MathCastle

USAMO (Olympiad Proofs)

Complete course booklet • 22 topics

Contents

1 Proof Techniques **4**

1.1 The Main Forms 4

2 Pigeonhole & Extremal **4**

2.1 Two Existence Principles 4

3 Invariants & Monovariants **5**

3.1 Process Problems 5

4 Inequalities **5**

4.1 The Essential Inequalities 6

4.2 Good-to-Know Inequalities 6

5 Invariants & Extremal Arguments **7**

5.1 Proof Ideas That Win 7

6 Calculus Foundations, Proved **8**

6.1 How to Find Limits 8

6.2 The Derivative Rules, Proved 8

6.3 The Fundamental Theorem, Explained 9

7 Everything USAMO Tests **10**

7.1 The Syllabus, Honestly 10

8 Olympiad Number Theory **10**

8.1 The Proof-Level Toolkit 10

9 Olympiad Combinatorics **11**

9.1 Existence and Impossibility 11

10 Olympiad Geometry **12**

10.1 The Configurations That Recur 12

11 Olympiad Algebra & Functional Equations **12**

11.1 Proof-Level Algebra 12

12 Olympiad Geometry II: Circles, Tangents & Cyclic Quadrilaterals **13**

12.1 The Circle Toolkit 13

12.2 Proofs & Why It Matters 14

12.3 Going Deeper: Worked Problems 15

13 Olympiad Combinatorics II: Colorings, Games & Graphs **15**

13.1 Structures and Strategies 15

13.2 Proofs & Why It Matters 16

13.3 Going Deeper: Worked Problems 17

14 Olympiad Number Theory II: Residues, Diophantine Equations & Factorials **17**

14.1 Deeper Arithmetic 17

14.2 Proofs & Why It Matters 18

14.3 Going Deeper: Worked Problems 19

15 Olympiad Algebra II: Polynomials, Recurrences & Radical Equations **19**

15.1 Algebra at Proof Level 20

15.2 Proofs & Why It Matters 21

15.3 Going Deeper: Worked Problems 21

16 Olympiad Inequalities II: The Full Ladder **21**

16.1 Every Standard Inequality, Placed 22

16.2 Proofs & Why It Matters 23

16.3 Going Deeper: Worked Problems 23

17 Olympiad Geometry III: Circumcircle, Power of a Point, Incircle **24**

17.1 Circles Doing the Work 24

18 Olympiad Number Theory III: Exponential Diophantine Equations **25**

18.1 Equations in Exponents 25

19 Functional Equations With Tricky Conditions **26**

19.1 Pinning Down the Function 26

20 Bijections, Homothety & Structured Counting **27**

20.1 Counting by Correspondence 27

21 USAMO Practice Tests & Write-Up Playbook **28**

21.1 Sit a Practice Test 28

22 Formulas & Methods **29**

22.1 Algebra & Inequalities 29

22.2 Number Theory & Combinatorics 30

22.3 Geometry 30

1 Proof Techniques

How to structure a rigorous argument

1.1 The Main Forms

Direct, contradiction, contrapositive

To prove $P \Rightarrow Q$: argue directly; or assume P and $\neg Q$ and reach a contradiction; or prove the contrapositive $\neg Q \Rightarrow \neg P$.

In plain terms. There are three standard ways to prove "if P then Q." Pick whichever gives you the most concrete facts to start from.

Example. To show $\sqrt{2}$ is irrational, assume it equals p/q in lowest terms (contradiction) and derive that p, q are both even.

Induction, weak and strong

Prove a base case, then show it for n (weak) — or for all values below n (strong) — implies it for $n + 1$.

In plain terms. Knock over the first domino, then show each domino knocks over the next, and they all fall.

Example. Prove $1 + 3 + \cdots + (2n - 1) = n^2$: true at $n = 1$, and adding $2n + 1$ to n^2 gives $(n + 1)^2$.

Well-ordering / minimal counterexample

Every nonempty set of positive integers has a least element, so assuming a smallest counterexample and building a smaller one is a contradiction.

In plain terms. If something could fail, look at the smallest case where it fails — then show you could make an even smaller one, which is impossible.

Example. To prove every $n > 1$ has a prime factor: the smallest divisor above 1 must itself be prime, or it would have a smaller one.

2 Pigeonhole & Extremal

Existence from counting and extremes

2.1 Two Existence Principles

Pigeonhole principle

If $n + 1$ objects go into n boxes, some box holds at least two; more generally some box holds at least $\lceil m/n \rceil$ of m objects.

In plain terms. More items than boxes forces a box to double up. The trick is choosing boxes so that "two in a box" is exactly what you want.

Example. Among any 13 people, two share a birth month: 13 people, 12 months, so some month repeats.

Extremal principle

Consider the largest, smallest, or closest object; its extremal property forces structure.

In plain terms. Look at the most extreme case in the setup — the biggest, smallest, or nearest — and its special status usually breaks the problem open.

Example. Among finitely many points, the two *closest* ones can't have a third point strictly between them.

3 Invariants & Monovariants

Quantities that never change, or move one way

3.1 Process Problems

Invariant

Find a quantity — a parity, a sum mod k, a coloring — that a process never changes. If start and target differ in it, the target is unreachable.

In plain terms. Spot something that stays the same no matter what moves you make; if the goal has a different value, you can never get there.

Example. On a chessboard, a domino always covers one black and one white square, so you can never tile a board with two same-color corners removed.

Monovariant

A quantity that only increases (or only decreases) each step proves the process must terminate.

In plain terms. Find something that always moves one direction; since it can't do so forever, the process has to stop.

Example. If each move strictly lowers a positive whole-number "energy," the moves must eventually end.

4 Inequalities

AM–GM, Cauchy–Schwarz, smoothing

4.1 The Essential Inequalities

AM–GM and Cauchy–Schwarz

AM–GM: $\dfrac{\sum a_i}{n} \geq \sqrt[n]{\prod a_i}$. Cauchy–Schwarz: $\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$.

In plain terms. AM–GM says an average beats a geometric mean; Cauchy–Schwarz bounds a "dot product" by the sizes of the two lists. Together they settle most olympiad inequalities.

Example. By AM–GM, $a+b+c \geq 3\sqrt[3]{abc}$; if $abc = 1$ this gives $a+b+c \geq 3$.

Rearrangement and smoothing

A sum $\sum a_i b_i$ is largest when both sequences are sorted the same way; "smoothing" nudges variables toward equality while keeping the constraint.

In plain terms. Pair big with big to maximize a sum of products; to find an extreme, gently push the variables together and watch the value improve.

Example. To maximize ab with $a+b=10$ fixed, smoothing pushes toward $a=b=5$, giving the maximum 25.

4.2 Good-to-Know Inequalities

Titu's lemma (Cauchy, Engel form)

$\dfrac{x_1^2}{a_1} + \dfrac{x_2^2}{a_2} + \cdots + \dfrac{x_n^2}{a_n} \;\geq\; \dfrac{(x_1+x_2+\cdots+x_n)^2}{a_1+a_2+\cdots+a_n}$ for positive denominators, with equality when the $\frac{x_i}{a_i}$ are all equal.

In plain terms. Any sum of "squares over things" is at least the square of the summed tops over the summed bottoms — the fastest tool for minimizing sums of fractions under a linear constraint.

Example. With $a+b+c=20$: $\dfrac{4}{a}+\dfrac{9}{b}+\dfrac{25}{c} \geq \dfrac{(2+3+5)^2}{20} = 5$, met at $(4,6,10)$.

The QM–AM–GM–HM chain

For positive reals: $\sqrt{\dfrac{\sum a_i^2}{n}} \;\geq\; \dfrac{\sum a_i}{n} \;\geq\; \sqrt[n]{\prod a_i} \;\geq\; \dfrac{n}{\sum \frac{1}{a_i}}$, all with equality exactly when the numbers are equal.

In plain terms. Four averages, always in this order: quadratic, arithmetic, geometric, harmonic. Contest problems hand you one end of the chain and ask about the other.

Example. $(a+b+c)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right) \geq 9$ is exactly AM $\geq$ HM in disguise.

Check the equality case first

Before hunting bounds, ask WHERE equality would hold and whether the constraint permits it — an unattainable equality point means the true extremum sits at a boundary instead.

In plain terms. AM–GM promising 12 means nothing if the balancing point violates the constraint: minimize $\frac{9}{u} + 4u$ on $0 < u \leq 1$ and the answer is 13 at the endpoint, not 12.

Example. Equality in Cauchy–Schwarz needs proportional sequences; if the constraint forbids proportionality, look at the boundary.

5 Invariants & Extremal Arguments

Quantities that never change, elements that must exist

5.1 Proof Ideas That Win

Invariants

An **invariant** is a quantity a process never changes. If the start and the goal have different invariant values, the goal is impossible.

