Olympiad Notebook

Vishal Raman

August 15, 2021

Abstract

An overview of topics from math olympiads with selected problems and solutions. The sources for handouts and expositions are provided when available. Any typos or mistakes are my own - kindly direct them to my inbox.

Contents

1 Combinatorics

1.1 Invariants and Monovariants

1.2 Bijections

1.3 Pigeonhole Principle

Theorem 1.1 (Pigeonhole Principle)**.** *Let m, n be positive integers with $m \geq n$. If $m+1$ pigeons fly to n pigeonholes, then at least one pigeonhole contains at least $\left\lfloor \frac{m}{n} \right\rfloor + 1$ pigeons.*

1.4 Extremal Principle

1.5 Combinatorial Games

The main strategies for analyzing combinatorial games are:

- Play the game: try to find some forced moves.
- Reduce the game to a simpler game.
- Start at the end of the game: find endgame positions which are winning and losing and work backwards.
- Find an invariant or monovariant that a player can control.

Problem 1.2. Four heaps contain $38, 45, 61,$ and 70 matches respectively. Two players take turns choosing any two of the heaps and removing a non-zero number of matches from each heap. The player who cannot make a move loses. Which one of the players has a winning strategy?

Proof. Denote the heaps with a 4-tuple (w, x, y, z) with $w \leq x \leq y \leq z$. We claim the winning positions are of the form (w, x, y, z) with $w < y$. It is clear that $(0, 0, y, z)$ leads to a win by removing y and z and $(0, x, y, z)$ leads to a win by reducing to $(0, 1, 1, z)$ which is forced to leave either 1 or 2 heaps.

Since we remove tiles on each move, the game must terminate. If we have (w, x, y, z) with $w < y$, we can reduce to (w, w, w, x) by sending y and z to w.

We show that (w, w, w, z) is a losing position. We have three cases:

1. If we remove from two of the w-heaps, we are left with (w', w'', w, z).
2. If we remove from a w-heap and the z-heap, we are left with either (w', z', w, w) or (w', w, z', w) or (w', w, w, z').
3. If we remove any number of heaps entirely, the resulting position is clearly winning.

It follows that (w, x, y, z) with $w < y$ is a winning position as desired. □

Problem 1.3. The number 10^{2015} is written on a blackboard. Alice and Bob play a game where each player can do one of the following on each turn:

- replace an integer x on the board with integers $a, b > 1$ so that $x = ab$
- erase one or both of two equal integers on the blackboard.

The player who is not able to make a move loses the game. Who has a winning strategy?

Proof. We claim Alice has a winning strategy. First, it is clear that the game must eventually terminate. On the first turn, Alice can replace 10^{2015} with 2^{2015} and 5^{2015}. We claim that after any of Bob's turns, Alice can move the board into the state

$$2^{\alpha_1}2^{\alpha_2}\dots 2^{\alpha_k}5^{\alpha_1}5^{\alpha_2}\dots 5^{\alpha_k}.$$

If Bob sends 2^{α_j} to $2^{\beta_1}, 2^{\beta_2}$, then Alice can send 5^{α_j} to $5^{\beta_1}, 5^{\beta_2}$ and vice versa. Otherwise, if Bob removes one or two integers 2^{α_j}, 2^{α_k}, then we have $\alpha_j = \alpha_j$ so Alice can remove one or two of $5^{\alpha_j}, 5^{\alpha_k}$ or vice versa. Since Alice can always follow the copycat strategy and the game eventually terminates, we must have that Bob is unable to make a move at some point, which implies that Alice wins the game as desired. □

1.6 Algorithms

1.7 Generating Functions

Problem 1.4 (Putnam 2020 A2)**.** Let k be a non-negative integer. Evaluate

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

Proof. We claim the sum evaluates to 4^k. Note that $\binom{k+j}{j} = \binom{k+j}{k}$. It follows that the sum is the coefficient of x^k in the power series $\sum_{j=0}^{n} 2^{k-j}(1+x)^{k+j}$. Evaluating this, we find

$$\begin{aligned}\sum_{j=0}^{n} 2^{k-j}(1+x)^{k+j} &= 2^k(1+x)^k\sum_{j=0}^{k} 2^{-j}(1+x)^j \\ &= 2^k(1+x)^k\frac{1-(1+x)^{k+1}/2^{k+1}}{1-(1+x)/2} \\ &= \frac{2^{k+1}(1+x)^k-(1+x)^{2k+1}}{1-x} \\ &= 2^{k+1}(1+x)^k-(1+x)^{2k+1}\sum_{n\geq 0} x^n.\end{aligned}$$

It follows that the coefficient of x^k is given by

$$2^{k+1}\sum_{j=0}^{k}\binom{k}{j} - \sum_{j=0}^{k}\binom{2k+1}{j} = 2^{2k+1}-2^{2k} = 4^k.$$

□

Problem 1.5. (CJMO 2020/1) Let N be a positive integer, and let S be the set of all tuples with positive integer elements and a sum of N. For all tuples t, let $p(t)$ denote the product of all the elements of t. Evaluate

$$\sum_{t\in S} p(t).$$

Proof. We claim the sum evaluates to F_{2N}, where F_k denotes the k-th Fibonacci number. Note that the sum can be represented as the coefficient of x^N in $\sum_{k=1}^N \left(\sum_{n\ge 0} nx^n\right)^k$. Evaluating this, we find

$$\begin{aligned}\sum_{k=1}^N \left(\sum_{n\ge 0} nx^n\right)^k &= \sum_{k=1}^N \left(\frac{x}{(1-x)^2}\right)^k \\ &= \sum_{k=1}^N \frac{x^k}{(1-x)^{2k}} \\ &= \sum_{k=1}^N \sum_{j\ge 0} \binom{2k-1+j}{2k-1} x^{j+k}.\end{aligned}$$

The coefficient of x^N is given by

$$\sum_{k=1}^N \binom{N+k-1}{2k-1} = \sum_{k=1}^N \binom{N+k-1}{N-k} = \sum_{j\ge 0}\binom{2N-1-j}{j} = F_{2N}.$$

□

Problem 1.6 (IMO 1995/6)**.** Let p be an odd prime number. How many p-element subsets A of $\{1, 2, \ldots, 2p\}$ are there, the sum of whose elements is divisible by p?

