The AMC Compendium

This is a compilation of various formulas, theorems, lemmas, and facts that are useful for competition math. I've ordered them by topic (geometry, number theory, algebra, and counting/probability)

Henry Zhang

February 4, 2020

Contents

Introduction

Throughout this opening section, we will focus almost entirely on Euclidean Geometry. Euclidean Geometry is based on five self evident assumptions.

- Any two points can be connected by a straight line
- We can extend a line segment infinitely
- Any two right angles are equal
- We can uniquely determine a circle given its center and radius
- In a plane, given a line and a point not on it, at most one line parallel to the given line can be drawn through the point.

The only problem is that they are not always correct. When they are false, we delve into a realm called Non-Euclidean Geometry. For example, when a triangle is drawn on a sphere, the angles don't add to. In fact, we can prove that the angles can never add to. We will be focused on starting from scratch (the five axioms) and proving all of the reasonable formulas given knowledge of other areas of mathematics like calculus. When I go over Non-Euclidean geometry, I will not be as rigorous. Note that the pages are ordered such that we start at the basics and go on to more advanced topics. During the proofs, I will only assume the five axioms, other areas of math, and what I have proven thus far.

Area of a Rectangle

Note that all of Euclid's Axioms are for lines; not areas. Therefore, to prove our first area formula, we need math beyond geometry.

Derivation

$$\int_0^a f(x)dx = \int_0^a bdx = b(a) - b(0) = ab$$

This gives a formula for the area of a rectangle: ab.

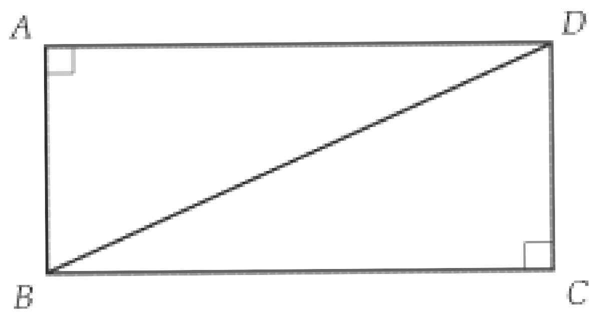
Corollary

If $a = b$, then we call this figure a square. The area of a square is therefore a^2.

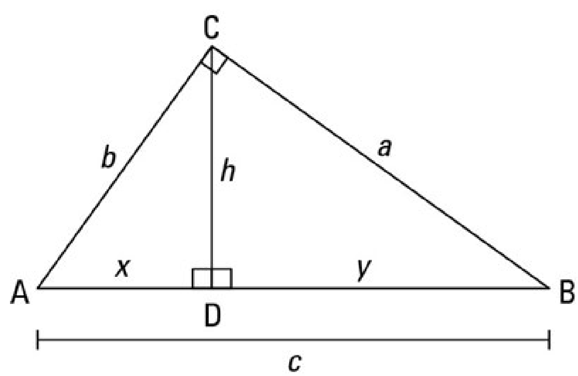
Area of Triangles Part 1

Derivation

First, we derive a formula for right triangles.



In this picture, there are two congruent triangles by symmetry. Together, their areas sum to $AB*AD$. Therefore, the area of one triangle is $\frac{AB \cdot AD}{2}$. Now consider an arbitrary triangle:

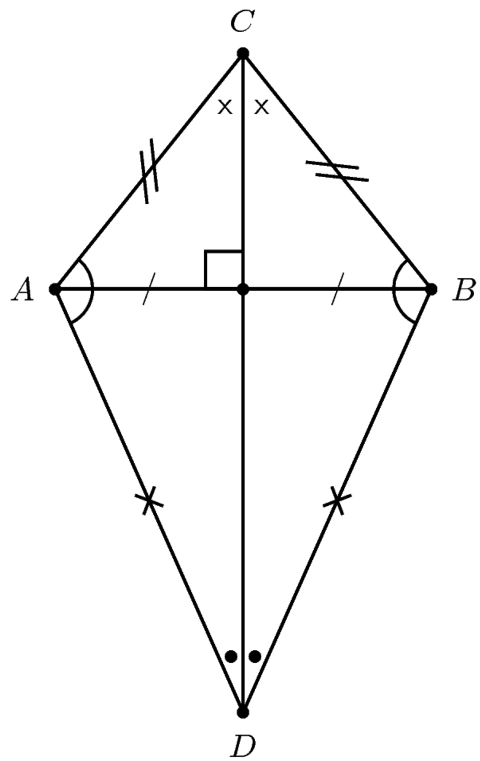


$\triangle CDB$ and $\triangle CDA$ are both right triangles. By the right triangle formula, the area of $\triangle CDB = \frac{yh}{2}$ and the area of $\triangle CDA = \frac{xh}{2}$. The sum of these is $\frac{(x+y)h}{2} = \frac{AB \cdot h}{2} = \frac{bh}{2}$

Area of a Quadrilateral With Perpendicular Diagonals

Derivation

We will derive a formula for the area of any quadrilateral with perpendicular diagonals.



The area of $\triangle CAB = \frac{AB \cdot h_1}{2}$ and the area of $\triangle ABD = \frac{AB \cdot h_2}{2}$. Adding these two together we get: $\frac{AB \cdot CD}{2}$ because $h_1 + h_2 = CD$. Therefore, the area of the quadrilateral is the product of the two diagonals divided by 2.

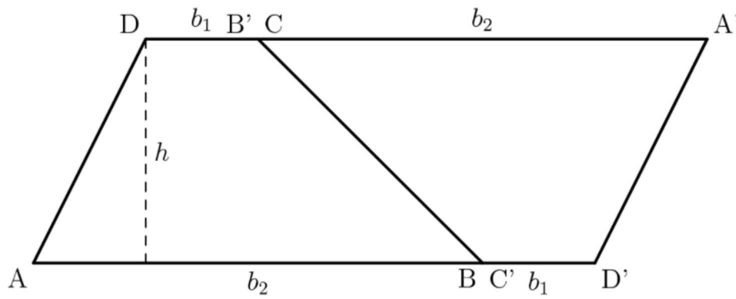
Corollary

In a square the area is $\frac{d^2}{2}$. Therefore, $d = s\sqrt{2}$ This tells us that the ratio of the sides of a $45 - 45 - 90$ triangle are: $1 - 1 - \sqrt{2}$

Area of a Trapezoid

Derivation

Consider the following diagram:



The area of the parallelogram is twice the area of the arbitrary trapezoid. We have proven that the area of the parallelogram is bh, but, the base is $b_1 + b_2$. Therefore, the area of the trapezoid is $\frac{h(b_1+b_2)}{2}$.

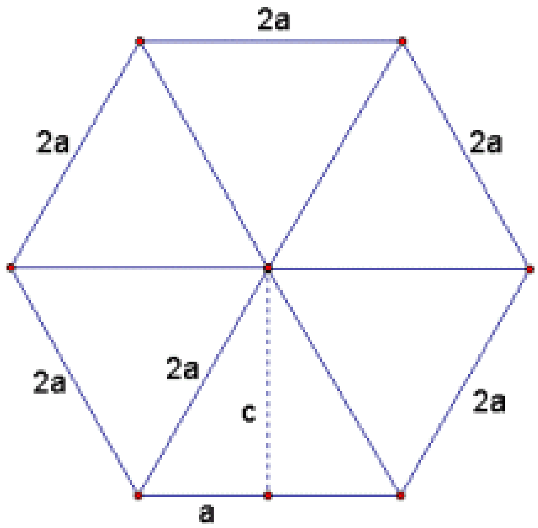
Remarks

In school, the derivation is taught by dropping perpendiculars from D and C. However, there are configuration issues with that. One possible remedy would be using directed segments, but that is overkill; just rotate the trapezoid.

Area of a Regular Hexagon

Derivation

We can split the hexagon into 6 equilateral triangles as shown



By the Pythagorean Theorem, $c = a\sqrt{3}$. Therefore, the area of each equilateral triangle is $\frac{a^2\sqrt{3}}{4}$. This is also an important formula to be able to rederive. Multiplying by 6, we get the desired expression and also the formula for the area of a regular hexagon: $\frac{3\sqrt{3}s^2}{2}$.

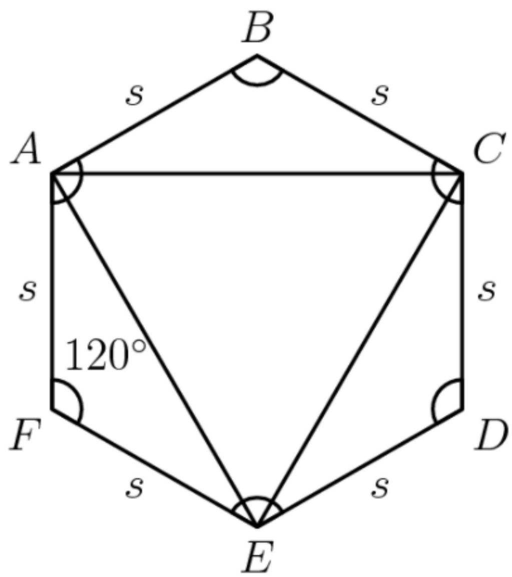
Notes

From this derivation, we also derived the formula for an equilateral triangle: $\frac{a^2\sqrt{3}}{4}$. Furthermore, we proved that the sides in a $30-60-90$ triangle are in the ratio of $1-\sqrt{3}-2$.

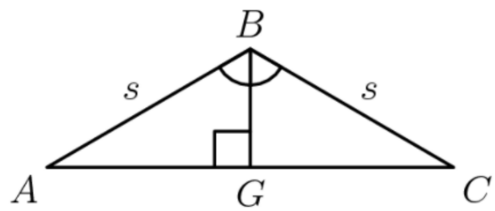
Equilateral Triangle Inscribed in a Regular Hexagon Lemma

Lemma: An equilateral triangle inscribed in a regular hexagon has half the area.

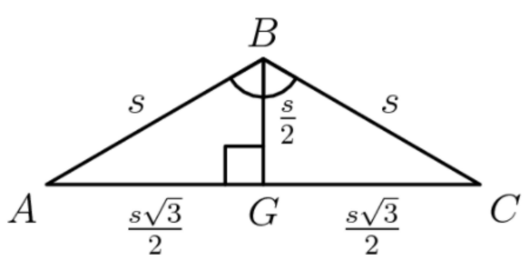
Derivation



We have an arbitrary regular hexagon with side length $ABCDEF$. We first note that the equilateral triangle with side length s. We first note that $\triangle ACE$ splits $ABCDEF$ into 4 triangles; the aforementioned equilateral triangle and 3 isosceles triangles. The isosceles triangles are clearly congruent by SAS due to the fact that the hexagon's angle measures and sides are all equal. Using our formula for finding the angle measures of regular polygons, $\frac{180(n-2)}{n}$, we see that $\frac{180(6-2)}{6} = 120$, so the angles of the hexagon all equal , we see that , so the angle measures of the hexagon all equal 120°.



We drop an altitude from point B of $\triangle ABC$ to point G ; BG is clearly also a median and angle bisector due to the fact that the altitude of an isosceles triangle that is dropped from the angle that is not equal to the other two is the same line as the median and angle bisector. We see that $\triangle CBG$ and $\triangle ABG$ are congruent $30-60-90$ triangles. This is because they are congruent through HL congruence since the hypotenuses of the two triangles are sides of the hexagon, which we already know are equal in length, and the triangles share a leg, BG. They are $30-60-90$ triangles since $\angle ABC$ was bisected into two $60°$ angles and BG is an altitude, so $m\angle BGA = m\angle BGC = 90$; thus, the last angle of both triangles must be $30°$ through the Angle Sum Theorem). Because of this, $BG = \frac{s}{2}$, so $AG = CG = \frac{s\sqrt{3}}{2} \implies AC = s\sqrt{3}$.