In plain terms. Find something the moves cannot alter, then compare start to finish.

Example. A domino covers one black and one white square, so the count (black squares covered) $-$ (white squares covered) is invariant — which is why a board missing two same-colored corners cannot be tiled.

The pigeonhole principle

Placing more than n objects into n boxes forces some box to hold at least two.

In plain terms. Too many things, too few slots — a collision is guaranteed.

Example. Among any 13 people, two share a birth month, because there are only 12 months.

The extremal principle

Look at the largest, smallest, or closest element — its extremeness forces structure the middle elements do not have.

In plain terms. Start the argument at the most extreme case; it has the least room to misbehave.

Example. Among finitely many points not all on one line, a pair at *minimum* distance is the classic starting move for contradiction arguments.

6 Calculus Foundations, Proved

Limits, derivative rules, and the fundamental theorem — with proofs

6.1 How to Find Limits

The ladder: five moves, in order

1. Plug in — if the function is continuous there, that IS the limit. **2. Factor and cancel** the $\frac{0}{0}$ — a common factor of top and bottom is why both vanish. **3. Multiply by the conjugate** when radicals block factoring. **4. L'Hôpital's rule** on genuine $\frac{0}{0}$ or $\frac{\infty}{\infty}$ forms. **5. Squeeze** an oscillating expression between two bounds that agree.

In plain terms. Try the cheap moves first. Each step of the ladder exists because the one before it can fail.

Example. $\lim_{x\to 3} \dfrac{x^2-9}{x-3}$: plug-in gives $\frac{0}{0}$; factoring gives $x+3 \to 6$.

***L'Hpital's* rule — one way, not the only way**

If $f, g \to 0$ (or both $\to \pm\infty$) and $g' \neq 0$ nearby, then $\lim \dfrac{f(x)}{g(x)} = \lim \dfrac{f'(x)}{g'(x)}$ when the right side exists. Sketch of why: near a, $f(x) \approx f'(a)(x-a)$ and $g(x) \approx g'(a)(x-a)$ — the ratio of two straight lines through zero is the ratio of their slopes.

In plain terms. When both parts race to zero, compare their SPEEDS. It is a tool of last resort — factoring is usually faster and never illegal.

Example. $\lim_{x\to 0} \dfrac{1-\cos x}{x^2} = \lim \dfrac{\sin x}{2x} = \frac{1}{2}$ (two applications, or the half-angle identity).

The squeeze theorem, with its classic

If $g \leq f \leq h$ near the point and $g, h \to L$, then $f \to L$: f has nowhere else to go. The classic: comparing areas of a triangle, a sector, and a bigger triangle in the unit circle pins $\cos x \leq \dfrac{\sin x}{x} \leq 1$, so $\lim_{x\to 0} \dfrac{\sin x}{x} = 1$. ■

In plain terms. Trap the wiggly thing between two tame things that meet.

Example. $\lim_{x\to 0} x^2 \sin\frac{1}{x} = 0$, squeezed between $\pm x^2$.

6.2 The Derivative Rules, Proved

Proof of the product rule

In $\dfrac{f(x+h)g(x+h) - f(x)g(x)}{h}$, add and subtract $f(x+h)g(x)$ in the numerator and split:

$f(x+h)\dfrac{g(x+h)-g(x)}{h} + g(x)\dfrac{f(x+h)-f(x)}{h} \to fg' + gf'$. ■

In plain terms. A product changes because the first factor changes OR the second does; the add-subtract trick separates the two effects.

Example. $\left(x^2 \sin x\right)' = 2x \sin x + x^2 \cos x$.

The power rule from the binomial theorem

For whole n: $(x+h)^n = x^n + nx^{n-1}h + \binom{n}{2}x^{n-2}h^2 + \cdots$, so $\dfrac{(x+h)^n - x^n}{h} = nx^{n-1} + h(\cdots) \to nx^{n-1}$. ■

In plain terms. Only the term with ONE h survives the divide-and-shrink; everything after it still carries an h and dies.

Example. $\left(x^5\right)' = 5x^4$ — the binomial's second column.

Quotient rule: nothing new to memorize

Write $\dfrac{f}{g} = f \cdot g^{-1}$ and apply the product and chain rules: $\left(fg^{-1}\right)' = f'g^{-1} - fg^{-2}g' = \dfrac{f'g - fg'}{g^2}$. The quotient rule is a corollary, not an axiom. ■

In plain terms. If you know product + chain, you already own the quotient rule.

Example. $\left(\dfrac{2x+1}{x-3}\right)' = \dfrac{2(x-3)-(2x+1)}{(x-3)^2} = \dfrac{-7}{(x-3)^2}$.

6.3 The Fundamental Theorem, Explained

Why accumulating area recovers the function

Let $A(x)$ be the area under f from a to x. Over a sliver $[x, x+h]$ the added area is a near-rectangle of height $\approx f(x)$: $\dfrac{A(x+h)-A(x)}{h} \approx f(x)$, and the approximation sharpens as $h \to 0$ (continuity). So $A'(x) = f(x)$ — differentiation undoes accumulation. ■

In plain terms. The rate at which area piles up IS the height of the curve right there.

Example. $\dfrac{d}{dx} \int_0^x t^2\, dt = x^2$, and indeed $\int_0^x t^2 dt = \frac{x^3}{3}$.

Why antiderivatives compute definite integrals

If $F' = f$, then F and the area function A have the SAME derivative, so they differ by a constant; evaluating at the endpoints kills the constant: $\int_a^b f = F(b) - F(a)$. ■

In plain terms. Any antiderivative works, because the constant cancels in the subtraction.

Example. $\int_0^\pi \sin x\,dx = [-\cos x]_0^\pi = 1 - (-1) = 2.$

7 Everything USAMO Tests

The four pillars and the complete checklist

7.1 The Syllabus, Honestly

What you need to know

Four pillars, each appearing on every USAMO/USAJMO: (1) ALGEBRA — inequalities (AM–GM, Cauchy–Schwarz, Schur, rearrangement, Jensen/convexity, smoothing, SOS), polynomials (Vieta, roots of unity, integer-coefficient divisibility), functional equations (substitution, Cauchy's equation, injectivity/surjectivity arguments), sequences and recurrences; (2) NUMBER THEORY — divisibility and gcd, modular arithmetic and orders, primitive roots, lifting the exponent, Vieta jumping, Diophantine equations, p-adic valuations, Zsigmondy as a citable tool; (3) COMBINATORICS — pigeonhole, extremal principle, invariants and monovariants, double counting, bijections, induction on structures, graph theory (degrees, trees, bipartite, Turn/Mantel), games and strategies, coloring arguments; (4) GEOMETRY — angle chasing, similar triangles, power of a point and radical axes, cyclic quadrilaterals, Ceva/Menelaus, homothety and spiral similarity, inversion, complex/coordinate bash as a last resort.

How the exam works

Six problems over two days, 7 points each, full proofs required. Graders reward complete rigorous arguments; a correct answer without proof earns 0. Write-ups matter: state what you are proving, label lemmas, handle equality cases and edge cases explicitly, and never skip the "why" of a claimed step. Problems 1 and 4 are entry-level; 3 and 6 are the hardest.

8 Olympiad Number Theory

Orders, LTE, Vieta jumping, and valuations

8.1 The Proof-Level Toolkit

Orders and primitive roots

The order of a mod n divides $\varphi(n)$ and divides any k with $a^k \equiv 1$. Use CRT to compute orders mod composite numbers: $\mathrm{ord}_{1000}(3) = \mathrm{lcm}(\mathrm{ord}_8, \mathrm{ord}_{125}) = \mathrm{lcm}(2, 100) = 100$. A primitive root exists mod p, p^k, $2p^k$ — and its existence converts multiplicative questions into additive ones on exponents.

Lifting the exponent

For odd prime $p \mid a-b$, $p \nmid ab$: $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$; for $p \mid a+b$ and odd n: $v_p(a^n + b^n) = v_p(a+b) + v_p(n)$. The $p = 2$ case adds $v_2(a+b) - 1$ for even n. Example: $v_3(2^{243} + 1) = 1 + 5 = 6$. LTE turns "how many times does p divide" into arithmetic.

Vieta jumping

For a symmetric quadratic Diophantine equation, take the solution with $a + b$ minimal; Vieta gives a second root $a' = kb - a$ that yields a smaller solution unless a boundary case holds — which then proves the required structure. The IMO 1988 classic: $\frac{a^2+b^2}{ab+1} = k$ forces k to be a perfect square.

Worked: SFFT on a unit-fraction equation

$\frac{1}{x} + \frac{1}{y} = \frac{1}{12}$ becomes $(x-12)(y-12) = 144$; positive solutions correspond to the $\tau(144) = 15$ divisor pairs. Simon's Favorite Factoring Trick — add the constant that completes the product — is the first thing to try on any equation with an xy term.

