integer such that

$$f(r) \equiv 0 \pmod{p^k}, \text{ and } f'(r) \not\equiv 0 \pmod{p}$$

then there exists an integer s such that

$$f(s) \equiv 0 \pmod{p^{k+m}}, \text{ and } r \equiv s \pmod{p^k}.$$

Exercise 1 (Putnam 2007)

Let f be a non-constant polynomial with positive integer coefficients. Prove that if n is a positive integer, then $f(n)$ divides $f(f(n)+1)$ if and only if $n = 1$.

Solution ($\Leftarrow$) Suppose $n = 1$.

Claim. $f(1) \mid f(f(1) + 1)$.

Note that since f is a polynomial with integer coefficients, $a - b \mid f(a) = f(b)$. Let $a = f(1) + 1$ and $b = 1$. Then

$$a - b \mid f(a) - f(b)$$
$$(f(1) + 1) - 1 \mid f(f(1) + 1) - f(1)$$
$$f(1) \mid f(f(1) + 1) - f(1),$$

so $f(1) \mid f(f(1) + 1) - f(1) + f(1) = f(f(1) + 1)$.

($\Rightarrow$) Suppose $f(n) \mid f(f(n) + 1)$. Since $f(n) = (f(n) + 1) - 1 \mid f(f(n) + 1) - f(1)$, $f(n) \mid f(1)$. Assume $n > 1$. Since f is a polynomial with positive coefficients, $f(x)$ is strictly increasing on $x \in \mathbb{R}_{>0}$. This gives $f(n) > f(1)$, which contradicts $f(n) \mid f(1)$. Therefore $n = 1$.

Exercise 2

Let p be a prime number. Show that $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

Solution Let $x = y + 1$. Then

$$\begin{aligned} f(x) &= f(y+1) \\ &= (y+1)^{p-1} + (y+1)^{p-2} + \cdots + (y+1) + 1 \\ &= y^{p-1} + \left(\binom{p-1}{1} + \binom{p-2}{0}\right) y^{p-2} + \left(\binom{p-1}{2} + \binom{p-2}{1} + \binom{p-3}{0}\right) y^{p-3} + \cdots \\ &= y^{p-1} + \sum_{k=1}^{p-2} \left(\binom{p-1}{k} + \binom{p-2}{k} + \cdots + \binom{k}{k}\right) y^k + p. \end{aligned}$$

Claim. p divides each of the coefficients from y^1 to y^{p-2}.

By the hockey-stick identity, we have

$$\binom{p-1}{k} + \binom{p-2}{k} + \cdots + \binom{k}{k} = \binom{p}{k+1}.$$

Since p is prime, $p \mid \binom{p}{k+1}$. This proves the claim. Thus $f(x)$ is irreducible by Eisenstein's criterion.

Exercise 3 (AMO 1974)

Let a, b, and c denote three distinct integers, and let P denote a polynomial having integer coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

Solution Suppose there exists a polynomial with integer coefficients such that $P(a) = b$, $P(b) = c$, and $P(c) = a$. Then

$$a - b \mid P(a) - P(b) = b - c$$

$$b - c \mid P(b) - P(c) = c - a$$

$$c - a \mid P(c) - P(a) = a - b,$$

so

$$a - b \mid b - c \mid c - a \mid a - b,$$

and $|a - b| = |b - c| = |c - a|$. Let this value be k. Then $a - b$, $b - c$, and $c - a$ can be either k or $-k$. However, none of these combinations can make $(a - b) + (b - c) + (c - a) = 0$.

Therefore, there doesn't exist a polynomial with integer coefficients such that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

Exercise 4 (Russia 2003)

The side lengths of a triangle are the roots of a cubic polynomial with rational coefficients. Prove that the altitudes of this triangle are roots of a polynomial of sixth degree with rational coefficients.

Solution In a triangle ABC, let the three side lengths be a, b, and c. Then by Vieta, $a+b+c$, $ab+bc+ca$, and abc are rational. Let h_a, h_b, h_c be the altitudes from A to BC, B to CA, and C to AB, respectively.

Claim. The square of the area of triangle is rational.

Let s be the semiperimeter. By Heron, we have $S = \sqrt{s(s-a)(s-b)(s-c)}$. Note that since $a+b+c$ is rational, s is rational. It is sufficient to prove that $(s-a)(s-b)(s-c)$ is rational. Expanding gives

$$(s-a)(s-b)(s-c) = s^3 - (a+b+c)s^2 + (ab+bc+ca)s - abc$$

and this is rational since all of s, $a+b+c$, $ab+bc+ca$, and abc are rational.

Claim. The six degree polynomial $(x^2-h_a^2)(x^2-h_b^2)(x^2-h_c^2)$ has rational coefficients.

We have

$$h_a^2 = \frac{4S^2}{a^2}$$

$$h_b^2 = \frac{4S^2}{b^2}$$

$$h_c^2 = \frac{4S^2}{c^2}$$

with S^2 rational. Expanding the sixth degree polynomial gives

$$(x^2-h_a^2)(x^2-h_b^2)(x^2-h_c^2) = x^6-(h_a^2+h_b^2+h_c^2)x^4+(h_a^2h_b^2+h_b^2h_c^2+h_c^2h_a^2)x^2-h_a^2h_b^2h_c^2$$

For each of the (absolute valeus of) coefficients,

$$h_a^2+h_b^2+h_c^2 = 4S^2\left(\frac{1}{a^2}+\frac{1}{b^2}+\frac{1}{c^2}\right)$$

$$h_a^2h_b^2+h_b^2h_c^2+h_c^2h_a^2 = 4S^2\left(\frac{1}{a^2b^2}+\frac{1}{b^2c^2}+\frac{1}{c^2a^2}\right)$$

$$h_a^2h_b^2h_c^2 = 4S^2\left(\frac{1}{a^2b^2c^2}\right)$$

and these are all rational since

$$4S^2\left(\frac{1}{a^2}+\frac{1}{b^2}+\frac{1}{c^2}\right)=4S^2\left(\frac{(ab+bc+ca)^2-2abc(a+b+c)}{(abc)^2}\right)$$
$$4S^2\left(\frac{1}{a^2b^2}+\frac{1}{b^2c^2}+\frac{1}{c^2a^2}\right)=4S^2\left(\frac{(a+b+c)^2-2(ab+bc+ca)}{(abc)^2}\right)$$
$$4S^2\left(\frac{1}{a^2b^2c^2}\right)=4S^2\left(\frac{1}{(abc)^2}\right).$$

Therefore, $(x^2-h_a^2)(x^2-h_b^2)(x^2-h_c^2)$ is a polynomial of sixth degree with rational coefficients having the altitudes of the triangle as roots.

Exercise 5 (Putnam 2008)

Let p be a prime number. Let $h(x)$ be a polynomial with integer coefficients such that $h(0)$, $h(1)$, …, $h(p^2-1)$ are distinct modulo p^2. Show that $h(0)$, $h(1)$, …, $h(p^3-1)$ are distinct modulo p^3.

Solution

Claim. $h(x+p) - h(x) \equiv ph'(x) \pmod{p^2}$.

Let $h(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where a_i are integers for $i = 1$, 2, …, n. We have

$$\begin{aligned} h(x+p) - h(x) &= a_n\big((x+p)^n - x^n\big) + a_{n-1}\big((x+p)^{n-1} - x^{n-1}\big) + \cdots + a_1 p \\ &\equiv p \cdot n a_n x^{n-1} + p \cdot (n-1)a_{n-1}x^{n-2} + \cdots + p \cdot 2a_2 x + p \cdot a_1 \pmod{p^2} \\ &= ph'(x) \pmod{p^2}. \end{aligned}$$

Claim. For all $i \in \{0, 1, \ldots, p^3-1\}$, there is some s such that $h(s) \equiv i \pmod{p^3}$.