Now, the proof is coming into form; applying the formulas for the area of an equilateral triangle and regular hexagon, we get $[ACE] = \frac{3s^2\sqrt{3}}{4}$ and $[ABCDEF] = \frac{3s^2\sqrt{3}}{2}$. Clearly, $\frac{3s^2\sqrt{3}}{4} \cdot 2 = \frac{3s^2\sqrt{3}}{2}$, so we are done.

Area of a Circle

We can calc bash any area. Just think: “area under the curve”. Though one may exist, we have not found a proof for the area of a circle that does not involve at least some basic calculus, as dealing with curves is difficult otherwise. Note that the area of a circle with radius 1 is

$$2\left[\int_{-1}^{1}\sqrt{1-x^2}dx\right]$$

The indefinite integral of this expression is

$$\frac{1}{2}\left(\arcsin(x)+\frac{1}{2}\sin\left(2\arcsin(x)\right)\right)$$

We compute the boundaries to get $\frac{\pi}{4}-(-\frac{\pi}{4})=\frac{\pi}{2}$. Since we need to multiply by 2, our expression is π which matches with the well known formula. Also, because we can scale all of this, our desired formula is πr^2.

Non-Euclidean Geometry

Proposition 1 and 2: Volume and Surface Area of a Cone

$$V = \frac{\pi r^2 h}{3} \text{ and } SA = \pi r^2 + \pi r l$$

Where V is the volume, SA is the surface area, r is the radius of the circular base, h is the height, and l is the slant height.

Proposition 3 and 4: Volume and Surface Area of a Sphere

$$V = \frac{4\pi r^3}{3} \text{ and } SA = 4\pi r^2$$

Where V is the volume, SA is the surface area, and r is the radius of central cross section (radius of the base of the semi-sphere).

Proposition 5 and 6: Volume and Surface Area of a Cylinder

$$V = \pi r^2 h \text{ and } SA = 2\pi r^2 + 2\pi r h$$

Where V is the volume, SA is the surface area, r is the radius of the circular base, and h is the height.

Proposition 7 and 8: Volume and Surface Area of a Cube

$$V = s^3 \text{ and } SA = 6s^2$$

Where V is the volume, SA is the surface area, and s is the length of a side.

Proposition 9 and 10: Volume and Surface Area of a Triangular/Rectangular Pyramid

$$V = \frac{1}{3}bh \text{ and } SA = 2sl + b$$

Where V is the volume, SA is the surface area, b is the area of the base, h is the height, l is the slant height, and s is the length of a side of the base. Note that a pyramid can have a base of any polygon, but if none is specified, assume a square base. A pyramid with a triangular base is known as a tetrahedron.

Proposition 11 and 12: Volume and Surface Area of a Prism

$$V = lwh \text{ and } SA = 2(lw + lh + wh)$$

Where V is the volume, SA is the surface area, l is the length, w is the width, and h is the height.

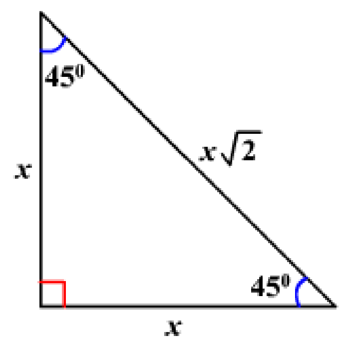
Proposition 13: Girard's Theorem

The area of any spherical triangle (triangle on a sphere) is $r^2 \cdot e$ where r is the radius and $e = \alpha + \beta + \gamma - \pi$.

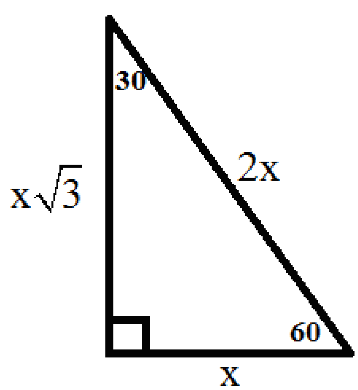
Note: The last proposition isn't coming up on AMC's any time soon. However, it's still fun to know.

Special Right Triangles

A special right triangle is a right triangle with some regular feature that makes calculations on the triangle easier, or for which simple formulas exist. For example, a right triangle may have angles that form simple relationships, such as $45° - 45° - 90°$ triangles or $30° - 60° - 90°$ triangles



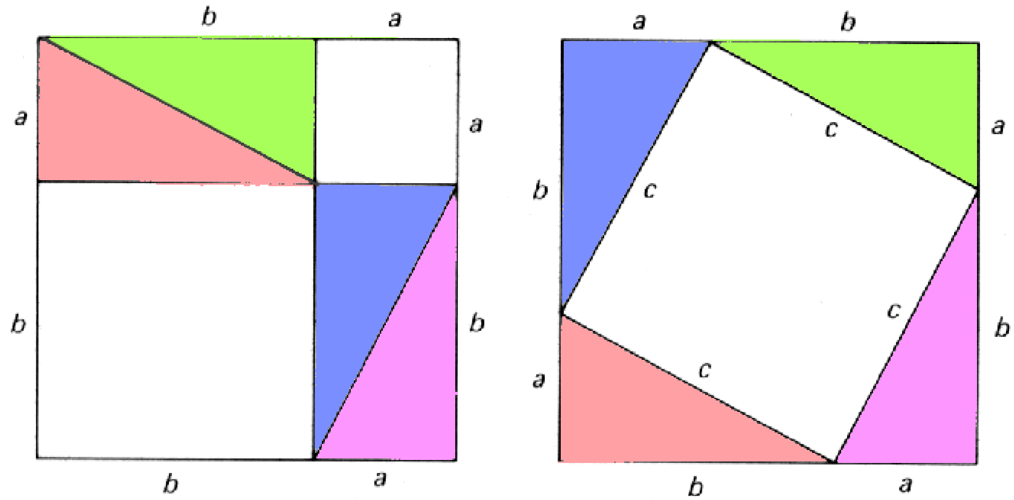
$45° - 45° - 90°$ triangles have the property that if either leg (they are identical) has length x, the hypotenuse has length $x\sqrt{2}$.



Similarly, $30° - 60° - 90°$ triangles have the property that if the side opposite the $30°$ angle has length x, the side opposite the $60°$ angle has length $x\sqrt{3}$, and the side opposite the $90°$ angle has length $2x$.

The Pythagorean Theorem

Consider the following figure:



- The area of the first square is given by: $\frac{4 \cdot ab}{2} + a^2 + b^2 = a^2 + 2ab + b^2 = (a + b)^2$
- The area of the second square is given by: $\frac{4 \cdot ab}{2} + c^2 = a^2 + 2ab + b^2 = (a + b)^2$ because $c^2 = a^2 + b^2$.

Since the squares have equal areas we can set them equal to another and subtract equals terms from both sides. The case $(a + b)^2 = (a + b)^2$ is not interesting. Let's do the other case: $\frac{4 \cdot ab}{2} + a^2 + b^2 = \frac{4 \cdot ab}{2} + c^2$ Subtracting equals terms from both sides we have:

$$a^2 + b^2 = c^2$$

Some Pythagorean Triples

A Pythagorean triple consists of three positive integers $a, b,$ and c, such that $a^2+b^2 = c^2$. Such a triple is commonly written (a, b, c) Some examples include: $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, $(8, 15, 17)$.

Heron's Formula

Heron's Formula: $A = \sqrt{(s)(s-a)(s-b)(s-c)}$

Where A is the area and s is the semiperimeter of the triangle with sides $a, b,$ and c

Proof

Let a, b, c be the sides of a triangle and α, β, γ the angles opposite those sides. Applying the law of cosines we get:

$$\cos\gamma = \frac{a^2+b^2-c^2}{2ab}$$

We know that the area of a triangle is:

$$A = \tfrac{1}{2}ab\sin\gamma$$

Replacing $\sin\gamma$ with $\sqrt{1-\cos^2\gamma}$, we get:

$$A = \frac{1}{2}ab\sqrt{1-\cos^2\gamma}$$

Replacing $\cos^2\gamma$ with $\frac{a^2+b^2-c^2}{2ab}$, we get:

$$A = \frac{1}{2}ab\sqrt{1-\left(\frac{a^2+b^2-c^2}{2ab}\right)^2}$$

Squaring the $\frac{1}{2}ab$ and putting it into the square root gives us:

$$\sqrt{\frac{a^2b^2}{4}\left[1-\frac{(a^2+b^2-c^2)^2}{4a^2b^2}\right]}$$

Expanding everything and solving gives us:

$$A = \sqrt{\frac{(a+b+c)(a+b-c)(b+c-a)(a+c-b)}{16}}$$

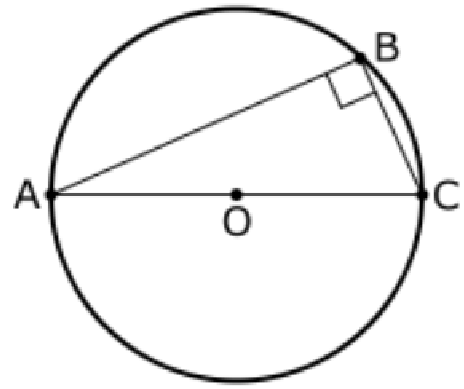
Setting $s = \frac{a+b+c}{2}$ and substituting into the above equation gives us the desired formula and our proof is done:

$$A = \sqrt{s(s-a)(s-b)(s-c)}$$

Heron's Formula is a useful result due to it being a cord bash type formula relying only on sides. Bretschneider's and Brahmagupta's can both be proven using repeated applications of this. In pre-Olympiad math Heron's Formula is one of - if not the - most commonly asked about formula not usually taught in school courses.

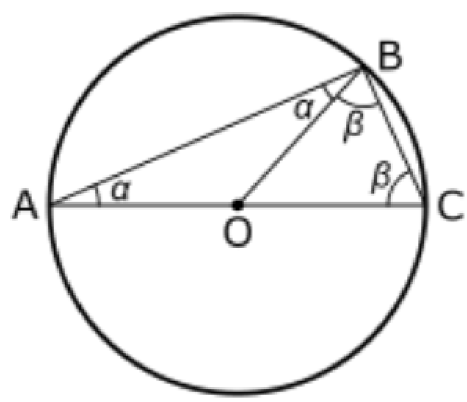
Thales' Theorem

If O is the center of a circle circumscribed about triangle ABC and $\overline{AC}$ is a diameter, then $m\angle ABC = 90$.



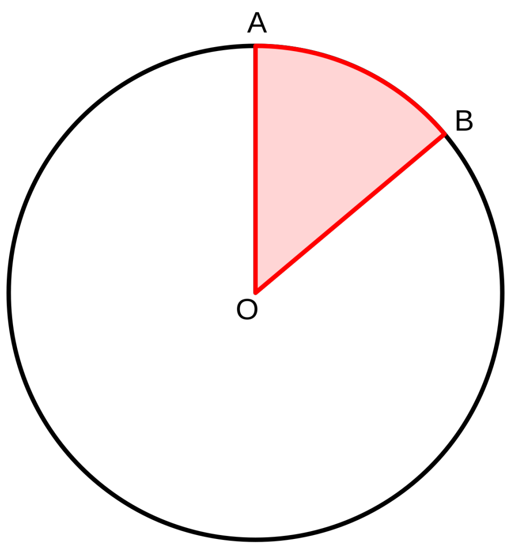
Proof

We draw the radius $\overline{OB}$. Clearly, $OB = AO = OC$ because the three lines are all radii, so AOB and BOC are both isosceles. We label $m\angle BAC = \alpha$ and $m\angle BCA = \beta$. Obviously, $m\angle BAC = m\angle OBA = \alpha$ and $m\angle BCA = m\angle OCB = \beta$, so $m\angle ABC = \alpha+\beta$. By the Angle Sum Theorem, we see that $m\angle BAC + m\angle BCA + m\angle ABC = 180 \implies \alpha + \beta + (\alpha + \beta) = 180 \implies 2(\alpha+\beta) = 180 \implies \alpha + \beta = 90$, and as we already established, $m\angle ABC = \alpha + \beta$, so $m\angle ABC = 90$, and we are done.



