

Putnam Solutions

VISHAL RAMAN

June 28, 2021

My sketches to problems from the Putnam exams. I tend to leave out a lot of the details for routine checks or brute force calculations. Any typos or mistakes found are mine - kindly direct them to my inbox.

Contents

1 Putnam - 2001	3
1.1 A1 - Algebra	3
1.2 A2 - Combinatorics	4
1.2.1 Official Solution	4
1.3 A3 - Algebra	5
1.4 A4 - Geometry	6
1.5 A5 - Number Theory	8
1.6 A6 - Calculus	9
1.7 B1 - Combinatorics	10
1.8 B2 - Algebra	11
1.9 B3 - Analysis	12
1.10 B4 - Number Theory	13
1.11 B5 - Algebra	14
1.12 B6 - Algebra/Combinatorics	15
2 Putnam - 2002	16
2.1 A1 - Algebra	16
2.1.1 Official Solution	16
2.2 A2 - Combinatorics	17
2.3 A3 - Combinatorics	18
2.4 A4 - Combinatorics	19
2.5 A5 - Number Theory	20
2.6 A6 - Analysis	21
2.7 B1 - Probability	22
2.8 B2 - Combinatorics	23
2.9 B3 - Analysis	24
2.10 B4 - Combinatorics	25
2.11 B5 - Number Theory	26
2.12 B6 - Number Theory	27
3 Putnam 2003	28
3.1 A1 - Combinatorics	28

3.2	A2 - Algebra	29
	3.2.1 Alternate Solution	29
3.3	A3 - Calculus	30
3.4	A4 - Algebra	31
3.5	A5 - Combinatorics	32
3.6	A6 - Combinatorics	33
3.7	B1 - Algebra	34
3.8	B2 - Combinatorics	35
3.9	B3 - Number Theory	36
3.10	B4 - Algebra	37
3.11	B5 - Geometry	38
3.12	B6 - Analysis	39

§1 Putnam - 2001

§1.1 A1 - Algebra

Consider a set S and a binary operation $*$. Assume $(a * b) * a = b$ for all $a, b \in S$. Prove that $a * (b * a) = b$ for all $a, b \in S$.

Proof. Note that

$$b = ((b * a) * b) * (b * a) = a * (b * a).$$

□

§1.2 A2 - Combinatorics

You have coins C_1, C_2, \dots, C_n . For each k , C_k is biased so that when tossed, is has probability $1/(2k+1)$ of falling heads. If the n coins are tossed, what is the probability that the number of heads is odd?

Proof. We claim the probability is $P(n) = \frac{n}{2n+1}$. We prove it by induction. We are given that $P(1) = \frac{1}{3}$, which satisfies the claim. Suppose $P(k) = \frac{k}{2k+1}$ for $k \geq 1$. In order to find $P(k+1)$, we condition on the result of the first k coin tosses. Namely, suppose the number of heads is even after k tosses. Then, the total number of heads is odd if we flip a head on the $k+1$ -th toss. Similarly, if the number of heads is odd after k tosses, then the total number of heads is odd if we flip a tail on the $k+1$ -th toss.

Putting this together gives

$$\begin{aligned} P(k+1) &= (1 - P(k))p_{k+1} + P(k)(1 - p_{k+1}) \\ &= P(k)(1 - 2p_{k+1}) + p_{k+1} \\ &= P(k) \left(1 - \frac{2}{2k+3}\right) + \frac{1}{2k+3} \\ &= P(k) \frac{2k+1}{2k+3} + \frac{1}{2k+3} \\ &= \frac{k}{2k+1} \frac{2k+1}{2k+3} + \frac{1}{2k+3} \\ &= \frac{k+1}{2k+3} \end{aligned}$$

which proves the result. \square

§1.2.1 Official Solution

There is another remarkable proof using generating functions.

Proof. Consider the polynomial $f(x) = \prod_{k=1}^n \left(\frac{x}{2k+1} + \frac{2k}{2k+1}\right)$. The coefficient of x^m gives the probability of exactly m heads. The sum of the odd coefficients is given by $\frac{f(1)-f(-1)}{2}$. It is clear that $f(1) = 1$ and note that

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

The overall probability is $\frac{n}{2n+1}$ as desired. \square

§1.3 A3 - Algebra

For each integer m , consider the polynomial

$$P_m(x) = x^4 - (2m + 4)x^2 + (m - 2)^2.$$

For what values of m is $P_m(x)$ the product of two non-constant polynomials with integer coefficients?

Proof. We claim that m is the square of an integer or twice the square of an integer. Set $y = x^2$. We look for square-integer solutions for y . From the quadratic formula,

$$\begin{aligned} y &= \frac{2m + 4 \pm \sqrt{(2m + 4)^2 - 4(m - 2)^2}}{2} \\ &= m + 2 \pm \sqrt{(m + 2)^2 - (m - 2)^2} \\ &= m + 2 \pm \sqrt{4(2m)} \\ &= m + 2 \pm 2\sqrt{2m} \\ &= (\sqrt{m} \pm \sqrt{2})^2. \end{aligned}$$

Hence, $x = \pm\sqrt{m} \pm \sqrt{2}$. Note that if m is neither the square of an integer nor twice the square of an integer then the field $\mathbb{Q}(\sqrt{m}, \sqrt{2})$ is of degree 4 and the Galois group acts transitively on the roots $\{\pm\sqrt{m} \pm \sqrt{2}\}$. It follows that the polynomial is irreducible.

It is easy to verify that if m is a square or twice a square, then $P_m(x)$ reduces into the product of non-constant integer polynomials.

□

§1.4 A4 - Geometry

Triangle ABC has area 1. Points E, F, G lie on sides BC, CA, AB such that AE bisects BF at point R , BF bisects CG at point S , and CG bisects AE at point T . Find the area of the triangle RST .

Proof. We claim that $[RST] = \frac{7-\sqrt{5}}{4}$. Let $EC/BC = r$, $FA/CA = s$, $GB/AB = t$.

Note that $[ABE] = [AFE]$ since they share a base AE and $BR = FR$ implies that they share the same altitude length as well (drop altitudes from F and B and use the congruent triangles).

Then, $[ABE] = [ABE]/[ABC] = BE/BC = 1 - EC/BC = 1 - r$. We also have $[ACE] = r$. It follows that $[FCE] = [ACE](FC/AC) = r(1 - s)$.

Now,

$$1 = [ABC] = [ABE] + [AFE] + [EFC] = (1 - r) + (1 - r) + r(1 - s) \implies r(1 + s) = 1.$$

Arguing similarly for the other sides, we have $s(1 + t) = 1$, and $t(1 + r) = 1$.

It follows that

$$r = \frac{1}{1 + s} = \frac{1}{1 + \frac{1}{1+t}} = \frac{1}{1 + \frac{1}{1+\frac{1}{r}}}.$$

Simplifying this, we find that $r = \frac{2+r}{3+2r}$, which gives $3r + 2r^2 = 2 + r$, or equivalently, $r^2 + r - 1 = 0$. Plugging into the quadratic formula and taking the positive root gives

$$r = \frac{-1 + \sqrt{5}}{2},$$

and by repeating the argument, we have $r = s = t = \frac{-1 + \sqrt{5}}{2}$.

