

NATIONAL SCIENCE TALENT CONTEST COMPANION

Volume 2: NMTC Mathematics Olympiad Proofs

Induction, 60-degree rotation geometry, Fermat-Euler totient, Cauchy-Schwarz, Ptolemy similarity & infinite descent proofs.

10

OLYMPIAD PROOFS

KaTeX

RIGOROUS KATEX LOGIC

100%

MARKING RUBRICS INCLUDED

Dual-Theme

MIDNIGHT & PRINT READY

PRIORITY TIER 1: EXAM CONCENTRATION

60% WEIGHT

> Diophantine Equations · > Cauchy-Schwarz Bounds · > Cyclic Quadrilaterals · > Modular Invariants

PRIORITY TIER 2: ANALYTICAL CORE

40% WEIGHT

> Pigeonhole Principle · > Vieta Root Jumping · > Functional Equations · > Graph Ramsey Bounds

1 Master Olympiad Proofs

>

2 Drill Topical QBank

>

3 Battle Swarm FLP Arena

VOLUME SYLLABUS SECTIONS CHECKLIST

- ☐ M-01: Divisibility of $n(n^2 + 5)$ by 6 for All Positive...

☐ M-02: Equilateral Triangle Interior Point & 60-Degree ...
- ☐ M-03: Fermat's Little Theorem and Euler's Totient Gene...

☐ M-04: Cauchy-Schwarz Inequality & Engel's Form (Titu's...
- ☐ M-05: Ptolemy's Theorem for Cyclic Quadrilaterals & Sp...

☐ M-06: Non-Existence of Non-Trivial Integer Solutions t...
- ☐ M-07: Principle of Inclusion-Exclusion & Derangement C...

☐ M-08: Erdős-Szekeres Theorem on Monotonic Subsequences...
- ☐ M-09: Arithmetic Mean - Geometric Mean (AM-GM) via Bac...

☐ M-10: Vieta's Formulas & Newton's Sums for Polynomial ...

Divisibility of $n(n^2 + 5)$ by 6 for All Positive Integers

OFFICIAL PROBLEM STATEMENT

Prove that for all positive integral values of n , the expression $n(n^2 + 5)$ is divisible by 6.

- Provide a rigorous proof using the Principle of Mathematical Induction.
- Provide an alternative algebraic proof using the product of consecutive integers and modular arithmetic.

Step 1: Proof by Mathematical Induction (Part a)

Let $P(n)$ be the proposition that $n(n^2 + 5)$ is divisible by 6 for $n \in \mathbb{Z}^+$.

****Base Case ($n = 1$):****

For $n = 1$, the expression evaluates to:

$$1(1^2 + 5) = 1(6) = 6$$

Since $6 = 6 \times 1$, $P(1)$ is true.

****Inductive Hypothesis:****

Assume $P(k)$ is true for some positive integer k . That is, there exists an integer m such that:

$$k(k^2 + 5) = k^3 + 5k = 6m$$

****Inductive Step ($n = k + 1$):****

Evaluate the expression for $n = k + 1$:

$$(k + 1) [(k + 1)^2 + 5] = (k + 1)(k^2 + 2k + 1 + 5) = (k + 1)(k^2 + 2k + 6)$$

Expanding the product:

$$(k + 1)(k^2 + 2k + 6) = k^3 + 2k^2 + 6k + k^2 + 2k + 6 = k^3 + 3k^2 + 8k + 6$$

Regroup this expression to isolate the inductive hypothesis $k^3 + 5k$:

$$k^3 + 3k^2 + 8k + 6 = (k^3 + 5k) + (3k^2 + 3k + 6) = 6m + 3k(k + 1) + 6$$

In the term $3k(k + 1)$, the product $k(k + 1)$ is the product of two consecutive integers, so one of them must be even. Therefore, $k(k + 1) = 2p$ for some integer p .

Substituting $k(k + 1) = 2p$:

$$3k(k + 1) = 3(2p) = 6p$$

Thus, the complete expression becomes:

$$(k + 1) [(k + 1)^2 + 5] = 6m + 6p + 6 = 6(m + p + 1)$$

Since $m, p \in \mathbb{Z}$, the quantity $m + p + 1$ is an integer. Therefore, $(k + 1)[(k + 1)^2 + 5]$ is divisible by 6, completing the inductive step.

By the Principle of Mathematical Induction, $n(n^2 + 5)$ is divisible by 6 for all $n \in \mathbb{Z}^+$.

Step 2: Direct Algebraic Modular Proof (Part b)

Decompose the term $+5n$ as $-n + 6n$:

$$n(n^2 + 5) = n^3 + 5n = n^3 - n + 6n = n(n^2 - 1) + 6n = (n - 1)n(n + 1) + 6n$$

Now examine the two additive terms:

1. The term $(n - 1)n(n + 1)$ is the product of three consecutive integers. Among any three consecutive integers:

- At least one is divisible by 2.
- Exactly one is divisible by 3.

Since $\gcd(2, 3) = 1$, the product must be divisible by $2 \times 3 = 6$.

Hence, $(n - 1)n(n + 1) = 6q$ for some integer q .

2. The term $6n$ is explicitly a multiple of 6.

Summing the two terms:

$$n(n^2 + 5) = 6q + 6n = 6(q + n)$$

Since $q + n \in \mathbb{Z}$, $n(n^2 + 5) \equiv 0 \pmod{6}$ for all $n \in \mathbb{Z}^+$.

EXAMINER MARKING RUBRIC

Base case verification and formal inductive hypothesis formulation (Part a)

4 Marks

Expansion, regrouping to $(k^3 + 5k) + 3k(k + 1) + 6$, and parity argument for $k(k + 1)$ (Part a)

6 Marks

Decomposition into $(n - 1)n(n + 1) + 6n$ and three-consecutive-integers divisibility theorem (Part b)

5 Marks

OLYMPIAD INSIGHT

Any expression of the form $n(n^2 + A)$ where $A \equiv -1 \pmod{6}$ factors into $(n - 1)n(n + 1) + (A + 1)n$. Because 3 consecutive integers always contain a multiple of 2 and a multiple of 3, the leading term is guaranteed divisible by 6.

COPYABLE LATEX SNIPPET

```
P(1): 1(1^2 + 5) = 6 \implies 6 \mid 6\\
(k+1)[(k+1)^2 + 5] = (k^3 + 5k) + 3k(k+1) + 6 = 6m + 6p + 6 = 6(m + p + 1)\\
n(n^2 + 5) = (n-1)n(n+1) + 6n \equiv 0 + 0 \equiv 0 \pmod{6}
```

Equilateral Triangle Interior Point & 60-Degree Rotation Proof

OFFICIAL PROBLEM STATEMENT

Let ABC be an equilateral triangle and let P be a point inside the triangle such that:

$$PA = x, \quad PB = y, \quad PC = z$$

If the lengths satisfy $z^2 = x^2 + y^2$, determine the length of the sides of triangle ABC in terms of x and y .

Step 1: Geometric Transformation by 60-Degree Rotation

Let s denote the side length of the equilateral triangle ABC , so $AB = BC = CA = s$ and $\angle ABC = 60^\circ$.

Rotate triangle $\triangle ABP$ counterclockwise by 60° about vertex B to new triangle $\triangle CBP'$.

Under this rigid rotation:

1. Vertex B is fixed.
2. Vertex A maps to vertex C because $BA = BC = s$ and $\angle ABC = 60^\circ$.
3. Point P maps to point P' .
4. Length $BP' = BP = y$, and length $CP' = AP = x$.
5. Angle $\angle PBP' = 60^\circ$ because the rotation angle is 60° .

Step 2: Analysis of the Auxiliary Triangle $\triangle PBP'$

Consider triangle $\triangle PBP'$:

- $BP = BP' = y$
- $\angle PBP' = 60^\circ$

An isosceles triangle with an apex angle of 60° is an equilateral triangle.