Proof. Define $f(x, y) = \prod_{k=1}^{2p}(1 + x^k y)$. We wish to find the sum of the coefficients of terms of the form $x^{p\ell}y^p$. We do this by first considering f as a generating function in x using the root of unity filter associated to $\omega = e^{\frac{2\pi i}{p}}$. Then, we read off the coefficient of y^p to find the desired expression.

Note that for $1 \le k \le p-1$,

$$f(\omega^k, y) = \prod_{k=1}^{2p}(1+\omega^k y) = \prod_{k=1}^{p}(1+\omega^k y)^2 = (1+y^p)^2.$$

It follows that

$$\begin{aligned}\frac{1}{p}\sum_{i=0}^{p-1} f(\omega^k, y) &= \frac{1}{p}\left((1+y)^{2p} + \sum_{i=1}^{p-1} f(\omega^k, y)\right) \\ &= \frac{(1+y)^{2p} + (p-1)(1+y^p)^2}{p}.\end{aligned}$$

Finally, the coefficient of y^p is given by

$$\frac{\binom{2p}{p} + 2(p-1)}{2}.$$

□

1.8 Enumerative Combinatorics

1.9 Probabilistic Method

Some tips for using the probabilistic method:

- A statement E can be true by showing that its probability is greater than 0. item Show that E is true is the same as showing $P(\neg E) < 1$.
- Show that X can be at least or at most a by showing $E[X] \geq a$ or $E[X] \leq a$ respectively.
- Show that it is possible for $|X|$ to be at least or at most $a > 0$ by showing $E[X] = 0$ and $\text{Var}(X) \geq a^2$ or $\text{Var}(X) \leq a^2$ respectively.

1.10 Algebraic Combinatorics

1.11 Combinatorial Geometry

1.11.1 Convex Hull

Problem 1.7 (Happy-Ending Problem)**.** Suppose we have five points in the plane with no three collinear. Show that we can find four points whose convex hull is a quadrilateral.

Proof. Take the convex hull of the five points. If it is a quadrilateral or pentagon, we are done(choose any 4 points in the latter case). Suppose the convex hull is a triangle. Label the points with A through E and without loss of generality, let the points A, B, C form the triangle and D, E, be the points inside the hull.

Extend the line DE. Note that two points must lie on one side of the line - if not then we have three collinear points. It is easy to show that these four points form a convex quadrilateral. □

Problem 1.8. There are $n > 3$ coplanar points, no three collinear and every four of them are the vertices of a convex quadrilateral. Prove that the n points are the vertices of a convex n-sided polygon.

Proof. Suppose that some point P is inside the convex hull of the n points. Let Q be some vertex of the convex hull. The diagonals from Q to the other vertices divide the convex hull into triangles and since no three points are collinear, P must lie inside some triangle $\triangle QRS$. But this is a contradiction since P, Q, R, S do not form a convex quadrilateral. □

Problem 1.9 (1985 IMO Longlist)**.** Let A, B be finite disjoint sets of points in the plane such that any three distinct points in $A \cup B$ are not collinear. Assume that at least one of the sets A, B contains at least five points. Show that there exists a triangle all of whose vertices are contained in A or in B that does not contain in its interior any point from the other set.

Proof. Suppose A has at least five points. Take A_1A_2 on the boundary of the convex hull of A. For any other $A_i \in A$, define $\theta_i = \angle A_1A_2A_i$. Without loss of generality, $\theta_3 < \theta_4 < \cdots < 180°$. It follows that $\text{conv}(\{A_1, A_2, A_3, A_4, A_5\})$ contains no other points of A. □

Problem 1.10 (Putnam 2001 B6)**.** Assume that $(a_n)_{n\geq 1}$ is an increasing sequence of positive real numbers such that $\lim \frac{a_n}{n} = 0$. Must there exist infinitely many positive integers n such that

$$a_{n-i} + a_{n+i} < 2a_n$$

for $i = 1, \ldots, n-1$?

Proof. We claim such a subsequence exists. Let $A = \operatorname{conv}\{(n, a_n) : n \in \mathbb{N}\}$ 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 $a_n/n \to 0$ and a_N, N are fixed, we have that

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

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. □

2 Algebra

2.1 Polynomials

Problem 2.1 (Putnam 2005/A3)**.** Let $p(z)$ be a polynomial of degree n, all of whose zeros have absolute value 1 in the complex plane. Put $g(z) = \frac{p(z)}{z^{n/2}}$. Show that all zeros of $g'(z) = 0$ have absolute value 1.