Now, note that $[ATC] = [AEC]/2 = r/2$, $[ATG] = [ACG] - [ATC] = 1 - t - r/2$. Similarly, $[BSC] = t/2$ and $[BRE] = 1 - r - s/2$, so it follows that $[BRTG] = [ABE] - [ATG] - [BRE] = r/2 + s/2 + t - 1$.

$$\begin{aligned} [RST] &= [ABC] - [ACG] - [BSC] - [BRTG] \\ &= 1 - (1 - t) - (t/2) - (r/2 + s/2 + t - 1) \\ &= 1 - \frac{r + s + t}{2} \\ &= 1 - \frac{3 \frac{\sqrt{5}-1}{2}}{2} \\ &= \frac{7 - \sqrt{5}}{4}. \end{aligned}$$

□

Proof. A brute-force calculation through vectors. Define A to be the origin and take B, C to be basis vectors from A . We can set $G = \beta B$, $F = (1 - \gamma)C$, $E = \alpha C + (1 - \alpha)C$. Furthermore, we set $R = (1 - \rho)E$, $S = \sigma B + (1 - \sigma)F$, $T = \tau C + (1 - \tau)G$. To satisfy the conditions of the problem, we must have that

$$2R = B + F, 2S = C + G, 2T = E.$$

After messy algebra, we obtain that

$$\alpha = \frac{1 - \beta}{2 - \beta}, \beta = \frac{1 - \gamma}{2 - \gamma}, \gamma = \frac{1 - \alpha}{2 - \alpha},$$

which has an obvious solution $\alpha = \beta = \gamma = \frac{3-\sqrt{5}}{2}$.

It follows that

$$(R - T, S - T) = \frac{1}{2} \begin{pmatrix} \alpha & 2\alpha - 1 \\ 1 - 2\alpha & 1 - \alpha \end{pmatrix},$$

so we can evaluate

$$[RST] = \frac{[ABC]}{4} \begin{vmatrix} \alpha & 2\alpha - 1 \\ 1 - 2\alpha & 1 - \alpha \end{vmatrix} = \frac{\alpha^2}{2} = \frac{7 - 3\sqrt{5}}{4}.$$

□

§1.5 A5 - Number Theory

Show that there are unique positive integers a, n such that $a^{n+1} - (a+1)^n = 2001$.

Proof. We claim the unique pair of positive integers satisfying the claim is $(a, n) = (13, 2)$. It is easy to verify that this is indeed a solution.

Considering the equation in \mathbb{Z}_3 , we see that $a \equiv 1 \pmod{3}$ - in the other cases, one of the terms vanishes and the other term is non-vanishing, so the difference cannot vanish.

Considering the equation in \mathbb{Z}_4 , we cannot have $a \equiv 0 \pmod{4}$, for the same reason as above. If $a \equiv 1 \pmod{4}$, we must have that $n > 1$ in order for the equivalence to be satisfied. If $a \equiv 2, 3 \pmod{4}$, we must have that n is even.

In the case with $a \equiv 1 \pmod{3}$ and $a \equiv 1 \pmod{4}$, we obtain $a \equiv 1 \pmod{12}$ and $n > 1$. We see easily that $a = 1$ does not satisfy the equation for any $n > 1$. For $a = 13$, we have a solution as above for $n = 2$. It is easy to see that no higher value of n also satisfies the equation since the function $f(x) = 13^{x+1} - 14^x$ is monotonically increasing. We can repeatedly apply similar arguments for the other cases to show that this is the unique solution. \square

§1.6 A6 - Calculus

Can an arc of a parabola inside a circle of radius 1 have a length greater than 4?

Proof. We claim that it is possible. Take a unit circle given by $x^2 + (y - 1)^2 = 1$ and a parabola $y = kx^2$. The length of the curve inside the arc is given by

$$L(k) = 2 \int_0^{\sqrt{2k-1}/k} \sqrt{1 + 4k^2x^2} dx = \frac{1}{4k} \int_0^{2\sqrt{2k-1}} \sqrt{1 + x^2} dx.$$

It is easy to show that $\sqrt{1 + x^2} \geq \frac{1}{x+1}$ so it follows that $\lim_{k \rightarrow \infty} L(k) = +\infty$. It follows that there exists some k so that $L(k) > 4$ as desired. \square

§1.7 B1 - Combinatorics

Let n be an even positive integer. Write the numbers $1, 2, \dots, n^2$ in the squares of an $n \times n$ grid from left to right. Color the squares of the grid so that half of the squares in each row and in each column are red and the other half are black. Prove that for each coloring, the sum of the numbers on the red squares is equal to the sum of the numbers on the black squares.

Proof. I have two proofs. An outline of the first follows the approach of invariants. Namely, we can start from a checkerboard pattern and repeatedly swap squares so that the sum of the numbers on the red squares is equal to the sum of the numbers on the black squares. It suffices to show that the group of colorings with the given conditions is transitive under the transposition. This is easy to show with an algorithm approach: for each square on a given board, we assign 1 if it differs from the checkerboard, otherwise we assign 0. Then, we take the sum of the values. We can choose transpositions so that the sum decreases on each turn, which must eventually terminate.

The other approach is as follows. For convenience, we subtract 1 from each square so that it starts at 0. We can take the expansion in base n , so the value of each square s is given by $nf(s) + g(s)$ where $0 \leq f(s), g(s) < n$. If we let R denote the set of red numbers and B the set of black numbers, note that $\sum_{s \in R} f(s) = \sum_{s \in B} f(s)$ since the number of red and black squares in each row is the same. Similarly, $\sum_{s \in R} g(s) = \sum_{s \in B} g(s)$ since the number of red and black squares in each column is the same. It follows that

$$\sum_{s \in R} nf(s) + g(s) = \sum_{s \in B} nf(s) + g(s).$$

□

§1.8 B2 - Algebra

Find all pairs $(x, y) \in \mathbb{R}^2$ satisfying the system

$$\begin{aligned}\frac{1}{x} + \frac{1}{2y} &= (x^2 + 3y^2)(3x^2 + y^2) \\ \frac{1}{x} - \frac{1}{2y} &= 2(y^4 - x^4).\end{aligned}$$

Proof. An easy algebra exercise. Expanding the right-hand sides, then adding/subtracting the equations, we obtain $(x + y)^5 = 3$ and $(x - y)^5 = 1$ respectively. This has a unique solution in \mathbb{R}^2 , $\left(\frac{3^{1/5}+1}{2}, \frac{3^{1/5}-1}{2}\right)$. \square

§1.9 B3 - Analysis

For any positive integer n , let $\langle n \rangle$ denote the closest integer to \sqrt{n} . Evaluate $\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n}$.