Therefore, $\triangle PBP'$ is equilateral, which establishes that:

$$PP' = y, \quad \angle BPP' = \angle BP'P = 60^\circ$$

Step 3: Characterization of Triangle $\triangle PCP'$

Now consider triangle $\triangle PCP'$:

- Side $PP' = y$
- Side $CP' = x$
- Side $PC = z$

The problem specifies the relation $z^2 = x^2 + y^2$, which can be rewritten as:

$$(PC)^2 = (CP')^2 + (PP')^2$$

By the Converse of the Pythagorean Theorem, $\triangle PCP'$ must be a right-angled triangle with the right angle opposite the hypotenuse PC :

$$\angle PP'C = 90^\circ$$

Step 4: Angle Sum and Law of Cosines for Side Length s

Compute the total angle $\angle BP'C$:

$$\angle BP'C = \angle BP'P + \angle PP'C = 60^\circ + 90^\circ = 150^\circ$$

Now apply the Law of Cosines to triangle $\triangle BCP'$ with sides $BP' = y$, $CP' = x$, $BC = s$, and included angle $\angle BP'C = 150^\circ$:

$$s^2 = BC^2 = (BP')^2 + (CP')^2 - 2(BP')(CP') \cos(\angle BP'C)$$

$$s^2 = y^2 + x^2 - 2xy \cos(150^\circ)$$

Since $\cos(150^\circ) = -\cos(30^\circ) = -\frac{\sqrt{3}}{2}$:

$$s^2 = x^2 + y^2 - 2xy \left(-\frac{\sqrt{3}}{2} \right) = x^2 + y^2 + \sqrt{3}xy$$

Taking the square root gives the side length of triangle ABC :

$$s = \sqrt{x^2 + y^2 + \sqrt{3}xy}$$

EXAMINER MARKING RUBRIC

Formulation of the 60° rotation about vertex B mapping $A \rightarrow C$

5 Marks

Proof that auxiliary triangle $\triangle PBP'$ is equilateral with side y

5 Marks

Application of the converse Pythagorean theorem on $\triangle PCP'$ to find $\angle PP'C = 90^\circ$

5 Marks

Law of Cosines on $\triangle BCP'$ with $\angle BP'C = 150^\circ$ and final side length formula

5 Marks

OLYMPIAD INSIGHT

Rotating by the polygon's vertex angle (60° for equilateral triangles, 90° for squares) transforms distance relations into directly adjacent triangles, allowing the Pythagorean relation to reveal a hidden right angle.

COPYABLE LATEX SNIPPET

```
\text{Rotate } \Delta ABP \text{ by } 60^\circ \text{ about } B \implies BP' = y, \quad CP' = x \\
\Delta PBP' \text{ is equilateral } \implies PP' = y, \quad \angle B P' P = 60^\circ \\
z^2 = x^2 + y^2 \implies (PC)^2 = (CP')^2 + (PP')^2 \implies \angle P P' C = 90^\circ \\
s^2 = x^2 + y^2 - 2xy \cos(150^\circ) = x^2 + y^2 + \sqrt{3}xy \implies s = \sqrt{x^2 + y^2 + \sqrt{3}xy}
```

Fermat's Little Theorem and Euler's Totient Generalization

OFFICIAL PROBLEM STATEMENT

- State and prove Fermat's Little Theorem: If p is a prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.
- Generalize this result to Euler's Totient Theorem: If $m \in \mathbb{Z}^+$ and $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is Euler's totient function.
- Use the theorem to find the last two digits of 7^{2026} .

Step 1: Proof of Fermat's Little Theorem via Complete Residue Systems (Part a)

Consider the set of non-zero residue classes modulo p :

$$S = \{1, 2, 3, \dots, p-1\}$$

Multiply each element in S by a , where $\gcd(a, p) = 1$:

$$T = \{a \cdot 1, a \cdot 2, a \cdot 3, \dots, a \cdot (p-1)\}$$

To prove that no two elements in T are congruent modulo p , suppose for $1 \leq j < k \leq p-1$:

$$a \cdot j \equiv a \cdot k \pmod{p} \implies a(k-j) \equiv 0 \pmod{p}$$

Since $\gcd(a, p) = 1$, by Euclid's lemma p must divide $k-j$. However, $1 \leq k-j \leq p-2$, so $p \nmid (k-j)$. This is a contradiction. Furthermore, since $p \nmid a$ and $p \nmid j$, no element of T is divisible by p .

Therefore, the elements of T modulo p must be a permutation of the set S .

Multiplying all elements together:

$$\prod_{j=1}^{p-1} (a \cdot j) \equiv \prod_{j=1}^{p-1} j \pmod{p} \implies a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}$$

Since $\gcd((p-1)!, p) = 1$, dividing both sides by $(p-1)!$ yields:

$$a^{p-1} \equiv 1 \pmod{p}$$

Step 2: Proof of Euler's Totient Generalization (Part b)

Let $R = \{r_1, r_2, \dots, r_{\phi(m)}\}$ be a reduced residue system modulo m , consisting of all integers $1 \leq r_i \leq m$ with $\gcd(r_i, m) = 1$.

Let $\gcd(a, m) = 1$. Multiply each element of R by a to form the set:

$$aR = \{ar_1, ar_2, \dots, ar_{\phi(m)}\}$$

1. If $ar_j \equiv ar_k \pmod{m}$, then $a(r_j - r_k) \equiv 0 \pmod{m}$. Since $\gcd(a, m) = 1$, $r_j \equiv r_k \pmod{m}$. Thus, all elements in aR are distinct modulo m .

2. Since $\gcd(a, m) = 1$ and $\gcd(r_i, m) = 1$, $\gcd(ar_i, m) = 1$. Thus, every element of aR belongs to the reduced residue system modulo m .

Therefore, $aR \pmod{m}$ is a permutation of R .

Multiplying all elements together:

$$\prod_{i=1}^{\phi(m)} (ar_i) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m} \implies a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

Since $\gcd(\prod r_i, m) = 1$, canceling the product yields:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Step 3: Finding the Last Two Digits of 7^{2026} (Part c)

The last two digits of a number correspond to its residue modulo 100.

Compute Euler's totient function for $m = 100 = 2^2 \times 5^2$:

$$\phi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 100 \times \frac{1}{2} \times \frac{4}{5} = 40$$

Since $\gcd(7, 100) = 1$, by Euler's Totient Theorem:

$$7^{40} \equiv 1 \pmod{100}$$

Now reduce the exponent 2026 modulo 40:

$$2026 = 40 \times 50 + 26 \implies 2026 \equiv 26 \pmod{40}$$

Therefore:

$$7^{2026} \equiv (7^{40})^{50} \cdot 7^{26} \equiv 1^{50} \cdot 7^{26} \equiv 7^{26} \pmod{100}$$

Now compute $7^{26} \pmod{100}$ using successive modular squaring:

$$- 7^2 = 49$$

$$- 7^4 = 49^2 = 2401 \equiv 1 \pmod{100}$$

Notice that $7^4 \equiv 1 \pmod{100}$! (The order of 7 modulo 100 is actually 4, dividing $\phi(100) = 40$).

Reducing the exponent modulo 4:

$$2026 \equiv 2 \pmod{4} \implies 7^{2026} \equiv 7^2 = 49 \pmod{100}$$

The last two digits of 7^{2026} are exactly 49.

EXAMINER MARKING RUBRIC

Rigorous proof that multiplication by a permutes non-zero residues mod p and cancellation of $(p-1)!$ (Part a)

7 Marks

Formulation of reduced residue system and proof of Euler's totient generalization (Part b)

7 Marks

Computation of $\phi(100) = 40$, order analysis, and exact determination of last two digits 49 (Part c)

6 Marks

OLYMPIAD INSIGHT

Because multiplication by an element coprime to the modulus is an automorphism of the finite abelian group $(\mathbb{Z}/m\mathbb{Z})^\times$, it permutes the reduced residues, leaving their product invariant and yielding $a^{\phi(m)} = 1$.