Proof. Note that we can write $p(z) = a\prod_{j=1}^{n}(z - \omega_j)$ where $|\omega_j| = 1$ for all j. It follows that

$$\log g(z) = \log a + \sum_{j=1}^{n} \log(z - \omega_j) - \frac{n}{2}\log z = \log a + \sum_{j=1}^{n}\left(\log(z-\omega_j) - \frac{\log z}{2}\right).$$

Taking the derivative of both sides, we obtain

$$\begin{aligned}\frac{g'(z)}{g(z)} &= \sum_{j=1}^{n}\left(\frac{1}{z-\omega_j} - \frac{1}{2z}\right) \\ &= \frac{1}{2z}\sum_{j=1}^{n}\frac{z+\omega_j}{z-\omega_j} \\ &= \frac{1}{2z}\sum_{j=1}^{n}\frac{|z|^2 - 1 + \omega_j\bar{z} - z\bar{\omega}_j}{|z-\omega_j|^2} \\ &= \frac{1}{2z}\sum_{j=1}^{n}\left(\frac{|z|^2-1}{|z-\omega_j|^2} + i\frac{\operatorname{Im}(\omega_j\bar{z})}{|z-\omega_j|^2}\right).\end{aligned}$$

It follows that

$$\operatorname{Re}\left(\frac{zg'(z)}{g(z)}\right) = \frac{|z|^2-1}{2}\sum_{j=1}^{n}\frac{1}{|z-\omega_j|^2}.$$

Since $\sum_{j=1}^{n}\frac{1}{|z-\omega_j|^2} > 0$, it follows that the real part of $\frac{zg'(z)}{g(z)}$ is zero if and only if $|z|^2 - 1 = 0$, which implies that $|z|^2 = 1$. It follows that all the zeros of $g'(z)$ must either satisfy $|z|^2 = 1$ or $g(z) = 0$ which gives the desired result since the zeros of $g(z)$ lie on the unit circle on the complex plane. □

2.2 Inequalities

Theorem 2.2 (QM-AM-GM-HM)**.** *Let $x_1, \ldots, x_n \in \mathbb{R}^+$. Then,*

$$\sqrt{\frac{x_1^2 + \cdots + x_n^2}{n}} \geq \frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n} \geq \frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}}$$

with equality if and only if $x_1 = \cdots = x_n$.

Definition 2.3 (Power Mean)**.** Given $p \in \mathbb{R}$, $x_1, \ldots, x_n \in \mathbb{R}^+$, define

$$M_p(x_1, \ldots, x_n) = \begin{cases} \left(\sum_{i=1}^{n} w_i x_i^p\right)^{1/p} & \text{if } p \neq 0 \\ \prod_{i=1}^{n} x_i^{w_i} & \text{else}\end{cases}.$$

Definition 2.4 (Weighted Power Mean)**.** Given $(w_i)_{i=1}^n$ with $\sum_i w_i = 1$, define

$$M_p^w(x_1, \dots, x_n) = \begin{cases} (\sum_{i=1}^n w_i x_i^p)^{1/p} & \text{if } p \neq 0 \\ \prod_{i=1}^n x_i^{w_i} & \text{else} \end{cases}.$$

Theorem 2.5. *Given $x_1, \dots, x_n \in \mathbb{R}^+$, the following properties hold:*

- $\min(x_1, \dots, x_n) \leq M_p(x_1, \dots, x_n) \leq M_p(x_1, \dots, x_n) \leq \max(x_1, \dots, x_n)$
- $M_p(x_1, \dots, x_n) = M_p(\sigma(x_1, \dots, x_n))$ *for* $\sigma \in S_n$
- $M_p(bx_1, \dots, bx_n) = bM_p(x_1, \dots, x_n)$
- $M_p(x_1, \dots, x_{nk}) = M_p(M_p(x_1, \dots, x_n), M_p(x_{k+1}, \dots, x_{2k}), \dots, M_p(x_{(n-1)k+1}, \dots, x_{nk}))$

Theorem 2.6 (Power Mean Inequality)**.** *If $p < q$,*

$$M_p(x_1, \dots, x_n) \leq M_q(x_1, \dots, x_n),$$

with equality if and only if $x_1 = \cdots = x_n$.

2.3 Functional Equations

2.4 Linear Algebra

Problem 2.7. Let $A \in M_n(\mathbb{R})$ be skew-symmetric. Show that $\det(A) \geq 0$.

Proof. If n is odd, note that

$$\det(A) = \det(A^\intercal) = \det(-A) = (-1)^n \det(A) = -\det(A).$$

It follows that $\det(A) = 0$.

Otherwise, suppose n is even and let $p(\lambda) = \det(A - I_n\lambda)$. If $\lambda \neq 0$ is an eigenvalue, note that $p(\lambda) = 0$ by the Cayley-Hamilton Theorem. Moreover,

$$p(-\lambda) = \det(A + I_n\lambda) = \det(A^\intercal + I_n^\intercal\lambda) = \det(-A + I_n\lambda) = 0.$$

Moreover, let v be an eigenvector with corresponding eigenvalue λ. Note that

$$\langle Av, v\rangle = \lambda\langle v, v\rangle = \lambda\|v\|^2,$$

$$\langle Av, v\rangle = \langle v, A^\intercal v\rangle = \langle v, -Av\rangle = -\bar{\lambda}\langle v, v\rangle = -\bar{\lambda}\|v\|^2.$$

It follows that $\lambda = -\bar{\lambda}$, which implies that $\lambda = ri$ for $r \in \mathbb{R}$. Hence,

$$\det(A) = \prod_{j=1}^{n/2}(i\lambda_j)(-i\lambda_j) = \prod_{j=1}^{n} \lambda_j^2 \geq 0.$$

□

Problem 2.8. Let $A \in M_n(\mathbb{R})$ with $A^3 = A + I_n$. Show that $\det(A) > 0$.