Note that it is sufficient to prove the claim since there are p^3 choices to map to.

Take any i from the set $\{0, 1, \ldots, p^3-1\}$. Then there is some $r \in \{0, 1, \ldots, p^2-1\}$ such that $h(r) \equiv i \pmod{p^2}$. Let $f(x) = h(x) - i$. Then $f(r) \equiv 0 \pmod{p^2}$. Since

$$f(r+p) - f(r) = h(r+p) - h(r) \equiv ph'(r) \not\equiv 0 \pmod{p^2},$$

we have

$$f'(r) \equiv h'(r) \not\equiv 0 \pmod{p}.$$

Hensel's lemma with $m = 1$ gives that $f(s) \equiv 0 \pmod{p^3}$, and $r \equiv s \pmod{p^2}$. Since there is $s \in \{1, 2, \ldots, p^3-1\}$ such that $h(s) \equiv i \pmod{p^3}$, this completes the proof.

6 September 24, 2024

Exercise 1

You have 49 rectangular tiles of length 6 and width 1. You would like to cover a 21×14 room. Show that you will need to cut a tile to do this.

Solution Assign the number $i + j \pmod 6$ for each grid in the ith row and jth column. Suppose it is possible to cover the 21×14 room with 6×1 tiles. For any tile, the six grid for each tile should have all different numbers, from 0 to 5. Therefore, there should be equal numbers of 0 to 5 written in the room, 49 of each.

However, this cannot happen. In the first column, the values of $i + j$ are 2, 3, $\ldots$, 22, so there are four 2, 3, 4, and three 5, 0, 1, written. In the second column, four of 3, 4, 5 and three of 0, 1, 2 are written. Repeating this for every column, it is calculated that in the 21×14 room, 48 of 0s and 1s, 49 of 2s and 5s, and 50 of 3 and 4s are written.

Therefore, it is impossible to fill the room using only 6×1 tiles.

Exercise 2 (Putnam 2023)

Consider an m-by-n grid of unit squares, indexed by (i, j) with $1 \leq i \leq m$ and $1 \leq j \leq n$. There are $(m-1)(n-1)$ coins, which are initially placed in the squares (i, j) with $1 \leq i \leq m-1$ and $1 \leq j \leq n-1$. If a coin occupies the square (i, j) with $i \leq m-1$ and $j \leq n-1$ and the squares $(i+1, j)$, $(i, j+1)$, and $(i+1, j+1)$ are unoccupied, then a legal move is to slide the coin from (i, j) to $(i+1, j+1)$. How many distinct configurations of coins can be reached starting from the initial configuration by a (possibly empty) sequence of legal moves?

Solution We claim that the number of possible configurations is $\binom{n+m-2}{n-1}$.

Claim. There is a bijective map between all possible configurations and paths from $(1, 1)$ to (m, n) of $m-1$ horizontal steps and $n-1$ vertical steps.

(Injective) Note that the initial configuration (before any move) corresponds to a path. After a legal move, there is still a path, connecting $(i, j+1)$, (i, j), $(i+1, j)$, which is changed from the path connecting $(i, j+1)$, $(i+1, j+1)$, $(i+1, j)$.

(Surjective) Suppose that there is a path from $(1, 1)$ to (m, n) such there is no configuration possible to make a path. If this path is not the initial path (the path before any move), then there is some i and j such that the path passes $(i, j+1)$, (i, j), and $(i+1, j)$, respectively. Then we undo this move, so change the path to pass $(i, j+1)$, $(i+1, j+1)$, and $(i+1, j)$ respectively. Repeating this will eventually give the initial path, which is a contradiction since there is a configuration corresponding to the initial path. Therefore the mapping is surjective.

Thus there is a bijective map between all possible configurations and paths from $(1, 1)$ to (m, n) of $m-1$ horizontal steps and $n-1$ vertical steps. The number of possible paths are $\binom{n+m-2}{n-1}$.

Exercise 3

The numbers 1, 2, 3, ..., 2024 are written on a blackboard. Each turn you may take 4 numbers of the form a, b, c, $a+b+c$ and replace them with $a+b$, $b+c$, $c+a$. Show that you cannot do this more than 600 times.

Solution

Claim. The sum of the numbers is an invariant.

At each move, the sum of the numbers is changed by

$$\big(a+b+c+(a+b+c)\big)-\big((a+b)+(b+c)+(c+a)\big),$$

which is zero. Thus the sum of the numbers is an invariant and this value is $1+2+\cdots+2024=(2024\cdot 2025)/2$.

Claim. The sum of the square of the numbers is an invariant.

At each move, the sum of the numbers is changed by

$$\big(a^2+b^2+c^2+(a+b+c)^2\big)-\big((a+b)^2+(b+c)^2+(c+a)^2\big),$$

which is zero. Thus the sum of the square of the numbers is an invariant and this value is $1^2+2^2+\cdots+2024^2=(2024\cdot 2025\cdot 4049)/6$.

Let the numbers be $a_1, a_2, \ldots, a_n$ after each move. Then n, the number of numbers, is strictly decreasing since four numbers are replaced to three. By Cauchy-Schwarz,

$$\begin{aligned}\sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} 1^2 &\geq \left(\sum_{i=1}^{n} a_i\right)^2\\ \frac{2024\cdot 2025\cdot 4049}{6}\cdot n &\geq \left(\frac{2024\cdot 2025}{2}\right)^2\\ n &\geq \frac{6\cdot 2024\cdot 2025}{4\cdot 4049}\\ &> 1518.\end{aligned}$$

Therefore, the number of numbers should be greater than 1518, and therefore the move cannot be done more than 600 times.

Exercise 4

A rectangular floor is covered by 2×2 and 1×4 tiles. One tile got smashed. There is a tile of the other kind available. Show that the floor cannot be covered by rearranging the tiles.

Solution Let the rectangular floor be $m \times n$, where the tile at mth row, nth column is assigned the number $m + n \pmod 4$. Then, the four grids in the 1×4 tile have all different numbers, while the four grids in the 2×2 tile is consisted of three numbers where two of them are repeated.

If the 2×2 tile got smashed, the remaining numbers to fill are three numbers, which two of them are repeated. It is impossible to fill this with a 1×4 tile. Also, if the 1×4 tile got smashed, the remaining numbers to fill are four different numbers. It is impossible to fill this with a 2×2 tile. This completes the proof.

Exercise 5

Several positive integers are written on a blackboard. One can erase any two distinct integers and write their greatest common divisor and least common multiple instead. Prove that eventually the numbers will stop changing.

Solution Let the positive integers written be $a_1, a_2, \ldots, a_n$. Note that for all positive integers a and b, $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

Take any positive integers a and b with $a \neq b$, and let $g = \gcd(a, b)$. We have

$$\begin{aligned}(\gcd(a, b) + \text{lcm}(a, b)) - (a + b) &= g(a'b' - a' - b' + 1) \\ &= g(a' - 1)(b' - 1) \\ &> 0\end{aligned}$$

so each move strictly increases $\sum_{i=1}^{n} a_i$ with the amount $g(a' - 1)(b' - 1)$.

Suppose by contradiction, it is possible to change the numbers infinite times. Since the sum is strictly increasing at every move, the sum should eventually diverge to infinity. However, this is impossible since the product of all numbers integers is fixed. If we have an infinite sum of finite amount of numbers, at least one of them should be infinite, which will led to the product being infinite.

Thus it is impossible to change the numbers infinite times, and this completes the proof.

7 October 1, 2024

Exercise 1

Show that every continuous function $f : [a,b] \to [a,b]$ has a fixed point, i.e. there is $c \in [a,b]$ such that $f(c) = c$.

Solution The codomain of the function f is $[a,b]$. Let $f([a,b]) = [p,q]$. Then $a \geq p \geq q \geq b$. Define the function $g(x) = f(x) - x$. Then g has range $[p-a, q-b]$. Since $p - a > 0$ and $q - b < 0$, $\exists c \in [a,b]$ such that $g(c) = f(c) - c = 0$. Thus $\exists c \in [a,b]$ such that $f(c) = c$.