Arcs and Angles in a Circle

An arc is a portion of the circle's circumference measured in degrees. The measure of an angle formed by the center of a circle and two point on the circumference is equal to the measure of the intercepted (subtended) arc. An angle formed by three points on the circumference of the circle is equal to $\frac{1}{2}$ the measure of the subtended arc.



Sum of the Angles and Number of Diagonals of a Polygon

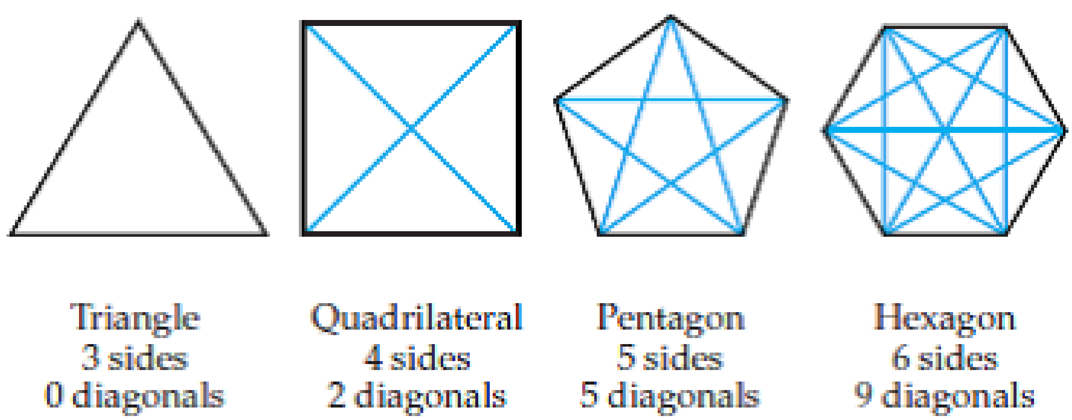
Derivations

Suppose a polygon has n sides. Consider a point in the interior of the polygon. Draw lines from the point to each vertex. We now have n triangles each with angles summing to $180°$. Now note that if we subtract a full $360°$ surrounding the point, we have the sum of all the angles. Therefore, the sum of angles is $180n - 360 = 180(n-2)$.

Sums of the Interior Angles of Polygons

Polygon	Sum
triangle	180°
quadrilateral	360°
pentagon	540°
hexagon	720°
heptagon	900°
octagon	1080°

Consider a polygon with n vertices. Let's try to count the number of diagonals. Take a random vertex of the polygon and call it P. There are $n-3$ diagonals including point P. Since there is nothing special about P, we can extend this logic to all vertices. However, we are counting each diagonal twice. Therefore, our expression is $\frac{n(n-3)}{2}$.

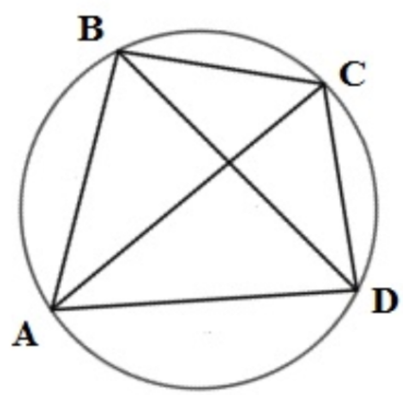


Cyclic Quadrilaterals

Cyclic quadrilaterals are those that can be inscribed in a circle. They have many properties, most notably that their opposite angles sum to 180°. If a cyclic quadrilateral contains a right angle, the diagonal not including that angle is the diameter of the circumcircle.

Ptolemy's Theorem

Consider the following diagram:



AC • BD = AB • CD + BC • AD

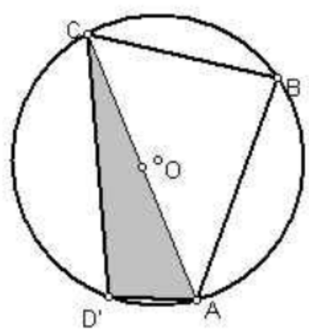
Proof

On the diagonal $\overline{BD}$ let there be a point M such that $\angle ACB$ and $\angle MCD$ be equal. Since $\angle BAC$ and $\angle BDC$ subtend the same arc, they are equal. Therefore, $\triangle ABC$ and $\triangle DMC$ are similar. Thus we get $\frac{CD}{MD} = \frac{AC}{AB}$, or $\overline{AB} \cdot \overline{CD} = \overline{AC} \cdot \overline{MD}$. Now, since $\angle BCM$ and $\angle ACD$ are also equal, $\triangle BCM$ and $\triangle ACD$ are similar which leads to $\frac{BC}{BM} = \frac{AC}{AD}$, or $\overline{BC} \cdot \overline{AD} = \overline{AC} \cdot \overline{BM}$. Summing up the two identities we obtain $\overline{AB} \cdot \overline{CD} + \overline{BC} \cdot \overline{AD} = \overline{AC} \cdot \overline{AD} + \overline{AC} \cdot \overline{BM} = \overline{AC} \cdot \overline{BD}$ and we are done.

Brahmagupta's Formula

$$K = \sqrt{(s-a)(s-b)(s-c)(s-d)}$$

Where K is the area and s is the semi-perimeter of the quadrilateral with sides $a, b, c,$ and d. For this formula to work, the quadrilateral must be cyclic.



Proof

If we draw AC, we find that $[ABCD] = \frac{ab \sin B}{2} + \frac{cd \sin D}{2} = \frac{ab \sin B + cd \sin D}{2}$. Since $B + D = 180°$, $\sin B = \sin D$. Hence, $[ABCD] = \frac{\sin B(ab+cd)}{2}$. Multiplying by 2 and squaring, we get: $4[ABCD]^2 = \sin^2 B(ab+cd)^2$. Substituting $\sin^2 B = 1 - \cos^2 B$ results in: $4[ABCD]^2 = (1-\cos^2 B)(ab+cd)^2 = (ab+cd)^2 - \cos^2 B(ab+cd)^2$. By the Law of Cosines, $a^2 + b^2 - 2ab\cos B = c^2 + d^2 - 2cd \cos D$. $\cos B = -\cos D$, so a little rearranging gives $2\cos B(ab + cd) = a^2 + b^2 - c^2 - d^2$. Rearranging this polynomial gives us the desired result:

$4[ABCD]^2 = (ab+cd)^2 - \frac{1}{4}(a^2+b^2-c^2-d^2)^2$

$16[ABCD]^2 = 4(ab+cd)^2 - (a^2+b^2-c^2-d^2)^2$

$16[ABCD]^2 = (2(ab+cd) + (a^2+b^2-c^2-d^2))(2(ab+cd) - (a^2+b^2-c^2-d^2))$

$16[ABCD]^2 = (a^2+2ab+b^2-c^2+2cd-d^2)(-a^2+2ab-b^2+c^2+2cd+d^2)$

$16[ABCD]^2 = ((a+b)^2-(c-d)^2)((c+d)^2-(a-b)^2)$

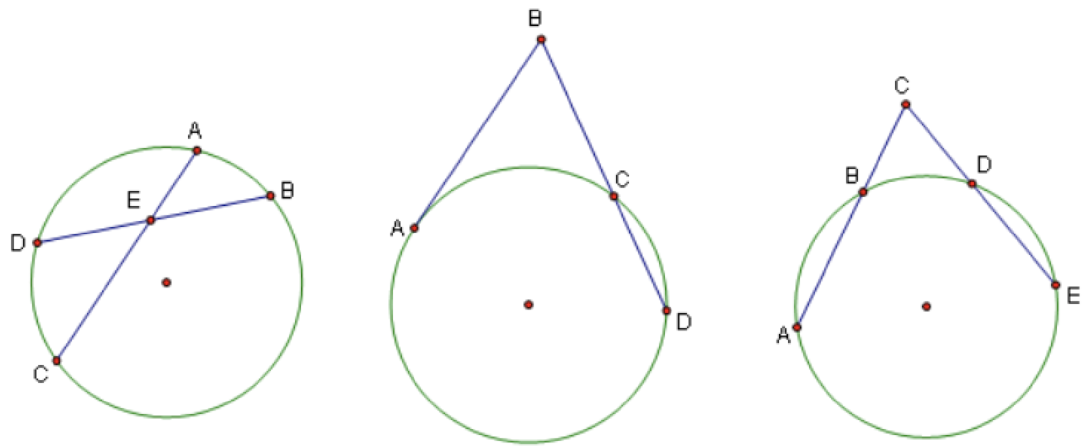
$$16[ABCD]^2 = (a+b+c-d)(a+b-c+d)(c+d+a-b)(c+d-b+a)$$

$$16[ABCD]^2 = 16(s-a)(s-b)(s-c)(s-d)$$

$$\boxed{[ABCD] = \sqrt{(s-a)(s-b)(s-c)(s-d)}}$$

Power of a Point Theorem

There are three cases for this theorem:



This theorem states that in the leftmost diagram (two intersecting internal chords) $\overline{AE} \cdot \overline{EC} = \overline{DE} \cdot \overline{EB}$, in the middle diagram (a tangent and a secant that meet at a point) $\overline{AB}^2 = \overline{BC} \cdot \overline{CD}$, and in the last diagram (secants that intersect outside the circle) $\overline{CB} \cdot \overline{CA} = \overline{CD} \cdot \overline{CE}$. As for a general version, think about it this way: A point has a constant power with respect to a given circle. The power is computed by taking any line that intersects the circle in at least one point.

Formal Version: Consider an arbitrary line intersecting the circle in at least one point that passes through P. Denote $\text{pow}_\omega(P)$ (power of point P with respect to circle ω) as the product of the distance from P to the first intersection point and the second intersection point. This is invariant no matter which line is picked.

Triangle Centers

A triangle has multiple centers. Consider the following propositions.

Propositions

- The medians are concurrent and meet at the centroid. This is also the "balancing point" of a triangle.
- The altitudes of a triangle are concurrent and meet at the orthocenter. Denote the triangle formed by the points where the altitude meet the sides as the orthic triangle.
- The incenter is the center of the circle that can be inscribed in a triangle such that the sides of the triangle are tangent to it.
- The circumcenter is the center of the circle that can be circumscribed about the triangle.
- The orthocenter is the incenter of the orthic triangle.
- The incenter is the intersection of the angle bisectors. It is also equidistant to all three sides.
- The circumcenter is equidistant from all three vertices and is the intersection of the perpendicular bisectors.