Proof. Let $p(x) = x^3 - x - 1$. Note that $p(0) = -1$, $p(2) = 5$, so the polynomial has a root in the interval $(0, 2)$ by the intermediate value theorem. Furthermore, $p'(x) = 3x^2 - 1$ so the polynomial has critical points at $\pm\frac{1}{\sqrt{3}}$. It is easy to see that at both of these values, $p(x) < 0$ so it follows that the other roots of $p(x)$ are conjugate complex numbers. Let the roots be $\lambda_1, \lambda_2, \lambda_3$ with λ_1 being the positive real root and λ_2, λ_3 the conjugate complex ones. If A satisfies $A^3 = A + I_n$, then we must have the eigenvalues of A are λ_1, λ_2 and λ_3, with multiplicity $\alpha_1, \alpha_2, \alpha_3$ respectively. Since λ_2, λ_3 are complex conjugates, we must have $\alpha_2 = \alpha_3$, so it follows that

$$\det(A) = \lambda_1^{\alpha_1}(\lambda_2\lambda_3)^{\alpha_2} = \lambda_1^{\alpha_1}|\lambda_2|^{\alpha_2} > 0.$$

□

Problem 2.9. If $A, B \in M_n(\mathbb{R})$ such that $AB = BA$, then $\det(A^2 + B^2) \geq 0$.

Proof.

$$\det(A^2 + B^2) = \det(A + iB)\det(A - iB) = \det(A + iB)\overline{\det(A + iB)} = |\det(A + iB)|^2 \geq 0.$$

□

Problem 2.10. Let $A, B \in M_2(\mathbb{R})$ such that $AB = BA$ and $\det(A^2 + B^2) = 0$. Show that $\det(A) = \det(B)$.

Proof. Let $p_{A,B}(\lambda) = \det(A + \lambda B) = \det(B)\lambda^2 + (\operatorname{tr} A + \operatorname{tr} B - \operatorname{tr}(AB))\lambda + \det(A)$. By Problem 1.3, we have $\det(A + iB)$ and $\det(A - iB) = 0$, which implies that $p_{A,B}(\lambda) = c(\lambda - i)(\lambda + i) = c(\lambda^2 + 1)$. It follows that $c = \det B = \det A$. □

Problem 2.11. Let $A \in M_2(\mathbb{R})$ with $\det A = -1$. Show that $\det(A^2 + I_2) \geq 4$. When does equality hold?

Proof. First, note the identity

$$\det(X + Y) + \det(X - Y) = 2(\det X + \det Y).$$

This follows from writing $p(z) = \det(X + zY) = \det(Y)z^2 + (\operatorname{tr} X + \operatorname{tr} Y - \operatorname{tr}(XY))z + \det(X)$ and taking

$$p(1) + p(-1) = \det(X + Y) + \det(X - Y) = 2\det Y + 2\det X.$$

Then, taking $X = A^2 + I$ and $Y = 2A$, we have

$$0 \leq \det(A + I)^2 + \det(A - I)^2 = 2(\det(A^2 + I) + \det(2A)) = 2(\det(A^2 + I) - 4).$$

It follows that $\det(A^2 + I) \geq 4$ as desired. We have equality when the eigenvalues of A are 1 and -1. □

Problem 2.12. Let $A, B \in M_3(\mathbb{C})$ with $\det(A) = \det(B) = 1$. Show that $\det(A + \sqrt{2}B) \neq 0$.

2.5 Group Theory

Theorem 2.13 (Lagrange's Theorem). *Let G be a finite field. If H is a subgroup of G, then $|G| = [G : H]|H|$.*

Theorem 2.14 (Chinese Remainder Theorem for Groups). *If $\gcd(m, n) = 1$, then $\mathbb{Z}_n \times \mathbb{Z}_m \equiv \mathbb{Z}_{mn}$.*

Theorem 2.15 (Fundamental Theorem of Cyclic Groups). *Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive integer divisor k or n, the group $\langle a\rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k}\rangle$.*

Theorem 2.16 (Fundamental Theorem of Finitely Generated Abelian Groups). *If G is a finitely generated abelian group, there exists a unique integer m and unique $p_1^{e_1}, p_2^{e_2}, \dots, p_n^{e^n}$ such that*

$$G \equiv \mathbb{Z}_{p_1^{e_1}} \times \cdots \times Z_{p_n^{e_n}} \times \mathbb{Z}^m.$$

Problem 2.17 (Putnam 2009/A5). Is there a finite abelian group G such that the product of the orders of all its elements is 2^{2009}.

Proof. Suppose such a group G existed. By FTFGAG, G is a product of finite cyclic groups. By Lagrange's theorem, the generators of the groups must have order that is a power of 2. Hence, it suffices to consider G of the form

$$G \equiv \prod_{k=1}^{\infty} (\mathbb{Z}_{2^k})^{n_k},$$

where all but finitely many of the n_k's are zero.

Let d_k denote the number of elements of G with order at most 2^k. Note that $d_0 = 1$ since G has a unique identity element. Then

$$d_1 = \prod_{k=1}^{\infty} 2^{n_k} = 2^{\sum_{k=1}^{\infty} n_k}.$$

since for each $\mathbb{Z}_{2^k}$, there are exactly two elements of order 1 or 2. Similarly,

$$d_2 = 2^{n_1} 4^{\sum_{k=2}^{\infty} n_k}.$$

It is easy to prove by induction that $d_1 \mid d_k$ for all $k > 0$ and d_1 is a power of 2.