Exercise 2 (Putnam 2015)

Let A and B be points on the same branch of the hyperbola $xy = 1$. Suppose that P is a point lying between A and B on this hyperbola, such that the area of the triangle APB is as large as possible. Show that the region bounded by the hyperbola and the chord AP has the same area as the region bounded by the hyperbola and the chord PB.

Solution Let $A\left(a, \frac{1}{a}\right)$ and $B = \left(b, \frac{1}{b}\right)$. WLOG let $a, b > 0$, $a < b$, and let $P\left(x, \frac{1}{x}\right)$ where $a < x < b$. Shoelace formula on $\triangle APB$ gives

$$\begin{aligned} S_{APB} &= \frac{1}{2}\begin{vmatrix} a & 1/a \\ b & 1/b \\ x & 1/x \\ a & 1/a \end{vmatrix} \\ &= \frac{1}{2}\left|\frac{a}{b} - \frac{b}{a} + \frac{b}{x} - \frac{x}{b} + \frac{x}{a} - \frac{a}{x}\right| \\ &= \frac{1}{2}\left|(b-a)\left(\frac{1}{x} + \frac{x}{ab} - \frac{1}{a} - \frac{1}{b}\right)\right| \\ &= \frac{1}{2}\left|\frac{1}{x}(b-a)\left(\frac{x}{a} - 1\right)\left(\frac{x}{b} - 1\right)\right|. \end{aligned}$$

Since $a < x < b$, the value inside the absolute value is negative, so

$$S_{APB} = -\frac{1}{2}(b-a)\left(\frac{1}{x} + \frac{x}{ab} - \frac{1}{a} - \frac{1}{b}\right).$$

To maximize this value, we need to minimize $\dfrac{1}{x} + \dfrac{x}{ab}$, which happens at $x = \sqrt{ab}$ by the AM-GM inequality. Thus $P\left(\sqrt{ab}, \dfrac{1}{\sqrt{ab}}\right)$.

We have the following equations for line AP and PB:

$$\begin{aligned} AP : y &= -\frac{1}{\sqrt{a^3 b}}x + \frac{1}{\sqrt{ab}} + \frac{1}{a} \\ PB : y &= -\frac{1}{\sqrt{ab^3}}x + \frac{1}{\sqrt{ab}} + \frac{1}{b}. \end{aligned}$$

The area of the region bounded by the hyperbola and the chord AP is

$$\begin{aligned} \int_a^{\sqrt{ab}} \left(-\frac{1}{\sqrt{a^3 b}}x + \frac{1}{\sqrt{ab}} + \frac{1}{a} - \frac{1}{x}\right)\, dx &= -\frac{1}{2}\frac{1}{\sqrt{a^3 b}}x^2 + \left(\frac{1}{\sqrt{ab}} + \frac{1}{a}\right)x - \ln x\Big|_a^{\sqrt{ab}} \\ &= -\frac{1}{2}\sqrt{\frac{b}{a}} + \frac{1}{2}\sqrt{\frac{a}{b}} + \frac{b-a}{\sqrt{ab}} - \frac{1}{2}\ln\frac{b}{a}. \end{aligned}$$

The area of the region bounded by the hyperbola and the chord AP is

$$\begin{aligned}\int_{\sqrt{ab}}^{b}\left(-\frac{1}{\sqrt{ab^3}}x+\frac{1}{\sqrt{ab}}+\frac{1}{b}-\frac{1}{x}\right)\,dx &= -\frac{1}{2}\frac{1}{\sqrt{ab^3}}x^2+\left(\frac{1}{\sqrt{ab}}+\frac{1}{b}\right)x-\ln x\Big|_{\sqrt{ab}}^{b} \\ &= -\frac{1}{2}\sqrt{\frac{b}{a}}+\frac{1}{2}\sqrt{\frac{a}{b}}+\frac{b-a}{\sqrt{ab}}-\frac{1}{2}\ln\frac{b}{a}.\end{aligned}$$

Therefore, the region bounded by the hyperbola and the chord AP has the same area as the region bounded by the hyperbola and the chord PB.

Exercise 3

Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. For $x \in \mathbb{R}$, define

$$g(x) = f(x) \int_0^x f(t)\ dt.$$

Show that if g is a (not necessarily strictly) decreasing function (i.e. for $a < b$, $g(a) \geq g(b)$) then f is identically equal to 0.

Solution Let $F(x) = \displaystyle\int_0^x f(t)\ dt$. Then $F'(x) = f(x)$. So $g(x) = F'(x)F(x)$. Taking the antiderivative gives

$$\int g(x) = \int F'(x)F(x) = \frac{1}{2}\big(F(x)\big)^2 + C.$$

Let $G(x) = \dfrac{1}{2}(F(x))^2 + C$. Then $G(0) = C$, and $G(x) \geq C$ for all x. Since $G'(0) = g(0) = 0$, $g(x) \leq 0$ if $x \geq 0$. If we choose $a > 0$, then

$$\frac{G(a) - G(0)}{a - 0} = g(b)$$

for some $b \in (0, a)$ by the Mean Value Theorem. However, the left-hand side is equal or greater than zero, and the right side is equal or less than zero. Thus

$$\frac{G(a) - G(0)}{a - 0} = g(b) = 0.$$

Since $a > 0$ was arbitrary, $G(x) = G(0) = C$ for all $x \geq 0$.

Now, choose $a' < 0$. Then

$$\frac{G(a') - G(0)}{a' - 0} = g(b')$$

for some $b \in (a', 0)$ by the Mean Value Theorem. Since g is monotonically decreasing, $g(b') \geq 0$. The left-hand side above is equal or less than zero, and the right side is equal or greater than zero. Thus

$$\frac{G(a') - G(0)}{a' - 0} = g(b') = 0.$$

Since $a' < 0$ was arbitrary, $G(x) = G(0) = c$ for all $x \leq 0$.

Thus $G(x) = C$ for all x, and $F(x) = 0$ for all x. Therefore $F'(x) = f(x) = 0$ for all x, and f is identically zero.

Exercise 4
Compute
$$\int (x^6 + x^3)\sqrt[3]{x^3+2}\ dx.$$

Solution Note that
$$\int (x^6 + x^3)\sqrt[3]{x^3+2}\ dx = \int (x^5 + x^2)\sqrt[3]{x^6+2x^3}\ dx.$$
Let $x^6 + 2x^3 = u$. Then $du = 6(x^5 + x^2)dx$. Thus
$$\begin{aligned}\int (x^6 + x^3)\sqrt[3]{x^3+2}\ dx &= \int (x^5 + x^2)\sqrt[3]{x^6+2x^3}\ dx \\ &= \frac{1}{6}\int \sqrt[3]{u}\ du \\ &= \frac{1}{6}\cdot\frac{3}{4}u^{4/3} + C \\ &= \frac{1}{8}(x^6 + 2x^3)^{4/3} + C \\ &= \frac{1}{8}x^4(x^3+2)^{4/3} + C.\end{aligned}$$

Exercise 5 (Putnam 1987)

Curves A, B, C, and D are defined in the plane $\mathbb{R}^2$ as follows:

$$A = \left\{(x, y) : x^2 - y^2 = \frac{x}{x^2 + y^2}\right\},$$

$$B = \left\{(x, y) : 2xy + \frac{y}{x^2 + y^2} = 3\right\},$$

$$C = \{(x, y) : x^3 - 3xy^2 + 3y = 1\},$$

$$D = \{(x, y) : 3x^2y - 3x - y^3 = 0\}.$$

Prove that $A \cap B = C \cap D$.