Trigonometric Identities

Definitions:

- $\sin\theta = \frac{O}{H}$
- $\cos\theta = \frac{A}{H}$
- $\sin\theta = \frac{O}{A}$

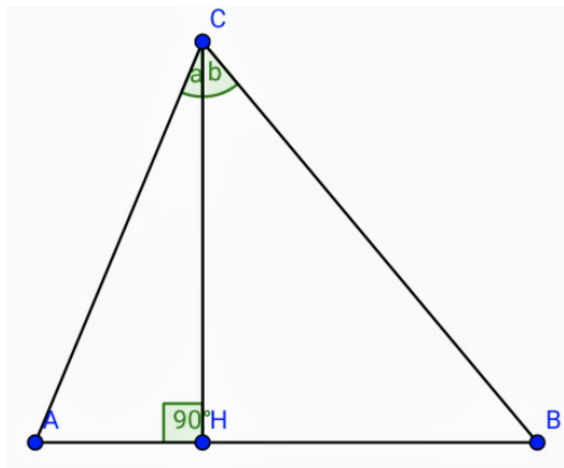
Note that $\tan\theta = \frac{\sin\theta}{\cos\theta}$ and $\cot\theta = \frac{\cos\theta}{\sin\theta}$. Also $\sec\theta = \frac{1}{\cos\theta}$ and $\csc\theta = \frac{1}{\sin\theta}$. Therefore, the identities for $\tan, \cot, \sec, \csc$ are easily derived from the identities for sin and cos.

Formulas and Identities:

- Double Angle Formula: $\sin 2\theta = 2\sin\theta\cos\theta$, $\cos 2\theta = \cos^2\theta - \sin^2\theta$
- Negative Angle Formula: $\sin\cos -\theta = \sin\cos\theta$, $\cos\sin -\theta = \cos - \sin\theta = \cos\sin\theta$
- Pythagorean Identities: $\sin^2\theta + \cos^2\theta = 1$, $\cot^2\theta + 1 = \csc^2\theta$, $\tan^2\theta + 1 = \sec^2\theta$
- Addition/Subtraction Identities: $\sin a \pm B = \sin a \cos B \pm \sin B \cos a$, $\cos a \pm B = \cos a \cos B \pm \sin a \sin B$
- Half Angle Identities: $\sin\frac{\theta}{2} = \pm\sqrt{\frac{1-cos\theta}{2}}$, $\cos\frac{\theta}{2} = \pm\sqrt{\frac{1+cos\theta}{2}}$

Proof:

Let's take a geometric approach, using $[ABC] = \frac{1}{2}ab\sin C$. Without loss of generality, let $AH = 1$ in the diagram below:



We have $[ABC] = \frac{1}{2}ab\sin{(a+b)} = [ACH] + [BCH] = \frac{1}{2}(AC\sin a + BC\sin b)$. We also know that $[ABC] = \frac{1}{2}ab\sin(a+b) = [ACH] + [BCH] = \frac{1}{2}(AC\sin a + BC\sin b)$ So, $\dfrac{1}{\cos a\cos b}\sin{(a+b)} = \dfrac{\sin a}{\cos a} + \dfrac{\sin b}{\cos b}$.

Extended Law of Sines

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R$$

Where $a, b,$ and c are sides of a triangle, each opposite its respective angle $A, B,$ and C. R is the circumradius.

Law of Cosines

For a triangle with sides $a, b,$ and c and $A, B,$ and C respectively, the Law of Cosines states:

$$c^2 = a^2 + b^2 - 2ab\cos C$$

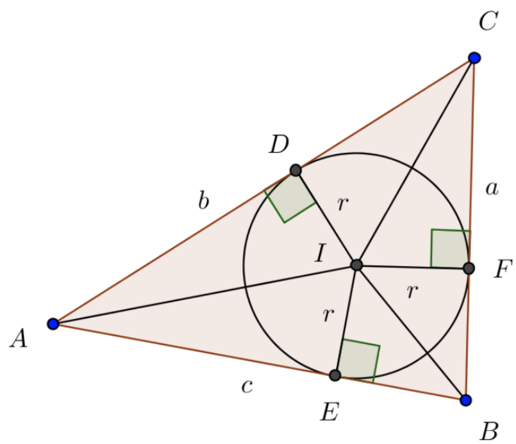
Area of a Triangle Part 2

$$A = \frac{bh}{2} = rs = \frac{ab\sin\theta}{2} = \frac{abc}{4R}$$

Where A is the area, b is the base, and h is the height. In the second equation, r is the inradius and s is the semiperimeter (which is half the perimeter). In the third equation, θ is the angle between two sides a, b of the triangle. In the final equation, a, b, c are the sides of the triangle with circumradius R.

Proofs:

First we prove $A = rs$, consider the following diagram:



Let I be the incenter of $\triangle ABC$, let r be the inradius of $\triangle ABC$.

The total area of $\triangle ABC$ is equal to the sum of the areas of the triangle formed by the vertices of $\triangle ABC$ and its incenter:

$$A = [\triangle AIB] + [\triangle CIB] + [\triangle CIA]$$

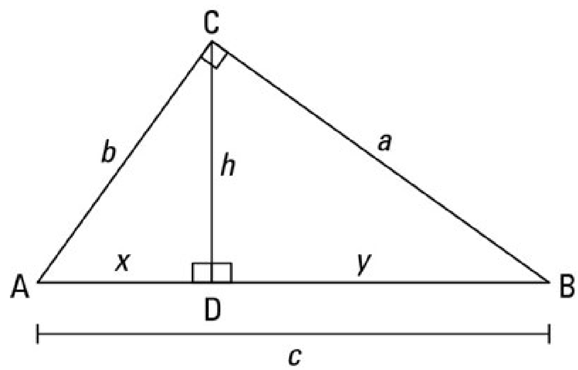
Let $AB, BC,$ and CA be the bases of $\triangle AIB, \triangle BIC, \triangle CIA$ respectively. The lengths of $AB, BC,$ and CA respectively are c, a, b. The length of each of these triangles is r. Thus, from the Area of Triangle in Terms of Side and Altitude theorem:

- $[\triangle AIB] = \frac{cr}{2}$
- $[\triangle BIC] = \frac{ar}{2}$
- $[\triangle CIA] = \frac{br}{2}$

Thus:

$$A = r\frac{a+b+c}{2} \implies A = rs \text{ because } s = \frac{a+b+c}{2}$$

Now we will derive the identity: $A = \frac{1}{2}ab\sin C$. Consider the following arbitrary triangle:



The area of the triangle is $\frac{bh}{2}$. Now note that $\sin A = \frac{h}{c} \implies c\sin A = h$. Plugging this into our basic area formula. We get our desired, $A = \frac{1}{2}ab\sin C$.

Now we will prove the final formula, the extended Law of Sines:

$$\frac{a}{\sin A} = 2R \implies \sin A = \frac{a}{2R}$$

We have proven that $\frac{1}{2}bc\sin A$ is the area. Hence, $\frac{1}{2}bc\frac{a}{2R}$ is the area which is equivalent to $\frac{abc}{4R}$ and we are done.

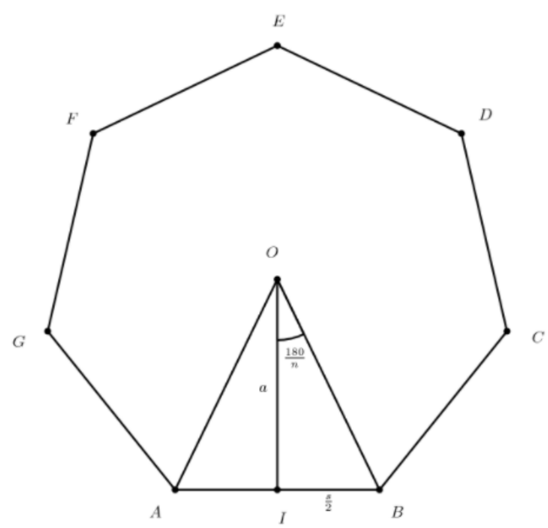
Area of a Regular Polygon

$$A = \frac{ap}{2} \text{ or } \frac{ns^2}{4\tan\left(\frac{180}{n}\right)}$$

Where A is the area, a is the apothem, p is the perimeter, n is the number of sides, and s is the side length

Proof:

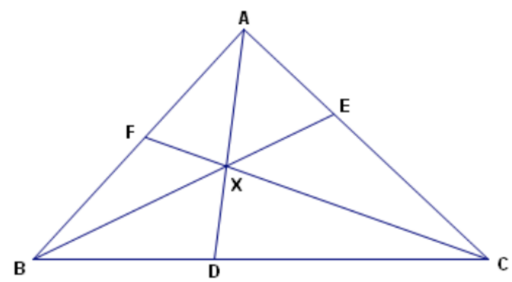
Consider the following diagram:



Note that the area of each of the n triangles is $\frac{as}{2}$. Summing all these up, $\frac{nsa}{2} = \frac{ap}{2}$ which proves the first formula. Consider $\tan(\angle IOB)$. This is equal to $\frac{s}{2a}$. Thus $a = \frac{s}{2\tan(\frac{180}{2})}$. Also note that the perimeter is equal to ns. Plugging these into $\frac{ap}{2}$ we get our desired formula, $\frac{ns^2}{4\tan\left(\frac{180}{n}\right)}$.

Ceva's Theorem

Ceva's theorem states that in $\triangle ABC$ with points $D, E,$ and F on sides $\overline{BC}, \overline{AC}, \overline{AB}$ respectively, $\overline{BE}, \overline{CF}, \overline{AD}$ are concurrent if, and only if, $\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = 1$.



Proof:

First, suppose AD, BE, CF meet at a point X. We note that triangles ABD, ADC have the same altitude to line BC, but bases BD and DC. It follows that $\frac{BD}{DC} = \frac{[ABD]}{[ADC]}$. The same is true for triangles XBD, XDC, so:

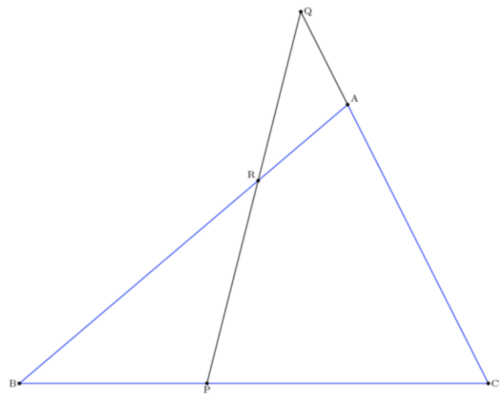
$$\frac{BD}{DC} = \frac{[ABD]}{[ADC]} = \frac{[XBD]}{[XDC]} = \frac{[ABD]-[XBD]}{[ADC]-[XDC]} = \frac{[ABX]}{[AXC]}$$

Similarly, $\frac{CE}{EA} = \frac{[BCX]}{[BXA]}$ and $\frac{AF}{FB} = \frac{[CAX]}{[CXB]}$, so $\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = \frac{[ABX]}{[AXC]} \cdot \frac{[BCX]}{[BXA]} \cdot \frac{[CAX]}{[CXB]} = 1$ Now, suppose D, E, F satisfy Ceva's criterion, and suppose AD, BE intersect at X. Suppose the line CX intersects line AB at F'. We have proven that F' must satisfy Ceva's criterion. This means that:

$$\frac{AF'}{F'B} = \frac{AF}{FB}, \text{ so } F' = F, \text{ and line } CF \text{ concurs with } AD \text{ and } BE.$$

Menelaus' Theorem

This configuration shows up from time to time, though not often. The theorem states that given a configuration as shown below, $\overline{BP} \cdot \overline{CQ} \cdot \overline{PC} = \overline{QA} \cdot \overline{RB} \cdot \overline{AR}$.