COPYABLE LATEX SNIPPET

```
a \cdot S \equiv S \pmod{p} \implies a^{p-1} (p-1)! \equiv (p-1)! \pmod{p} \implies a^{p-1} \equiv 1 \pmod{p} \\ a^{\phi(m)} \prod r_i \equiv \prod r_i \pmod{m} \implies a^{\phi(m)} \equiv 1 \pmod{m} \\ \phi(100) = 40, \quad 7^4 \equiv 1 \pmod{100} \implies 7^{2026} \equiv 7^2 = 49 \pmod{100}
```

Cauchy-Schwarz Inequality & Engel's Form (Titu's Lemma)

OFFICIAL PROBLEM STATEMENT

a) Prove the Cauchy-Schwarz Inequality for real sequences: For any real numbers $a_1, \dots, a_n$ and $b_1, \dots, b_n$:

$$\left(\sum_{i=1}^n a_i^2 \right) \left(\sum_{i=1}^n b_i^2 \right) \geq \left(\sum_{i=1}^n a_i b_i \right)^2$$

State the exact necessary and sufficient condition for equality.

b) Derive Engel's Form of the Cauchy-Schwarz Inequality (often known as Titu's Lemma): For real x_i and positive reals $a_i > 0$:

$$\sum_{i=1}^n \frac{x_i^2}{a_i} \geq \frac{\left(\sum_{i=1}^n x_i \right)^2}{\sum_{i=1}^n a_i}$$

c) Use Titu's Lemma to prove that for positive reals a, b, c with $a + b + c = 1$:

$$\frac{a^2}{b+c} + \frac{b^2}{c+a} + \frac{c^2}{a+b} \geq \frac{1}{2}$$

Step 1: Proof of Cauchy-Schwarz via Quadratic Discriminant (Part a)

Consider the quadratic polynomial in real variable t :

$$P(t) = \sum_{i=1}^n (a_i t - b_i)^2$$

Since $P(t)$ is a sum of squares of real numbers, $P(t) \geq 0$ for all $t \in \mathbb{R}$.

Expanding the square inside the summation:

$$P(t) = \sum_{i=1}^n (a_i^2 t^2 - 2a_i b_i t + b_i^2) = \left(\sum_{i=1}^n a_i^2 \right) t^2 - 2 \left(\sum_{i=1}^n a_i b_i \right) t + \left(\sum_{i=1}^n b_i^2 \right)$$

Let $A = \sum a_i^2$, $B = \sum a_i b_i$, and $C = \sum b_i^2$. Then $P(t) = At^2 - 2Bt + C$.

If $A = 0$, then all $a_i = 0$, in which case both sides of the inequality are 0, and the inequality trivially holds.

For $A > 0$, since $P(t) \geq 0$ for all real t , the quadratic polynomial cannot have two distinct real roots. Therefore, its discriminant Δ must be non-positive:

$$\Delta = (-2B)^2 - 4AC = 4B^2 - 4AC \leq 0$$

Dividing by 4:

$$B^2 - AC \leq 0 \implies B^2 \leq AC$$

Substituting back the original summations:

$$\left(\sum_{i=1}^n a_i b_i \right)^2 \leq \left(\sum_{i=1}^n a_i^2 \right) \left(\sum_{i=1}^n b_i^2 \right)$$

Equality holds if and only if $\Delta = 0$, which occurs when there exists a real t_0 such that $P(t_0) = 0$. This requires $a_i t_0 - b_i = 0$ for all i , meaning the vectors $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ are linearly dependent (proportional).

Step 2: Derivation of Engel's Form / Titu's Lemma (Part b)

In the Cauchy-Schwarz inequality, make the following substitutions for $i = 1, \dots, n$:

$$u_i = \frac{x_i}{\sqrt{a_i}}, \quad v_i = \sqrt{a_i}$$

where $a_i > 0$ and $x_i \in \mathbb{R}$.

Applying Cauchy-Schwarz to sequences u_i and v_i :

$$\left(\sum_{i=1}^n u_i^2 \right) \left(\sum_{i=1}^n v_i^2 \right) \geq \left(\sum_{i=1}^n u_i v_i \right)^2$$

Substitute the values of u_i and v_i :

$$\left(\sum_{i=1}^n \frac{x_i^2}{a_i} \right) \left(\sum_{i=1}^n a_i \right) \geq \left(\sum_{i=1}^n \frac{x_i}{\sqrt{a_i}} \cdot \sqrt{a_i} \right)^2 = \left(\sum_{i=1}^n x_i \right)^2$$

Since $a_i > 0$, the sum $\sum a_i > 0$. Dividing both sides by $\sum a_i$:

$$\sum_{i=1}^n \frac{x_i^2}{a_i} \geq \frac{(\sum_{i=1}^n x_i)^2}{\sum_{i=1}^n a_i}$$

Equality holds if and only if $\frac{x_1}{a_1} = \frac{x_2}{a_2} = \dots = \frac{x_n}{a_n}$.

Step 3: Application to Nesbitt-Type Symmetric Inequality (Part c)

We seek to prove that for $a, b, c > 0$ with $a + b + c = 1$:

$$S = \frac{a^2}{b+c} + \frac{b^2}{c+a} + \frac{c^2}{a+b} \geq \frac{1}{2}$$

Apply Titu's Lemma directly with $x_1 = a, x_2 = b, x_3 = c$ and denominators $a_1 = b+c, a_2 = c+a, a_3 = a+b$:

$$S \geq \frac{(a+b+c)^2}{(b+c) + (c+a) + (a+b)} = \frac{(a+b+c)^2}{2(a+b+c)} = \frac{a+b+c}{2}$$

Since $a+b+c = 1$:

$$S \geq \frac{1}{2}$$

Equality holds if and only if $\frac{a}{b+c} = \frac{b}{c+a} = \frac{c}{a+b}$, which occurs when $a = b = c = \frac{1}{3}$.

EXAMINER MARKING RUBRIC

Formulation of non-negative quadratic polynomial $P(t) \geq 0$ and discriminant argument (Part a)

8 Marks

Substitution of $u_i = x_i/\sqrt{a_i}$ and $v_i = \sqrt{a_i}$ to derive Titu's Lemma (Part b)

6 Marks

Application of Titu's Lemma with denominator summation $2(a+b+c)$ and equality condition (Part c)

6 Marks

OLYMPIAD INSIGHT

Engel's form (Titu's Lemma) collapses fractional sum inequalities into a single squared sum in the numerator over a linear sum in the denominator, completely eliminating difficult cross-multiplications.

COPYABLE LATEX SNIPPET

```
P(t) = \sum(a_i t - b_i)^2 \ge 0 \implies \Delta = 4(\sum a_i b_i)^2 - 4(\sum a_i^2)(\sum b_i^2) \le 0 \\ u_i = \frac{x_i}{\sqrt{a_i}}, v_i = \sqrt{a_i} \implies \sum \frac{x_i^2}{a_i} \ge \frac{(\sum x_i)^2}{\sum a_i} \\ \frac{a^2}{b+c} + \frac{b^2}{c+a} + \frac{c^2}{a+b} \ge \frac{(a+b+c)^2}{2(a+b+c)} = \frac{a+b+c}{2} = \frac{1}{2}
```

Ptolemy's Theorem for Cyclic Quadrilaterals & Spiral Similarity

OFFICIAL PROBLEM STATEMENT

Let $ABCD$ be a convex quadrilateral inscribed in a circle (cyclic quadrilateral) with side lengths AB, BC, CD, DA and diagonals AC and BD .

a) Prove Ptolemy's Theorem: The product of the lengths of the diagonals equals the sum of the products of the lengths of the pairs of opposite sides:

$$AC \cdot BD = AB \cdot CD + BC \cdot AD$$

b) Derive the extension known as Ptolemy's Inequality for any general convex quadrilateral, stating when equality holds.