9 Olympiad Combinatorics

Invariants, extremal arguments, double counting, graphs

9.1 Existence and Impossibility

Invariants and monovariants

To prove a process can never reach a state, find a quantity it preserves (parity, a sum mod m, a coloring count) that differs between start and goal. To prove it terminates, find a monovariant — an integer quantity that strictly decreases. The 1..2026 difference game: the parity of the sum is invariant and odd, so the last number is odd — at least 1.

Extremal principle and pigeonhole

Look at the largest, smallest, or closest object — extremeness forces structure. Pigeonhole with $kn + 1$ objects in n boxes forces $k + 1$ together; the generalized and infinite versions and "pigeonhole on residues" cover a huge fraction of olympiad existence proofs.

Double counting and graphs

Count incidences two ways to derive an identity or inequality (the handshake lemma is the prototype). Graph theory: degree sums, trees have $n-1$ edges, bipartite iff no odd cycle, Mantel/Turn bound edges without a triangle ($\leq n^2/4$; 25 for $n = 10$). Model the problem as a graph the moment "pairs" or "relations" appear.

10 Olympiad Geometry

Power of a point, radical axes, spiral similarity, inversion

10.1 The Configurations That Recur

Power of a point and radical axes

For a point P and circle, $PA \cdot PB$ is constant over lines through P (negative inside). The locus of equal power to two circles is the RADICAL AXIS — a line through their intersections, found by subtracting the circle equations (for $x^2 + y^2 = 25$ and $(x-6)^2 + y^2 = 9$ it is $x = \frac{13}{3}$). Three circles' radical axes concur at the radical center.

Homothety, spiral similarity, inversion

Homothety maps a figure to a scaled copy (tangent circles, midpoints, the nine-point circle). Spiral similarity (rotation + scaling about a center) explains why two segments AB, CD have a unique center of spiral similarity sending one to the other — the Miquel point of the configuration. Inversion turns circles through the center into lines: the tool for "circles tangent to circles" problems.

When to bash

Coordinates, complex numbers, or barycentrics are legitimate when the configuration is computationally tame (a triangle with one circle, fixed ratios). Set up so symmetries are visible (unit circle for cyclic configurations in complex numbers), and remember a synthetic lemma often shortens the bash to two lines.

11 Olympiad Algebra & Functional Equations

Inequalities at proof level, polynomials, functional equations

11.1 Proof-Level Algebra

The inequality ladder

AM–GM (with equality iff all equal: $\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \geq 3$), Cauchy–Schwarz and its Engel form $\sum \frac{a_i^2}{b_i} \geq \frac{(\sum a_i)^2}{\sum b_i}$, rearrangement, Chebyshev, Jensen for convex functions, Schur, and the SOS (sum of squares) method. Always locate the equality case first; it tells you which inequality to apply and where to apply it.

Functional equations

Substitute strategically ($x = y = 0$, $y = -x$, $y = 1$), look for injectivity or surjectivity, and guess the form ($f(x + y) = f(x) + f(y) + xy$ suggests $\frac{x^2}{2} + cx$). Cauchy's equation $f(x + y) = f(x) + f(y)$ has only linear solutions under any regularity (monotone, bounded, continuous). Always verify the found function satisfies the original equation.

Polynomials at proof level

Integer polynomials: $a - b \mid P(a) - P(b)$. Roots of unity filter and symmetric-function book-keeping ($r^2+s^2+t^2 = 4$ for x^3-2x+5 without touching the roots). Irreducibility via Eisenstein or reduction mod p. Degree and leading-coefficient comparison to pin down polynomial identities.

12 Olympiad Geometry II: Circles, Tangents & Cyclic Quadrilaterals

Tangent lengths, Brahmagupta, Ptolemy, the British flag, and where circles hide

12.1 The Circle Toolkit

Tangent lengths and the incircle

From an external point the two tangent segments to a circle are equal. For the incircle of a triangle the contact point D on BC satisfies $BD = s - b$, where s is the semiperimeter.

The three pairs of equal tangents from A, B, C give a linear system whose solution is $s - a$, $s - b$, $s - c$ — in the 13-14-15 triangle, $BD = 21 - 15 = 6$ and $DC = 8$. Combined with $r = \frac{\text{Area}}{s}$ ($= 4$ there) and $R = \frac{abc}{4\cdot\text{Area}}$ ($= \frac{65}{8}$), every incircle and circumcircle length is available before any angle is chased. Common tangent lengths between two circles are right triangles: external $\sqrt{d^2 - (r_1 - r_2)^2}$, internal $\sqrt{d^2 - (r_1 + r_2)^2}$.

Cyclic quadrilaterals: Ptolemy and Brahmagupta

A quadrilateral is cyclic iff opposite angles sum to 180° (or iff an angle equals the exterior angle at the opposite vertex). Ptolemy: $AC \cdot BD = AB \cdot CD + AD \cdot BC$. Brahmagupta: Area $= \sqrt{(s - a)(s - b)(s - c)(s - d)}$.

Ptolemy is the workhorse: it computes the diagonal of an inscribed quadrilateral from its sides, and its equality case (Ptolemy's INEQUALITY holds for all quadrilaterals, with equality iff cyclic) is a cyclicity criterion in disguise. Brahmagupta is Heron with a fourth factor; sides $5, 6, 7, 8$ enclose $4\sqrt{105}$. The cyclic configuration maximizes area among quadrilaterals with given sides — Bretschneider's formula shows why.

Coordinate lemmas that save an hour

British flag: for a point P and rectangle $ABCD$, $PA^2 + PC^2 = PB^2 + PD^2$. Stewart: $b^2m + c^2n = a(d^2 + mn)$ for a cevian of length d splitting a into $m+n$. Apollonius: the median $m_a^2 = \frac{2b^2+2c^2-a^2}{4}$.

The British flag theorem makes $PC^2 - PD^2 = PB^2 - PA^2$ regardless of where P is; Stewart computes any cevian from the sides; Apollonius is Stewart's special case. All three are Pythagoras or the law of cosines applied twice, and all three turn "find the length" problems into arithmetic — worth memorizing precisely because they are so easy to rederive under pressure that people never do.

Where the circle is hiding

When a problem mentions equal angles subtended from two points, a right angle over a segment, or a point equidistant from three others, there is a circle — draw it. Cyclic quadrilaterals appear whenever two angles "see" the same segment; the moment you find one, Ptolemy, inscribed angles, and power of a point all become available at once.

Try it: Try it: Ptolemy on a rectangle

Use Ptolemy's theorem to prove the Pythagorean theorem.

Answer. A rectangle $ABCD$ with sides a, b is cyclic (opposite angles 90°). Ptolemy: $AC \cdot BD = AB \cdot CD + AD \cdot BC$ becomes $d \cdot d = a \cdot a + b \cdot b$, i.e. $d^2 = a^2 + b^2$. Pythagoras is Ptolemy for rectangles.

12.2 Proofs & Why It Matters

Proof: Ptolemy's theorem

For cyclic $ABCD$: $AC \cdot BD = AB \cdot CD + AD \cdot BC$.

Choose E on diagonal AC with $\angle ABE = \angle DBC$. Then triangles ABE and DBC are similar (two angles: the constructed one, and $\angle BAE = \angle BDC$ as inscribed angles on arc BC), giving $\frac{AE}{DC} = \frac{AB}{DB}$, i.e. $AE \cdot DB = AB \cdot DC$. Similarly triangles EBC and ABD are similar, giving $EC \cdot DB = BC \cdot AD$. Add: $(AE + EC) \cdot DB = AB \cdot DC + BC \cdot AD$, and $AE + EC = AC$. ■ Significance: the same construction with E off the diagonal proves Ptolemy's inequality for non-cyclic quadrilaterals — the equality case is exactly cyclicity.

Proof: tangent lengths $BD = s - b$

The incircle contact points split the sides into the tangent lengths $s - a$, $s - b$, $s - c$.

Let the tangent lengths from A, B, C be x, y, z (equal tangents from each vertex). Then $y + z = a$, $z + x = b$, $x + y = c$; adding, $x + y + z = s$, so $y = s - (z + x) = s - b$. ■ The identical bookkeeping with an EXCIRCLE gives tangent lengths s and $s - c$ etc., which is why $s - a$ appears everywhere in triangle geometry.

12.3 Going Deeper: Worked Problems

Worked: a length via Stewart

In triangle ABC with $AB = 7$, $AC = 9$, $BC = 8$, the angle bisector from A meets BC at D. Find AD.