Proof. We reindex the sum by summing over the fixed values of $\langle n \rangle$, which is non-decreasing. Namely, we have

$$\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n} = \sum_{m=1}^{\infty} \sum_{\langle n \rangle=m} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n} = \sum_{m=1}^{\infty} \left((2^m + 2^{-m}) \sum_{\langle n \rangle=m} 2^{-n} \right).$$

Note that $\langle n \rangle = m$ whenever $n \in ((m-1/2)^2, (m+1/2)^2) = (m^2-m+1/4, m^2+m+1/4)$. This happens for $n \in [m^2-m+1, m^2+m]$. Then, note that

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

Combining the results, we have

$$\begin{aligned} \sum_{m=1}^{\infty} (2^m + 2^{-m})(2^{-m^2+m} - 2^{-m^2-m}) &= \sum_{m=1}^{\infty} 2^{-m^2+2m} - 2^{-m^2-2m} \\ &= \sum_{m=1}^{\infty} 2^{-m(m-2)} - 2^{-m(m+2)} \\ &= \sum_{m=1}^{\infty} 2^{-m(m-2)} - \sum_{m=3}^{\infty} 2^{-(m-2)m} \\ &= 2^1 + 2^0 = 3. \end{aligned}$$

□

§1.10 B4 - Number Theory

Let $S = \mathbb{Q} \setminus \{-1, 0, 1\}$. Define $f : S \rightarrow S$ by $f(x) = x - 1/x$. Prove or disprove that

$$\bigcap_{n=1}^{\infty} f^{(n)}(S) = \emptyset.$$

Proof. The claim is true. Suppose we had $x = \frac{p}{q} \in \bigcap_{n=1}^{\infty} f^{(n)}(S)$, where $(p, q) = 1$. Then, there is some $m \in \mathbb{N}$ so that $f^{(m)}(x) = x$. However, note that

$$f\left(\frac{p}{q}\right) = \frac{p^2 - q^2}{pq},$$

and $|pq| > |q|$ since $p \notin \{-1, 0, 1\}$. Furthermore, note that $(p^2 - q^2, pq) = 1$. If there is some prime r dividing both $p^2 - q^2$ and pq , then we have that r divides one of $p - q, p + q$ and one of p, q . However, from these we could conclude that r divides both p, q which contradicts the fact that $(p, q) = 1$. It follows that since the denominators strictly increase, we cannot have $f^{(m)}(x) = x$. \square

§1.11 B5 - Algebra

let $a, b \in (0, 1/2)$ and let g be a continuous real-valued function such that $g(g(x)) = ag(x) + bx$ for all real x . Prove that $g(x) = cx$ for some constant c .

Proof. First, note that g is injective. This is because $g(x) = g(y)$ implies that $g(g(x)) = g(g(y))$, which implies that $ag(x) + bx = ag(y) + by$, which implies that $x = y$. Since g is continuous and injective, it follows that g is monotone.

We claim that g is unbounded, which implies that it is surjective. Suppose $|g(x)| \leq M$ for all $x \in \mathbb{R}$. Then,

$$(a+1)M \geq |g(g(x)) - ag(x)| = |bx|,$$

which is a contradiction since bx is unbounded.

Now, let $x_0 \in \mathbb{R}$ be arbitrary and define $x_{n+1} = g(x_n)$, $x_{n-1} = g^{-1}(x_n)$. The original functional equation gives a linear recurrence relation

$$x_{n+2} = ax_{n+1} + bx_n.$$

The corresponding characteristic polynomial is $\lambda^2 - a\lambda - b$, which has two distinct roots $\lambda_{\pm} = \frac{a \pm \sqrt{a^2 + 4b}}{2}$, since $a, b \in (0, 1/2)$. It follows that

$$x_n = c_+ \lambda_+^n + c_- \lambda_-^n$$

for constants c_+, c_- .

Note that $\lambda_+ > 0$, $\lambda_- < 0$ and $1 > |\lambda_+| > |\lambda_-|$.

Suppose f is monotone increasing (the case where f is monotone decreasing is similar). If $c_- \neq 0$ then as n gets sufficiently small, λ_-^n dominates λ_+^n , so there is some large enough n so that $0 < x_n < x_{n+2}$ and $x_{n+3} < x_{n+1} < 0$, which would give that $g(x_n) > g(x_{n+2})$, a contradiction. It follows that $c_- = 0$, so we have $x_0 = c_+$ and $g(x_0) = x_1 = c_+ \lambda_+ = \lambda_+ x_0$, which gives the result. □

§1.12 B6 - Algebra/Combinatorics

Assume $(a_n)_{n \geq 1}$ is an increasing sequence of positive real numbers such that $\lim a_n/n = 0$. Must there exist infinitely many positive integers n such that $a_{n-i} + a_{n+i} < 2a_n$ for $i = 1, 2, \dots, n-1$?

Proof. Let $A = \text{Conv}\{(n, a_n) : n \in \mathbb{N}\}$ and let ∂A denote the set of points on the boundary of the convex hull.

We claim that ∂A contains infinitely many elements. Suppose not. Then, ∂A has a last point (N, a_N) . If we let $m = \sup_{n > N} \frac{a_n - a_N}{n - N}$, the slope of the line between (N, a_N) and (n, a_n) , then the line through (N, a_N) with slope m lies above (or contains) each point (n, a_n) for $n > N$. However, since $a_n/n \rightarrow 0$ and a_N, N are fixed, we have that

$$\frac{a_n - a_N}{n - N} \rightarrow 0.$$

This implies that the set of slopes attains a maximum, i. e. there is some point (M, a_M) with $M > N$ so that $m = \frac{a_M - a_N}{M - N}$. But then, we must also have that $(M, a_M) \in \partial A$, contradicting the fact that (N, a_N) is the last point in ∂A .

For each point on the boundary $(n, a_n) \in \partial A$, we must have that midpoint of the line through $(n-i, a_{n-i})$ and $(n+i, a_{n+i})$ for $i \in [n-1]$ must lie below (n, a_n) . From this, it follows that $a_n > \frac{a_{n-i} + a_{n+i}}{2}$, which implies the result. \square

§2 Putnam - 2002

§2.1 A1 - Algebra

Let $k \in \mathbb{N}$. The n -th derivative of $1/(x^k - 1)$ has the form $P_n(x)/(x^k - 1)^{n+1}$ where $P_n(x)$ is a polynomial. Find $P_n(1)$.

Proof. We can write

$$\begin{aligned} \frac{P_n(x)}{(x^k - 1)^{n+1}} &= \frac{d}{dx} \left(\frac{P_{n-1}(x)}{(x^k - 1)^n} \right) \\ &= \frac{(x^k - 1)^n P'_{n-1}(x) - nkx^{k-1}(x^k - 1)^{n-1} P_{n-1}(x)}{(x^k - 1)^{2n}} \\ \implies P_n(x) &= (x^k - 1)P'_{n-1}(x) - nkx^{k-1}P_{n-1}(x). \end{aligned}$$

Plugging in $x = 1$ gives a recurrence relation $P_n(1) = -nkP_{n-1}(1)$. It follows that

$$P_n(1) = n!(-k)^n P_0(1) = n!(-k)^n.$$

□

§2.1.1 Official Solution

An alternate solution comes from expanding $\frac{1}{x^k - 1}$ in a Laurent series around 1.

Proof. It suffices to keep track of the $O((x - 1)^{-1})$ terms since the others vanish upon plugging in 1.

Note that

$$\frac{1}{x^k - 1} = \frac{1}{k(x - 1) + \dots} = \frac{1}{k}(x - 1)^{-1} + \dots$$

Taking the n -th, derivative, we have obtain

$$\frac{d^n}{dx^n} \frac{1}{x^k - 1} = \frac{(-1)^n n!}{k(x - 1)^{-n-1}} + \dots$$

It follows that

$$\begin{aligned} P_n(x) &= (x^k - 1)^{n+1} \frac{d^n}{dx^n} \frac{1}{x^k - 1} \\ &= (k(x - 1) + \dots)^{n+1} \left(\frac{(-1)^n n!}{k(x - 1)^{-n-1}} + \dots \right) \\ &= k^n (-1)^n n! + \dots \end{aligned}$$

□

§2.2 A2 - Combinatorics

Given any five points on a sphere, show that some four of them must lie on a closed hemisphere.