Step 1: Construction of Auxiliary Point via Angle Chasing

Let $ABCD$ be inscribed in circle Γ . Construct a point K on diagonal AC such that:

$$\angle ABK = \angle CBD$$

Now examine triangle $\triangle ABK$ and triangle $\triangle DBC$:

1. By construction, $\angle ABK = \angle DBC$.
2. Angle $\angle BAK = \angle BAC$ and $\angle BDC = \angle BDC$ subtend the same circular arc BC of circle Γ . Therefore, by the Inscribed Angle Theorem:

$$\angle BAK = \angle BDC$$

Since two angles are equal, the triangles are similar by AA similarity:

$$\triangle ABK \sim \triangle DBC$$

Step 2: First Side Ratio from Similarity

From the similarity $\triangle ABK \sim \triangle DBC$, write the ratio of corresponding sides:

$$\frac{AK}{CD} = \frac{AB}{BD} \implies AK = \frac{AB \cdot CD}{BD} \implies AK \cdot BD = AB \cdot CD$$

Step 3: Second Pair of Similar Triangles

Now consider triangle $\triangle KBC$ and triangle $\triangle ABD$:

1. Since $\angle ABK = \angle CBD$, adding $\angle KBD$ to both sides yields:

$$\angle ABK + \angle KBD = \angle CBD + \angle KBD \implies \angle ABD = \angle KBC$$

2. Angle $\angle BCK = \angle BCA$ and $\angle BDA$ subtend the common circular arc AB of circle Γ . Therefore:

$$\angle BCK = \angle BDA$$

By AA similarity, the triangles are similar:

$$\triangle KBC \sim \triangle ABD$$

Write the ratio of corresponding sides:

$$\frac{KC}{AD} = \frac{BC}{BD} \implies KC = \frac{BC \cdot AD}{BD} \implies KC \cdot BD = BC \cdot AD$$

Step 4: Addition of Segments and Ptolemy's Theorem (Part a)

Point K was chosen to lie strictly on diagonal segment AC . Therefore:

$$AC = AK + KC$$

Add the two equations derived in Steps 2 and 3:

$$AK \cdot BD + KC \cdot BD = AB \cdot CD + BC \cdot AD$$

Factor out BD on the left hand side:

$$(AK + KC) \cdot BD = AB \cdot CD + BC \cdot AD$$

Substituting $AK + KC = AC$ yields Ptolemy's Theorem:

$$AC \cdot BD = AB \cdot CD + BC \cdot AD$$

Q.E.D.

Step 5: Ptolemy's Inequality via Triangle Inequality (Part b)

If the four points A, B, C, D do not lie on a common circle, we construct point K in the plane such that $\triangle ABK \sim \triangle DBC$ with matching orientations.

From this similarity:

1. $\frac{BA}{BD} = \frac{BK}{BC}$, which rearranges to $\frac{BK}{BA} = \frac{BC}{BD}$.
2. The angle satisfies $\angle KBC = \angle KBD + \angle DBC = \angle KBD + \angle ABK = \angle ABD$.

By SAS similarity (the dual of spiral similarity about vertex B), $\triangle KBC \sim \triangle ABD$ holds unconditionally for any four points in the plane without requiring cyclicity.

Therefore, the two distance relations hold universally:

$$AK = \frac{AB \cdot CD}{BD} \quad \text{and} \quad KC = \frac{BC \cdot AD}{BD}$$

In general, points A, K, C form a triangle in the plane. Applying the Triangle Inequality:

$$AC \leq AK + KC$$

Multiplying both sides by BD :

$$AC \cdot BD \leq (AK + KC) \cdot BD = AK \cdot BD + KC \cdot BD = AB \cdot CD + BC \cdot AD$$

Equality holds if and only if K lies strictly on segment AC , which requires $\angle BCK = \angle BCA$.

Since $\triangle KBC \sim \triangle ABD$ guarantees $\angle BCK = \angle BDA$, equality forces $\angle BCA = \angle BDA$, which is the exact condition for quadrilateral $ABCD$ to be concyclic with vertices ordered A, B, C, D .

EXAMINER MARKING RUBRIC

Construction of point K on AC and proof of $\triangle ABK \sim \triangle DBC$ (Part a)

6 Marks

Angle addition proof of $\angle KBC = \angle ABD$ and similarity $\triangle KBC \sim \triangle ABD$ (Part a)

6 Marks

Segment summation $AK + KC = AC$ yielding $AC \cdot BD = AB \cdot CD + BC \cdot AD$ (Part a)

4 Marks

Extension to Ptolemy's Inequality via the Triangle Inequality and concyclic equality condition (Part b)

4 Marks

Constructing an angle $\angle ABK = \angle CBD$ splits diagonal AC into two segments proportional to the opposite side products, converting the non-linear four-body geometry into a linear segment addition.

COPYABLE LATEX SNIPPET

```
\angle ABK = \angle CBD \implies \Delta ABK \sim \Delta DBC \implies AK \cdot BD = AB \cdot CD\\
\angle KBC = \angle ABD \implies \Delta KBC \sim \Delta ABD \implies KC \cdot BD = BC \cdot AD\\
(AK + KC) \cdot BD = AC \cdot BD = AB \cdot CD + BC \cdot AD\\
\text{General: } AC \cdot BD \leq AB \cdot CD + BC \cdot AD \text{ (Equality iff cyclic)}
```

Non-Existence of Non-Trivial Integer Solutions to $x^3 + y^3 = z^3$

$$x^3 + y^3 = z^3$$

OFFICIAL PROBLEM STATEMENT

Prove that the Diophantine equation:

$$x^3 + y^3 = z^3$$

has no solutions in non-zero integers $x, y, z \in \mathbb{Z} \setminus \{0\}$ (Fermat's Last Theorem for exponent $n = 3$).

- Prove that if a non-trivial solution exists, there exists a primitive pairwise coprime solution x, y, z with $3 \mid z$ and $3 \nmid xy$.
- Factor $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ and apply the method of infinite descent to derive a contradiction.

Step 1: Modular Arithmetic Parity & Divisibility by 3 (Part a)

Rewrite the equation symmetrically as $x^3 + y^3 + z^3 = 0$ by replacing z with $-z$.

Without loss of generality, assume $\gcd(x, y, z) = 1$. If two variables share a prime factor p , then p^3 divides the sum of the two cubes, so $p^3 \mid z^3 \implies p \mid z$, contradicting pairwise coprimality.

Now analyze cubes modulo 9. For any integer n :

$$n^3 \equiv 0, 1, \text{ or } 8 \equiv 0, \pm 1 \pmod{9}$$

If none of x, y, z were divisible by 3, then $x^3, y^3, z^3 \in \{\pm 1\} \pmod{9}$.

The possible sums of three terms from $\{\pm 1\}$ modulo 9 are $\pm 1, \pm 3$, none of which can be $\equiv 0 \pmod{9}$.

Therefore, exactly one of the three integers must be divisible by 3. Without loss of generality, let $3 \mid z$ and $3 \nmid xy$.

Step 2: Factoring in the Ring of Integers

Since x and y are both coprime to 3, $x^3 + y^3 = -z^3$ factors over integers as:

$$(x + y)(x^2 - xy + y^2) = -z^3$$

Let $d = \gcd(x + y, x^2 - xy + y^2)$. Since:

$$x^2 - xy + y^2 = (x + y)^2 - 3xy$$

any common divisor d must divide $3xy$. Since $\gcd(x, y) = 1$, d can only share factors with 3.