Solution Let $z = x + iy$. Then the curves can be written as

$$A = \{z : \Re(z^2) = \Re(1/z)\}$$

$$B = \{z : \Im(z^2) - \Im(1/z) = 3\}$$

$$C = \{z : \Re(z^3) + 3\Im(z) = 1\}$$

$$D = \{z : \Im(z^3) - 3\Re(z) = 0\}.$$

($\subseteq$) Suppose $z \in A \cap B$. Then

$$\Re(z^2) = \Re(1/z)$$

$$\Im(z^2) = \Im(1/z) + 3.$$

Adding the bottom equation multiplied by i to the top equation gives $z^2 = 1/z + 3i$, so $z^3 - 3iz = 1$. Then

$$\Re(z^3 - 3iz) = \Re(1 + 0i) = 1$$

$$\Im(z^3 - 3iz) = \Im(1 + 0i) = 0.$$

Since $\Re(z^3 - 3iz) = x^3 - 3xy^2 + 3y$ and $\Im(z^3 - 3iz) = 3x^2y - 3x - y^3$, $z \in C$ and $z \in D$, so $z \in C \cap D$.

($\supseteq$) Suppose $z \in C \cap D$. Then

$$\Re(z^3 - 3iz) = 1$$

$$\Im(z^3 - 3iz) = 0,$$

so $z^3 - 3iz = 1$. Since $z \neq 0$ (because if $z = 0$, $z \notin C$), $z^2 - 1/z = 3i$. Thus

$$\begin{aligned} \Re(z^2) - \Re(1/z) &= 0 \\ \Re(z^2) &= \Re(1/z) \\ \Im(z^2) - \Im(1/z) &= 3. \end{aligned}$$

So $z \in A$ and $z \in B$, and hence $z \in A \cap B$.

8 October 15, 2024

Exercise 1 (British Math Olympiad 1980)

Find all a_0 such that the sequence defined by $a_{n+1} = 2^n - 3a_n$ for $n \geq 0$ is increasing.

Solution We start with a formula of a_n in terms of a_0.

Claim. $a_n = \dfrac{2^n - (-3)^n}{5} + (-3)^n a_0.$

We use induction to prove the claim. For $n = 1$, $a_1 = \dfrac{2+3}{5} - 3a_0 = 1 - 3a_0$.

Suppose $a_k = \dfrac{2^k - (-3)^k}{5} + (-3)^k a_0$ for some $k \in \mathbb{Z}^+$. Then

$$\begin{aligned}
a_{k+1} &= 2^k - 3a_k \\
&= 2^k - 3\left(\frac{2^k - (-3)^k}{5} + (-3)^k a_0\right) \\
&= \frac{2^{k+1} + 3 \cdot (-3)^k}{5} - 3 \cdot (-3)^k a_0 \\
&= \frac{2^{k+1} - (-3)^{k+1}}{5} + (-3)^{k+1} a_0.
\end{aligned}$$

To make the sequence $\{a_n\}$ increasing, since $(-3)^n$ dominates 2^n and oscillates between positive and negative, the constant multiplied to $(-3)^n$ should be zero. Thus $a_0 = 1/5$.

Exercise 2 (Iberoamerican Math Olympiad 2009)
The sequence $\{a_n\}_{n=1}^{\infty}$ satisfies $a_1 = 1$ and for $n \geq 1$,

$$a_{2n} = a_n + 1, \text{ and } a_{2n+1} = \frac{1}{a_{2n}}.$$

Prove that every positive rational number occurs in the sequence.

Solution Note that it is sufficient to prove that every positive rational number $r > 1$ appears in the sequence since the term right after will always be smaller than 1.

Claim. n is even if and only if $a_n > 1$.

First notice that all terms in the sequence are positive. By contradiction, suppose there exists some even n such that $a_n < 1$. Then $a_{n/2} = a_n - 1 < 0$, which is impossible. So $a_n > 1$ for even n. Now, suppose that there exists some odd n such that $a_n > 1$. Then $a_{n-1} < 1$ with $n-1$ even, which is impossible. This proves the claim.

Claim. For p, $q \in \mathbb{Z}^+$ with $\gcd(p,q) = 1$ and $p > q$, $\dfrac{p}{q}$ appears in the sequence.

We prove with induction on $p + q$. If $p + q = 3$, the only possible case is $(p,q) = (2,1)$, which is a_2.

Now, suppose every $p/q > 1$ appears in the sequence for $p + q \leq k$ for some $k \in \mathbb{Z}^+$.

We claim that every p/q when $\gcd(p,q) = 1$ and $p + q = k + 1$ appears in the sequence. Suppose not so that there exists some $p_0/q_0 > 1$ that doesn't appear in the sequence. Then $p_0/q_0 - 1$ also should not appear in the sequence since if $a_n = p_0/q_0 - 1$ for some n, $a_{2n} = p_0/q_0$. This contradicts that every rational of the form p/q with $\gcd(p,q) = 1$ and $p + q \leq k$ appears in the sequence since

$$\frac{p_0}{q_0} - 1 = \frac{p_0 - q_0}{q_0}$$

and $p_0 - q_0 + q_0 = p_0 \leq k$.

This completes the proof by induction.

Exercise 3 (Putnam 2017)

Suppose that $f(x) = \sum_{i=0}^{\infty} c_i x^i$ is a power series for which each coefficient c_i is 0 or 1. Show that if $f(2/3) = 3/2$, then $f(1/2)$ must be irrational.

Solution Suppose by contradiction that $f(1/2)$ is rational. Then

$$f\left(\frac{1}{2}\right) = \sum_{i=0}^{\infty} \frac{c_i}{2^i} \in \mathbb{Q}$$

so c_i eventually repeats. Suppose this repetition starts from a_n and has period m so that

$$\begin{aligned} c_{n+km} &= c_n \\ c_{n+1+kn} &= c_{n+1} \\ \vdots &= \vdots \\ c_{n+m-1+km} &= c_{n+m-1} \end{aligned}$$

for all $k \in \mathbb{Z}^+$. Then

$$\begin{aligned} & f\left(\frac{2}{3}\right) \\ &= c_0 + c_1 \cdot \frac{2}{3} + c_2\left(\frac{2}{3}\right)^2 + \cdots + c_{n-1}\left(\frac{2}{3}\right)^{n-1} + c_n\left(\frac{2}{3}\right)^n + \cdots + c_{n+m-1}\left(\frac{2}{3}\right)^{n+m-1} \\ &\qquad + c_n\left(\frac{2}{3}\right)^{n+m} + \cdots + c_{n+m-1}\left(\frac{2}{3}\right)^{n+2m-1} \\ &\qquad + \cdots \\ &= c_0 + c_1 \cdot \frac{2}{3} + c_2\left(\frac{2}{3}\right)^2 + \cdots + c_{n-1}\left(\frac{2}{3}\right)^{n-1} + \frac{c_n\left(\frac{2}{3}\right)^n + \cdots + c_{n+m-1}\left(\frac{2}{3}\right)^{n+m-1}}{1-\left(\frac{2}{3}\right)^m}, \end{aligned}$$

which has a odd common denominator. Thus $f(2/3)$ can never be $3/2$, which is a contradiction. Therefore, $f(1/2)$ is irrational.

Exercise 4 (Putnam 2010)

Is there an infinite sequence of real numbers $a_1, a_2, a_3, \ldots$ such that

$$a_1^m + a_2^m + a_3^m + \cdots = m$$

for every positive integers m?

Solution We first start with a claim.

Claim. Some of the terms has absolute value greater than 1.

Suppose not, so that every term has absolute value equal or smaller than 1. Define the sequence $\{b_n\}$ by $b_n = \sum_{i=1}^{\infty} a_i^n$. Then $\lim_{n\to\infty} b_n = 0$ since $|a_i|^n \to 0$ as $n \to \infty$. This contradicts that $a_1^m + a_2^m + \cdots = m$ since the LHS eventually goes to 0 and RHS eventually goes to infinity. Thus it is impossible to have every term's absolute value equal or smaller than 1.