Proof. Draw a great circle through any two points and consider the remaining three. By the pigeonhole principle, there is closed hemisphere with at least two points, and choosing this hemisphere gives the result. \square

§2.3 A3 - Combinatorics

Let $n \geq 2$ be an integer and T_n the number of nonempty subsets S of $\{1, 2, \dots, n\}$ with the property that the average of the elements of S is an integer. Prove that $T_n - n$ is always even.

Proof. Note that each one element subset $\{1\}, \{2\}, \dots, \{n\}$ has the property that the average of the element is an integer. It suffices to consider the subsets at least 2 elements. For set of size at least 2, we can pair them into $(S, S \cup \{a\})$, where $a \notin S$ and the average of the elements in S is a . Each subset is contained in exactly one pair, so each of them don't contribute to the parity of $T_n - n$. It follows that $T_n - n$ is even as desired. \square

§2.4 A4 - Combinatorics

in Determinant Tic-Tac-Toe, Player 1 enters a 1 in an empty 3×3 matrix. Player 0 counters with a 0 in a vacant position, and play continues in turn until the matrix is completed with five 1's and four 0's. Player 0 wins if the determinant is 0 and player 1 wins otherwise. Who wins and how?

Proof. Player 0 wins. After exchanging rows and columns (which doesn't change the norm of the determinant), we can assume without loss of generality that player 1 enters a 1 in the a_{11} square.

In the optimal strategy, player 0 enters a 0 in the a_{22} square. There are 3 possible cases to check for player 1's next move:

1. a_{12} or a_{21} ,
2. a_{13} or a_{31} ,
3. a_{23} or a_{32} ,
4. a_{33} .

For each of these cases, it suffices to check the first since we can exchange a_{ij} with a_{ji} in order to obtain the strategy in the other corresponding case. Note that if player 0 creates a row/column of 0's or a 2×2 block of 0's, the determinant of the matrix will be 0.

(1) When player 1 enters a 1 in a_{12} , player 0 enters a 0 in square a_{32} . If player 1 enters in a_{21} or a_{23} , player 0 enters in a_{33} or a_{31} respectively. In this position, player 1 cannot stop player 0 from creating a 2×2 block or a row of 0's. Alternatively, if player 1 enters in a_{13} , player 0 enters in a_{21} . In this position, player 1 cannot stop player 0 from creating a 2×2 block or a row of 0's. In the other cases, we take a knight's move across whatever player 1 plays and in this position, player 1 cannot stop player 0 from creating a 2×2 block or a row of 0's.

The other cases follow a similar analysis, creating a triangle block of 0's in other to create two threats. \square

§2.5 A5 - Number Theory

Define a sequence by $a_0 = 1$, together with the rules $a_{2n+1} = a_n$ and $a_{2n+2} = a_n + a_{n+1}$ for each integer $n \geq 0$. Prove that every positive rational number appears in the set $\{a_n/a_{n+1} : n \geq 0\}$.

Proof. We proceed by induction on $k = \max\{p, q : \gcd(p, q) = 1\}$. For $k = 1$, we know that $a_0 = a_1 = 1$ so we have $1/1$, which contains all the rational numbers p/q with $\max\{p, q\} \leq 1$. Suppose the set contains all the rationals p/q with $\max\{p, q : \gcd(p, q) = 1\} \leq n$. Then it contains $\frac{n+1-k}{k}$ for $1 \leq k \leq n$ whenever $\gcd(n+1-k, k) = 1$. Note that $\gcd(n+1-k, k) = 1 \Leftrightarrow \gcd(n+1, k) = 1$.

It follows that we have $a_m = \ell(n+1-k)$, $a_{m+1} = \ell(k)$ for some $\ell \in \mathbb{N}$. Then, $a_{2m+1} = \ell(n+1-k)$, $a_{2m+2} = \ell(n+1)$ and $a_{2m+3} = \ell(k)$. It follows that the set contains

$$\frac{n+1-k}{n+1}, \frac{n+1}{k}$$

for each $1 \leq k \leq n$ so that $\gcd(n+1, k) = 1$, which proves the inductive step. \square

§2.6 A6 - Analysis

Fix an integer $b \geq 2$. Let $f(1) = 1$, $f(2) = 2$, and for each $n \geq 3$, define $f(n) = nf(d)$, where d is the number of base- b digits of n . For which values of b does the sum $\sum_{n \geq 1} 1/f(n)$ converge?

Proof. The sum converges for $b = 2$ and diverges for $b \geq 3$.

We first consider $b \geq 3$. Suppose the sum converges. Note that we can write

$$\sum_{n=1}^{\infty} \frac{1}{f(n)} = \sum_{d=1}^{\infty} \frac{1}{f(d)} \sum_{n=b^{d-1}}^{b^d-1} \frac{1}{n}.$$

Note that $\sum_{n=b^{d-1}}^{b^d-1} \frac{1}{n}$ is a left-endpoint Riemann approximation for the integral $\int_{b^{d-1}}^{b^d} \frac{1}{x}$ and the function $\frac{1}{x}$ is monotonically decreasing on this interval so it follows that

$$\sum_{n=b^{d-1}}^{b^d-1} \frac{1}{n} > \int_{b^{d-1}}^{b^d} \frac{1}{x} = \log b.$$

However, this implies that

$$\sum_{n=1}^{\infty} \frac{1}{f(n)} > \log b \sum_{d=1}^{\infty} \frac{1}{f(d)},$$

which is a contradiction since $\log b > 1$.

Now, we show that the sum converges in the case of $b = 2$. Let $C = \log 2 + \frac{1}{8} < 1$. We prove by induction that for each $m \in \mathbb{N}$,

$$\sum_{n=1}^{2^m-1} \frac{1}{f(n)} < 1 + \frac{1}{2} + \frac{1}{6(1-C)} = L.$$

For $m = 1, 2$, the result is clear. Suppose it is true for all $m \in \{1, 2, \dots, N-1\}$. Note that

$$\sum_{n=1}^{2^N-1} \frac{1}{f(n)} = 1 + \frac{1}{2} + \frac{1}{6} + \sum_{d=3}^N \frac{1}{f(d)} \sum_{n=2^{d-1}}^{2^d-1} \frac{1}{n}.$$

Then, using a right-endpoint Riemann approximation, we have

$$\begin{aligned} \sum_{n=2^{d-1}}^{2^d-1} \frac{1}{n} &= \frac{1}{2^{d-1}} - \frac{1}{2^d} + \sum_{n=2^{d-1}+1}^{2^d} \frac{1}{n} \\ &< 2^{-d} + \int_{2^{d-1}}^{2^d} \frac{dx}{x} \\ &< \frac{1}{8} + \log 2 = C. \end{aligned}$$

It follows that

$$1 + \frac{1}{2} + \frac{1}{6} + \sum_{d=3}^N \frac{1}{f(d)} < 1 + \frac{1}{2} + \frac{1}{6} + C \sum_{d=3}^N \frac{1}{f(d)} \quad (1)$$

$$< 1 + \frac{1}{2} + \frac{1}{6} + \frac{C}{6(1-C)} \quad (2)$$

$$= 1 + \frac{1}{2} + \frac{1}{6(1-C)} = L, \quad (3)$$

where we used the strong induction hypothesis to obtain (2). \square

§2.7 B1 - Probability

Shanille shoots free throws on a basketball court. She hits the first and misses the second, and thereafter the probability that she hits the next shot is equal to the proportion of shots she has hit so far. what is the probability she hits exactly 50 of her first 100 shots?