Then, note that if we let N denote the product of the orders of the elements of G, we have

$$N = 1^{d_0} 2^{d_1 - d_0} 4^{d_2 - d_1} \cdots = \prod_{k=0}^{\infty} (2^k)^{d_{k+1} - d_k}.$$

Then,

$$\log_2 N = \sum_{k=1}^{\infty} k(d_{k+1} - d_k).$$

If we would like $2009 = \log_2 N$, note that we have

$$2010 = d_1 + \sum_{k=2}^{\infty} k(d_{k+1} - d_k),$$

and the right hand side divides d_1 which is a power of 2. However, $2010 = 2 \cdot 1005$, so it follows that $d_1 = 2$. Hence,

$$1 = \log_2 d_1 = \sum_{k=0}^{\infty} d_1.$$

It follows that $G \equiv \mathbb{Z}_{2^k}$ for some k. This has 1 element of order 1 and 2^{k-1} elements of order 2^j, so it follows that

$$\log_2 N = \sum_{j=1}^{k} j(2^{j-1}) = 2^k(k-1) + 1.$$

If $2009 = \log_2 N$, then

$$2^k(k-1) = 2008 = 2^3 \cdot 251.$$

This is a contradiction since $k \leq 3$, but $8(3-1) = 16 < 2008$. □

2.6 Field Theory

3 Number Theory

3.1 Orders

3.2 P-adic Valuation

Definition 3.1. Let p be a prime and let n be a non-zero integer. We define $\nu_p(n)$ to be the exponent of p in the prime factorization of n.

Some properties which can be easily verified:

- $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$
- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
- $v_p(\gcd(a_1, \ldots, a_n)) = \min\{\nu_p(a_1), \ldots, \nu_p(a_n)\}$
- $v_p(\operatorname{lcm}(a_1, \ldots, a_n)) = \max\{\nu_p(a_1), \ldots, \nu_p(a_n)\}$

Theorem 3.2 (Legendre's Theorem)**.**

$$\nu_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ denotes the sum of the digits when written in base p.

Problem 3.3 (Putnam 2003/B3)**.** Show that for each positive integer n,

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

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

Proof. Note that

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

This is exactly $\nu_p(n!)$ by Legendre's Theorem. ∎

Problem 3.4. Prove that for any positive integer n, $n!$ is a divisor of

$$\prod_{k=0}^{n-1}(2^n - 2^k).$$

Proof. It suffices to show that for each prime $p \le n$, $\nu_p(n!) \le \nu_p\left(\prod_{k=0}^{n-1}(2^n - 2^k)\right) = \sum_{k=0}^{n-1}\nu_p(2^n - 2^k)$.

For $p = 2$,

$$\nu_2(n!) = n - s_2(n) \le n - 1,$$
$$\sum_{k=0}^{n-1}\nu_p(2^n - 2^k) \ge n - 1,$$

since $2^n - 2^k$ is even for $k \ge 1$. For $p > 2$, note that $2^{p-1} - 1 \equiv 0 \pmod{p}$ by Fermat's little theorem, which implies that $p \mid 2^{k(p-1)} - 1$ for all $k \ge 1$. Then

$$\prod_{k=0}^{n-1}(2^n - 2^k) = 2^{n(n-1)/2}\prod_{k=1}^{n}(2^k - 1),$$

and $p \nmid 2^{n(n-1)/2}$, which implies that

$$\begin{aligned}\nu_p\left(\prod_{k=0}^{n-1}(2^n - 2^k)\right) &= \sum_{k=1}^{n}\nu_p(2^k - 1)\\ &\ge \sum_{1 \le k(p-1) \le n}\nu_p(2^{k(p-1)} - 1)\\ &\ge \sum_{1 \le k(p-1) \le n} 1\\ &= \left\lfloor \frac{n}{p-1} \right\rfloor.\end{aligned}$$

But note that

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1} \le \frac{n-1}{p-1} \le \left\lfloor \frac{n}{p-1} \right\rfloor \le \nu_p\left(\prod_{k=0}^{n-1}(2^n - 2^k)\right).$$

□

Theorem 3.5 (Lifting-the-Exponent(LTE) Lemma)**.** *Let p be prime, $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$ and $p \mid (x-y)$, $p \nmid x$, $p \nmid y$.*

- *if p is odd, $\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n)$,*
- *for $p = 2$ and even n, $\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(n) + \nu_2(x+y) - 1$.*

3.3 Cyclotomic Polynomials

3.4 Finite Field Arithmetic

Refer to Evan Chen, Summations.

Theorem 3.6 (Fermat's Little Theorem)**.** *Let p be a prime. Then $a^{p-1} \equiv 1 \pmod p$ whenever* $\gcd(p, q) = 1$*.*

Theorem 3.7 (Lagrange's Theorem)**.** *If p is prime and $f(x) \in Z[x]$, then either*

- *every coefficient of $f(x)$ is divisible by p, or*
- *$f(x) \equiv 0 \pmod p$ has at most $\deg(f)$ incongruent solutions.*

Theorem 3.8 (Wilson's Theorem)**.** *For any prime p,*

$$(p-1)! \equiv -1.$$

Proof. Let $g(x) = (x-1)(x-2)\dots(x-(p-1))$ and $h(x) = x^{p-1} - 1$. Both polynomials have degree $p-1$ and leading term x^{p-1}. The constant term for $g(x)$ is $(p-1)!$. By Fermat's little theorem, $h(x)$ has roots $1, 2, \dots, p-1$ in $\mathbb{F}_p$.