The claim above gives that there is some a_k in the sequence such that $|a_k| > 1$. Then, for sufficiently large n,

$$a_1^{2n} + a_2^{2n} + \cdots \geq a_k^{2n} > 2n$$

since exponential functions of base greater than 1 eventually gets greater than linear functions.

Therefore, it is impossible to have $a_1^m + a_2^m + a_3^m + \cdots = m$ for all $m \in \mathbb{Z}^+$.

9 October 22, 2024

Useful Results

Definition : Cauchy Sequence

In a metric space, a sequence $\{a_n\}$ is called a **Cauchy sequence** if for all $\epsilon > 0$, there is $N \in \mathbb{Z}^+$ such that

$$\forall m, n > N, \qquad |a_m - a_n| < \epsilon.$$

Theorem : Cauchy Criterion

In a complete metric space, a sequence is convergent if and only if it is a Cauchy sequence.

Exercise 1 (Putnam 1988)

Prove that if $\sum_{n=1}^{\infty} a_n$ is a convergent series of positive real numbers, then so is $\sum_{n=1}^{\infty} (a_n)^{n/(n+1)}$.

Solution

Claim. $(a_n)^{n/(n+1)} < ca_n$ for some constant c if and only if $a_n > \dfrac{1}{c^{n+1}}$.

We have

$$\begin{aligned}(a_n)^{n/(n+1)} &< ca_n\\ (a_n)^n &< c^{n+1}(a_n)^{n+1}\\ \frac{1}{c^{n+1}} &< a_n.\end{aligned}$$

If $a_n > \dfrac{1}{2^{n+1}}$, then $(a_n)^{n/(n+1)} < 2a_n$. If $a_n \le \dfrac{1}{2^{n+1}}$, we have $(a_n)^{n/(n+1)} \le \dfrac{1}{2^n}$. In either case, we have

$$(a_n)^{n/(n+1)} < 2a_n + \frac{1}{2^n}.$$

Thus,

$$\sum_{n=1}^{\infty}(a_n)^{n/(n+1)} < 2\sum_{n=1}^{\infty} a_n + \sum_{n=1}^{\infty}\frac{1}{2^n} = 2\sum_{n=1}^{\infty} a_n + 1.$$

Since the left side converge, the right side should also converge, which completes the proof.

Exercise 2 (Putnam 1990)
Is $\sqrt{2}$ the limit of sequence of numbers of the form $\sqrt[3]{m} - \sqrt[3]{n}$ for non-negative integers m, n?

Claim. $(n+1)^{1/3} - n^{1/3} \to 0$ as $n \to \infty$.

It is suffient to prove that $\forall \epsilon > 0$, there is N such that if $n > N$, then $(n+1)^{1/3} - n^{1/3} < \epsilon$.

Fix $\epsilon > 0$, and let $N = \dfrac{1}{27\epsilon^6}$. Then

$$\begin{aligned} \epsilon^3 + 3\epsilon^2 n^{1/3} + 3\epsilon n^{2/3} &> 3\epsilon^2 n^{1/3} \\ &> 3\epsilon^2 \cdot \left(1/27\epsilon^6\right)^{1/3} \\ &> 1 \end{aligned}$$

and

$$\begin{aligned} (\epsilon + n^{1/3})^3 &= \epsilon^3 + 3\epsilon^2 n^{1/3} + 3\epsilon n^{2/3} + n \\ &> n+1, \end{aligned}$$

so $(n+1)^{1/3} < \epsilon + n^{1/3}$ and $(n+1)^{1/3} - n^{1/3} < \epsilon$.

Claim. Let a and k be integers. If a is fixed, then the sequence $\{a_k\}$ defined by $a_k = (a+k)^{1/3} - a^{1/3}$ is unbounded.

Since a is fixed, $a^{1/3}$ is fixed. Letting $k \to \infty$ gives $(a+k)^{1/3} \to \infty$, to $a_k \to \infty$ and $\{a_k\}$ is unbounded.

Claim. For all $\epsilon > 0$, we can find a pair (m, n) such that $|\sqrt[3]{m} - \sqrt[3]{n} - \sqrt{2}| < \epsilon$.

Fix $\epsilon > 0$. Then there is N such that if $n > N$, then $(n+1)^{1/3} - n^{1/3} < \epsilon$. Fix $n > N$. Then there is some integer k such that

$$(n+k)^{1/3} - n^{1/3} < \sqrt{2} < (n+k+1)^{1/3} - n^{1/3}$$

since the sequence $\{n_k\}$ defined by $n_k = (n+k)^{1/3} - n^{1/3}$ is unbounded. Since

$$\left((n+k)^{1/3} - n^{1/3}\right) - \left((n+k+1)^{1/3} - n^{1/3}\right) = (n+k+1)^{1/3} - (n+k)^{1/3} < \epsilon,$$

we should have $|(n+k)^{1/3} - n^{1/3} - \sqrt{2}| < \epsilon$ or $|(n+k+1)^{1/3} - n^{1/3} - \sqrt{2}| < \epsilon$. This completes the proof with $(m, n) = (n+k+1, n)$ or $(n+k, n)$.

Exercise 3 (Putnam 2016)

Let $x_0, x_1, x_2, \ldots$ be the sequence such that $x_0 = 1$ and for $n \geq 0$,

$$x_{n+1} = \ln(e^{x_n} - x_n).$$

Show that the infinite series $x_0 + x_1 + x_2 + \cdots$ converges and find its sum.

Solution Let $y_n = e^{x_n}$ for $n \geq 0$. Then $e^{x_{n+1}} = e^{x_n} - x_n$ gives $y_{n+1} - y_n = -\ln y_n = -x_n$. We have

$$\sum_{n=0}^{\infty} x_n = \sum_{n=0}^{\infty} (y_n - y_{n+1}) = \lim_{n\to\infty} (y_1 - y_n).$$

Claim. The sequence $\{x_n\}$ converges.

We first prove that all terms in $\{x_n\}$ is positive. x_n is clearly positive when $n = 0$. Suppose x_k is positive. Then

$$\begin{aligned} e^{x_{k+1}} - x_{k+1} &= \left(1 + x_{k+1} + \frac{1}{2!}x_{k+1}^2 + \cdots\right) - x_{k+1} \\ &= 1 + \frac{1}{2!}x_{k+1}^2 + \frac{1}{3!}x_{k+1}^3 + \cdots \\ &> 1. \end{aligned}$$

So $e^{x_{k+1}} - x_{k+1} > 1$, and $x_{k+1} \ln(e^{x_{k+1}} - x_{k+1}) > 0$. This proves that x_n is positive for all $n \geq 0$ by induction. Now, since $e^{x_n} - x_n < e^{x_n}$, we have

$$x_{n+1} = \ln(e^{x_n} - x_n) < \ln(e^{x_n}) = x_n,$$

so $\{x_n\}$ is strictly decreasing. Since the sequence $\{x_n\}$ is bounded below by 0, $\{x_n\}$ converges by the monotone convergence theorem. Thus $\{y_n\}$ also converges. Therefore,

$$\sum_{n=0}^{\infty} x_n = y_0 - \lim_{n\to\infty} y_n = e - \lim_{n\to\infty} e^{x_n}$$

Which gives that $\sum_{n=0}^{\infty} x_n$ converges. Since $\sum_{n=0}^{\infty} x_n$ converges, $\lim_{n\to\infty} x_n = 0$, so

$$\sum_{n=0}^{\infty} x_n = e - \lim_{n\to\infty} e^0 = e - 1.$$

10 October 29, 2024

Tips

- Consider the convex hull.
- In a set of points, consider the extremes (the farthest points, the largest triangle, the smallest triangle, etc)

Exercise 1

Show that there are no equilateral triangles in $\mathbb{R}^2$ whose vertices all have integer coordinates.