Since $3 \mid z^3$, $3 \mid (x + y)$. Furthermore, $(x + y)^2$ is divisible by 9, while $3xy$ is divisible by 3 but not 9 (since $3 \nmid x, y$).

Thus, $\gcd(x + y, x^2 - xy + y^2) = 3$.

Step 3: Infinite Descent Construction (Part b)

Let $z = 3^k w$ where $3 \nmid w$ and $k \geq 1$. Then $z^3 = 3^{3k} w^3$.

Dividing the factors by their greatest common divisor 3:

$$\frac{x + y}{3^{3k-1}} \quad \text{and} \quad \frac{x^2 - xy + y^2}{3}$$

are coprime integers whose product is w^3 .

By unique factorization in $\mathbb{Z}$, each factor must be a perfect cube:

$$x + y = 3^{3k-1} u^3, \quad x^2 - xy + y^2 = 3v^3$$

where $\gcd(u, v) = 1$ and $w = uv$.

Because x and y are odd and coprime, the auxiliary variables:

$$a = \frac{x+y}{2}, \quad b = \frac{x-y}{2}$$

are coprime integers of opposite parity. Substituting $x = a + b$ and $y = a - b$:

$$x^2 - xy + y^2 = a^2 + 3b^2 = 3v^3 \implies 3 \mid a$$

Let $a = 3c$ for some integer c . Substituting gives:

$$(3c)^2 + 3b^2 = 9c^2 + 3b^2 = 3v^3 \implies b^2 + 3c^2 = v^3$$

Since $\gcd(a, b) = 1$, we have $\gcd(3c, b) = 1$, so $\gcd(b, 3c) = 1$ and v is odd.

In the ring of Eisenstein integers $\mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$, this factors as:

$$(b + c\sqrt{-3})(b - c\sqrt{-3}) = v^3$$

Any common factor of $b + c\sqrt{-3}$ and $b - c\sqrt{-3}$ must divide their sum $2b$ and their difference $2c\sqrt{-3}$. Since $\gcd(b, 3c) = 1$ and v is odd, the two factors are coprime in $\mathbb{Z}[\omega]$.

Because $\mathbb{Z}[\omega]$ is a Unique Factorization Domain and all units in $\mathbb{Z}[\omega]$ are perfect cubes ($\{\pm 1, \pm\omega, \pm\omega^2\}$), each factor is a cube.

Furthermore, since $b, c \in \mathbb{Z}$ and v is odd, the cube root must have integer components:

$$b + c\sqrt{-3} = (p + q\sqrt{-3})^3$$

for coprime integers p, q of opposite parity with $3 \nmid p$.

Expanding this cube:

$$(p + q\sqrt{-3})^3 = p(p^2 - 9q^2) + 3q(p^2 - q^2)\sqrt{-3}$$

Equating imaginary parts yields:

$$c = 3q(p^2 - q^2) = 3q(p - q)(p + q)$$

Since $a = 3c$, we have $x + y = 2a = 6c = 18q(p - q)(p + q)$.

Equating this to our earlier expression $x + y = 3^{3k-1}u^3$:

$$18q(p - q)(p + q) = 3^{3k-1}u^3 \implies 2q(p - q)(p + q) = 3^{3(k-1)}u^3$$

Because $\gcd(p, 3q) = 1$ and p, q have opposite parity, the three factors $2q$, $p - q$, and $p + q$ are pairwise coprime. By unique factorization in $\mathbb{Z}$, each factor must be a cube:

$$p - q = X^3, \quad p + q = Y^3, \quad 2q = 3^{3(k-1)}Z^3$$

Notice the linear identity $(p - q) + 2q = p + q$, which directly translates to:

$$X^3 + (3^{k-1}Z)^3 = Y^3$$

Setting $z_1 = 3^{k-1}Z$, we obtain a new non-trivial integer solution $X^3 + z_1^3 = Y^3$.

Comparing magnitudes shows that:

$$|z_1|^3 = 3^{3(k-1)}|Z|^3 \leq |2q(p - q)(p + q)| = 3^{3(k-1)}|u|^3 < 3^{3k}|u|^3|v|^3 = |z|^3$$

Thus $0 < |z_1| < |z|$.

By Fermat's Method of Infinite Descent, this yields an infinite strictly decreasing sequence of positive integers $|z| > |z_1| > |z_2| > \dots$

$\dots > 0$, an impossibility.

Therefore, $x^3 + y^3 = z^3$ has no solutions in $\mathbb{Z} \setminus \{0\}$.

EXAMINER MARKING RUBRIC

Modular cube residues mod 9 proving exactly one variable is divisible by 3 (Part a)

8 Marks

Factoring $(x + y)(x^2 - xy + y^2)$ and proving $\gcd = 3$ (Part b)

8 Marks

Descent step in $\mathbb{Z}[\omega]$ producing smaller solution $z_1 < z$ and infinite descent conclusion (Part b)

9 Marks

OLYMPIAD INSIGHT

Working in the algebraic integer ring $\mathbb{Z}[\omega]$ allows the prime 3 to ramify as $3 = -\omega^2(1 - \omega)^2$. Because $\mathbb{Z}[\omega]$ is a Unique Factorization Domain, coprime factor products must be perfect cubes, triggering infinite descent.

COPYABLE LATEX SNIPPET

```
x^3, y^3, z^3 \equiv 0, \pm 1 \pmod 9 \implies 3 \mid z, \quad 3 \nmid xy \\
(x+y)(x^2 - xy + y^2) = -z^3 \implies x+y = 3^{3k-1}u^3, \quad x^2-xy+y^2 = 3v^3 \\
b^2 + 3c^2 = v^3 \implies c = 3q(p-q)(p+q) \implies 2q(p-q)(p+q) = 3^{3(k-1)}u^3 \\
(p-q) + 2q = p+q \implies X^3 + (3^{k-1}Z)^3 = Y^3 \implies 0 < |z_1| < |z|
```

Principle of Inclusion-Exclusion & Derangement Count

Formula

Marks Total

OFFICIAL PROBLEM STATEMENT

- a) State and prove the Principle of Inclusion-Exclusion (PIE) for n finite sets $A_1, A_2, \dots, A_n$ using indicator variables.
- b) A derangement is a permutation of $\{1, 2, \dots, n\}$ such that no element appears in its original position (zero fixed points). Using PIE, derive the exact derangement formula:

$$D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!} = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right)$$

- c) Show that as $n \rightarrow \infty$, the probability that a random permutation is a derangement approaches $\frac{1}{e}$, and prove that $D_n = \left[\frac{n!}{e} \right]$ (the nearest integer).

Step 1: Proof of Principle of Inclusion-Exclusion via Indicator Functions (Part a)

Let S be a universal set containing finite sets $A_1, A_2, \dots, A_n$. For any subset $A \subseteq S$, let $\mathbf{1}_A(x)$ denote its indicator function:

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

An element x belongs to the union $\bigcup_{i=1}^n A_i$ if and only if it does not belong to the complement $\bigcap_{i=1}^n A_i^c$:

$$\mathbf{1}_{\bigcup A_i}(x) = 1 - \prod_{i=1}^n (1 - \mathbf{1}_{A_i}(x))$$

Expand the product over all n factors:

$$\prod_{i=1}^n (1 - \mathbf{1}_{A_i}(x)) = 1 - \sum_i \mathbf{1}_{A_i}(x) + \sum_{i < j} \mathbf{1}_{A_i}(x) \mathbf{1}_{A_j}(x) - \dots + (-1)^n \mathbf{1}_{A_1}(x) \dots \mathbf{1}_{A_n}(x)$$

Substituting back and summing over all $x \in S$:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{x \in S} \mathbf{1}_{\bigcup A_i}(x) = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

This establishes the Principle of Inclusion-Exclusion.