Now, consider $f(x) = g(x) - h(x)$. Note that $\deg(f) \le p-2$ since the leading terms cancel. In $\mathbb{F}_p$, it also has the same roots $1, 2, \dots, p-1$. By Lagrange's Theorem(3.2), we must have that $f(x) \equiv 0 \pmod p$. It follows that $f(0) = (p-1)! + 1 \equiv 0 \pmod p$ which proves the result. □

Theorem 3.9 (Sums of Powers)**.** *Let p be a prime and n and integer. Then,*

$$\sum_{k=1}^{p-1} k^m \equiv \begin{cases} 0 \pmod p & \text{if } p-1 \nmid m \\ -1 \pmod p & \text{if } p-1 \mid m \end{cases}$$

Proof. If $p-1 \mid m$, then $(p-1)\ell = m$ for some ℓ, so it follows that

$$\sum k = 1^{p-1} k^m \equiv \sum_{k=1}^{p-1} (k^{p-1})^\ell \equiv \sum_{k=1}^{p-1} 1 \equiv p-1 \equiv -1 \pmod p.$$

Otherwise, if we let g be a generator for $(\mathbb{Z}/p\mathbb{Z})^\times$, we have

$$\sum_{k=1}^{p-1} k^m \equiv \sum_{k=0}^{p-2} g^{km} \equiv \frac{g^{(p-1)m} - 1}{g^m - 1} \equiv 0 \pmod p$$

since $g^m - 1 \not\equiv 0 \pmod p$. □

Theorem 3.10 (Wolstenholme's Theorem)**.** *Let $p > 3$ be prime. THen*

$$(p-1)! \left(\frac{1}{1} + \dots + \frac{1}{p-1} \right) \equiv 0 \pmod{p^2}.$$

Theorem 3.11 (Harmonic modulo p)**.** *For any integer $k = 1, 2, \ldots, p-1$, we have*

$$\frac{1}{k} \equiv (-1)^{k-1}\frac{1}{p}\binom{p}{k} \pmod{p}.$$

Problem 3.12 (ELMO 2009)**.** Let p be an odd prime and x be an integer such that $p \mid x^3 - 1$ but $p \nmid x - 1$. Prove that p divides

$$(p-1)!\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1}\right).$$

Proof. Note that $p \mid x^3 - 1$ and $x \nmid x - 1$ implies that $p \mid x^2 + x + 1$, so we have $1 + x \equiv -x^2 \pmod{p}$. Using Theorem 3.6, we can rewrite the expression as

$$\begin{aligned} x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1} &\equiv \frac{x}{p}\binom{p}{1} + \frac{x^2}{p}\binom{p}{2} + \cdots + \frac{x^{p-1}}{p}\binom{p}{p-1} \pmod{p} \\ &= \frac{1}{p}\left((1+x)^p - 1 - x^p\right) \pmod{p} \\ &= -\frac{1}{p}\left(1 + x^p + x^{2p}\right). \end{aligned}$$

Note that $x^{2p} + x^p + 1 \equiv (x^2 + x)^p + 1 \pmod{p}$. By the Lifting-The-Exponent(LTE) lemma,

$$\nu_p((x^2+x)^p + 1^p) = \nu_p(x^2 + x + 1) + \nu_p(p) \geq 2.$$

It follows that $1 + x^p + x^{2p} \equiv 0 \pmod{p^2}$, which proves the result. □

3.5 Arithmetic Functions

Definition 3.13. A function $f : \mathbb{N} \to \mathbb{C}$ is **multiplicative** if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. It is **completely multiplicative** if $f(mn) = f(m)f(n)$ for any $m, n \in \mathbb{N}$.

Definition 3.14 (Möbius Function)**.** The Möbius Function, μ, is defined by

$$\mu(n) = \begin{cases} (-1)^m & \text{if } n \text{ has } m \text{ distinct prime factors,} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

Definition 3.15 (Dirichlet Convolution)**.** Given two arithmetic functions, $f, g : \mathbb{N} \to \mathbb{C}$, we define

$$(f * g)(n) = \sum_{d \mid n} f(d)g(n/d) = \sum_{de=n} f(d)g(e).$$

Theorem 3.16 (Möbius Inversion)**.** *Given two arithmetic functions $f, g : \mathbb{N} \to \mathbb{C}$,*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu(d)g(n/d).$$

In other words, $g = f * 1$ if and only if $f = g * \mu$.

Problem 3.17 (Bulgaria 1989)**.** Let $\Omega(n)$ denote the number of prime factors of n, counted with multiplicity. Evaluate

$$\sum_{n=1}^{1989}(-1)^{\Omega(n)}\left\lfloor\frac{1989}{n}\right\rfloor.$$

Proof. Note that $g(n) = -1^{\Omega(n)}$ is (completely) multiplicative. Then,

$$\begin{aligned}\sum_{n=1}^{1989}(-1)^{\Omega(n)}\left\lfloor\frac{1989}{n}\right\rfloor &= \sum_{n=1}^{1989}\sum_{k\le 1989, n|k}(-1)^{\Omega(n)} \\ &= \sum_{k=1}^{1989}\sum_{n|k}(-1)^{\Omega(n)}.\end{aligned}$$

Note that $g*1$ is multiplicative so it suffices to evaluate $(g*1)(k) = \sum_{n|k}(-1)^{\Omega(n)}$ for prime powers. Note that

$$(g*1)(p^k) = \sum_{r=0}^{k}(-1)^r = \begin{cases}1 & \text{if k is even}\\ 0 & \text{else}\end{cases}.$$