Proof. We claim the probability of hitting exactly k shots after n throws for $k \in \{1, \dots, n-1\}$ is $\frac{1}{n-1}$. For $n = 2$, this is clear. If we suppose the result is true for $n = m$, the probability of making k shots after $m+1$ throws is

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

which proves the inductive hypothesis. □

§2.8 B2 - Combinatorics

Consider a polyhedron with at least five faces such that exactly three edges emerge from each of its vertices. Two players play the following game: Each, in turn, signs his or her name on a previously unsigned face. The winner is the player who first succeeds in signing three faces that share a common vertex. Show that the player who signs first will always win by playing as well as possible.

Proof. First, we claim that any such polyhedron has a face with at least 4 edges. The proof is as follows. Let V, E, F denote the number of vertices, edges, and faces respectively. For sake of contradiction, suppose that each face has exactly 3 edges. We can count the number of edges by counting 3 edges for each face, but dividing by 2 since each edge connects exactly 2 faces. It follows that $E = \frac{3F}{2}$. Similarly, $V = \frac{2E}{3} = F$, since we can count two vertices for each edge, but dividing by 3 since each vertex has exactly 3 outgoing edges. By Euler's formula, we have

$$2 = V - E + F = 2F - \frac{3F}{2} = \frac{F}{2} \implies F = 4,$$

which is a contradiction since $F \geq 5$.

Now, take the face with at least 4 edges, call it F_0 . Player 1 signs in F_0 . If player 2 does not sign in a face adjacent to F_0 , then player 1 can sign in any face adjacent to F_0 . At this point, player 2 cannot stop player 1 from signing three faces that share a common vertex since there are two threats. Hence, we can suppose player 2 does sign in a face adjacent to F_0 , call it F_1 . Since the face has at least 4 edges, we can sign in a square adjacent to F_0 that is not adjacent to F_1 . at this point, player 2 cannot stop player 1 from signing three faces that share a common vertex since there are two threats. \square

§2.9 B3 - Analysis

Show that for $n > 1$,

$$\frac{1}{2ne} < \frac{1}{e} - \left(1 - \frac{1}{n}\right)^n < \frac{1}{ne}.$$

Proof. Multiplying by e and subtracting from 1, we have

$$1 - \frac{1}{n} < e \left(1 - \frac{1}{n}\right)^n < 1 - \frac{1}{2n}.$$

Taking the logarithm(which is monotonically increasing), we equivalently have

$$\log(1 - 1/n) < 1 + n \log(1 - 1/n) < \log(1 - 1/(2n)).$$

Finally, noting the Taylor series expansion of $\log(1+x) = -\sum_{k \geq 1} \frac{(-x)^k}{k}$ (which converges for $x \in (-1, 1)$), we have

$$-\sum_{k \geq 1} \frac{1}{kn^k} < 1 - n \sum_{k \geq 1} \frac{1}{kn^k} < -\sum_{k \geq 1} \frac{1}{k(2n)^k}$$

or equivalently

$$\sum_{k \geq 1} \frac{1}{k(2n)^k} < \sum_{k \geq 1} \frac{1}{(k+1)n^k} < \sum_{k \geq 1} \frac{1}{kn^k},$$

which is evidently true since $k2^k > k+1$ and $k+1 > k$ for $k \geq 1$. □

§2.10 B4 - Combinatorics

An integer n , unknown to you, has been randomly chosen in the interval $[1, 2002]$ with uniform probability. Your objective is to select n in an odd number of guess. After each incorrect guess, you are informed whether n is higher or lower, and you **must** guess an integer on your next turn among the numbers that are still feasibly correct. Show that you have a strategy so that the chance of winning is greater than $\frac{2}{3}$.

Proof. Guess the sequence of numbers $1, 3, 4, 6, 7, \dots$ alternating between $x \equiv 1 \pmod{3}$ and $x \equiv 1 \pmod{3}$. If the chosen integer is $1 \pmod{3}$, then it will be chosen in an odd turn. If the chosen integer is $0 \pmod{3}$, then it will be chosen in an even turn. Otherwise, it is $n \equiv 2 \pmod{3}$ so it will be chosen immediately after $n + 1$ is chosen, which happens after an even turn, so it is an odd turn. This gives a chance of winning of at least $2/3$ as desired. \square

§2.11 B5 - Number Theory

A palindrome in base b is a positive integer whose base- b digits read the same backwards and forwards; for example, 2002 is a 4-digit palindrome in base 10. Note that 200 is not a palindrome in base 10, but it is a 3-digit palindrome: 242 in base 9, and 404 in base 7. Prove that there is an integer which is a 3-digit palindrome in base b for at least 2002 different values of b .

Proof. Let $N = 2002!$. We claim that N^2 is a 3-digit palindrome in base $b_d = \frac{N}{d} - 1$ for each $d \in \{1, 2, \dots, 2002\}$. Note that $2d^2 < \frac{2002!}{d} - 1$ for each $d \in \{1, 2, \dots, 2002\}$. It follows that we can write

$$\begin{aligned} ([d^2][2d^2][d^2])_{b_d} &= d^2 \left(\frac{N}{d} - 1 \right)^2 + 2d^2 \left(\frac{N}{d} - 1 \right) + d^2 \\ &= N^2 - 2Nd - d^2 + 2Nd - 2d^2 + d^2 \\ &= N^2. \end{aligned}$$

□

§2.12 B6 - Number Theory

Let p be a prime number. Prove that the determinant of the matrix

$$\begin{bmatrix} x & y & z \\ x^p & y^p & z^p \\ x^{p^2} & y^{p^2} & z^{p^2} \end{bmatrix}$$

is congruent modulo p to a product of polynomials of the form $ax + by + cz$, where a , b , and c are integers. (We say two integer polynomials are congruent modulo p if corresponding coefficients are congruent modulo p .)

Proof. Note that the determinant

$$P(x, y, z) = \sum_{\text{cyc}} x(y^p z^{p^2} - z^p y^{p^2}),$$

which is a polynomial of degree $p^2 + p + 1$ in x, y, z .

Suppose not all of a, b, c are zero. Without loss of generality, $a \neq 0$. Note that

$$\begin{aligned} aP(x, y, z) &= \begin{vmatrix} ax & y & z \\ ax^p & y^p & z^p \\ ax^{p^2} & y^{p^2} & z^{p^2} \end{vmatrix} \\ &= \begin{vmatrix} ax + by + cz & y & z \\ ax^p + by^p + cz^p & y^p & z^p \\ ax^{p^2} + by^{p^2} + cz^{p^2} & y^{p^2} & z^{p^2} \end{vmatrix} \\ &= \begin{vmatrix} ax + by + cz & y & z \\ a^p x^p + b^p y^p + c^p z^p & y^p & z^p \\ a^{p^2} x^{p^2} + b^{p^2} y^{p^2} + c^{p^2} z^{p^2} & y^{p^2} & z^{p^2} \end{vmatrix} \\ &= \begin{vmatrix} ax + by + cz & y & z \\ (ax + by + cz)^p & y^p & z^p \\ (ax + by + cz)^{p^2} & y^{p^2} & z^{p^2} \end{vmatrix} \\ &= (ax + by + cz) \begin{vmatrix} 1 & y & z \\ (ax + by + cz)^{p-1} & y^p & z^p \\ (ax + by + cz)^{p^2-1} & y^{p^2} & z^{p^2} \end{vmatrix} \end{aligned}$$