Step 1 — the angle bisector theorem: $\frac{BD}{DC} = \frac{AB}{AC} = \frac{7}{9}$, so $BD = \frac{7}{16} \cdot 8 = 3.5$, $DC = 4.5$. Step 2 — Stewart with $a = 8$, $m = 3.5$, $n = 4.5$, $b = 9$, $c = 7$: $81 \cdot 3.5 + 49 \cdot 4.5 = 8(d^2 + 3.5 \cdot 4.5)$, i.e. $283.5 + 220.5 = 8d^2 + 126$, so $8d^2 = 378$, $d^2 = 47.25$, $d = \frac{3\sqrt{21}}{2}$. Step 3 — cross-check with the bisector-length formula $AD^2 = bc - mn = 63 - 15.75 = 47.25$ ✓. Two formulas, one number — always run the second when the first is arithmetic-heavy.

Worked: cyclicity proves concurrency

Show that the perpendicular bisectors of the sides of a triangle are concurrent (the circumcenter exists).

Step 1 — the perpendicular bisector of AB is the locus of points equidistant from A and B; likewise for BC. Step 2 — their intersection O (they are not parallel since AB and BC are not) satisfies $OA = OB$ and $OB = OC$, hence $OA = OC$. Step 3 — so O lies on the perpendicular bisector of AC as well: all three concur, and the circle centered at O through A passes through B and C. The proof is one sentence once "perpendicular bisector = equidistance locus" is internalized; the same locus argument gives the incenter (angle bisectors = equidistance from lines).

13 Olympiad Combinatorics II: Colorings, Games & Graphs

Extremal boards, matchings, no-adjacency counts, forests and cycles

13.1 Structures and Strategies

Extremal boards: bound by partition, achieve by pattern

To maximize black cells on a 6×6 board with no fully black 2×2: partition into nine 2×2 blocks, each holding at most 3 — bound 27; achieve it by whitening every cell with both coordinates even.

The two halves of every extremal argument: an UPPER BOUND from a partition or a counting/pigeonhole argument, and a CONSTRUCTION that attains it. Boards and grids love partitions into small blocks; the construction is usually a periodic pattern (a lattice of white cells, a checkerboard, stripes). If the bound and the construction differ, one of them is wrong — and the gap tells you which direction to think in.

Matchings, gaps, and forced adjacency

Perfect matchings of $2n$ people: $(2n-1)!! = \frac{(2n)!}{2^n n!}$ (945 for ten). "No two X adjacent": place the other items, then choose gaps for the X's.

MISSISSIPPI with no two I's adjacent: arrange the seven non-I letters ($\frac{7!}{4!2!} = 105$), choose 4 of the 8 gaps (70): 7350. The gap method generalizes to circular arrangements (gaps = items) and to "at least k apart" (reserve $k-1$ spacers per gap). A forest on n vertices has $n-c$ edges, so n edges force a cycle — the pigeonhole of graph theory.

Games: work backward from the end

A position is losing (P) iff every move leads to a winning (N) position; label backward from the terminal state. Subtraction games (take 1–3) are losing at multiples of 4; Nim is losing iff the XOR of heap sizes is 0.

The backward-induction table is mechanical; the SKILL is spotting the pattern (a modulus, a parity, an invariant) so it can be proved for all n: state the claimed set of P-positions, then show every move from a P-position lands in N and every N-position has a move into P. Symmetry strategies ("mirror the opponent") are the other standard family — valid only when the mirror move is always available, which must be argued.

Colorings as invariants

A domino covers one black and one white cell; a 2×1 tiling of a mutilated board fails because the color counts differ. Tile shapes suggest colorings with more colors (three for 1×3 trominoes, diagonals for L-shapes). When a coloring argument fails, try a weighting: assign $x^i y^j$ to cell (i, j) and compare polynomial sums.

Try it: Try it: a coloring impossibility

Can a 10×10 board be tiled by 1×4 tiles?

Answer. Color the board with four colors by $(i + j) \bmod 4$. Every 1×4 tile covers one cell of each color, but the 10×10 board has color counts $26, 25, 25, 24$ (they are not all equal, since 100 is divisible by 4 but the diagonal count pattern is uneven). Unequal counts mean no tiling exists.

13.2 Proofs & Why It Matters

Proof: a forest on n vertices with c components has $n - c$ edges

Hence any graph with at least n edges contains a cycle.

Each component is a tree; a tree on k vertices has $k - 1$ edges (induct: a tree with $k \geq 2$ vertices has a leaf — a longest path's endpoint — and removing it leaves a tree on $k - 1$ vertices with one fewer edge). Summing over components gives $n - c$. ■ Significance: "n edges force a cycle" is the first nontrivial fact about graphs, and it underlies spanning-tree algorithms and the rank of the cycle space.

Proof: Bouton's theorem for Nim

A Nim position is losing for the player to move iff the XOR of heap sizes is 0.

Two facts. (i) From a position with XOR 0, every move changes exactly one heap, hence changes the XOR to nonzero (XOR-ing a nonzero change). (ii) From XOR $s \neq 0$, take the highest bit of s; some heap h has that bit set, and $h \oplus s < h$, so reducing that heap to $h \oplus s$ is a legal move making the total XOR 0. The terminal position (all zero) has XOR 0 and is a loss for the mover; induction on the total stones finishes it. ■ Significance: every impartial game is equivalent to a Nim heap (Sprague–Grundy) — this single proof classifies a whole genre.

13.3 Going Deeper: Worked Problems

Worked: an invariant in a token game

Tokens sit on $1, 2, \dots, 2026$ on a number line. A move takes two tokens at $a < b$ and moves them to $a - 1$ and $b + 1$. Can all tokens end up on a single point? Prove your answer.

Step 1 — look for an invariant: the SUM of positions is preserved (a decreases by 1, b increases by 1), and so is... the sum of SQUARES? $(a-1)^2+(b+1)^2 = a^2+b^2+2(b-a)+2 > a^2+b^2$ — strictly increases (a monovariant). Step 2 — if all tokens sat at one point x, then $2026x = \sum k = 2026 \cdot \frac{2027}{2}$, so $x = 1013.5$ — not an integer position. Step 3 — so the configuration is impossible: the conserved sum forces a non-integer center. (The monovariant separately shows the process, if unrestricted, never cycles.) Invariants answer "can it be done"; monovariants answer "must it stop."

Worked: a strategy-stealing argument

In the game where players alternately claim unclaimed cells of an $n \times n$ board and the first to complete a full row or column wins, show the second player cannot have a winning strategy.

Step 1 — suppose the second player had a winning strategy S. Step 2 — the first player makes an arbitrary move, then pretends to be the second player and follows S; if S ever asks for the cell already claimed, make another arbitrary move instead. Step 3 — an extra claimed cell never hurts in this game (claiming can only help complete lines), so the first player wins — contradicting that S was winning for the second player. Step 4 — hence with best play the first player wins or draws. The argument is non-constructive: it proves the first player CAN'T lose without saying how to play — a classic olympiad move.

14 Olympiad Number Theory II: Residues, Diophantine Equations & Factorials

Quadratic residues, difference-of-squares counts, Legendre gaps, Euler at work

14.1 Deeper Arithmetic

Quadratic residues and the two supplements

For an odd prime p: -1 is a QR iff $p \equiv 1 \pmod 4$; 2 is a QR iff $p \equiv \pm 1 \pmod 8$. Euler's criterion: $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$.

Eleven odd primes up to 100 have -1 as a residue — exactly the primes that are sums of two squares (Fermat). Quadratic reciprocity $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ then decides every $\left(\frac{a}{p}\right)$ by a Euclid-like descent. Olympiad use: showing an equation like $x^2 + 1 \equiv 0 \pmod p$ has no solution for $p \equiv 3 \pmod 4$ kills whole families of Diophantine equations mod a well-chosen prime.

Difference of squares and factorization counts

$x^2 - y^2 = N$ has positive solutions in bijection with factorizations $N = de$, $d < e$, $d \equiv e \pmod 2$. For odd N the count is $\frac{\tau(N)-1}{2}$ when N is a square, $\frac{\tau(N)}{2}$ otherwise.

$x^2 - y^2 = 2025 = 3^4 \cdot 5^2$: $\tau = 15$, so 7 solutions (the factorization $45 \cdot 45$ gives $y = 0$ and is excluded). For even N both factors must be even, so $N \equiv 2 \pmod 4$ has NO solutions — the standard parity obstruction. Every "sum/difference of squares" count is a divisor count in disguise.

Factorials: gaps in trailing zeros and Euler's theorem

$v_5(n!)$ jumps by 2 at multiples of 25 and by 3 at multiples of 125, so some zero-counts $(5, 11, 17, \ldots, 29, 30)$ never occur. Euler: $a^{\varphi(n)} \equiv 1$ when $\gcd(a, n) = 1$ — $2^{100} \equiv 1 \pmod{125}$.