Proof:

Draw a line parallel to QP through A to intersect BC at K:

$$\triangle RBP \sim \triangle ABK \implies \frac{AR}{RB} = \frac{KP}{PB} \text{ and } \triangle QCP \sim \triangle ACK \implies \frac{QC}{QA} = \frac{PC}{PK}$$

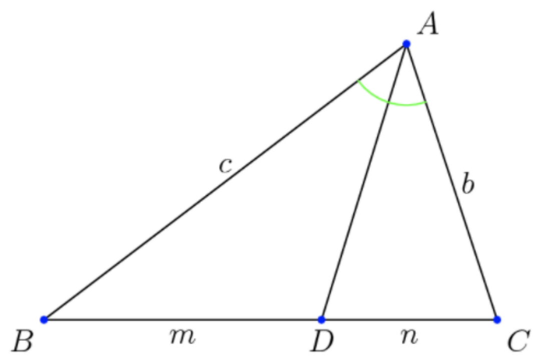
Multiplying the two equalities together to eliminate the PK factor, we get:

$$\frac{AR}{RB} \cdot \frac{QC}{QA} = \frac{PC}{PB} \implies \frac{AR}{RB} \cdot \frac{QC}{QA} \cdot \frac{PB}{PC} = 1$$

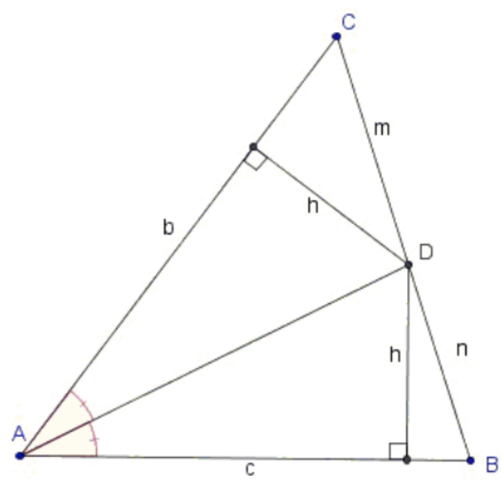
and we are done.

Angle Bisector Theorem

The Angle Bisector Theorem states that given $\triangle ABC$ and angle bisector $\overline{AD}$, where D is on side $\overline{BC}$, then $\frac{c}{m} = \frac{b}{n}$. Likewise, the converse of this theorem holds as well.



Proof:



Consider the diagram above for arbitrary $\triangle ABC$. Because the triangles share the altitude from A, $\frac{ACD}{ABD} \Rightarrow \frac{m}{n}$. Since, point D is equidistant from the sides b and c (because it lies on the angle bisector), the altitudes of the smaller triangles (denoted h) from D are equal. Thus we have $\frac{ACD}{ABD} \Rightarrow \frac{\frac{bh}{2}}{\frac{ch}{2}} \Rightarrow \frac{b}{c}$. This implies $\frac{m}{n} = \frac{b}{c}$ and we are done.

Triangle Inequality

The Triangle Inequality says that in non-degenerate $\triangle ABC$:

- $\overline{AB} + \overline{BC} > \overline{AC}$
- $\overline{BC} + \overline{AC} > \overline{AB}$
- $\overline{AC} + \overline{AB} > \overline{BC}$

For a formal definition, the shortest distance between two points is a straight line.

Pick's Theorem

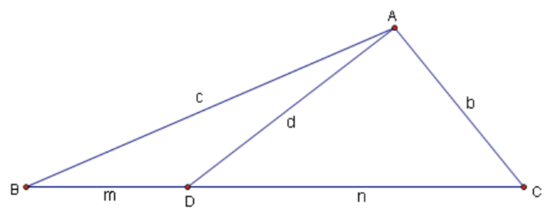
$$A = I + \frac{1}{2}B - 1$$

Where A is the area, I is the number of lattice points in the interior, and B is the number of lattice points on the boundary of a figure in the coordinate plane.

Stewart's Theorem

Take $\triangle ABC$ with sides of length a, b, c opposite vertices A, B, C respectively. If cevian $\overline{AD}$ is drawn so that $\overline{BD} = m, \overline{DC} = n, \overline{AD} = d$ we have that $man + dad = bmb + cnc$, which can be remembered using the mnemonic device, "A man and his dad put a bomb in the sink."

Proof:



From the diagram above, we see that $\angle ADB = 180° - \angle ADC$. Thus, $\cos ADB = -\cos ADC$. Now we apply Law of Cosines on $\triangle ABD$ and $\triangle ADC$:

$$c^2 = m^2 + d^2 - 2md \cos ABD$$

Manipulating this equation around, we finally get:

$$\cos ADC = \frac{n^2 + d^2 - b^2}{2nd}$$

Thus, $-\cos ADB = \dfrac{c^2 - m^2 - d^2}{2md} = \cos ADC$. We equate the two equations to get $\cos ADC$:

$$\frac{c^2 - m^2 - d^2}{2md} = \frac{n^2 + d^2 - b^2}{2nd}$$

$$2nd\,(c^2 - m^2 - d^2) = 2md\,(n^2 + d^2 - b^2)$$

$$c^2n - m^2n - d^2n = mn^2 + d^2m - b^2m$$

$$c^2n + b^2m = mn^2 + m^2n + d^2m + d^2n$$

$$mn(m + n) + d^2(m + n) = bmb + cnc$$

We know that $m + n = a$, so substituting it in gives us the desired result:

$$man + dad = bmb + cnc$$

Shoelace Theorem

Suppose the polygon P has vertices $(a_1, b_1), (a_2, b_2), ..., (a_n, b_n)$ listed in clockwise order. Then the area of P is:

$$\frac{1}{2}|(a_1b_2 + a_2b_3 + ... + a_nb_1) - (b_1a_2 + b_2a_3 + ... + b_na_1)|$$

The Shoelace Theorem gets its name because if one lists the coordinates in a column and marks the pairs of coordinates to be multiplied, the resulting image looks like laced-up shoes:

$$(a_1, b_1)$$

$$(a_2, b_2)$$

$$...$$

$$(a_n, b_n)$$

$$(a_1, b_1)$$

Girard's Theorem

Girard's Theorem: The area of any spherical triangle (triangle on a sphere) is $r^2 \cdot e$ where r is the radius and $e = \alpha + \beta + \gamma - \pi$.

We can use the Gauss-Bonnet theorem, which can be used for other 2-dimensional manifolds as well, e.g. the hyperbolic plane. It states that if M is a 2-dimensional Riemannian manifold with piecewise smooth boundary, then:

$$\int_M K dA + \int_{\partial M} k_g + \sum_i \alpha_i = 2\pi\chi(M)$$

where K is the Gauss curvature, k_g the geodesic curvature (which is zero for geodesics), α_i the angles by which the tangent to the boundary turns at points where ∂M is not smooth, and $\chi(M)$ the Euler characteristic of M.

In our case M is the triangle, K is identically $\frac{1}{R^2}$, the angles α_i are $\pi - \alpha, \pi - \beta, \pi - \gamma$ and $\chi(M) = 1$. Therefore the formula becomes:

$$\frac{A}{R^2} + (\pi - \alpha + \pi - \beta + \pi - \gamma) = 2\pi \implies \boxed{A = (\alpha + \beta + \gamma - \pi)R^2}.$$

Formulas for Series

Sum of an Arithmetic Series

$$\boxed{S_n = \frac{n}{2}(a_1 + a_n)}$$

Where n is the number of terms, S_n is the sum, and a_1 is the first term.

Sum of the First n Terms of a Geometric Series

$$\boxed{S = \frac{a_1(1-r^n)}{1-r}}$$

Where S is the sum, a_1 is the first term, and r is the common ratio.

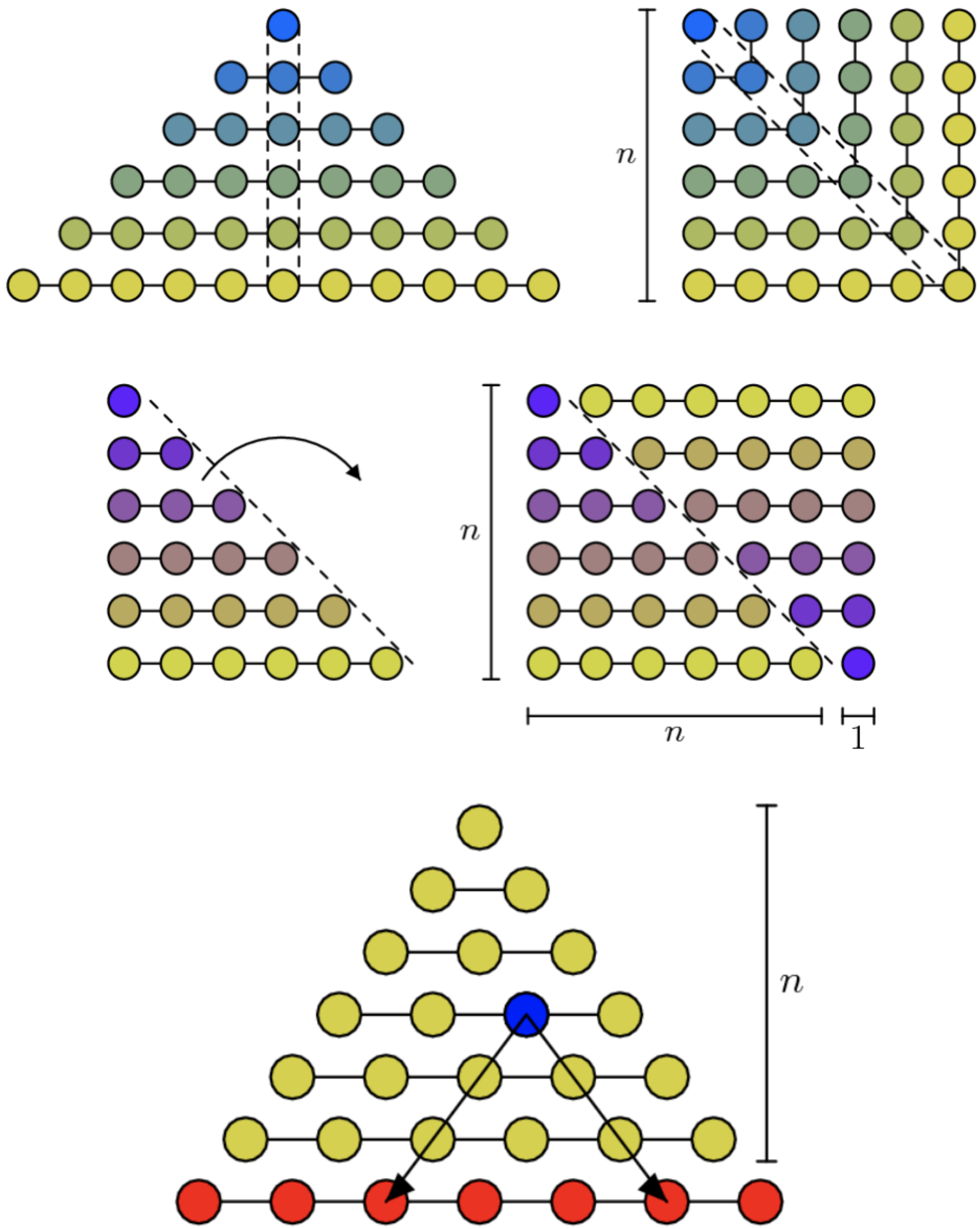
Sum of an Infinite Geometric Series

$$\boxed{S = \frac{a_1}{1-r}}$$

Where S is the sum, a_1 is the first term, and r is the common ratio.

Sum of the first n Even/Odd Numbers

The sum of the first n odd numbers is simply n^2. The sum of the first n numbers is $\frac{n(n+1)}{2} = \binom{n+1}{2}$. The sum of the first n even numbers is $n(n+1)$.