It follows that $(g*1)(n) = 1$ when n is a perfect square and is 0 otherwise. Hence, the sum evaluates to $\lfloor\sqrt{1989}\rfloor = 44$. □

3.6 Quadratic Reciprocity

Definition 3.18 (Legendre Symbol)**.** For a prime p and integer a, set

$$\left(\frac{a}{p}\right) = \begin{cases}0 & p \mid a\\ 1 & a \not\equiv 0 \text{ is a quadratic residue}\\ -1 & a \not\equiv 0 \text{ is not a quadratic residue}\end{cases}.$$

Definition 3.19 (Legendre's Definition)**.** For odd primes p,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Definition 3.20 (Jacobi Symbol)**.** For any integer a and any odd positive integer $n = p_1^{e_1}\dots p_n^{e_n}$,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\cdots\left(\frac{a}{p_n}\right)^{e_n}$$

Some properties of the Jacobi Symbol:

- $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ when $a \equiv b \pmod n$
- $\left(\frac{a}{n}\right) = 0$ if and only if $\gcd(a,n) > 1$
- $\left(\frac{a}{2}\right) \in \{0,1\}$.

Theorem 3.21 (Quadratic Reciprocity)**.** *Let m, n be relatively prime positive odd integers. Then*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

and

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$$

or equivalently

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}.$$

Problem 3.22. Is 481 a quadratic residue modulo 2017?

Proof.

$$\left(\frac{481}{2017}\right) = \left(\frac{2017}{481}\right) = \left(\frac{93}{481}\right) = \left(\frac{481}{93}\right) = \left(\frac{16}{93}\right) = 1.$$

□

Problem 3.23. Show that $2^n + 1$ has no prime factors of the form $p = 8k + 7$.

Proof. Suppose $p \mid 2^n + 1$. If n is even, then $2^{2k} \equiv -1 \pmod{p}$ so $p \equiv 1 \pmod{4}$. Otherwise, we have $2^{2k+1} \equiv -1 \pmod{p}$ which implies that $-2 \equiv 2^{2(k+1)} \pmod{p}$ so -2 is a quadratic residue modulo p. Then

$$1 = \left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}} = (-1)^{\frac{p^2+4p-5}{8}} = (-1)^{\frac{(p+5)(p-1)}{8}}.$$

If $p = 8k+7$, then $4 \nmid p-1 = 8k+6$ and $8 \nmid p+5 = 8k+12$, so we cannot have $16 \mid (p+5)(p-1)$, a contradiction. □

4 Analysis

4.1 Sequences and Series

Problem 4.1 (Putnam 2020/A3). Let $a_0 = \pi/2$, and let $a_n = \sin(a_{n-1})$ for $n \geq 1$. Determine whether

$$\sum_{n=1}^{\infty} a_n^2$$

converges.

Proof. We claim the series diverges. It suffices to show that $a_n \geq \frac{1}{\sqrt{n}}$. We proceed by induction. It is clear that $a_1 = 1 \geq \frac{1}{\sqrt{1}} = 1$. Suppose that $a_k \geq \frac{1}{\sqrt{k}}$. Since $\sin x \geq x - x^3/6$ and $\sin x$ is monotonically increasing in $[0, \pi/2]$, we have

$$a_{k+1} \geq \sin\left(\frac{1}{\sqrt{k}}\right) > \frac{1}{\sqrt{k}} - \frac{1}{6k\sqrt{k}} = \frac{6k-1}{6k\sqrt{k}}.$$

It suffices to show that

$$\frac{6k-1}{6k} \geq \frac{\sqrt{k}}{\sqrt{k+1}} \Leftrightarrow 24k^2 - 11k + 1 \geq 0,$$

which is true for $k \geq 1$. □

4.2 Measure Theory and Integration

Problem 4.2 (Putnam 2002/A6). 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 $m \in \mathbb{N}$,

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

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

$$\begin{aligned}1 + \frac{1}{2} + \frac{1}{6} + \sum_{d=3}^{N} \frac{1}{f(d)} &< 1 + \frac{1}{2} + \frac{1}{6} + C\sum_{d=3}^{N} \frac{1}{f(d)} && (1)\\ &< 1 + \frac{1}{2} + \frac{1}{6} + \frac{C}{6(1-C)} && (2)\\ &= 1 + \frac{1}{2} + \frac{1}{6(1-C)} = L, && (3)\end{aligned}$$

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

Problem 4.3 (Putnam 2003/B6)**.** Let $f(x)$ be a continuous real-valued function defined on $[0, 1]$. Show that

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

Proof. Let $f^+ = \max(f(x), 0)$ and $f^- = f^+ - f$. Let $A = \operatorname{supp} f^+$, $B = \operatorname{supp} f^-$. We will denote $\|g\| = \int_0^1 |g(x)|\, dx$.

Note that

$$\int_0^1 \int_0^1 |f(x) + f(y)|\, dxdy = \left(\iint_{A\times A} + \iint_{B\times B} +2 \iint_{A\times B} \right) |f(x) + f(y)|\, dxdy.$$

Note that

$$\begin{aligned}\iint_{A\times A} |f(x) + f(y)|\, dxdy &= \iint_{A\times A} (f(x) + f(y))\, dxdy \\ &= \iint_{A\times A} f(x)\, dxdy + \iint_{A\times A} f(y)\, dxdy \\ &= 2|A|\|f^+\|.\end{aligned}$$

Similarly, $\iint_{B\times B} |f(x)+f(y)|\,dxdy = 2|B|\|f^-\|$.