Solution Suppose there is an equilateral triangle in $\mathbb{R}_2$ with all vertices in integer coordinates. WLOG fix one point $O(0,0)$. Let $A(a,b)$ and $B(c,d)$, and X be any point on the x-axis. If we let $\angle AOX = \theta$, then $\angle BOX = \theta + 60°$. We have

$$\tan\theta = \frac{a}{b}$$
$$\tan(\theta + 60°) = \frac{c}{d}.$$

By the tangent addition formula,

$$\begin{aligned}\tan(\theta + 60°) &= \frac{\tan\theta + \sqrt{3}}{1 - \sqrt{3}\tan\theta}\\ &= \frac{\frac{a}{b} + \sqrt{3}}{1 - \sqrt{3}\frac{a}{b}}\\ &= \frac{a + \sqrt{3}b}{b - \sqrt{3}a}\\ &= \frac{(a + \sqrt{3}b)(b + \sqrt{3}a)}{b^2 - 3a^2}\\ &= \frac{4ab + \sqrt{3}(a^2 + b^2)}{b^2 - 3a^2}\\ &= \frac{c}{d}.\end{aligned}$$

So $\dfrac{4ab + \sqrt{3}(a^2 + b^2)}{b^2 - 3a^2}$ should be rational, but this is impossible unless $a = b = 0$, which is a contradiction. Therefore, there are no equilateral triangles in $\mathbb{R}^2$ whose vertices all have integer coordinates.

Exercise 2 (Putnam 2008)

What is the maximum number of rational points that can lie on a circle in $\mathbb{R}^2$ whose center is not a rational point? (A *rational point* is a point both of whose coordinates are rational numbers.)

Solution Note that it is possible to find two rational points that lie on a circle whose center is not a rational point. If we let the center $(1, \sqrt{2})$, then there are two rational points $(0, 0)$ and $(2, 0)$ that lies on a circle of radius $\sqrt{3}$ and center $(1, \sqrt{2})$.

Claim. The maximum number of rational points is two.

Suppose there are three rational points A, B, and C that lie on a circle whose center is not a rational point.

If the three points all have different x and y-coordinates, the equations of line AB and AC will both be of the form $y = mx+n$, where m and n are rational numbers. Let P and Q be the midpoints of AB and AC, respectively. Then P and Q are rational points. Then perpendicular bisector of AB and AC both be of the form $y = px + q$, where p and q are rational points. Since these two lines meet at the center, solving the system of linear equations should give that the center is also the rational point, which is a contradiction.

If two of the points have the same y-coordinates, WLOG say A and B. Then the perpendicular bisector of AB will be of the form $x = k$, where k is rational. Since the perpendicular bisector of AC will still be a line with rational coefficients, this also gives that the center is a rational point.

Therefore, it is impossible to have three rational points on a circle with center not a rational point, so the maximum number of points is two.

Exercise 3 (Putnam 2010)

Given that A, B, and C are noncollinear points in the plane with integer coordinates such that the distances AB, AC, and BC are integers, what is the smallest possible value of AB?

Solution Note that $AB = 3$ is achievable by setting $A(0, 0)$, $B(3, 0)$, and $C(3, 4)$. We claim that this is the smallest value.

Let $AB = 1$. Then by the triangular inequality, $AB + BC > AC$, but since BC and AC are integers, $BC = AC$. This is a contradiction since the C should lie on $x = 1/2$.

Now, let $AB = 2$, and WLOG let $A(0, 0)$ and $B(2, 0)$, and let AC the longest side. By the triangular inequality, $AB + BC > AC$, so $AC = BC + 1$ or $AC = BC$.

If $AC = BC$, $C(1, y)$. However, $AC^2 = 1 + y^2$ cannot be a perfect square.

If $AC = BC + 1$, let $C(x, y)$. Then $S_{ABC} = \frac{1}{2} \cdot 2 \cdot y = y$, which is an integer. Let $BC = a$. Then $s = \frac{1}{2}(2a + 3)$, which is odd. By Heron,

$$S_{ABC}^2 = s(s-2)(s-a)(s-a-1) = \frac{1}{16}(2a+3)(2a-1) \cdot 3 \cdot 1$$

which is not an integer, a contradiction.

Therefore, $AB = 1$ and $AB = 2$ is not possible, and the smallest possible value of AB is 3.

Exercise 4

Find all sets S of finitely many points in the plane, no three of which are collinear and such that for any three points A, B, C in S, there is another point D in S such that A, B, C, D (in some order) are the vertices of a parallelogram.

Solution We claim that all sets of S are the sets of four points which forms a parallelogram.

Consider the parallelogram $ABCD$ formed by the points of S that has the largest area.

Claim. It is impossible to have a fifth point $X \in S$ outside of $ABCD$.

Suppose such X exists. Let h_1 be the distance from D to AB, p the distance between X and AB, and q the distance between X and CD. Then $\max\{p,q\} > h_1$. WLOG let $p > h_1$. Since X, A, $B \in S$, there is some $Y \in S$ such that either $XAYB$, $XYAB$, or $XABY$ is a parallelogram. For any of these three, its area is the twice of S_{XAB}, which is

$$2 \cdot \frac{1}{2} \cdot AB \cdot p > AB \cdot h_1 > S_{ABCD}.$$

This contradicts that $ABCD$ is the parallelogram with the largest area, so X cannot be outside of $ABCD$.

Claim. It is impossible to have a fifth point $X \in S$ inside of $ABCD$.

Suppose such X exists. Since X, A, $B \in S$, there is some $Y \in S$ such that either $XAYB$, $XYAB$, or $XABY$ is a parallelogram.

If $XAYB$ is a parallelogram, Y is the reflection of X across the midpoint of AB and X is inside $ABCD$, Y should be outside of $ABCD$. If either $XYAB$ or $XABY$ is a parallelogram, then $XY \parallel AB$. But since $XY = AB$, so one of X and Y should be outside of $ABCD$ or both should lie on the sides of $ABCD$. However, if X and Y lie on the sides of the parallelogram, we have three collinear points, so it is impossible to make X and Y both lie on the sides of the parallelogram.

For any of the three cases, Y is outside of $ABCD$, which cannot happen by the first claim. Therefore, there couldn't be a fifth point besides A, B, C, and D, and this completes the proof.

11 November 5, 2024

Useful Results

Theorem

Trace is a linear map. That is, if A and B are $n \times n$ matrices and α and β are constants, then

$$\operatorname{tr}(\alpha A + \beta B) = \alpha \operatorname{tr}(A) + \beta \operatorname{tr}(B).$$

Theorem

$\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Theorem

eterminant is multiplicative. That is, for any $n \times n$ matrices over the same commutative field, $\det(AB) = \det(A) \cdot \det(B)$.

Definition : Characteristic Polynomial

Suppose A is a $n \times n$ matrix over a field K. The **characteristic polynomial** of A is defined as $P_A(t) = \det(tI - A)$, which is a nth degree polynomial in t.

Definition : Eigenvalue and Eigenvector

An **eigenvector** $\mathbf{v} \in K^n$ is a non-zero vector that satisfies the relation $A\mathbf{v} = \lambda\mathbf{v}$, for some scalar $\lambda \in K$. The value λ is called the **eigenvalue**.

The eigenvalues of a square matrix are the roots of the characteristic polynomial of the matrix.

Theorem : Cayley-Hamilton

Let P be the characteristic polynomial of A. Then $P(A) = 0$.

Theorem : Jordan Normal Form Theorem

For any $n \times n$ matrix A over $\mathbb{C}$, there is an invertible matrix U such that UAU^{-1} can be written in Jordan normal form, which is of the form

$$\begin{pmatrix} r & 1 & 0 & \cdots & 0 \\ 0 & r & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r \end{pmatrix}$$

where r is an eigenvalue. If the characteristic polynomial has distinct roots, then the blocks can be taken to be 1×1, i.e. the matrix is diagonalizable.