The smallest n with at least 30 trailing zeros is 125 (v_5 leaps from 28 at 124 to 31). Euler plus CRT computes huge powers modulo composites: $2^{100} \equiv 1 \pmod{125}$ and $\equiv 0 \pmod 8$ give $2^{100} \equiv 376 \pmod{1000}$. Wilson's theorem $(p-1)! \equiv -1$ handles factorials modulo primes; pairing each residue with its inverse is the proof.

The mod-m obstruction menu

Squares are $0, 1$ mod 4 and $0, 1, 4$ mod 8; cubes are $0, \pm 1$ mod 9 and mod7; fourth powers are $0, 1$ mod 16. Powers of 2 cycle with short periods mod small odd numbers. Before any heavy machinery, reduce a Diophantine equation modulo $4, 8, 9, 7, 16$ — one of them usually shows there are no solutions, or restricts them to a residue class you can then handle.

Try it: Try it: kill an equation mod 4

Show $x^2 + y^2 = 4z + 3$ has no integer solutions.

Answer. Squares are 0 or 1 mod 4, so $x^2 + y^2 \in \{0, 1, 2\}$ mod 4 — never 3. Done in one line; the same idea shows no integer of the form $4k + 3$ is a sum of two squares.

14.2 Proofs & Why It Matters

Proof: Euler's criterion

For odd prime p and $p \nmid a$: $a^{(p-1)/2} \equiv 1$ if a is a QR, $\equiv -1$ otherwise.

The multiplicative group mod p is cyclic of order $p-1$ with generator g; write $a = g^k$. Then $a^{(p-1)/2} = g^{k(p-1)/2}$, which is 1 iff $(p-1) \mid k\frac{p-1}{2}$ iff k is even iff a is a square ($a = (g^{k/2})^2$). Since $a^{p-1} = 1$, the value $a^{(p-1)/2}$ is a square root of 1, hence ± 1. ■ The first supplement follows immediately: $(-1)^{(p-1)/2} = 1$ iff $\frac{p-1}{2}$ is even iff $p \equiv 1 \pmod 4$.

Proof: Wilson's theorem

$(p-1)! \equiv -1 \pmod p$ for every prime p.

In the product $1 \cdot 2 \cdots (p-1)$, pair each residue with its multiplicative inverse mod p. A residue is its own inverse iff $x^2 \equiv 1$ iff $x \equiv \pm 1$ (a polynomial of degree 2 over a field has at most 2 roots). All other residues pair off into products $\equiv 1$, leaving $1 \cdot (p-1) \equiv -1$. ■ Significance: the converse holds too (n composite $\Rightarrow (n-1)! \equiv 0$ for $n > 4$), so Wilson characterizes primes — and the pairing trick reappears in every "product of all elements of a group" problem.

14.3 Going Deeper: Worked Problems

Worked: a two-squares count

How many ordered pairs of positive integers (x, y) satisfy $x^2 - y^2 = 720$?

Step 1 — $(x-y)(x+y) = 720$ with both factors of the SAME parity; since 720 is even, both must be even. Step 2 — write $x - y = 2d$, $x + y = 2e$: $de = 180$ with $d < e$. Step 3 — $180 = 2^2 \cdot 3^2 \cdot 5$ has $\tau = 18$ divisors, so 9 pairs with $d < e$ (no square root since 180 is not a square). Step 4 — each gives $x = d + e$, $y = e - d > 0$: nine solutions. The parity step is where most attempts go wrong — an odd-times-even factorization of 720 gives non-integer x, y.

Worked: an order argument for a divisibility claim

Show that $2^n + 1$ is never divisible by 7 for any positive integer n.

Step 1 — the powers of 2 mod 7 cycle: $2, 4, 1, 2, 4, 1, \ldots$ (the order of 2 mod 7 is 3). Step 2 — so $2^n \bmod 7 \in \{1, 2, 4\}$ and $2^n + 1 \bmod 7 \in \{2, 3, 5\}$ — never 0. ■ Step 3 — the general principle: $p \mid 2^n + 1$ requires $2^{2n} \equiv 1$ but $2^n \not\equiv 1$, i.e. the order of 2 mod p is exactly $2 \cdot$(something dividing n) — an EVEN order. Mod 7 the order is 3, odd: impossible. This "order must be even" lemma settles every $a^n + 1$ divisibility question.

15 Olympiad Algebra II: Polynomials, Recurrences & Radical Equations

Vieta in reverse, Newton in miniature, characteristic roots, extraneous solutions

15.1 Algebra at Proof Level

Building polynomials from symmetric data

Given $r+s+t$, $rs+st+tr$, rst, the monic cubic with those roots is $x^3-e_1x^2+e_2x-e_3$. Power sums convert through Newton: $x^2+y^2=(x+y)^2-2xy$, $x^3+y^3=(x+y)^3-3xy(x+y)$.

Sums $6, 11, 6$ give $(x-1)(x-2)(x-3)$, whose value at 4 is 6; $x+y=4$, $x^3+y^3=28$ forces $xy=3$ and $x^2+y^2=10$. Every "find this symmetric expression" problem is a two-step: reach $e_1, e_2, (e_3)$, then rebuild. If the problem wants the actual roots, factor the rebuilt polynomial by testing small integers (rational root theorem).

Linear recurrences and their characteristic roots

$a_{n+2}=pa_{n+1}+qa_n$ has general term $A\alpha^n+B\beta^n$ where α,β solve $r^2=pr+q$ (with $(A+Bn)\alpha^n$ for a double root).

$a_{n+2}=a_{n+1}+2a_n$ has roots $2,-1$: $a_n=\frac{2^n-(-1)^n}{3}$, so $a_{10}=341$. The method IS diagonalization of the companion matrix (Linear Algebra course), which is why it also handles k-term recurrences and why a root of modulus >1 dominates growth. Nonhomogeneous recurrences add a particular solution, exactly as for differential equations.

Radical and rational equations: the ghost problem

Squaring, clearing denominators, and cross-multiplying can INTRODUCE solutions. Solve, then verify every candidate in the original equation.

$\sqrt{x+5}=x-1$ squares to $(x-4)(x+1)=0$; $x=-1$ is a ghost (the left side is 2, the right -2). The clean discipline: record the domain and sign constraints BEFORE squaring ($x-1\geq 0$ here), then squaring is reversible on that domain. For nested radicals, isolate one radical per squaring; for $\sqrt{a}\pm\sqrt{b}$ forms, multiply by the conjugate.

Substitutions that linearize

$x+\frac{1}{x}=t$ collapses palindromic polynomials; $u=x^2$ halves the degree of even polynomials; $x=y-\frac{a}{3}$ removes the x^2 term of a cubic (Cardano's first step); $x=\frac{1-t}{1+t}$ and $x=\tan\theta$ tame $\frac{1\pm x}{1\mp x}$ and $\sqrt{1+x^2}$. Recognizing WHICH substitution the equation is asking for is the algebra half of the USAMO.

Try it: Try it: a palindromic quartic

Solve $x^4-5x^3+6x^2-5x+1=0$.

Answer. Divide by x^2: $\left(x^2+\frac{1}{x^2}\right)-5\left(x+\frac{1}{x}\right)+6=0$. With $t=x+\frac{1}{x}$, $x^2+\frac{1}{x^2}=t^2-2$: $t^2-5t+4=0$, $t=1$ or 4. $t=4$ gives $x=2\pm\sqrt{3}$; $t=1$ gives complex roots. Real solutions: $2\pm\sqrt{3}$.

15.2 Proofs & Why It Matters

Proof: the characteristic-root formula for two-term recurrences

If $\alpha \neq \beta$ solve $r^2 = pr + q$, every solution of $a_{n+2} = pa_{n+1} + qa_n$ is $A\alpha^n + B\beta^n$.

Both α^n and β^n satisfy the recurrence (substitute and factor out r^n). Solutions form a vector space closed under linear combinations, and a solution is determined by (a_0, a_1) — two numbers — so the space is 2-dimensional. α^n and β^n are independent (their initial pairs $(1, \alpha)$, $(1, \beta)$ are independent for $\alpha \neq \beta$), hence a basis. ■ For a double root, $n\alpha^n$ is the second basis element — verify by substitution, exactly as for xe^{rx} in differential equations.

Proof: the rational root theorem

If $\frac{p}{q}$ in lowest terms is a root of $a_n x^n + \cdots + a_0$ with integer coefficients, then $p \mid a_0$ and $q \mid a_n$.

Multiply $\sum a_k (p/q)^k = 0$ by q^n: $\sum a_k p^k q^{n-k} = 0$. Every term except $a_0 q^n$ is divisible by p, so $p \mid a_0 q^n$, and $\gcd(p, q) = 1$ forces $p \mid a_0$. Symmetrically every term except $a_n p^n$ is divisible by q, so $q \mid a_n$. ■ Significance: it makes "factor by finding an integer root" a finite search, and its special case "a monic integer polynomial has no non-integer rational roots" is why $\sqrt{2}$ is irrational.