Number/Sum of Divisors

Let $p_1^x p_2^y ... p_m^n$ be the prime factorization of some number a. The number of divisors a has is given by:

$$(x-1)(y-1)...(n-1)$$

Similarly, the sum of the divisors of a is given by:

$$(p_1^0 + p_1^1 ... p_1^x)(p_2^0 + p_2^1 ... p_2^y)...(p_m^0 + p_m^1 ... p_m^n)$$

Chinese Remainder Theorem

The Chinese Remainder Theorem (or CRT) allows you to solve a system of linear congruences. Let $m_1, m_2, ..., m_r$ be a collection of pairwise relatively prime integers. Then the system of simultaneous congruences $x \equiv a_1 (\mod m_1), x \equiv a_2 (\mod m_2), ..., x \equiv a_r (\mod m_r)$ has a unique solution modulo $M = m_1 m_2, m_r$, for any given integers $a_1, a_2, ..., a_r$.

Chicken McNugget Theorem

The Chicken McNugget Theorem states that for any two relatively prime positive integers, m, n, the greatest integer that cannot be written in the form $am + bn$ the greatest number that can not be expressed as a sum of the two numbers) where a, b are positive integers is $mn - m - n$. It follows that there are positive integers which cannot be expressed as the sum of some number of mn and ns.

Euler's Totient/Phi Function

$$\phi n = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_n})$$

Where n is any positive integer and p_n are prime divisors of n. This gives the number of relatively prime positive integers less than or equal to some number n.

GCD and LCM Identities

- $\gcd(m,n) \cdot \mathrm{lcm}[m,n] = mn$
- $gcd[gcd[m,n],p] == gcd[m,gcd[n,p]]$
- $gcd(n_1, gcd((n_2),(n_3),...,n_m)) = gcd(n_1,n_2,n_3,...,n_m)$
- $gcd[m,n,p] == gcd[m,gcd[n,p]]$

Bézout's identity

Bézout's identity — For any nonzero integers a and b, of which the greatest common divisor is d, all three of the following hold:

- there exist integers x and y such that $ax + by = d$,
- d is the smallest positive integer that can be written as $ax + by$, and
- every integer of the form $ax + by$ is a multiple of d.

Euclidean Algorithm

The Euclidean algorithm, also called Euclid's algorithm, is an algorithm for finding the greatest common divisor of two numbers a and b. It proceeds as the following: Let $a = bq+r$, then find a number u which divides both a and b (so that $a = su$ and $b = tu$), then u also divides r since:

$$r = a - bq = su - qtu = (s - qt)u$$

Similarly, find a number v which divides b and r (so that $b = s'v$ and $r = t'v$), then v divides a since:

$$a = bq + r = s'vq + t'v = (s'q + t')v.$$

Therefore, every common divisor of a and b is a common divisor of b and r, so the procedure can be iterated as follows:

$$\begin{array}{lll}
q_1 = \left\lfloor \frac{a}{b} \right\rfloor & a = b\,q_1 + r_1 & r_1 = a - b\,q_1 \\
q_2 = \left\lfloor \frac{b}{r_1} \right\rfloor & b = q_2\,r_1 + r_2 & r_2 = b - q_2\,r_1 \\
q_3 = \left\lfloor \frac{r_1}{r_2} \right\rfloor & r_1 = q_3\,r_2 + r_3 & r_3 = r_1 - q_3\,r_2 \\
q_4 = \left\lfloor \frac{r_2}{r_3} \right\rfloor & r_2 = q_4\,r_3 + r_4 & r_4 = r_2 - q_4\,r_3 \\
q_n = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor & r_{n-2} = q_n\,r_{n-1} + r_n & r_n = r_{n-2} \\
 & & \quad -q_n\,r_{n-1} \\
q_{n+1} = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor & r_{n-1} = q_{n+1}\,r_n + 0 & r_n = r_{n-1} / q_{n+1}
\end{array}$$

For integers, the algorithm terminates when $q_(n+1)$ divides $r_(n-1)$ exactly, at which point r_n corresponds to the greatest common divisor of a and b, $gcd(a, b) = r_n$. For real numbers, the algorithm yields either an exact relation or an infinite sequence of approximate relations. An important consequence of the Euclidean algorithm is finding integers x and y such that:

$$ax + by = gcd(a, b).$$

This can be done by starting with the equation for r_n, substituting for $r_(n-1)$ from the previous equation, and working upward through the equations. Note that the r_i are just remainders, so the algorithm can be easily applied by hand by repeatedly computing remainders of consecutive terms starting with the two numbers of interest (with the larger of the two written first). As an example, consider applying the algorithm to $(a, b) = (42, 30)$. This gives 42, 30, 12, 6, 0, so $gcd(42, 30) = 6$. Similarly, applying the algorithm to $(144, 55)$ gives 144, 55, 34, 21, 13, 8, 5, 3, 2, 1, 0, so $gcd(144, 55) = 1$ and 144 and 55 are relatively prime.

Extended Euclidean Algorithm

Wilson's Theorem

Wilson's theorem states that a natural number $n > 1$ is a prime number if and only if the product of all the positive integers less than n is one less than a multiple of n. Wilson's Theorem is rather uncommon, but it is very powerful when you use it since it's a bijection. Also, note that Wilson's Theorem provides a primality test. However, there is no quick way to compute $n!$. It states that for any prime n:

$$(n-1)! \equiv -1 \mod n$$

Trivial Inequality

Yes, this is a real thing. It states that $x^2 \geq 0$ for all real x (now you know why it is called "trivial"). You don't really need this for anything, but many other well known theorems and inequalities are based on this.

Fibonacci Numbers

Define a sequence F_n such that $F_0 = 1, F_1 = 1, F_n = F_n - 1 + F_n - 2$. The first few terms look like $0, 1, 1, 2, 3, 5, 8, \ldots$. Consider the following propositions involving Fibonacci Numbers.

- (Binet's Formula) If F_n is the nth Fibonacci number, then:

  $$[F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)]$$

- (Quotient) The quotient of two consecutive terms approaches the golden ratio: $\frac{1+\sqrt{5}}{2}$

- (Famous Identity)

  $$\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$$

- (Yet another famous identity)

  $$\sum_{i=1}^{n} F_i = F_{n+2} - 1$$

Note

All of these identities can be proven with induction.

Pigeonhole Principle

If we distribute n balls into k boxes such that $n > k$ then at least one box must have multiple balls. This is just common sense - the proof is trivial. However, there are some really tricky problems utilizing this fact.

Example

Jessica is studying combinatorics during a 7-week period. She will study a positive integer number of hours every day during the 7 weeks, but she won't study more than 11 hours in any 7-day period. Prove that there must exist some period of consecutive days during which Jessica studies exactly 20 hours.

Solution

For $0 \leq k \leq 49$, let s_k be the total number of hours Jessica studies during the first k days (note that $s_0 = 0$). By the pigeonhole principle, some three of $s_0, s_1, s_2, \ldots, s_{49}$ leave the same remainder when divided by 20. Let's say these are s_p, s_q, and s_r, where $p < q < r$. Then Jessica studies a multiple of 20 hours during days $p+1$ through q, and also studies a multiple of 20 hours during days $q+1$ through r. If each of these multiples is 40 or more, then Jessica studies at least 80 hours total, which contradicts our knowledge that she studies at most $7 \cdot 11 = 77$ hours over the entire 7-week period. So one of these multiples of 20 must be exactly 20, which shows that there is a period of consecutive days during which Jessica studies exactly 20 hours.

Logarithm Rules

- Logarithm to Exponential: $\log_a b = x \Rightarrow a^x = b$
- Addition: $\log_a b + \log_a c = \log_a bc$
- Subtraction: $\log_a b - \log_a c = \log_a \frac{b}{c}$
- Exponent Reducing: $\log_a b^n = n \log_a b$
- Change of Base: $\log_a b = \frac{\log_c b}{\log_c a}$
- Reciprocals: $\log_a b = \frac{1}{\log_b a}$

Notes

All of these rules are essential and extremely effective in solving problems involving logarithms.

Vieta's Formulas

Vieta's Formulas were discovered by the French mathematician François Viète. Vieta's Formulas can be used to relate the sum and product of the roots of a polynomial to its coefficients. The simplest application of this is with quadratics. If we have a quadratic $x^2 + ax + b = 0$ with solutions p and q, then we know that we can factor it as:

$$x^2 + ax + b = (x - p)(x - q)$$

(Note that the first term is x^2, not ax^2.) Using the distributive property to expand the right side we now have:

$$x^2 + ax + b = x^2 - (p + q)x + pq$$

We know that two polynomials are equal if and only if their coefficients are equal, so $x^2 + ax + b = x^2 - (p+q)x + pq$ means that $a = -(p+q)$ and $b = pq$. In other words, the product of the roots is equal to the constant term, and the sum of the roots is the opposite of the coefficient of the x term. A similar set of relations for cubics can be found by expanding $x^3 + ax^2 + bx + c = (x - p)(x - q)(x - r)$. We can state Vieta's formulas more rigorously and generally. Let $P(x)$ be a polynomial of degree n, so $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where the coefficient of x^i is a_i and $a_n \neq 0$. As a consequence of the Fundamental Theorem of Algebra, we can also write $P(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n)$, where r_i are the roots of $P(x)$. We thus have that:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n(x - r_1)(x - r_2)\cdots(x - r_n).$$

Expanding out the right-hand side gives us:

$$a_n x^n - a_n(r_1 + r_2 + \cdots + r_n)x^{n-1} + a_n(r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n)x^{n-2} + \cdots + (-1)^n a_n r_1 r_2 \cdots r_n.$$

The coefficient of x^k in this expression will be the $(n-k)$-th elementary symmetric sum of the r_i. We now have two different expressions for $P(x)$. These must be equal. However, the only way for two polynomials to be equal for all values of x is for each of their corresponding coefficients to be equal. So, starting with the coefficient of x^n, we see that:

$$a_n = a_n$$

$$a_{n-1} = -a_n(r_1 + r_2 + \cdots + r_n)$$

$$a_{n-2} = a_n(r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n)$$

More commonly, these are written with the roots on one side and the a_i on the other (this can be arrived at by dividing both sides of all the equations by a_n). If we denote σ_k as the k-th elementary symmetric sum, then we can write those formulas more compactly as $\sigma_k = (-1)^k \cdot \frac{a_{n-k}}{a_n}$, for $1 \leq k \leq n$.

Newton's Sum

Consider a polynomial $P(x)$ of degree n,

$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ Let $P(x) = 0$ have roots $x_1, x_2, \ldots, x_n$.

Define the following sums:

$P_1 = x_1 + x_2 + \cdots + x_n$

$P_2 = x_1^2 + x_2^2 + \cdots + x_n^2$

$\vdots$

$P_k = x_1^k + x_2^k + \cdots + x_n^k$

$\vdots$

Newton sums tell us that,

$a_n P_1 + a_{n-1} = 0$

$a_n P_2 + a_{n-1} P_1 + 2a_{n-2} = 0$

$a_n P_3 + a_{n-1} P_2 + a_{n-2} P_1 + 3a_{n-3} = 0$

$\vdots$

(Define $a_j = 0$ for $j < 0$.)

We also can write:

$P_1 = S_1$

$P_2 = S_1 P_1 - 2S_2$

etc., where S_n denotes the n-th elementary symmetric sum.

Proof

Let $\alpha, \beta, \gamma, ..., \omega$ be the roots of a given polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + .. + a_1 x + a_0$.