It follows that $P(x, y, z)$ divides $(ax + by + cz)$ whenever a, b, c are not all zero in $\mathbb{Z}/p\mathbb{Z}$. This includes $\frac{p^3-1}{p-1} = p^2 + p + 1$ terms (where we divide $p-1$ to account for scaling), which is exactly the degree of the polynomial. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, it is a unique factorization domain, so it follows that $P(x, y, z)$ is exactly the product of $ax + by + cz$ for each a, b, c not all zero in $\mathbb{Z}/p\mathbb{Z}$ (up to some constant), which proves the result. \square

§3 Putnam 2003

§3.1 A1 - Combinatorics

Let n be a fixed positive integer. How many ways are there to write n as a sum of positive integers,

$$n = a_1 + a_2 + \cdots + a_k$$

with k an arbitrary positive integer and $a_1 \leq a_2 \leq \cdots \leq a_k \leq a_1 + 1$? For example, with $n = 4$, there are four ways: 4 , $2 + 2$, $1 + 1 + 2$, $1 + 1 + 1 + 1$.

Proof. We claim that for each fixed positive integer n , there are exactly n ways to write it as a sum of positive integers satisfying the above conditions. We can prove this by induction on n . For $m = 1$, the result is clear. Suppose it is true for $n = k$. It suffices to prove the result for $n = k + 1$. By the inductive hypothesis, we can write $k = a_1 + a_2 + \cdots + a_\ell$ in k ways. For each combination, note that if we take $b_\ell = a_\ell + 1$ and $b_j = a_{j+1}$ for $1 \leq j \leq \ell - 1$, then

$$k + 1 = 1 + a_1 + \cdots + a_\ell = b_1 + b_2 + \cdots + b_\ell$$

is a valid combination for $k + 1$. There is exactly one indistinguishable way to group the extra 1 since grouping with another $a_j = a_1$ is indistinguishable and if we group with $a_j = a_1 + 1$, then the overall sum does not satisfy the condition that the last term is bounded by one more than the first term. Hence, we have exactly k sums of the above form. We have exactly one additional combination given by the sum of $k + 1$ 1's, which is a total of $k + 1$ ways, as desired.

□

§3.2 A2 - Algebra

Let a_1, a_2, \dots, a_n and b_1, b_2, \dots, b_n be nonnegative real numbers. Show that

$$(a_1 a_2 \cdots a_n)^{1/n} + (b_1 b_2 \cdots b_n)^{1/n} \leq ((a_1 + b_1)(a_2 + b_2) \cdots (a_n + b_n))^{1/n}$$

Proof. This is a direct application of Holder's Inequality. \square

§3.2.1 Alternate Solution

Proof. Note that

$$\begin{aligned} \left(\frac{\prod_{k=1}^n a_k}{\prod_{k=1}^n (a_k + b_k)} \right)^{1/n} + \left(\frac{\prod_{k=1}^n b_k}{\prod_{k=1}^n (a_k + b_k)} \right)^{1/n} &= \left(\prod_{k=1}^n \frac{a_k}{a_k + b_k} \right)^{1/n} + \left(\prod_{k=1}^n \frac{b_k}{a_k + b_k} \right)^{1/n} \\ &\leq \frac{1}{n} \sum_{k=1}^n \frac{a_k}{a_k + b_k} + \frac{1}{n} \sum_{k=1}^n \frac{b_k}{a_k + b_k} \\ &= \frac{1}{n} \sum_{k=1}^n \frac{a_k + b_k}{a_k + b_k} \\ &= \frac{1}{n} \sum_{k=1}^n 1 = 1. \end{aligned}$$

Multiplying both sides of the inequality by $\prod_{k=1}^n (a_k + b_k)^{1/n}$ gives the desired result. \square

§3.3 A3 - Calculus

Find the minimum value of

$$|\sin x + \cos x + \tan x + \cot x + \sec x + \csc x|$$

for real numbers x .

Proof. We claim the minimum value is given by $2\sqrt{2} - 1$. Let $y = \pi/4 - x$. Note that

$$\sin x + \cos x = \sqrt{2} \cos(\pi/4 - x) = \sqrt{2} \cos y,$$

$$\sin x \cos x = \frac{1}{2} \sin(2x) = \frac{1}{2} \cos(\pi/4 - 2x) = \frac{1}{2} \cos 2y = \cos^2 y - \frac{1}{2}.$$

Let $u = \sqrt{2} \cos y$.

$$\begin{aligned} \sin x + \cos x + \tan x + \cot x + \sec x + \csc x &= \sin x + \cos x + \frac{1}{\sin x \cos x} + \frac{\sin x + \cos x}{\sin x \cos x} \\ &= u + \frac{2}{u^2 - 1} + \frac{2u}{u^2 - 1} \\ &= u + \frac{2(u+1)}{u^2 - 1}. \end{aligned}$$

We wish to find the minimum value of $|f(u)|$ where $f(u) = u + \frac{2(u+1)}{u^2-1}$ and $u \in [-\sqrt{2}, \sqrt{2}]$. Note that at for $u = -1$, the possible values of y are $5\pi/4$ and $7\pi/4$. At these values, the desired expression takes the values 2 and $2 + \sqrt{2}$ respectively. Assuming $u \neq 1$, we can write $f(u) = u + \frac{2}{u-1}$.

Note that

$$f(\sqrt{2}) = \sqrt{2} + \frac{2}{\sqrt{2} - 1} = \frac{4 - \sqrt{2}}{\sqrt{2} - 1} = 2 + 3\sqrt{2},$$

$$f(-\sqrt{2}) = -\sqrt{2} - \frac{2}{\sqrt{2} + 1} = -\frac{4 + \sqrt{2}}{\sqrt{2} + 1} = 3\sqrt{2} - 2.$$

Furthermore,

$$f'(u) = 1 - \frac{2}{(u-1)^2},$$

which has critical points at $u = 1 \pm \sqrt{2}$, but $1 + \sqrt{2}$ is outside of $[-\sqrt{2}, \sqrt{2}]$, so it suffices to check $u_0 = 1 - \sqrt{2}$.

At this point

$$f(u_0) = 1 - \sqrt{2} - \frac{2}{\sqrt{2}} = 1 - 2\sqrt{2}.$$

Comparing all the critical values using the approximation $\sqrt{2} = 1.41 + O(|.01|)$, we find that the minimum possible value of $|f(u)|$ is given by $2\sqrt{2} - 1$.

□

§3.4 A4 - Algebra

Suppose that a, b, c, A, B, C are real numbers, $a \neq 0$ and $A \neq 0$, such that

$$|ax^2 + bx + c| \leq |Ax^2 + Bx + C|$$

for all real numbers x . Show that

$$|b^2 - 4ac| \leq |B^2 - 4AC|$$

Proof. First, note that we must have that $|a| \leq |A|$ which we can show by taking the limit in the given expression. Let $\delta = b^2 - 4ac$, $\Delta = B^2 - 4AC$. We can also define $p(x) = ax^2 + bx + c$ and $P(x) = Ax^2 + Bx + C$. We proceed by cases on the sign on Δ .

- Case 1: $\Delta > 0$.