15.3 Going Deeper: Worked Problems

Worked: a system solved by Vieta in reverse

Find all real triples with $x + y + z = 6$, $x^2 + y^2 + z^2 = 14$, $x^3 + y^3 + z^3 = 36$.

Step 1 — $e_1 = 6$; $e_2 = \frac{e_1^2 - p_2}{2} = \frac{36-14}{2} = 11$; Newton: $p_3 = e_1 p_2 - e_2 p_1 + 3e_3$ gives $36 = 84 - 66 + 3e_3$, so $e_3 = 6$. Step 2 — the triple consists of the roots of $t^3 - 6t^2 + 11t - 6 = (t-1)(t-2)(t-3)$. Step 3 — all permutations of $(1, 2, 3)$: six solutions. Symmetric systems never require solving for one variable at a time; rebuild the polynomial and factor.

Worked: a recurrence with a nonhomogeneous term

Solve $a_{n+1} = 2a_n + 3$ with $a_0 = 1$, and find a_{10}.

Step 1 — the fixed point: $L = 2L + 3$ gives $L = -3$. Step 2 — shift: $b_n = a_n + 3$ satisfies $b_{n+1} = 2b_n$, so $b_n = 2^n b_0 = 4 \cdot 2^n$. Step 3 — $a_n = 4 \cdot 2^n - 3 = 2^{n+2} - 3$; $a_{10} = 4096 - 3 = 4093$. Step 4 — check: $a_1 = 2 + 3 = 5 = 8 - 3$ ✓. Subtracting the fixed point is the recurrence version of "particular solution plus homogeneous," and it works for any $a_{n+1} = ka_n + c$ with $k \neq 1$.

16 Olympiad Inequalities II: The Full Ladder

AM–GM with constraints, Engel form, Cauchy as geometry, QM–AM, SOS and Schur

16.1 Every Standard Inequality, Placed

AM–GM under a product or sum constraint

With $abc = 1$: $a + b + c + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \geq 6$ (six terms with product 1). With $a + b + c = 3$: $ab + bc + ca \leq 3$ (from $a^2 + b^2 + c^2 \geq ab + bc + ca$).

The constraint tells you how to group: a product constraint suggests AM–GM across terms whose product is a power of it; a sum constraint suggests QM–AM or the identity $(a + b + c)^2 = \sum a^2 + 2\sum ab$. Homogenize first when degrees differ — replace a constant by the appropriate power of $(a + b + c)$ or $(abc)^{1/3}$ — so that the inequality becomes scale-free and the standard tools apply.

Cauchy–Schwarz: Engel form and the geometric form

Engel (Titu): $\sum \frac{a_i^2}{b_i} \geq \frac{(\sum a_i)^2}{\sum b_i}$. Geometric: $|\mathbf{u} \cdot \mathbf{v}| \leq |\mathbf{u}||\mathbf{v}|$ — so $3a + 4b \leq 5$ on the unit circle and $\frac{1}{x} + \frac{4}{y} + \frac{9}{z} \geq 36$ when $x + y + z = 1$.

Engel form is Cauchy–Schwarz with $u_i = \frac{a_i}{\sqrt{b_i}}$, $v_i = \sqrt{b_i}$; it is the fastest route to bounds on sums of fractions. Equality in Engel: $\frac{a_i}{b_i}$ all equal — so the minimizer of $\frac{1}{x} + \frac{4}{y} + \frac{9}{z}$ has $x : y : z = 1 : 2 : 3$. Write the equality case down before computing; it often IS the answer.

Schur, SOS, and smoothing

Schur ($t = 1$): $a^3 + b^3 + c^3 + abc \geq \sum_{\text{sym}} a^2b$... precisely $\sum a(a - b)(a - c) \geq 0$. SOS: write the difference as $\sum S_c(a - b)^2$ with nonnegative coefficients. Smoothing: replace two variables by their mean and show the expression moves the right way.

Schur handles the inequalities AM–GM cannot (it is the one with equality at $a = b = c$ AND at $(a, a, 0)$). SOS is a systematic finishing move for symmetric three-variable inequalities: expand, group into squares. Smoothing (or "mixing variables") proves that the extremum occurs when variables are equal or when one hits the boundary — reducing a three-variable problem to one variable. These three are the difference between AIME-level and USAMO-level inequality work.

Equality cases are the map

Before any manipulation, guess where equality holds: all variables equal (AM–GM, Jensen, QM–AM), proportional (Cauchy–Schwarz), one variable zero (Schur, boundary cases). A candidate inequality with the wrong equality case cannot be the right tool — this single check saves more time than any technique.

Try it: Try it: homogenize, then AM–GM

For positive a, b, c with $a + b + c = 1$, prove $\left(1 + \frac{1}{a}\right)\left(1 + \frac{1}{b}\right)\left(1 + \frac{1}{c}\right) \geq 64$.

Answer. Homogenize: $1 + \frac{1}{a} = \frac{a+b+c+a}{a}$... simpler: $1 + \frac{1}{a} = 1 + \frac{a+b+c}{a} = \frac{2a+b+c}{a}$. By AM–GM $2a + b + c = a + a + b + c \geq 4\sqrt[4]{a^2bc}$; multiply the three: numerator $\geq 64\sqrt[4]{a^4b^4c^4} = 64abc$, denominator abc. Equality at $a = b = c = \frac{1}{3}$ ✓.

16.2 Proofs & Why It Matters

Proof: Schur's inequality

For nonnegative a, b, c: $a(a-b)(a-c) + b(b-a)(b-c) + c(c-a)(c-b) \geq 0$.

By symmetry assume $a \geq b \geq c$. Group the first two terms: $(a-b)\,[a(a-c) - b(b-c)] \geq 0$ because $a - b \geq 0$ and $a(a-c) \geq b(b-c)$ (both factors on the left dominate). The third term $c(c-a)(c-b) = c(a-c)(b-c) \geq 0$ is a product of nonnegatives. ■ Equality iff $a = b = c$ or two are equal and the third is 0 — the two-equality-case signature that makes Schur indispensable when AM–GM's single equality case is too restrictive.

Proof: the rearrangement inequality

For $a_1 \leq \cdots \leq a_n$ and $b_1 \leq \cdots \leq b_n$, the sum $\sum a_i b_{\sigma(i)}$ is maximized by $\sigma = \mathrm{id}$ and minimized by the reversing permutation.

If σ is not the identity, some $i < j$ has $\sigma(i) > \sigma(j)$; swapping the two assignments changes the sum by $(a_j - a_i)(b_{\sigma(i)} - b_{\sigma(j)}) \geq 0$. Repeated swaps reach the identity without ever decreasing the sum. ■ Significance: Chebyshev's inequality (similarly ordered sequences have $\frac{1}{n}\sum a_i b_i \geq \bar{a}\bar{b}$) is rearrangement averaged over all cyclic shifts, and both are the tool when AM–GM's symmetry is broken by an ordering assumption.

16.3 Going Deeper: Worked Problems

Worked: an SOS finish

Prove $a^2+b^2+c^2 \geq ab+bc+ca$ and use it to show $\dfrac{a^2+b^2+c^2}{ab+bc+ca} \geq 1$ with equality iff $a = b = c$.

Step 1 — $2(a^2+b^2+c^2) - 2(ab+bc+ca) = (a-b)^2 + (b-c)^2 + (c-a)^2 \geq 0$: a sum of squares. Step 2 — equality iff every square vanishes iff $a = b = c$. Step 3 — divide by the positive $ab + bc + ca$. Step 4 — the same SOS identity gives $(a+b+c)^2 \geq 3(ab+bc+ca)$ and $3(a^2+b^2+c^2) \geq (a+b+c)^2$ — three inequalities from one line of algebra, all sharing the equality case $a = b = c$.

Worked: a smoothing argument

Among nonnegative a, b, c with $a + b + c = 3$, find the maximum of $ab + bc + ca - abc$.

Step 1 — test the symmetric point $a = b = c = 1$: value $3 - 1 = 2$. Test a boundary point $(1.5, 1.5, 0)$: 2.25. So the maximum is NOT at the symmetric point — smoothing must be done carefully. Step 2 — fix c and set $a + b = 3 - c = s$; the expression is $ab(1-c) + cs$. For $c < 1$ it increases with ab, maximized at $a = b$; for $c > 1$ it is maximized at $ab = 0$. Step 3 — case $a = b = \frac{s}{2}$: $f(c) = \frac{(3-c)^2}{4}(1-c) + c(3-c)$ on $[0, 1]$; $f(0) = 2.25$, $f(1) = 2$, and $f' < 0$ on the interval

— max 2.25 at $c = 0$. Case $ab = 0$ with $c \geq 1$: value $c(3-c) \leq 2.25$. Step 4 — maximum $\frac{9}{4}$ at $(\frac{3}{2}, \frac{3}{2}, 0)$ and permutations. Boundary cases are where symmetric-point intuition fails; smoothing finds them systematically.