Finally, note that

$$\begin{aligned}\iint_{A\times B} |f(x)+f(y)|\,dxdy &= \iint_{A\times B} |f^+(x)-f^-(y)|\,dxdy \\ &\geq \left|\iint_{A\times B} (f^+(x)-f^-(y))\,dxdy\right| \\ &= ||B|\|f^+\| - |A|\|f^-\||.\end{aligned}$$

Combining the results, we have that

$$\int_0^1\int_0^1 |f(x)+f(y)|\,dxdy \geq 2|A|\|f^+\| + 2|B|\|f^-\| + 2||B|\|f^+\| - |A|\|f^-\||.$$

Squaring both sides of the expression, we have that

$$\begin{aligned}&\left(\int_0^1\int_0^1 |f(x)+f(y)|\,dxdy\right)^2 \geq \left(2|A|\|f^+\| + 2|B|\|f^-\| + 2||B|\|f^+\| - |A|\|f^-\||\right)^2 \\ &= 4(|A|\|f^+\| + |B|\|f^-\| + ||B|\|f^+\| - |A|\|f^-\||)^2 \\ &= 4(|A|\|f^+\| + |B|\|f^-\|)^2 + 4(|B|\|f^+\| - |A|\|f^-\|)^2 + 8(|A|\|f^+\| + |B|\|f^-\|)||B|\|f^+\| - |A|\|f^-\|| \\ &\geq 4(|A|^2\|f^+\|^2 + |B|^2\|f^-\|^2 + |A|^2\|f^-\|^2 + |B|^2\|f^+\|^2) \\ &\geq 4(|A|^2+|B|^2)(\|f^+\|^2+\|f^-\|^2) \\ &\geq (|A|+|B|)^2(\|f^+\|+\|f^-\|)^2 \\ &= (1)^2(\|f\|)^2 \\ &= \left(\int_0^1 |f(x)|\,dx\right)^2.\end{aligned}$$

□

4.3 Vector Calculus

4.4 Complex Analysis

5 Geometry

5.1 Classical Results

Theorem 5.1 (Incenter-Excenter Lemma).

Theorem 5.2 (Euler's Theorem). *Let ABC be a triangle. Let R and r denote its circumradius and inradius, respectively. Let O and I denote the circumcenter and incenter. then $OI^2 = R(R-2r)$. In particular, $R \geq 2r$.*

5.2 Complex Numbers

Theorem 5.3 (Complex Special Points). *Let (ABC) be the unit circle. We have*

- *the circumcenter, $o = 0$.*
- *the orthocenter, $h = a + b + c$.*
- *the centroid, $g = \frac{a+b+c}{3}$.*
- *the nine-point center, $n_9 = \frac{a+b+c}{2}$.*

Theorem 5.4 (Complex Incenter). *Given ABC on the unit circle, it is possible to pick u, v, w such that*

- $a = u^2, b = v^2, c = w^2$,
- *the midpoint of $\widehat{BC}$ is $-vw$, the midpoint of $\widehat{CA}$ is $-wu$ and the midpoint of $\widehat{ab}$ is $-uv$,*
- *the incenter $I = -(uv - vw - wu)$.*

Theorem 5.5 (Complex Foot). *If $a \neq b$ are on the unit circle and $z \in \mathbb{C}$, then the foot from Z to AB is given by*

$$\frac{a + b + z - ab\bar{z}}{2}$$

Theorem 5.6 (Complex Shoelace). *If $a, b, c \in \mathbb{C}$, the signed area of $\triangle ABC$ is given by*

$$\frac{i}{4}\begin{vmatrix} a & \bar{a} & 1 \\ b & \bar{b} & 1 \\ c & \bar{c} & 1 \end{vmatrix}.$$

Theorem 5.7 (Concyclic Complex Numbers). *Let a, b, c, d be distinct complex numbers, not all collinear. Then A, B, C, D are concyclic if and only if*

$$\frac{b-a}{c-a} \div \frac{b-d}{c-d} \in \mathbb{R}.$$

Problem 5.8 (Putnam 2003/B5). 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

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

which is a function of z, as desired. □

Problem 5.9. Let H be the orthocenter of $\triangle ABC$. Let X be the reflection of H over $\overline{BC}$ and Y the reflection over the midpoint of $\overline{BC}$. Prove that X and Y lie on (ABC), and $\overline{AY}$ is a diameter.

Proof. Let $A = a, B = b, C = c$ be the complex number representation and without loss of generality, suppose that (ABC) is the unit circle. Note that the orthocenter is given by $h = a+b+c$. Then,

$$\begin{aligned} x &= b + (c-b)\overline{\left(\frac{h-b}{c-b}\right)} \\ &= b + (c-b)\left(\frac{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-\frac{1}{b}}{\frac{1}{c}-\frac{1}{b}}\right) \\ &= b - bc\left(\frac{a+c}{ac}\right) \\ &= b(1-1-\frac{c}{a}) \\ &= -\frac{bc}{a} \in (ABC). \end{aligned}$$

Next, if we let $m = \frac{b+c}{2}$, note that we have

$$y - m = -(h-m) \Rightarrow y = 2m - h = -a \in (ABC).$$

Furthermore, since $y = -a$, we have that $\overline{AY}$ is a diameter of (ABC). □

Sources:

1. Arthur Engel, Problem Solving Strategies

2. Evan Chen, Expected Uses of Probability

3. Evan Chen, Summation

4. Evan Chen, Euclidean Geometry in Mathematical Olympiads

5. Espen Slettnes, Probabilistic Method