Step 2: Derivation of the Derangement Formula D_n (Part b)

Let S_n be the set of all $n!$ permutations of $\{1, 2, \dots, n\}$. For $i \in \{1, 2, \dots, n\}$, let A_i be the set of permutations where element i is a fixed point (i.e. $\pi(i) = i$).

A permutation is a derangement if it has zero fixed points: $\pi \in S_n \setminus \bigcup_{i=1}^n A_i$.

The number of derangements is:

$$D_n = n! - \left| \bigcup_{i=1}^n A_i \right|$$

Now compute the cardinality of the intersections:

1. For single set A_i : element i is fixed, while the remaining $n - 1$ elements can be permuted arbitrarily in $(n - 1)!$ ways. There are $\binom{n}{1}$ such sets.

2. For intersection $A_i \cap A_j$ ($i \neq j$): both elements i and j are fixed, leaving $(n - 2)!$ arrangements. There are $\binom{n}{2}$ pairs.

3. In general, for k fixed indices $|A_{i_1} \cap \dots \cap A_{i_k}| = (n - k)!$, with $\binom{n}{k}$ such combinations.

Applying PIE:

$$D_n = n! - \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n - k)! = n! + \sum_{k=1}^n (-1)^k \frac{n!}{k!(n - k)!} (n - k)!$$

$$D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!} = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right)$$

Step 3: Asymptotic Behavior & Nearest Integer Formula (Part c)

The probability of a randomly chosen permutation being a derangement is:

$$P(\text{Derangement}) = \frac{D_n}{n!} = \sum_{k=0}^n \frac{(-1)^k}{k!}$$

Recall the Taylor series expansion for the exponential function evaluated at $x = -1$:

$$e^{-1} = \frac{1}{e} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots$$

Therefore, in the limit:

$$\lim_{n \rightarrow \infty} \frac{D_n}{n!} = \frac{1}{e} \approx 0.367879$$

For an alternating series with strictly decreasing term magnitudes, the error is strictly bounded by the magnitude of the first omitted term:

$$\left| \frac{D_n}{n!} - \frac{1}{e} \right| < \frac{1}{(n+1)!} \implies \left| D_n - \frac{n!}{e} \right| < \frac{n!}{(n+1)!} = \frac{1}{n+1}$$

For all $n \geq 1$, $\frac{1}{n+1} \leq \frac{1}{2} = 0.5$. Since $|D_n - \frac{n!}{e}| < 0.5$ strictly, the integer D_n is at a distance strictly less than 0.5 from $\frac{n!}{e}$. Therefore, D_n is the unique nearest integer:

$$D_n = \left\lceil \frac{n!}{e} \right\rceil = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$$

EXAMINER MARKING RUBRIC

Proof of PIE using indicator function expansion $1 - \prod(1 - \mathbf{1}_{A_i})$ (Part a)

6 Marks

Formulation of fixed point sets A_i and rigorous evaluation of $\binom{n}{k}(n - k)!$ (Part b)

8 Marks

Taylor expansion connection to e^{-1} and error bound $|D_n - n!/e| < 1/(n+1) \leq 0.5$ (Part c)

6 Marks

OLYMPIAD INSIGHT

The probability of zero fixed points converges to $1/e$ with remarkable speed: already for $n = 7$, the difference $|D_7/7! - 1/e| < 0.000025$.

COPYABLE LATEX SNIPPET

```
\mathbf{1}_{\bigcup A_i} = 1 - \prod(1 - \mathbf{1}_{A_i}) \implies |\bigcup A_i| = \sum |A_i| - \sum |A_i \cap A_j| + \dots
```

$$D_n = n! - \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n-k)! = n! \sum_{k=0}^n \frac{(-1)^k}{k!} \\ \left| D_n - \frac{n!}{e} \right| < \frac{1}{n+1} \leq 0.5 \implies D_n = \left\lfloor \frac{n!}{e} \right\rfloor$$

Erdős-Szekeres Theorem on Monotonic Subsequences

Marks Total

OFFICIAL PROBLEM STATEMENT

Prove the Erdős-Szekeres Theorem: Every sequence of $N = (r - 1)(s - 1) + 1$ distinct real numbers contains either:

- A monotonically increasing subsequence of length r , or
- A monotonically decreasing subsequence of length s .

a) Provide a rigorous proof using the Pigeonhole Principle by assigning a coordinate pair (a_i, b_i) to each element.

b) Prove that the bound $N = (r - 1)(s - 1) + 1$ is sharp by constructing a counterexample sequence of length $(r - 1)(s - 1)$ containing no such subsequences.

Step 1: Pigeonhole Coordinate Assignment Proof (Part a)

Let the sequence of $N = (r - 1)(s - 1) + 1$ distinct real numbers be denoted by $(x_1, x_2, \dots, x_N)$.

For each index $i \in \{1, 2, \dots, N\}$, associate an ordered pair of positive integers (a_i, b_i) defined as follows:

- a_i is the length of the longest monotonically increasing subsequence ending at x_i .
- b_i is the length of the longest monotonically decreasing subsequence ending at x_i .

We claim that all N pairs $(a_1, b_1), (a_2, b_2), \dots, (a_N, b_N)$ are distinct.

Suppose for the sake of contradiction that there exist two indices $j < k$ such that:

$$(a_j, b_j) = (a_k, b_k)$$

Since the numbers are distinct, either $x_j < x_k$ or $x_j > x_k$:

1. If $x_j < x_k$: We can append x_k to the longest increasing subsequence ending at x_j . This yields an increasing subsequence of length $a_j + 1$ ending at x_k . Therefore, $a_k \geq a_j + 1 > a_j$, contradicting $a_j = a_k$.
2. If $x_j > x_k$: We can append x_k to the longest decreasing subsequence ending at x_j . This yields a decreasing subsequence of length $b_j + 1$ ending at x_k . Therefore, $b_k \geq b_j + 1 > b_j$, contradicting $b_j = b_k$.

In either case, $(a_j, b_j) \neq (a_k, b_k)$, proving that all N pairs are strictly distinct.

Step 2: Pigeonhole Application & Contradiction

Now suppose that the sequence contains neither an increasing subsequence of length r nor a decreasing subsequence of length s .

This assumption implies that for all $i \in \{1, 2, \dots, N\}$:

$$1 \leq a_i \leq r - 1 \quad \text{and} \quad 1 \leq b_i \leq s - 1$$

The number of possible distinct coordinate pairs (a, b) satisfying these constraints is:

$$|\text{Possible Pairs}| = (r - 1) \times (s - 1)$$

However, we have $N = (r - 1)(s - 1) + 1$ distinct pairs (a_i, b_i) .

By the Pigeonhole Principle, placing $(r - 1)(s - 1) + 1$ distinct pairs into $(r - 1)(s - 1)$ pigeonholes is impossible. Therefore, there must exist at least one index i where either:

$$a_i \geq r \quad \text{or} \quad b_i \geq s$$

This proves the theorem.

Step 3: Sharpness Construction of Length $(r - 1)(s - 1)$ (Part b)

To prove that the bound is sharp, we must construct a sequence of length $(r-1)(s-1)$ that contains no increasing subsequence of length r and no decreasing subsequence of length s .

Partition the integers $\{1, 2, \dots, (r-1)(s-1)\}$ into $r-1$ blocks of size $s-1$. Arrange the blocks in increasing order, but order the numbers within each block in decreasing order:

$$B_k = \{k(s-1), k(s-1)-1, \dots, (k-1)(s-1)+1\} \quad (k = 1, 2, \dots, r-1)$$

For example, with $r = 3, s = 3$, $N = (2)(2) = 4$, we have 2 blocks of size 2:

Sequence: (2, 1, 4, 3)

Any increasing subsequence can pick at most one element from each of the $r-1$ blocks, so its maximum length is $r-1 < r$.