17 Olympiad Geometry III: Circumcircle, Power of a Point, Incircle

Arc midpoints, the incenter–excenter lemma, power of a point, Euler's OI, bisector lengths

17.1 Circles Doing the Work

Power of a point, three ways

For a point P and a circle with center O, radius r: every line through P meeting the circle at X, Y has $PX \cdot PY = |PO^2 - r^2|$ — equal to the tangent length squared when P is outside.

The proof is one similarity: for two chords XY, $X'Y'$ through P, the inscribed angles make $PXX' \sim PY'Y$, so $PX \cdot PY = PX' \cdot PY'$. Use it (i) to compute a length from a secant and a tangent, (ii) to prove four points concyclic (the converse holds: $PA \cdot PB = PC \cdot PD$ with the right configuration forces $ABCD$ cyclic), and (iii) through the radical axis — the locus of equal power with respect to two circles is a line, and three radical axes concur.

The arc midpoint and the incenter–excenter lemma

If the bisector from A meets the circumcircle again at M, then $MB = MC = MI = MI_A$: M is the center of the circle through B, C, the incenter I, and the A-excenter I_A.

Angle chase: $\angle MBI = \angle MBC + \angle CBI = \frac{A}{2} + \frac{B}{2}$ and $\angle MIB = \angle IAB + \angle IBA = \frac{A}{2} + \frac{B}{2}$ (exterior angle of AIB), so $MB = MI$. Combined with the power of D (where the bisector meets BC), $DB \cdot DC = DA \cdot DM$, and the bisector-length formula $AD^2 = bc - DB \cdot DC$, every length on the bisector is computable — including $AM = \frac{bc}{AD}$ from $ABD \sim AMC$. Euler's $OI^2 = R(R - 2r)$ is the power of I: $R^2 - OI^2 = AI \cdot IM = AI \cdot MB = \frac{r}{\sin(A/2)} \cdot 2R \sin\frac{A}{2} = 2Rr$.

Incircle lengths

Tangent lengths $s-a, s-b, s-c$; $r = \frac{K}{s}$; $AI = \frac{r}{\sin(A/2)}$, so $AI^2 = (s-a)^2 + r^2$; the A-excircle has radius $r_a = \frac{K}{s-a}$ and tangent length s from A.

Every incircle problem reduces to right triangles formed by a radius and a tangent. The 13-14-15 triangle is the standard test case: $s = 21$, $K = 84$, $r = 4$, $R = \frac{65}{8}$, $AI^2 = 7^2 + 4^2 = 65$, $OI^2 = \frac{65}{64}$ — keep these numbers in your head to sanity-check formulas under pressure.

Homothety with circles

Two circles are related by two homotheties whose centers are the internal and external centers of similitude — the intersections of the common tangents. For tangent circles the tangency point is one of them, so a line through the tangency point meets the circles at points P, Q with $\frac{TQ}{TP} = \frac{r_2}{r_1}$. This is the tool for "the line TP passes through the arc midpoint" problems.

Try it: Try it: Euler in numbers

A triangle has $R = 5$ and $r = 2$. Compute OI.

Answer. $OI^2 = R(R - 2r) = 5 \cdot 1 = 5$, so $OI = \sqrt{5}$. Note $R \geq 2r$ always (Euler's inequality) since $OI^2 \geq 0$.

18 Olympiad Number Theory III: Exponential Diophantine Equations

Powers of two, difference of squares, Catalan-type equations, and the parity–valuation reflex

18.1 Equations in Exponents

Divide out the smallest power, then look at parity

$2^x + 2^y = 2^z$: dividing by $2^{\min(x,y)}$ leaves $1 + 2^k = 2^m$, forcing $k = 0$; so the solutions are exactly $(x, x, x + 1)$. In general, comparing p-adic valuations of both sides is the first move.

An exponential equation is a statement about valuations: the side with the smaller valuation must be matched exactly. After dividing out, one side is a unit modulo p and the other is a power of p — usually a contradiction unless an exponent is 0. The same reflex settles $3^x + 3^y = 3^z$, $2^x + 3^y = 5^z$ (mod small numbers), and most "find all positive integers" equations of contest size.

Difference of squares and difference of powers

$m^2 - n^2 = 2^k$ splits as $(m - n)(m + n)$ with both factors powers of 2 of the same parity; $2^n + 1 = m^2$ becomes $2^n = (m-1)(m+1)$, two powers of 2 differing by 2, so $n = 3$; $3^x - 2^y = 1$ needs x even (mod 8) and then $(3^{x/2} - 1)(3^{x/2} + 1) = 2^y$ gives $(2, 3)$ besides $(1, 1)$.

Factoring is the second reflex. The pattern "two powers of p whose difference is small" has finitely many solutions, all tiny — that is the elementary heart of Catalan's equation $x^a - y^b = 1$ (Mihilescu proved the general case; the powers-of-2 and 3 cases are exercises). Always finish with the small cases you excluded along the way (here $y \leq 2$).

Growth arguments and $a^b = b^a$

$a^b = b^a$ with $a < b$ has the unique solution $(2, 4)$: $\frac{\ln t}{t}$ increases on $(0, e)$ and decreases after, so one of the two is ≤ 2.

When modular arithmetic and factoring both fail, compare growth rates: an exponential beats a polynomial eventually, and a calculus fact about a real function can bound integer solutions. State the monotonicity precisely (with the derivative), then check the finitely many small cases by hand — the proof is incomplete without both halves.

The bounding checklist

Every "find all positive integer solutions" problem is solved by some mix of: valuations/parity, a modulus that kills a residue class (mod $3, 4, 7, 8, 9, 16$), factoring into coprime pieces, size comparison (squeezing between consecutive squares or powers), and descent. Write which one you are using at each step; graders award partial credit per correctly justified reduction.

Try it: Try it: squeeze

Show that $n^2 + n + 1$ is never a perfect square for $n \geq 1$.

Answer. Since $n^2 < n^2 + n + 1 < n^2 + 2n + 1 = (n + 1)^2$ for $n \geq 1$, it lies strictly between consecutive squares.

19 Functional Equations With Tricky Conditions

Substitutions that isolate f, injectivity from the equation, monotone f(f(n)) = 3n, Mbius orders, d'Alembert

19.1 Pinning Down the Function

Substitute to isolate, then verify

$f(x^2 + y) = f(x)^2 + y$: replace y by $y - x^2$ to get $f(y) = y + c$, then substitute back to force $c = 0$. $f(x)f(y) - f(xy) = x + y$: $y = 0$ gives $f(x) = x + 1$ once $f(0) = 1$ is forced.

The two-step structure is mandatory: (1) derive what f MUST be by substitutions that isolate a single value of f; (2) verify that the candidate actually satisfies the equation for all inputs — step (1) alone proves nothing, because it only used a few special cases of the hypothesis. Most lost points on USAMO functional equations are a missing verification or a missing "for all x" quantifier.

Injectivity, surjectivity, and iteration

From $f(f(n)) = n + 4$: f is injective (compose the hypothesis), and applying f once more gives $f(n + 4) = f(n) + 4$, so f is determined by four values. From strictly increasing f with $f(f(n)) = 3n$: $f(1) = 2$ is forced, and the values propagate upward.

Iterated equations $f(f(x)) = g(x)$ hide two facts: injectivity of f (if g is injective), and the commutation $f(g(x)) = g(f(x))$ (apply f to both sides). With monotonicity, the values between known ones are squeezed — $f(3) = 6$ and $f(6) = 9$ force $f(4) = 7$, $f(5) = 8$ — and the whole function unrolls. In base 3 the $f(f(n)) = 3n$ solution is a digit rule; finding the pattern is not required, but proving the forced values is.

Mbius substitutions and cyclic systems

If $g(x) = \frac{1}{1-x}$ then $g^3 = \text{id}$: an equation $f(x) + f(g(x)) = x$ yields three linear equations in $f(x), f(gx), f(g^2x)$, solved by adding and subtracting. Involutions ($g^2 = \text{id}$, like $x \mapsto \frac{1}{x}$ or $\frac{x+1}{x-1}$) give two equations.

Recognize the order of the substitution map first — compose it with itself until it returns to x — then write the cyclic system. The solution is a formula valid wherever all the substituted points are in the domain; say so. d'Alembert's equation $f(x+y) + f(x-y) = 2f(x)f(y)$ is the cosine/cosh addition law: $x = y = 0$ pins $f(0) = 1$, and $f(2) = 2f(1)^2 - 1$ follows with no regularity.