In this case, we have that $P(x) = A(x - r_1)(x - r_2)$ for $r_1, r_2 \in \mathbb{R}$. Then, we have that $|p(r_1)| \leq |P(r_1)| = 0$ and $|p(r_2)| \leq |P(r_2)| = 0$ so it follows that $p(x) = a(x - r_1)(x - r_2)$. Since both polynomials have the same roots, it follows that $\frac{\sqrt{\delta}}{a} = \frac{\sqrt{\Delta}}{A}$, which is exactly the distance between r_1 and r_2 . It follows that

$$|\delta| \leq \frac{|a|^2}{|A|^2} |\Delta| \leq |\Delta|.$$

- Case 2: $\Delta = 0$.

In this case, we have that $P(x) = A(x - r)^2$ for $r \in \mathbb{R}$. As before, we have that $p(r) = 0$. Suppose that $p(x) = a(x - r)(x - s)$ for some $s \in \mathbb{R}$. Note that we also have $P'(r) = 0$ since this is the vertex of the parabola. If $s \neq r$, then we must have that $|p'(r)| > 0$ since r is not the vertex. It follows that the graphs of $|p(x)|$ and $|P(x)|$ intersect in the interval $[s, r]$ (or $[r, s]$ depending on r), which is a contradiction. It follows that $p(x) = a(x - r)^2$. Hence, $\delta = \Delta = 0$.

- Case 3: $\Delta < 0$.

In this case, we have that $P(x) = A(x - Z_1)(x - Z_2)$ for $Z_1, Z_2 \in \mathbb{C}$. Note that $|P(x)|$ is minimized at $Z_* = \frac{Z_1 + Z_2}{2}$. Suppose that $p(x) = a(x - z_1)(x - z_2)$ and let $z_* = \frac{z_1 + z_2}{2}$. We have that

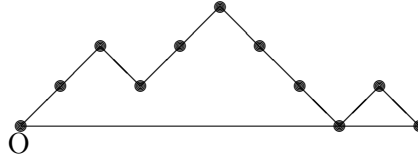
$$\frac{|A(Z_1 - Z_2)^2|}{4} = |P(Z_*)| \geq |P(z_*)| \geq |p(z_*)| = \frac{|a(z_1 - z_2)^2|}{4},$$

so it follows that $|z_1 - z_2| \geq |Z_1 - Z_2|$ which proves that $|\delta| \leq |\Delta|$ using the same method as in Case 1.

□

§3.5 A5 - Combinatorics

A Dyck n -path is a lattice path of n upsteps $(1, 1)$ and n downsteps $(1, -1)$ that starts at the origin O and never dips below the x -axis. A return is a maximal sequence of contiguous downsteps that terminates on the x -axis. For example, the Dyck 5-path illustrated has two returns, of length 3 and 1 respectively. Show that there is a one-to-one correspondence between the Dyck n -paths with no return of even length and the Dyck $(n - 1)$ paths.



Proof. Let D_{n-1} be the set of $(n - 1)$ -Dyck paths and let O_n be the set of n -Dyck paths with no return of even length. We can define functions $f : D_{n-1} \rightarrow O_n$ and $g : O_n \rightarrow D_{n-1}$ with $f \circ g = \text{id}_{O_n}$ and $g \circ f = \text{id}_{D_{n-1}}$.

We define f as follows. Let $p = a_1 a_2 \dots a_{2n-2} \in D_{n-1}$. If p has no return of even length, we can construct a path $f(p) = (1, 1)(1, -1)p \in O_n$. Otherwise, suppose p has at least one return of even length. Suppose that $a_i \dots a_j$ is the last return of even length in p . Then, we can define $f(p) = (1, 1)a_1 \dots a_i \dots a_j(1, -1)a_{j+1} \dots a_{2n-2}$. This is in O_n because the operation $f(p)$ removes all the returns before the last return of even length, which we extend to a return of odd length.

Next, we define g . Let $p = a_1 a_2 \dots a_{2n} \in O_n$. Suppose $a_i \dots a_j$ is the first return of p . We can define $f(p) = a_2 \dots a_i \dots a_{j-1} a_{j+1} \dots a_{2n}$. This is in D_{n-1} because $a_1 = (1, 1)$ and $a_j = (1, -1)$, so the remaining path remains above 0 at all times.

It is easy to verify that these functions satisfy the desired condition which gives the desired 1 - 1 correspondence. \square

§3.6 A6 - Combinatorics

For a set S of nonnegative integers, let $r_S(n)$ denote the number of ordered pairs (s_1, s_2) such that $s_1 \in S$, $s_2 \in S$, $s_1 \neq s_2$, and $s_1 + s_2 = n$. Is it possible to partition the nonnegative integers into two sets A and B in such a way that $r_A(n) = r_B(n)$ for all n ?

Proof. WLOG suppose $1 \in A$, $0 \in B$. Define $f(x) = \sum_{n \in A} x^n$, $g(x) = \sum_{n \in B} x^n$ with $|x| < 1$. Note that $f(x) + g(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$. Furthermore, note that

$$r_A(n) = [x^n](f(x^2) - f(x)^2), r_B(n) = [x^n](g(x^2) - g(x)^2),$$

where $[x^n](\cdot)$ denotes the n -th coefficient of the power series \cdot .

We wish to show that there exists a choice $A \sqcup B = \mathbb{N}$ so that $f(x^2) - f(x)^2 = g(x^2) - g(x)^2$. Equivalently, we have

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

and replacing $x \rightarrow x^{2^k}$ we obtain

$$\frac{f(x^{2^k}) - g(x^{2^k})}{f(x^{2^{k+1}}) - g(x^{2^{k+1}})} = 1 - x^{2^k}.$$

Taking the product of successive terms gives a telescoping product

$$f(x) - g(x) = \left(\prod_{k=0}^{n-1} (1 - x^{2^k}) \right) (f(x^{2^{n+1}}) - g(x^{2^{n+1}})).$$

Taking the limit as $n \rightarrow \infty$ and noting that $f(0) = 1$, $g(0) = 0$ by assumption, we have

$$f(x) - g(x) = \prod_{k=0}^{\infty} (1 - x^{2^k}).$$

Furthermore, if we let $s_j = 0$ if $j \in A$, $s_j = 1$ if $j \in B$, then we have

$$f(x) - g(x) = \sum_{n=0}^{\infty} (-1)^{s_n} x^n = \prod_{k=0}^{\infty} (1 - x^{2^k}).$$

The positive terms in the product correspond to an even number of terms, or equivalently the integers n where the sum of the digits in the binary expansion is even. It follows that taking A to be the integers where the sum of the digits in the binary expansion is even and B the integers where the sum of the digits in the binary expansion is odd satisfies the problem statement. \square

§3.7 B1 - Algebra

Do there exist polynomials $a(x)$, $b(x)$, $c(y)$, $d(y)$ such that

$$1 + xy + x^2y^2 = a(x)c(y) + b(x)d(y)$$

holds identically?