- Over $\mathbb{C}$, diagonalizable matrices are dense in the space of matrices seen as $\mathbb{C}^{n \times n}$.
- If A is an $n \times n$ matrix over a field K, with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, and P is any polynomial in $K[x]$, then $P(A)$ has eigenvalues $P(\lambda_i)$.

Exercise 1 (Putnam 2014)
Let A be the $n \times n$ matrix whose entry in the i-th row and j-th column is

$$\frac{1}{\min(i,j)}$$

for $1 \le i,\ j \le n$. Compute $\det(A)$.

Solution We have

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n}. \end{pmatrix}.$$

Then

$$\begin{aligned}
\det(A) &= \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{3} & \frac{1}{3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n-1} & \frac{1}{n-1} \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n-1} & \frac{1}{n} \end{pmatrix} \\
&= \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{3} & \frac{1}{3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n-1} & \frac{1}{n-1} \\ 0 & 0 & 0 & \cdots & 0 & \frac{1}{n(n-1)} \end{pmatrix} \\
&= \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} \\ 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{3} & \frac{1}{3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -\frac{1}{(n-1)(n-2)} & \frac{1}{n-1} \\ 0 & 0 & 0 & \cdots & 0 & -\frac{1}{n(n-1)} \end{pmatrix} \\
&= \cdots
\end{aligned}$$

$$= \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & -\frac{1}{6} & * & \cdots & * & * \\ 0 & 0 & -\frac{1}{12} & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -\frac{1}{(n-1)(n-2)} & \frac{1}{n-1} \\ 0 & 0 & 0 & \cdots & 0 & -\frac{1}{n(n-1)} \end{pmatrix}.$$

Since the last matrix is an upper triangular matrix, the determinant is the product of all diagonal entries. Therefore

$$\det(A) = \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & -\frac{1}{6} & * & \cdots & * & * \\ 0 & 0 & -\frac{1}{12} & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -\frac{1}{(n-1)(n-2)} & \frac{1}{n-1} \\ 0 & 0 & 0 & \cdots & 0 & -\frac{1}{n(n-1)} \end{pmatrix} = \frac{(-1)^{n-1}}{(n-1)!n!}.$$

Exercise 2

Suppose A and B are $n \times n$ real matrices such that $\operatorname{tr}(AA^T + BB^T) = \operatorname{tr}(AB + A^T B^T)$. Show that $A = B^T$.

Solution We have

$$\begin{aligned}
\operatorname{tr}(AA^T + BB^T) - \operatorname{tr}(AB + A^T B^T) &= \operatorname{tr}(AA^T + BB^T - AB - A^T B^T) \\
&= \operatorname{tr}\left((A - B^T)(A^T - B)\right) \\
&= \operatorname{tr}\left((A - B^T)(A - B^T)^T\right) \\
&= 0.
\end{aligned}$$

Claim. For a $n \times n$ matrix M, if $\operatorname{tr}(MM^T) = 0$, M is the zero matrix.

Let

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Then

$$MM^T = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$$

and $\operatorname{tr}(MM^T) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}^2$. So if $\operatorname{tr}(MM^T) = 0$, all entries of M should be zero, and M should be the zero matrix.

Since $\operatorname{tr}\left((A - B^T)(A - B^T)^T\right) = 0$, $A - B^T$ is the zero matrix, and thus $A = B^T$.

Exercise 3

Let A and B be 2×2 matrices with real entries satisfying $(AB - BA)^n = I_2$ for some positive integer n. Prove that n is even and $(AB - BA)^4 = I_2$.

Solution Note that $n \neq 1$ since $\operatorname{tr}(AB - BA) = 0$ but $\operatorname{tr}(I_2) = 2$.

Since $\operatorname{tr}(AB - BA) = 0$, let $AB - BA = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$. Then

$$(AB - BA)^2 = \begin{bmatrix} a^2 + bc & 0 \\ 0 & a^2 + bc \end{bmatrix} = (a^2 + bc)I_2.$$

Claim. n is even.

Suppose n is odd, and let $n = 2k + 1$. Then

$$\begin{aligned}(AB - BA)^n &= (AB - BA)^{2k} \cdot (AB - BA) \\ &= (a^2 + bc)^k I_2^k (AB - BA) \\ &= (a^2 + bc)^k (AB - BA).\end{aligned}$$

If $(AB - BA)^n = I_2$, then $\operatorname{tr}(AB - BA) = (a^2 + bc)^k \operatorname{tr}\left((AB - BA)^n\right) = 0$ but $\operatorname{tr}(I_2) = 2$, which is a contradiction. Thus n cannot be odd.

Let $n = 2k$. Then $(AB - BA)^n = (a^2 + bc)^k I_2 = I_2$, so $(a^2 + bc)^k = 1$. Since $a^2 + bc \in \mathbb{Z}$, $a^2 + bc$ is either 1 or -1. Thus $(a^2 + bc)^2 = 1$, and

$$(AB - BA)^4 = (a^2 + bc)^2 I_2^2 = I_2.$$

12 November 12, 2024

Exercise 1

Find all continuous functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(x + y) = f(x)f(y)$.

Solution We have $f(x + x) = f(x) \cdot f(x)$, so $f(2x) = f(x)^2 \geq 0$. This gives that $f(x) \geq 0$ for all $x \in \mathbb{R}$.

If there is some x such that $f(x) = 0$, then f is identically zero since $\forall a \in \mathbb{R}$, $f(a) = f(x)f(a - x) = 0$.

If f is not zero anywhere, then $\ln f$ should be linear, so $f = e^{cx}$.

Therefore, $f = ce^x$ is the only solution where $c \geq 0$.

Exercise 2 (Putnam 1971)

Let X be the set of all reals except 0 and 1. Find all real valued functions $f(x)$ on X which satisfy $f(x) + f(1 - 1/x) = 1 + x$ for all x in X.

Solution Take any $x \in X$. We have

$$f(x) + f\left(1 - \frac{1}{x}\right) = 1 + x$$

$$f\left(1 - \frac{1}{x}\right) + f\left(1 - \frac{1}{1 - 1/x}\right) = f\left(1 - \frac{1}{x}\right) + f\left(-\frac{1}{x-1}\right) = 1 + 1 - \frac{1}{x}$$

$$f\left(-\frac{1}{x-1}\right) + f\left(1 - \frac{1}{-1/(x-1)}\right) = f\left(-\frac{1}{x-1}\right) + f(x) = 1 - \frac{1}{x-1}$$

Adding the first and third equations and subtracting the second gives

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

so

$$f(x) = \frac{1}{2}\left(x + \frac{1}{x} - \frac{1}{x-1}\right).$$

Exercise 3 (Putnam 1988)

Prove that there is a unique function $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ satisfying $f(f(x)) = 6x - f(x)$ for all x.

Solution Fix some $x_0 \in \mathbb{R}_{>0}$ and let $a_0 = x_0$. Define the recursive sequence by $a_{n+1} = f(a_0)$ for $n \geq 0$. Then $a_{n+2} + a_{n+1} - 6 = 0$, so

$$a_n = \alpha \cdot 2^n + \beta \cdot (-3)^n.$$

Since $a_i \geq 0$ for all $i \in \mathbb{N}$, β should be zero since as n goes to infinity, a_n will oscillate between positive and negative values. So $a_n = \alpha \cdot 2^n$ and $x_0 = a_0 = \alpha$. Since $a_{n+1} = f(x_0) = 2\alpha = 2x$, $f(x) = 2x$ for all $x \in \mathbb{R}_{>9}$.

Exercise 4

The function $f : \mathbb{R} \to \mathbb{R}$ satisfies $x + f(x) = f(f(x))$ for every $x \in \mathbb{R}$. Find all solutions to the equation $f(f(x)) = 0$.