Regularity: when you need it and when you don't

Cauchy's $f(x + y) = f(x) + f(y)$ is linear on $\mathbb{Q}$ unconditionally, and on $\mathbb{R}$ only with continuity, monotonicity, or boundedness on an interval. If a problem gives no regularity, either the answer is a specific value that follows from finitely many substitutions (most USAMO problems), or the domain is $\mathbb{N}/\mathbb{Q}/\mathbb{Z}$ where induction replaces continuity. Never assume continuity silently.

Try it: Try it: a forced value

$f : \mathbb{R} \to \mathbb{R}$ with $f(x + y) = f(x) + f(y) + 2xy$ and $f(1) = 3$. Find $f(4)$.

Answer. $g(x) = f(x) - x^2$ is additive, $g(1) = 2$, so $g(4) = 8$ and $f(4) = 8 + 16 = 24$. Verify: $f(x) = x^2 + 2x$ satisfies the equation ✓.

20 Bijections, Homothety & Structured Counting

Reflection, rooks and derangements, Fibonacci diagonals, matchings by inclusion–exclusion, homothety in figures

20.1 Counting by Correspondence

The reflection bijection

Paths from $(0, 0)$ to (n, n) that never go above $y = x$ number $\binom{2n}{n} - \binom{2n}{n-1} = C_n$: reflect each bad path across $y = x+1$ after its first touch to get a bijection with all paths to $(n-1, n+1)$.

A bijection is a proof when both the map and its inverse are described and shown to land in the right set; "reflect" must come with "and the reflected path ends at $(n-1, n+1)$, and reflecting again recovers the original". Catalan numbers count triangulations, parenthesizations, and non-crossing matchings by the same recurrence — an answer of 132 or 429 is a strong hint that Catalan is behind it.

Rooks, permutations, and forbidden positions

Non-attacking rook placements on an $n \times n$ board are permutations; forbidding the main diagonal gives derangements $D_n = n! \sum_{k \le n} (-1)^k / k!$, and forbidding neighbors around a circle of $2n$ people gives a matching count by inclusion–exclusion over the cycle's edges: $\sum_k (-1)^k m_k (2n-2k-1)!!$ with $m_k = \frac{2n}{2n-k}\binom{2n-k}{k}$.

Inclusion–exclusion over a STRUCTURED family (the edges of a cycle, the diagonal cells) needs the count m_k of k pairwise-compatible forbidden objects — for a cycle that is the number of k-matchings, a Lucas-number-like quantity. Write the general term, compute m_k separately, and only then assemble the alternating sum.

Fibonacci diagonals and subset conditions

Subsets of $\{1..n\}$ whose size equals their minimum number F_n: sum $\binom{n-k}{k-1}$ over k, a shallow diagonal of Pascal's triangle. Subsets with no two consecutive elements number F_{n+2}.

Two proofs to know: the diagonal identity $\sum_j \binom{n-j}{j} = F_{n+1}$ by Pascal's rule (both sides satisfy the Fibonacci recurrence), and the tiling bijection (squares and dominoes). When a count comes out Fibonacci, one of these is the intended proof.

Homothety in figures

The medial triangle is the image of ABC under the homothety at the centroid with ratio $-\frac{1}{2}$; the anticomplementary triangle (lines through each vertex parallel to the opposite side) has ratio -2 and four times the area. Tangent circles are homothetic from their tangency point with ratio $\pm r_2/r_1$.

A homothety sends lines to parallel lines, circles to circles, and scales every length by $|k|$ and every area by k^2. Locating its center — a centroid, a tangency point, an intersection of common tangents — is the whole problem; the ratio then reads off any pair of corresponding lengths.

Try it: Try it: Catalan by reflection

How many sequences of 5 H's and 5 T's have every prefix containing at least as many H's as T's?

Answer. $\binom{10}{5} - \binom{10}{4} = 252 - 210 = 42 = C_5$.

21 USAMO Practice Tests & Write-Up Playbook

Timed sets from the USAMO pool, and how to write proofs that score

21.1 Sit a Practice Test

How the practice tests work

The USAMO practice sets draw six problems at a time from the hand-verified USAMO pool (number theory, combinatorics, geometry, algebra, inequalities, games). Answers are numeric so they can be checked — but write the PROOF on paper as you would on the real exam.

Treat each set as a session: 4.5 hours for six problems, no calculator. After finishing, read every solution in full and compare the write-up to yours line by line: did you justify the step the solution justifies? Did you handle the equality/edge case? The gap between "I saw the idea" and "I wrote a 7" is the entire game.

The write-up checklist

State what you will prove. Define your notation. Label lemmas and prove each before using it. Justify every non-obvious step with a named tool. Handle equality cases and degenerate configurations. End with a clear conclusion sentence.

Graders read for GAPS: an unproved claim, a case not covered, a "clearly" that is not clear. Proof by contradiction must state the negated assumption precisely; induction must state the hypothesis and prove the base. Diagrams help but are not proofs — every geometric fact you read off a picture must be justified (angle chase, similar triangles, power of a point) in words. Numbered steps are your friend.

Scoring reality

USAMO problems are 7 points: 7 for a complete proof, 5–6 for a complete proof with a minor gap, 1–2 for substantial progress (a correct key lemma), 0 for the answer alone. A partial solution that clearly states what was proved and what was not can earn more than a confident but flawed "complete" one — honesty about gaps is rewarded.

22 Formulas & Methods

The USAMO reference: every tool, with the proof-level method that wields it

22.1 Algebra & Inequalities

Inequalities

AM–GM (weighted too); Cauchy–Schwarz and Engel; QM–AM–GM–HM; power means; Jensen; rearrangement and Chebyshev; Schur; SOS; Hlder $\left(\sum a_i^3\right)\left(\sum b_i^3\right)\left(\sum c_i^3\right) \geq \left(\sum a_i b_i c_i\right)^3$; Muirhead for symmetric sums; tangent-line trick; smoothing.

Locate the equality case; homogenize; choose the inequality whose equality case matches; finish with SOS if stuck. Write the equality condition explicitly in the proof.

Polynomials and functional equations

Vieta and Newton; $a-b \mid P(a)-P(b)$; rational root theorem; Eisenstein and mod-p irreducibility; Lagrange interpolation and finite differences; roots of unity filter; Chebyshev polynomials for boundedness. FE: substitutions (0, 1, $-x$, $\frac{1}{x}$, $x=y$), Cauchy's equation on $\mathbb{Q}$ and with regularity on $\mathbb{R}$, injectivity/surjectivity lemmas, fixed points, subtracting a particular solution.

Verify every FE candidate in the original equation. For polynomials, compare degrees and leading coefficients, count roots, and use integer-value constraints.

22.2 Number Theory & Combinatorics

Number theory

Orders, primitive roots, CRT; Fermat, Euler, Wilson; LTE (all cases); Legendre, Kummer; quadratic residues, Euler's criterion, reciprocity and both supplements; Vieta jumping; infinite descent; Zsigmondy (citable); $\gcd(a^m-1, a^n-1)$; sums over divisors and Mbius inversion; p-adic valuation bookkeeping; bounding between consecutive powers.

Reduce mod $4, 8, 9, 7, 16$ first; then valuations; then orders. For "$p \mid a^n+1$", the order of a must be even. For symmetric quadratic Diophantines, Vieta jump from a minimal solution.

Combinatorics

Pigeonhole (all forms); extremal principle; invariants and monovariants; colorings and weightings; double counting; bijections; induction on structures; PIE; generating functions; Catalan and reflection; Erds–Szekeres; graph theory (degrees, trees, bipartite, Mantel/Turn, Hall, Euler's formula); games (backward induction, P/N positions, Nim and XOR, symmetry and strategy stealing).

Ask: what never changes (invariant)? what only decreases (monovariant)? which object is extreme? which two things can I count? If the problem is a game, build the P/N table backward and prove the pattern.

22.3 Geometry

Synthetic and analytic geometry

Angle chasing and cyclic quadrilaterals (opposite angles, equal inscribed angles, the exterior-angle criterion); power of a point and radical axes/center; Ptolemy (and its inequality); Brahmagupta; Ceva and Menelaus (trig forms too); Stewart, Apollonius, angle-bisector length; incircle tangent lengths $s-a$; Euler line and nine-point circle; homothety; spiral similarity and Miquel points; inversion; the British flag theorem; complex numbers on the unit circle; barycentric coordinates for cevian-heavy problems.

Find the circle. Then: inscribed angles, power of a point, Ptolemy — in that order. Concurrency: Ceva (trig form for angles). Collinearity: Menelaus or a well-chosen homothety. Bash only when the configuration is tame, and set up coordinates to exploit symmetry.

The proof-writing method

Restate the claim; fix notation; prove lemmas before use; name every theorem; cover every case (including degenerate ones); state the equality condition; conclude.

A USAMO solution is a piece of technical writing. Numbered steps, one idea per paragraph, every ”clearly” replaced by a reason. After writing, read it as a hostile grader looking for the step you skipped.