Any decreasing subsequence must come entirely from within a single block (since all elements of block B_j are strictly less than all elements of block B_k for $j < k$), so its maximum length is $s-1 < s$.

Thus, the bound $(r-1)(s-1)+1$ is strictly sharp for all $r, s \geq 2$.

EXAMINER MARKING RUBRIC

Definition of coordinates (a_i, b_i) and proof that all pairs are distinct (Part a)

8 Marks

Pigeonhole application with $(r-1)(s-1)$ capacity (Part a)

6 Marks

Sharpness construction of block-reversed sequence of length $(r-1)(s-1)$ (Part b)

6 Marks

OLYMPIAD INSIGHT

Associating an ordered pair of length indicators (a_i, b_i) creates an injective map from the sequence elements into $\mathbb{N}^2$. Because elements cannot match on both coordinates without violating transitivity, the Pigeonhole Principle guarantees the bound.

COPYABLE LATEX SNIPPET

```
a_i = \text{max increasing ending at } x_i, \quad b_i = \text{max decreasing ending at } x_i \\
j < k \implies (a_j, b_j) \neq (a_k, b_k) \text{ \text{ (Injective map)}} \\
N = (r-1)(s-1) + 1 > (r-1)(s-1) \implies \exists i: a_i \geq r \text{ or } b_i \geq s
```

Arithmetic Mean - Geometric Mean (AM-GM) via Backward Induction

OFFICIAL PROBLEM STATEMENT

Prove the Arithmetic Mean - Geometric Mean (AM-GM) inequality: For any n non-negative real numbers $x_1, x_2, \dots, x_n$:

$$\frac{x_1 + x_2 + \dots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \dots x_n}$$

with equality if and only if $x_1 = x_2 = \dots = x_n$.

- Prove the base case for $n = 2$.
- Prove by forward induction that the inequality holds for all powers of two: $n = 2^k$ for $k \in \mathbb{Z}^+$.
- Use Cauchy's backward induction (decreasing from n to $n - 1$) to prove that the inequality holds for all positive integers n .

Step 1: Base Case $n = 2$ Proof (Part a)

For any real numbers $x_1, x_2 \geq 0$, consider the square of the difference of their square roots:

$$(\sqrt{x_1} - \sqrt{x_2})^2 \geq 0$$

Expanding the square:

$$x_1 - 2\sqrt{x_1 x_2} + x_2 \geq 0 \implies x_1 + x_2 \geq 2\sqrt{x_1 x_2}$$

Dividing by 2:

$$\frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2}$$

Equality holds if and only if $\sqrt{x_1} - \sqrt{x_2} = 0 \iff x_1 = x_2$.

Step 2: Forward Induction for Powers of Two $n = 2^k$ (Part b)

Assume AM-GM holds for $n = 2^{k-1}$. Consider 2^k non-negative numbers $x_1, \dots, x_{2^k}$. Group them into two sets of size 2^{k-1} :

$$\frac{x_1 + \dots + x_{2^k}}{2^k} = \frac{1}{2} \left(\frac{x_1 + \dots + x_{2^{k-1}}}{2^{k-1}} + \frac{x_{2^{k-1}+1} + \dots + x_{2^k}}{2^{k-1}} \right)$$

Apply the base case $n = 2$ to the two grouped averages:

$$\frac{x_1 + \dots + x_{2^k}}{2^k} \geq \sqrt{\left(\frac{x_1 + \dots + x_{2^{k-1}}}{2^{k-1}} \right) \left(\frac{x_{2^{k-1}+1} + \dots + x_{2^k}}{2^{k-1}} \right)}$$

Now apply the inductive hypothesis for $n = 2^{k-1}$ to each group:

$$\frac{x_1 + \dots + x_{2^k}}{2^k} \geq \sqrt{\left(\prod_{i=1}^{2^{k-1}} x_i \right)^{1/2^{k-1}} \left(\prod_{i=2^{k-1}+1}^{2^k} x_i \right)^{1/2^{k-1}}} = \left(\prod_{i=1}^{2^k} x_i \right)^{1/2^k}$$

By mathematical induction, AM-GM holds for all $n = 2^k$.

Step 3: Cauchy's Backward Induction for Arbitrary n (Part c)

Suppose AM-GM holds for some integer n . We will prove it holds for $n - 1$.

Let $x_1, x_2, \dots, x_{n-1}$ be $n - 1$ non-negative real numbers. Define their arithmetic mean as:

$$A = \frac{x_1 + x_2 + \dots + x_{n-1}}{n - 1}$$

Construct an n -th number equal to this mean: $x_n = A$.

Now apply the AM-GM inequality to the n numbers $x_1, \dots, x_{n-1}, A$:

$$\frac{x_1 + \dots + x_{n-1} + A}{n} \geq (x_1 x_2 \dots x_{n-1} A)^{1/n}$$

Notice that $x_1 + \dots + x_{n-1} = (n - 1)A$, so the numerator becomes:

$$\frac{(n - 1)A + A}{n} = \frac{nA}{n} = A$$

Substituting back:

$$A \geq \left(\prod_{i=1}^{n-1} x_i \cdot A \right)^{1/n}$$

Raise both sides to the n -th power:

$$A^n \geq \left(\prod_{i=1}^{n-1} x_i \right) A$$

If $A = 0$, then $x_1 = \dots = x_{n-1} = 0$ since all $x_i \geq 0$, in which case the inequality holds trivially ($0 \geq 0$). For $A > 0$, dividing both sides by A yields:

$$A^{n-1} \geq \prod_{i=1}^{n-1} x_i \implies A \geq \left(\prod_{i=1}^{n-1} x_i \right)^{1/(n-1)}$$

Substituting back $A = \frac{x_1 + \dots + x_{n-1}}{n-1}$:

$$\frac{x_1 + \dots + x_{n-1}}{n - 1} \geq \left(\prod_{i=1}^{n-1} x_i \right)^{1/(n-1)}$$

This proves that if AM-GM holds for n , it must hold for $n - 1$.

Since every positive integer m is bounded above by some power of two 2^k , we can reach any m by ascending to 2^k and descending backward step by step.

Thus, AM-GM holds for all $n \in \mathbb{Z}^+$.

EXAMINER MARKING RUBRIC

Proof of $n = 2$ base case via $(\sqrt{x_1} - \sqrt{x_2})^2 \geq 0$ (Part a)

4 Marks

Forward induction proof for all powers of two $n = 2^k$ (Part b)

7 Marks

Cauchy backward induction by substituting $x_n = A$ and algebraic simplification (Part c)

9 Marks

OLYMPIAD INSIGHT

Cauchy's backward induction is a celebrated technique in Olympiad mathematics: setting the n -th variable equal to the average A preserves the left-hand mean while isolating the $(n - 1)$ -th product on the right.

COPYABLE LATEX SNIPPET

$n = 2: \frac{x_1 + x_2}{2} - \sqrt{x_1 x_2} = \frac{(\sqrt{x_1} - \sqrt{x_2})^2}{2} \geq 0 \backslash$

$n = 2^k \implies \text{Forward induction across pairs} \backslash$

$x_n = A = \frac{\sum_{i=1}^{n-1} x_i}{n-1} \implies A \geq (x_1 \dots x_{n-1})^{1/n} \implies A^{n-1} \geq \prod_{i=1}^{n-1} x_i$

Vieta's Formulas & Newton's Sums for Polynomial Roots

Marks Total

OFFICIAL PROBLEM STATEMENT

Let $P(x) = x^n - e_1x^{n-1} + e_2x^{n-2} - \dots + (-1)^n e_n$ be a monic polynomial of degree n with roots $r_1, r_2, \dots, r_n$, where e_k is the k -th elementary symmetric polynomial.