Then, we have that

$P(\alpha) = P(\beta) = P(\gamma) = ... = P(\omega) = 0$

Thus,

$$\begin{cases} a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0 \\ a_n\beta^n + a_{n-1}\beta^{n-1} + ... + a_0 = 0 \\ \vdots \\ a_n\omega^m + a_{n-1}\omega^{n-1} + ... + a_0 = 0 \end{cases}$$

Multiplying each equation by $\alpha^{k-n}, \beta^{k-n}, ..., \omega^{k-n}$, respectively,

$$\begin{cases} a_n\alpha^{n+k-n} + a_{n-1}\alpha^{n-1+k-n} + ... + a_0\alpha^{k-n} = 0 \\ a_n\beta^{n+k-n} + a_{n-1}\beta^{n-1+k-n} + ... + a_0\beta^{k-n} = 0 \\ \vdots \\ a_n\omega^{n+k-n} + a_{n-1}\omega^{n-1+k-n} + ... + a_0\omega^{k-n} = 0 \end{cases}$$

$$\begin{cases} a_n\alpha^k + a_{n-1}\alpha^{k-1} + ... + a_0\alpha^{k-n} = 0 \\ a_n\beta^k + a_{n-1}\beta^{k-1} + ... + a_0\beta^{k-n} = 0 \\ \vdots \\ a_n\omega^k + a_{n-1}\omega^{k-1} + ... + a_0\omega^{k-n} = 0 \end{cases}$$

Sum,

$$a_n \underbrace{\left(\alpha^k + \beta^k + ... + \omega^k\right)}_{P_k} + a_{n-1} \underbrace{\left(\alpha^{k-1} + \beta^{k-1} + ... + \omega^{k-1}\right)}_{P_{k-1}}$$
$$+ a_{n-2} \underbrace{\left(\alpha^{k-2} + \beta^{k-2} + ... + \omega^{k-2}\right)}_{P_{k-2}} + ... + a_0 \underbrace{\left(\alpha^{k-n} + \beta^{k-n} + ... + \omega^{k-n}\right)}_{P_{k-n}} = 0$$

Therefore,

$$\boxed{a_nP_k + a_{n-1}P_{k-1} + a_{n-2}P_{k-2} + ... + a_0P_{k-n} = 0}$$

Common Factorizations

Listed below are some common factorizations that are very helpful in solving difficult problems.

Factoring Formulas

- $a^2 - b^2 = (a+b)(a-b)$
- $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$
- $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$
- $a^4 - b^4 = (a-b)(a+b)(a^2 - b^2)$
- $a^5 - b^5 = (a-b)(a^4 - a^3b + a^2b^2 + ab^3 + b^4)$

Product Formulas

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
- $(a-b)^3 = a^3 - 3a^2b + 3ab^2 - b^3$
- $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$
- $(a-b)^4 = a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4$
- $(a+b+c)^2 = a^2 + b^2 + c^2 + 2ab + 2ac + 2bc$
- $(a+b+c+...)^2 = a^2 + b^2 + c^2 + ... + 2(ab + ac + bc + ...)$

Simon's Favorite Factoring Trick

The general statement of SFFT is: $xy+xk+jy+jk=(x+j)(y+k)$. Two special common cases are: $xy+x+y+1=(x+1)(y+1)$ and $xy-x-y+1=(x-1)(y-1)$. The act of adding jk to $xy+xk+jy$ in order to be able to factor it could be called "completing the rectangle" in analogy to the more familiar "completing the square."

Quadratic Formula

The quadratic formula states that for a quadratic $ax^2 + bx + c$, $x = \frac{b \pm \sqrt{b^2 - 4ac}}{2a}$

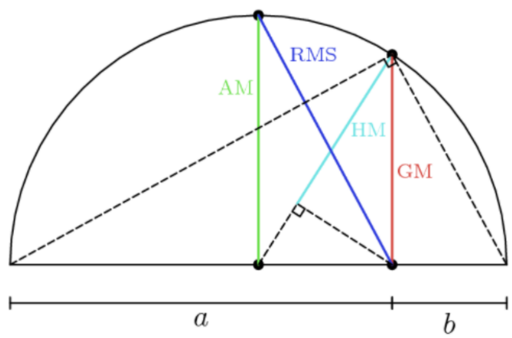
Proof

RMS-AM-GM-HM

The Root-Mean Square-Arithmetic Mean-Geometric Mean-Harmonic Mean Inequality, is an inequality of the root-mean square, arithmetic mean, geometric mean, and harmonic mean of a set of positive real numbers $x_1, \ldots, x_n$ that says:

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

with equality if and only if $x_1 = x_2 = \cdots = x_n$. This inequality can be expanded to the power mean inequality.



The inequality is clearly shown in this diagram for $n = 2$ As a consequence we can have the following inequality: If $x_1, x_2, \cdots, x_n$ are positive reals, then:

$$(x_1 + x_2 + \cdots + x_n)\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots \frac{1}{x_n}\right) \geq n^2$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$; which follows directly by cross multiplication from the AM-HM inequality. This is extremely useful in problem solving Essentially, it states that the root-mean square is greater than or equal to the arithmetic mean is greater than or equal to the geometric mean is greater than or equal to the harmonic mean. The most important part of this inequality is AM-GM, which states that the arithmetic mean is greater than or equal to the geometric mean. Equality holds when all the s are the same. It is often used for maximization and minimization problems.

Proof

The inequality $\sqrt{\frac{x_1^2+\cdots+x_n^2}{n}} \geq \frac{x_1+\cdots+x_n}{n}$ is a direct consequence of the Cauchy-Schwarz Inequality; $(x_1^2+x_2^2+\cdots+x_n^2)(1+1+\cdots+1) \geq (x_1+x_2+\cdots+x_n)^2$, so $\frac{x_1^2+x_2^2+\cdots+x_n^2}{n} \geq \left(\frac{x_1+x_2+\cdots+x_n}{n}\right)^2$, so $\sqrt{\frac{x_1^2+\cdots+x_n^2}{n}} \geq \frac{x_1+\cdots+x_n}{n}$.

Alternatively, the RMS-AM can be proved using Jensen's inequality: Suppose we let $F(x) = x^2$ (We know that $F(x)$ is convex because $F'(x) = 2x$ and therefore $F''(x) = 2 > 0$). We have: $F\left(\frac{x_1}{n} + \cdots + \frac{x_n}{n}\right) \leq \frac{F(x_1)}{n} + \cdots + \frac{F(x_n)}{n}$;

Factoring out the $\frac{1}{n}$ yields:

$F\left(\frac{x_1+\cdots+x_n}{n}\right) \leq \frac{F(x_1)+\cdots+F(x_n)}{n}$

$\left(\frac{x_1+\cdots+x_n}{n}\right)^2 \leq \frac{x_1^2+\cdots+x_n^2}{n}$

Taking the square root to both sides (remember that both are positive):

$\sqrt{\frac{x_1^2+\cdots+x_n^2}{n}} \geq \frac{x_1+\cdots+x_n}{n}$.

The inequality $\frac{x_1+\cdots+x_n}{n} \geq \sqrt[n]{x_1\cdots x_n}$ is called the AM-GM inequality, and proofs can be found here.

The inequality $\sqrt[n]{x_1\cdots x_n} \geq \frac{n}{\frac{1}{x_1}+\cdots+\frac{1}{x_n}}$ is a direct consequence of AM-GM;

$$\frac{\sum_{i=1}^{n} \sqrt[n]{\frac{x_1x_2\cdots x_n}{x_i^n}}}{n} \geq 1, \text{ so } \sqrt[n]{x_1x_2\cdots x_n}\frac{\sum_{i=1}^{n} \frac{1}{x_i}}{n} \geq 1, \text{ so } \sqrt[n]{x_1\cdots x_n} \geq \frac{n}{\frac{1}{x_1}+\cdots+\frac{1}{x_n}}.$$

Therefore the original inequality is true. The Root Mean Square is also known as the quadratic mean, and the inequality is therefore sometimes known as the QM-AM-GM-HM Inequality.

DeMoivre's Theorem

DeMoivre's Theorem is a very useful theorem in the mathematical fields of complex numbers. It allows complex numbers in polar form to be easily raised to certain powers. It states that for $x \in \mathbb{R}$ and $n \in \mathbb{Z}$, $(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)$. It states that for a rational x and integral n, $\text{cis}(x)^n = \text{cis}(nx)$. This uses trigonometry and the fact that the roots of a polynomial are equally spaced out on the complex plane to find the n^{th} root of a polynomial.

Proof

This is one proof of De Moivre's theorem by induction:

If $n > 0$, for $n = 1$, the case is obviously true. Assume true for the case $n = k$. Now, the case of $n = k + 1$:

$$\begin{aligned} (\cos x + i \sin x)^{k+1} &= (\cos x + i \sin x)^k (\cos x + i \sin x) && \text{by Exponential laws} \\ &= [\cos(kx) + i \sin(kx)](\cos x + i \sin x) && \text{by the Assumption in Step II} \\ &= \cos(kx) \cos x - \sin(kx) + i[\cos(kx) \sin x + \sin(kx) \cos x] \\ &= \text{cis } (k+1) && \text{Various Trigonometric Identities} \end{aligned}$$

Therefore, the result is true for all positive integers n. If $n = 0$, the formula holds true because $\cos(0x) + i \sin(0x) = 1 + i0 = 1$. Since $z^0 = 1$, the equation holds true. If $n < 0$, one must consider $n = -m$ when m is a positive integer.

$$\begin{aligned} (\text{cis } x)^n &= (\text{cis } x)^{-m} \\ &= \frac{1}{(\text{cis } x)^m} \\ &= \frac{1}{\text{cis } (mx)} \\ &= \cos(mx) - i \sin(mx) && \because \text{rationalization of the denominator} \\ &= \text{cis } (-mx) \\ &= \text{cis } (nx) \end{aligned}$$

And thus, the formula proves true for all integral values of n. Note that from the functional equation $f(x)^n = f(nx)$ where $f(x) = \cos x + i \sin x$, we see that $f(x)$ behaves like an exponential function. Indeed, Euler's formula states that $e^{ix} = \cos x + i \sin x$. This extends De Moivre's theorem to all $n \in \mathbb{R}$.

Exponential Form of Complex Numbers

A complex number is a number of the form $a + bi$, where a and b are real numbers. Note that every point every (a, b) can be expressed as $(r \sin \theta, r \cos \theta)$.

Combinations and Permutations

Combinations and permutations are extremely important in competition mathematics. Many problems involve deep application of these tow formulas.

Combinations

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Where n is the total number of objects from which you are choosing k objects (order does matter).

Derivation

Consider the set of letters A, B, and C. There are 3! different permutations of those letters. Since order doesn't matter with combinations, there is only one combination of those three.($ABC, ACB, BAC, BCA, CAB, CBA$ are all equivalent in combination but different in permutation.)

In general, since for every permutation of r objects from n elements $P(n,r)$ which is $\frac{n!}{n-r!}$. Now since in permutation the order of arrangement matters(ABC is not same as ACB) but in combinations the order of arrangement does not matter(ABC is equivalent to ACB).For its derivation see this video.

Suppose r elements are selected out.For permutation r elements can be arranged in $r!$ ways. We have overcounted the number of combinations by $r!$ times.So We have $r!C(n,r) = P(n,r)$, or $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

Common Formulae and Identities

- $\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r}$

- $\binom{n}{r} = \frac{n}{r}\binom{n-1}{r-1}$
- $\sum_{x=0}^{n} \binom{n}{x} = 2^n$
- $\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}$
- $\binom{n}{r} = \binom{n}{n-r}$

<u>Permutations</u>

$${}_nP_k = \frac{n!}{(n-k)!}$$

Where n is the total number of objects from which you are choosing k objects (order does matter).

Derivation

Let us assume that there are r boxes and each of them can hold one thing. There will be as many permutations as there are ways of filling in r vacant boxes by n objects.