Proof. We claim no such polynomials exist. For a polynomial $P(x, y) = \sum_{i=0}^n \sum_{j=0}^n a_{ij}x^i y^j$ where n is the degree of P , we can alternatively represent it with the matrix $A = (a_{ij})$. Let $n = \max(\deg a, \deg b, \deg c, \deg d)$. Note that $1 + xy + x^2y^2$ corresponds to the $n \times n$ matrix $P = (p_{ij})$ with $p_{11} = p_{22} = p_{33} = 1$ and $p_{ij} = 0$ for all other entries. We can represent $a(x), b(x), c(y), d(y)$ with column and row vectors respectively given by A, B, C, D . Note that $\text{rank}(AC) \leq \min(\text{rank } A, \text{rank } C)$ and the rank of the row and column vectors are at most 1. It follows that

$$\text{rank}(AC + BD) \leq \text{rank } AC + \text{rank } BD \leq 2,$$

but we know that $\text{rank } P = 3$, so we cannot have $P = AC + BD$. □

§3.8 B2 - Combinatorics

Let n be a positive integer. Starting with the sequence $1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}$, form a new sequence of $n-1$ entries $\frac{3}{4}, \frac{5}{12}, \dots, \frac{2n-1}{2n(n-1)}$, by taking the averages of two consecutive entries in the first sequence. Repeat the averaging of neighbors on the second sequence to obtain a third sequence of $n-2$ entries and continue until the final sequence consists of a single number x_n . Show that $x_n < \frac{2}{n}$.

Proof. We claim that $x_n = \frac{2}{n} - \frac{1}{n2^{n-1}}$, which proves the result.

First, we show by induction that the j -th entry of the k -th sequence is given by

$$\frac{1}{2^{k-1}} \sum_{i=1}^k \frac{1}{i+j-1} \binom{k-1}{i-1}.$$

For $k=1$, the formula gives the desired starting sequence. If we suppose it holds for the k -th row, then note that

$$\begin{aligned} & \frac{1}{2} \left(\frac{1}{2^{k-1}} \sum_{i=1}^k \frac{1}{i+j-1} \binom{k-1}{i-1} + \frac{1}{2^{k-1}} \sum_{i=1}^k \frac{1}{i+(j+1)-1} \binom{k-1}{i-1} \right) \\ &= \frac{1}{2^k} \left(\frac{1}{j} + \frac{1}{k+j} + \sum_{i=2}^{k-1} \frac{1}{i+j} \left(\binom{k-1}{i-2} + \binom{k-1}{i-1} \right) \right) \\ &= \frac{1}{2^k} \left(\frac{1}{j} + \frac{1}{k+j} + \sum_{i=2}^{k-1} \frac{1}{i+j} \binom{k}{i-1} \right) \\ &= \frac{1}{2^k} \sum_{i=1}^k \frac{1}{i+j-1} \binom{k}{i-1}. \end{aligned}$$

Using this result, it follows that

$$\begin{aligned} x_n &= \frac{1}{2^{n-1}} \sum_{i=1}^n \frac{1}{i} \binom{n-1}{i-1} \\ &= \frac{1}{2^{n-1}} \sum_{i=1}^n \frac{1}{n} \binom{n}{i} \\ &= \frac{1}{n2^{n-1}} (2^n - 1) \\ &= \frac{2}{n} - \frac{1}{n2^{n-1}}. \end{aligned}$$

□

§3.9 B3 - Number Theory

Show that for each positive integer n ,

$$n! = \prod_{i=1}^n \text{lcm} \left\{ 1, 2, \dots, \left\lfloor \frac{n}{i} \right\rfloor \right\}$$

(Here lcm denotes the least common multiple, and $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.)

Proof. Let $v_p(n)$ for p prime, $n \in \mathbb{N}$ denote the exponent of p in the prime factorization of n . Note that

$$\begin{aligned} v_p \left(\prod_{k=1}^n \text{lcm} \{ 1, 2, \dots, \lfloor n/k \rfloor \} \right) &= \sum_{k=1}^n v_p (\text{lcm} \{ 1, 2, \dots, \lfloor n/k \rfloor \}) \\ &= \sum_{k=1}^n \lfloor \log_p \lfloor n/k \rfloor \rfloor \\ &= \sum_{k=1}^n \sum_{\ell: \lfloor n/k \rfloor \geq p^\ell} 1 \\ &= \sum_{\ell=1}^{\infty} \left\lfloor \frac{n}{p^\ell} \right\rfloor. \end{aligned}$$

This is exactly $v_p(n!)$ by Legendre's Theorem. □

§3.10 B4 - Algebra

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

Proof. Let $s_1 = r_1 + r_2$, $s_2 = r_3 + r_4$, $p_1 = r_1 r_2$, $p_2 = r_3 r_4$. Without loss of generality, we may assume f is a monic polynomial with rational coefficients. Note that we can write

$$\begin{aligned} f(z) &= (z^2 - s_1 z + p_1)(z^2 - s_2 z + p_2) \\ &= z^4 - (s_1 + s_2)z^3 + (p_1 + p_2 + s_1 s_2)z^2 - (s_1 p_2 + s_2 p_1)z + p_1 p_2. \end{aligned}$$

Now, note the following:

1. Since $-s_1 - s_2 = b \in \mathbb{Q}$ and $s_1 \in \mathbb{Q}$, we have that $s_2 = -s_1 - b \in \mathbb{Q}$.
2. Since $p_1 + p_2 + s_1 s_2 = c \in \mathbb{Q}$ and $s_1 s_2 \in \mathbb{Q}$, we have that $p_1 + p_2 = c - s_1 s_2 \in \mathbb{Q}$.
3. We can write

$$\begin{aligned} d &= -s_1 p_2 - s_2 p_1 \\ &= -s_1 p_2 - s_2 p_1 + s_1 p_1 - s_1 p_1 \\ &= -s_1(p_1 + p_2) + (s_1 - s_2)p_1. \end{aligned}$$

Since $s_1 \neq s_2$, it follows that

$$p_1 = \frac{d + s_1(p_1 + p_2)}{s_1 - s_2} \in \mathbb{Q}.$$

□

§3.11 B5 - Geometry

Let A , B and C be equidistant points on the circumference of a circle of unit radius centered at O , and let P be any point in the circle's interior. Let a , b , c be the distances from P to A , B , C respectively. Show that there is a triangle with side lengths a , b , c , and that the area of this triangle depends only on the distance from P to O .

Proof. Let $\omega = e^{2\pi i/3}$, $A = 1$, $B = \omega$, $C = \omega^2$, $P = z \in \mathbb{C}$ with $|z| < 1$. We have

$$a = |z - 1|, b = |z - \omega|, c = |z - \omega^2|.$$

Note that

$$(z - 1) + \omega(z - \omega) + \omega^2(z - \omega^2) = z(1 + \omega + \omega^2) - (1 + \omega^2 + \omega^4) = 0.$$

The corresponding triangle, where we visualize the complex numbers as vectors that are sides of the triangle, has side lengths of a, b, c as desired.

The area of the triangle is given by

$$\begin{aligned} |(z - 1)\overline{\omega(z - \omega)} - \overline{z - 1}\omega(z - \omega)|/4 &= |(z - 1)(\omega^2\bar{z} - \omega) - (\bar{z} - 1)(\omega z - \omega^2)|/4 \\ &= |z\bar{z}\omega^2 - \omega^2\bar{z} - z\omega + \omega - z\bar{z}\omega + \omega z + \bar{z}\omega^2 - \omega^2|/4 \\ &= |(z\bar{z} - 1)(\omega^2 - \omega)|/4 \\ &= \frac{(1 - |z|^2)\sqrt{3}}{4}, \end{aligned}$$

which is a function of z , as desired. □

§3.12 B6 - Analysis

Let $f(x)$ be a continuous real-valued function defined on $[0, 1]$. Show that

$$\int_0^1 \int_0^1 |f(x) + f(y)| \, dx dy \geq \int_0^1 |f(x)| \, dx.$$