Let $p_k = \sum_{i=1}^n r_i^k$ denote the k -th power sum of the roots.

- a) Derive Vieta's formulas relating coefficients e_k to roots r_i .
 b) Derive Newton's Sums recurrence relation for $k \geq 1$:

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} - \dots + (-1)^{k-1} e_{k-1} p_1 + (-1)^k k e_k = 0, \quad (1 \leq k \leq n)$$

- c) For a cubic polynomial $x^3 - 2x^2 + 3x - 4 = 0$, compute the power sum $p_4 = r_1^4 + r_2^4 + r_3^4$.

Step 1: Vieta's Formulas Derivation (Part a)

By the Fundamental Theorem of Algebra, any monic polynomial $P(x)$ factors over $\mathbb{C}$ as:

$$P(x) = \prod_{i=1}^n (x - r_i)$$

Expand the product using combinatorial selection:

$$\prod_{i=1}^n (x - r_i) = x^n - \left(\sum_i r_i \right) x^{n-1} + \left(\sum_{i < j} r_i r_j \right) x^{n-2} - \dots + (-1)^n (r_1 r_2 \dots r_n)$$

Equating coefficients with $P(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \dots + (-1)^n e_n$ yields Vieta's formulas:

$$e_1 = \sum_i r_i, \quad e_2 = \sum_{i < j} r_i r_j, \quad \dots, \quad e_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} r_{i_1} \dots r_{i_k}, \quad e_n = \prod_{i=1}^n r_i$$

Step 2: Derivation of Newton's Sums Recurrence (Part b)

Take the logarithmic derivative of $P(x) = \prod_{i=1}^n (x - r_i)$:

$$\ln P(x) = \sum_{i=1}^n \ln(x - r_i) \implies \frac{P'(x)}{P(x)} = \sum_{i=1}^n \frac{1}{x - r_i} = \frac{1}{x} \sum_{i=1}^n \frac{1}{1 - r_i/x}$$

Expand each term as a formal geometric series for $|x| > |r_i|$:

$$\frac{1}{1 - r_i/x} = \sum_{k=0}^{\infty} \left(\frac{r_i}{x} \right)^k = 1 + \frac{r_i}{x} + \frac{r_i^2}{x^2} + \dots$$

Summing across all n roots:

$$\frac{P'(x)}{P(x)} = \frac{1}{x} \sum_{k=0}^{\infty} \frac{1}{x^k} \left(\sum_{i=1}^n r_i^k \right) = \frac{n}{x} + \frac{p_1}{x^2} + \frac{p_2}{x^3} + \frac{p_3}{x^4} + \dots = \sum_{k=0}^{\infty} \frac{p_k}{x^{k+1}}$$

Multiply both sides by $P(x) = x^n - e_1x^{n-1} + e_2x^{n-2} - \dots + (-1)^ne_n$:

$$P'(x) = (x^n - e_1x^{n-1} + e_2x^{n-2} - \dots) \left(\frac{n}{x} + \frac{p_1}{x^2} + \frac{p_2}{x^3} + \dots \right)$$

Also, directly differentiate $P(x)$ term-by-term:

$$P'(x) = nx^{n-1} - (n-1)e_1x^{n-2} + (n-2)e_2x^{n-3} - \dots + (-1)^{n-1}e_{n-1}$$

Equating corresponding powers of x^{n-k} on both sides yields Newton's Sums:

$$p_1 - e_1 = 0 \implies p_1 = e_1$$

$$p_2 - e_1p_1 + 2e_2 = 0$$

$$p_3 - e_1p_2 + e_2p_1 - 3e_3 = 0$$

$$p_k - e_1p_{k-1} + e_2p_{k-2} - \dots + (-1)^k ke_k = 0 \quad (1 \leq k \leq n)$$

For $k > n$, since $P(r_i) = 0$, multiplying by r_i^{k-n} and summing gives:

$$p_k - e_1p_{k-1} + e_2p_{k-2} - \dots + (-1)^ne_np_{k-n} = 0$$

Step 3: Calculating p_4 for $x^3 - 2x^2 + 3x - 4 = 0$ (Part c)

For the polynomial $x^3 - 2x^2 + 3x - 4 = 0$, the elementary symmetric polynomials are:

$$e_1 = 2, \quad e_2 = 3, \quad e_3 = 4$$

Apply Newton's Sums sequentially:

1. $k = 1$:

$$p_1 = e_1 = 2$$

2. $k = 2$:

$$p_2 - e_1p_1 + 2e_2 = 0 \implies p_2 = e_1p_1 - 2e_2 = (2)(2) - 2(3) = 4 - 6 = -2$$

3. $k = 3$:

$$p_3 - e_1p_2 + e_2p_1 - 3e_3 = 0 \implies p_3 = e_1p_2 - e_2p_1 + 3e_3$$

$$p_3 = (2)(-2) - (3)(2) + 3(4) = -4 - 6 + 12 = 2$$

4. $k = 4$ (here $k > n$, so the constant multiplier is e_3):

$$p_4 - e_1p_3 + e_2p_2 - e_3p_1 = 0 \implies p_4 = e_1p_3 - e_2p_2 + e_3p_1$$

$$p_4 = (2)(2) - (3)(-2) + (4)(2) = 4 + 6 + 8 = 18$$

Therefore, the fourth power sum of the roots is exactly $p_4 = r_1^4 + r_2^4 + r_3^4 = 18$.

Expansion of monic factored form $\prod (x - r_i)$ and derivation of Vieta's formulas (Part a)

5 Marks

Logarithmic derivative $P'(x)/P(x) = \sum p_k x^{-(k+1)}$ generating function derivation (Part b)

9 Marks

Step-by-step computation of $p_1, p_2, p_3, p_4 = 18$ using Newton's sums (Part c)

6 Marks

OLYMPIAD INSIGHT

Newton's sums connect linear algebra and generating functions to polynomial roots without explicitly solving for radicals. The logarithmic derivative acts as a bridge between the elementary symmetric polynomials e_k and power sums p_k .

COPYABLE LATEX SNIPPET

```
\frac{P'(x)}{P(x)} = \sum_{k=0}^{\infty} \frac{p_k}{x^{k+1}} \implies P'(x) = P(x) \sum_{k=0}^{\infty} p_k x^{-(k+1)} \\ p_k - e_1 p_{k-1} + e_2 p_{k-2} - \dots + (-1)^k e_k = 0 \\ e_1 = 2, e_2 = 3, e_3 = 4 \implies p_1 = 2, p_2 = -2, p_3 = 2, p_4 = 18
```



THE APIS RETENTION PROTOCOL

Active Recall Launchpad

Transition immediately from passive derivation reading to high-stakes retrieval practice.

The Recognition Illusion: Why Familiarity Isn't Mastery

Reading step-by-step mathematical proofs produces fluent cognitive familiarity that vanishes during competitive exam pressure. True Olympiad problem solving requires closed-book active reconstruction and timed MCQ drills.



Drill NSTC QuestionBank

[beambeprep.com/qbank/start/14/ >](https://beambeprep.com/qbank/start/14/)



Descriptive Web Vault

[beambeprep.com/olympiads/resources/ >](https://beambeprep.com/olympiads/resources/)

ESSENTIAL NUMERICAL VALUES & CONSTANTS

EULER NUMBER (E)

2.718281828

PI CONSTANT (PI)

3.141592653

GOLDEN RATIO (PHI)

1.618033988

SQRT(2) DIAGONAL

1.414213562

SQRT(3) TRIANGULAR

1.732050807

EULER-MASCHERONI (GAMMA)

0.577215664

APERY CONSTANT ZETA(3)

1.202056903

TOTIENT PHI(100)

40

1 Proofs Mastered

2 QBank Accuracy > 85%

3 FLP Screening Qualified