Solution Letting $x = 0$ gives $f(0) = f(f(0))$. Letting $x = f(0)$ gives $f(0) + f(f(0)) = f(f(f(0)))$. Since $f(0) = f(f(0))$, we have

$$f(f(f(0))) = f(f(0)) = f(f(0)) + f(0),$$

so $f(0) = 0$. We claim this is the only solution.

Claim. f is injective.

Let $f(x) = f(y)$. Then

$$f(f(x)) - x = f(x) = f(y) = f(f(y)) - y,$$

so $f(f(x)) - x = f(f(y)) - y$. But since $f(f(x)) = f(f(y))$, we have $x = y$.

Then there is only one solution to $f(x) = 0$, which is $x = 0$. So $f(f(x)) = 0$ gives $f(x) = 0$, and $f(x) = 0$ gives $x = 0$.

13 November 19, 2024

Facts to Know

Theorem : Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ can be written as a product of primes uniquely, up to orders.

Theorem : Chinese Remainder Theorem

Let m be relatively prime to n. Then each residue class mod mn is equal to the intersection of a unique residue class mod m and a unique residue class mod n, and the intersection of each residue class mod m with a residue class mod n is a residue class mod mn.

Theorem : Fermat's Little Theorem

If a is an integer, p a prime number and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem : Euler Totient Theorem

If a is an integer and m is an integer relatively prime to a, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem : Wilson's Theorem

If p is an integer, then $(p-1)! + 1$ is divisible by p if and only if p is a prime number.

Theorem : Bezout's Identity

$\gcd(a, b) = g$ if and only if there exists integers x and y such that $g = ax + by$.

Definition : Legendre Symbol

Let p be prime and a be an integer. Then define the **Legendre symbol** $\left(\frac{a}{p}\right)$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise} \end{cases}.$$

The Legendre symbol is multiplicative. That is, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Lemma

- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Theorem : Quadratic Reciprocity

If p and q are distinct primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Theorem

Let p be a prime and $v_p(n)$ be the exponent of p in the prime factorization of n. Then

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

Exercise 1

Find all integers n such that there is an integer a with $2^n - 1 \mid a^2 + 1$.

Solution We claim that $n = 1$ is the only possible integer. If $n = 1$ and $a = 1$, then $1 \mid 1^2 + 1$.

Suppose $n > 1$. Then $2^n - 1 \equiv -1 \equiv 3 \pmod 4$.

Claim. There is a $p \equiv 3 \pmod 4$ such that $p \mid 2^n - 1$.

Suppose not. Then, for all prime dividing $2^n - 1$, p should either be 2 or 1 mod 4. But $p \neq 2$ since $2^n - 1$ is odd. If all prime factors are odd, then

$$2^n - 1 = p_1^{e_1} p_2^{e_2} \cdot \dots \equiv 1 \cdot 1 \cdot \dots \equiv 1 \pmod 4,$$

which is a contradiction.

Take a 3 mod 4 prime p such that $p \mid 2^n - 1$. Then $p \mid a^2 + 1$. This gives $a^2 \equiv -1 \pmod p$, so -1 is a quadratic residue modulo p. However,

$$\left(\frac{-1}{p} \right) = (-1)^{(p-1)/2} = -1,$$

which is a contradiction to the fact that -1 is a quadratic residue modulo p. Therefore, n cannot be greater than 1.

Exercise 2

Let a and b be positive integers. Prove that the greatest common divisor of 2^a+1 and 2^b+1 divides $2^{\gcd(a,b)}+1$.

Solution Let $d=\gcd(2^a+1, 2^b+1)$. Then $2^a \equiv -1 \pmod{d}$ and $2^b \equiv -1 \pmod{d}$. We have

$$4^a \equiv (-1)^2 = 1 \pmod{d}$$

$$4^b \equiv (-1)^2 = 1 \pmod{d}.$$

Let $g=\gcd(a,b)$. Then there exists integers x and y such that $g = ax+by$. This gives

$$4^{ax+by} \equiv 1^x \cdot 1^y = 1 \pmod{d}.$$

so $d \mid 4^g - 1 = (2^g+1)(2^g-1)$.

Claim. $\gcd(d, 2^g-1) = 1$.

Note that d is odd since it is a greatest common divisor of two odd numbers. Take any prime p dividing d. Then p is also odd. Suppose $p \mid 2^g - 1$. Since $g \mid a$, $2^g - 1 \mid 2^a - 1$, and $p \mid 2^a - 1$. However, $p \mid 2^a + 1$, so $p \mid (2^a+1) - (2^a-1) = 2$, which is a contradiction since p should be an odd prime. Therefore, there is no prime $p \mid d$ such that $p \mid 2^g - 1$, and $\gcd(d, 2^g-1) = 1$.

Since $d \mid (2^g+1)(2^g-1)$ and $\gcd(d, 2^g-1) = 1$, we should have $d \mid 2^g+1$. Therefore, $\gcd(2^a+1, 2^b+1) \mid 2^{\gcd(a,b)}+1$ and this completes the proof.

> **Exercise 3 (Putnam 2006)**
> Alice and Bob play a game in which they take turns removing stones from a heap that initially has n stones. The number of stones removed at each turn must be one less than a prime number. The winner is the player who takes the last stone. Alice plays first. Prove that there are infinitely many n such that Bob has a winning strategy.

Solution Suppose there are only finitely many n such that Bob has a winning strategy. Let B be the set of numbers which Bob has a winning strategy. Then B is bounded above by some integer k.

For some $n > k$, Alice should have a prime number p such that $n - (p - 1)$ is in B since Bob does not have a winning strategy for n. That is, for all $n > k$. There is some $b \in B$ and prime p such that $n = b + p - 1$. However, this cannot happen if we set $n = (k+1)! + k$. Since $b < k$, we should have $(k+1)! + 2 < n - b + 1 < (k+1)! + (k+1)$, with $n - b + 1 = p$, but every integer between $(k+1)! + 2$ and $(k+1)! + (k+1)$ is composite, a contradiction.

Therefore, there are infinitely many n such that Bob has a winning strategy.

Exercise 4

Let $a_0 = 1$, $a_1 = 2$, and $a_n = 4a_{n-1} - a_{n-2}$ for $n \geq 2$. Find an odd prime factor of a_{2015}.

Solution The characteristic equation is $X^2 - 4X + 1 = 0$, which gives $X = 2 \pm \sqrt{3}$. So the general formula of a_n is

$$a_n = \alpha(2+\sqrt{3})^n + \beta(2-\sqrt{3})^n.$$

Letting $n = 0$ and $n = 1$ gives a system of equation for α and β, and we have

$$a_n = \frac{1}{2}\big((2+\sqrt{3})^n + (2-\sqrt{3})^n\big).$$

Claim. $a_5 \mid a_{2015}$.

Note that $5 \mid 2015$. Let $(2+\sqrt{3})^5 = a$ and $(2-\sqrt{3})^5 = b$. Then a and b are irrational conjugates. We have

$$\begin{aligned} 2a_{2015} &= a^{403} + b^{403} \\ &= (a+b)(a^{402} + a^{401}b + \cdots + ab^{401} + b^{402}). \end{aligned}$$

Here, $a + b$ should be an integer, and

$$a^{402} + a^{401}b + \cdots + ab^{401} + b^{402} = \sum_{i=i}^{201}(a^{201+i}b^{201-i} + a^{201-i}b^{201+i}) + a^{201}b^{201}$$

is also an integer since $a^{201+i}b^{201-i} + a^{201-i}b^{201+i}$ and $a^{201}b^{201}$ are integers. So we have $2a_5 \mid 2a_{2015}$, and $a_5 \mid a_{2015}$.

Since $a_5 = \frac{1}{2}\big((2+\sqrt{3})^5 + (2-\sqrt{3})^5\big) = 362$, we have that $181 \mid a_5 \mid a_{2015}$.