No. of ways first box can be filled: n

No. of ways second box can be filled: $(n-1)$

No. of ways third box can be filled: $(n-2)$

No. of ways fourth box can be filled: $(n-3)$

No. of ways r^{th} box can be filled: $(n-(r-1))$

Therefore, no. of ways of filling in r boxes in succession can be given by:

$n(n-1)(n-2)(n-3)...(n-(r-1))$

This can be written as:

$n(n-1)(n-2)...(n-r+1)$

The no. of permutations of n different objects taken r at a time, where $0 < r \leq n$ and the objects do not repeat is $n(n-1)(n-2)(n-3)...(n-r+1) \implies nPr = n(n-1)(n-2)(n-3)...(n-r+1)$

Multiplying numerator and denominator by $(n-r)(n-r-1)...3 \cdot 2 \cdot 1$, we get

$nP_r = \frac{[n(n-1)(n-2)(n-3)...(n-r+1)(n-r)(n-r-1)..3\times2\times1]}{(n-r)(n-r-1)..3\times2\times1} = \frac{n!}{(n-r)!}$

Hence,

$nP_r = \frac{n!}{(n-r)!}$

Where $0 < r \leq n$

Pascal's Identity

Pascal's Identity is a useful theorem of combinatorics dealing with combinations (also known as binomial coefficients). It can often be used to simplify complicated expressions involving binomial coefficients. Pascal's Identity is also known as Pascal's Rule, Pascal's Formula, and occasionally Pascal's Theorem.

Pascal's Identity states that:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

for any positive integers k and n. Here, $\binom{n}{k}$ is the binomial coefficient $\binom{n}{k} = nCk = C_k^n$. This result can be interpreted combinatorially as follows: the number of ways to choose k things from n things is equal to the number of ways to choose $k-1$ things from $n-1$ things added to the number of ways to choose k things from $n-1$ things.

Proof

If $k > n$ then $\binom{n}{k} = 0 = \binom{n-1}{k-1} + \binom{n-1}{k}$ and so the result is trivial. So assume $k \leq n$. Then:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} \\
&= (n-1)!\left(\frac{k}{k!(n-k)!} + \frac{n-k}{k!(n-k)!}\right) \\
&= (n-1)! \cdot \frac{n}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}.
\end{aligned}$$

Note

This provides a basis for Pascal's Triangle. Can you see why each number in Pascal's Triangle is a binomial coefficient?

A Useful Identity in Combinatorics

$$\binom{n}{m}\binom{m}{r} = \binom{n}{r}\binom{n-r}{m-r}$$

Proof

$$\begin{aligned}
\binom{n}{m}\binom{m}{r} \quad &= \quad \binom{n}{r}\binom{n-r}{m-r} \\
\implies \quad & \frac{n!}{m!(n-m)!}\frac{m!}{r!(m-r)!} = \frac{n!}{r!(n-r)!}\frac{(n-r)!}{(m-r)!((n-r)-(m-r))!} \\
\implies \quad & \frac{n!}{r!(n-m)!(m-r)!} = \frac{n!}{r!(n-m)!(m-r)!}
\end{aligned}$$

Binomial Theorem

The Binomial Theorem states that for real or complex a, b, and non-negative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is a binomial coefficient. In other words, the coefficients when $(a+b)^n$ is expanded and like terms are collected are the same as the entries in the nth row of Pascal's Triangle. For example, $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$, with coefficients $1 = \binom{5}{0}$, $5 = \binom{5}{1}$, $10 = \binom{5}{2}$, etc.

Proof

We can write $(a+b)^n = \underbrace{(a+b)\cdot(a+b)\cdot(a+b)\cdot\cdots\cdot(a+b)}_{n}$. Repeatedly using the distributive property, we see that for a term $a^m b^{n-m}$, we must choose m of the n terms to contribute an a to the term, and then each of the other $n-m$ terms of the product must contribute a b. Thus, the coefficient of $a^m b^{n-m}$ is the number of ways to choose m objects from a set of size n, or $\binom{n}{m}$. Extending this to all possible values of m from 0 to n, we see that $(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} \cdot a^m \cdot b^{n-m}$, as claimed. Similarly, the coefficients of $(x+y)^n$ will be the entries of the n^{th} row of Pascal's Triangle.

Generalizations

The Binomial Theorem was generalized by Isaac Newton, who used an infinite series to allow for complex exponents: For any real or complex a, b, and r,

$$(a+b)^r = \sum_{k=0}^{\infty} \binom{r}{k} a^{r-k} b^k$$

Pascal's Triangle

Pascal's triangle is a triangle which contains the values from the binomial expansion; its various properties play a large role in combinatorics.

Binomial Coefficients

Pascal's Triangle is defined such that the number in row n and column k is $\binom{n}{k}$. For this reason, convention holds that both row numbers and column numbers start with 0. Thus, the apex of the triangle is row 0, and the first number in each row is column 0. As an example, the number in row 4, column 2 is $\binom{4}{2} = 6$. Pascal's Triangle thus can serve as a "look-up table" for binomial expansion values. Also, many of the characteristics of Pascal's Triangle are derived from combinatorial identities; for example, because $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, the sum of the values on row n of Pascal's Triangle is 2^n.

Sum of Previous Values

One of the best known features of Pascal's Triangle is derived from the combinatorics identity $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$. Thus, any number in the interior of Pascal's Triangle will be the sum of the two numbers appearing above it. For example, $\binom{5}{1} + \binom{5}{2} = 5 + 10 = 15 = \binom{6}{2}$. This property allows the easy creation of the first few rows of Pascal's Triangle without having to calculate out each binomial expansion.

Fibonacci Numbers

The Fibonacci numbers appear in Pascal's Triangle along the "shallow diagonals." That is, $\binom{n}{0} + \binom{n-1}{1} + \cdots + \binom{n-\lfloor \frac{n}{2} \rfloor}{\lfloor \frac{n}{2} \rfloor} = F(n+1)$, where $F(n)$ is the Fibonacci sequence. For example,

$\binom{6}{0} + \binom{5}{1} + \binom{4}{2} + \binom{3}{3} = 1 + 5 + 6 + 1 = 13 = F(7)$. A "shallow diagonal" is plotted in the diagram.

Hockey-Stick Identity/Theorem

The Hockey-stick theorem states: $\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}$. Its name is due to the "hockey-stick" which appears when the numbers are plotted on Pascal's Triangle, as shown in the representation of the theorem below (where $n = 2$ and $k = 3$).

Number Parity

Consider writing the row number n in base two as $(n)_{10} = (a_x a_{x-1} \cdots a_1 a_0)_2 = a_x 2^x + a_{x-1} 2^{x-1} + \cdots + a_1 2^1 + a_0 2^0$. The number in the kth column of the nth row in Pascal's Triangle is odd if and only if k can be expressed as the sum of some $a_i 2^i$. For example, $(9)_{10} = (1001)_2 = 2^3 + 2^0$. Thus, the only 4 odd numbers in the 9th row will be in the $(0000)_2 = 0$th, $(0001)_2 = 2^0 = 1$st, $(1000)_2 = 2^3 = 8$th, and $(1001)_2 = 2^3 + 2^0 = 9$th columns. Additionally, marking each of these odd numbers in Pascal's Triangle creates a Sierpinski triangle.

Patterns and Properties of the Pascal's Triangle

The zeroth row has a sum of $1 = 2^0$. The first row has a sum of $2 = 2^1$. The n^{th} row has a sum of 2^n. The 1st downward diagonal is a row of 1's, the 2nd downward diagonal on each side consists of the natural numbers, the 3rd diagonal the triangular numbers, and the 4th the pyramidal numbers.

Fundamental Theorem of Counting

If one event has n possible outcomes and another event has possible outcomes, the total number of events if both events occur is $m \cdot n$. We can inductively prove this for multiple events.

Burnside's Lemma

Burnside's Lemma is a combinatorial result in group theory that is useful for counting the orbits of a set on which a group acts. The lemma was apparently first stated by Cauchy in 1845. Hence it is also called the Cauchy-Frobenius Lemma, or the lemma that is not Burnside's. The lemma was (mistakenly) attributed to Burnside because he quoted and proved in his 1897 book *Theory of groups of finite order* without attribution, apparently because he thought it was sufficiently well known.

Statement

Let G be a group acting on a set S. For $\alpha \in G$, let $\text{fix}(\alpha)$ denote the set of fixed points of α. Then:

$$|G| \cdot |S/G| = \sum_{\alpha \in G} |\text{fix}(\alpha)|.$$

Proof

The quantity $\sum_{\alpha \in G} |\text{fix}(\alpha)|$ enumerates the ordered pairs $(\alpha, x) \in G \times S$ for which $\alpha(x) = x$. Hence:

$$\sum_{\alpha \in G} |\text{fix}(\alpha)| = |\{(\alpha, x) \in G \times S | \alpha(x) = x\}| = \sum_{x \in S} |\text{stab}(x)| = \sum_{H \in S/G} \sum_{x \in H} |\text{stab}(x)|,$$

where stab(x) denotes the stabilizer of x. Without loss of generality, let G operate on S from the left. Now, if x, y are elements of the same orbit, and g is an element of G such that $g(x) = y$, then the mapping $\alpha \mapsto g\alpha g^{-1}$ is a bijection from stab(x) onto stab(y). It then follows from the orbit-stabilizer theorem that for any i in an orbit H of S,

$$\sum_{x\in H} |\mathrm{stab}(x)| = \sum_{x\in H} |\mathrm{stab}(i)| = |\mathrm{orb}(i)| \cdot |\mathrm{stab}(i)| = |G|.$$

Therefore

$$\sum_{\alpha\in G} |\mathrm{fix}(\alpha)| = \sum_{H\in S/G} \sum_{x\in H} |\mathrm{stab}(x)| = \sum_{H\in S/G} |G| = |G| \cdot |S/G|,$$

as desired.

Stars and Bars or Ball and Urn

The ball-and-urn technique, also known as stars-and-bars, is a commonly used technique in combinatorics. It is used to solve problems of the form: how many ways can one distribute k indistinguishable objects into n bins? We can imagine this as finding the number of ways to drop k balls into n urns, or equivalently to drop k balls amongst $n-1$ dividers. The number of ways to do such is $\binom{n+k-1}{k}$.

Reasoning

If you could only put one ball in each urn, then there would be $\binom{n}{k}$ possibilities; the problem is that you can repeat urns, so this does not work. You can, however, reframe the problem as so: imagine that you have the n urns (numbered 1 through n) and then you also have $k-1$ urns labeled "repeat 1st", "repeat 2nd", ..., "repeat $k-1$st". After the balls are in urns you can imagine that any balls in the "repeat" urns are moved on top of the correct balls in the first n urns, moving from left to right. There is a one-to-one correspondence between the non-repeating arrangements in these new urns and the repeats-allowed arrangements in the original urns. For a simple example, consider 4 balls and 5 urns. The one to one correspondence between several of the possibilities and the "repeated urns" version is shown. Since there are 4 balls, these examples will have three possible "repeat" urns. For simplicity, I am listing the numbers of the urns with balls in them, so "1,1,2,4" means 2 balls in urn 1, 1 in urn 2, and 1 in urn 4. The same is true for the "repeat" urns options but I use the notation r_1 etc.

- $1, 2, 3, 4 <-> 1, 2, 3, 4 (norepeats)$
- $1, 1, 2, 4 <-> 1, 2, 4, r_1$

- $1, 2, 2, 2 < - > 1, 2, r_2, r_3$
- $4, 4, 5, 5 < - > 4, 5, r_1, r_2$

Since the reframed version of the problem has n+k-1 urns, and k balls that can each only go in one urn, the number of possible scenarios is simply $\binom{n+k-1}{k}$

Expected Value

Given an event with a variety of different possible outcomes, the expected value is what one should expect to be the average outcome if the event were to be repeated many times. Note that this is not the same as the "most likely outcome."

Definition

More formally, we can define expected value as follows: if we have an event Z whose outcomes have a discrete probability distribution, the expected value $E(Z) = \sum_z P(z) \cdot z$ where the sum is over all outcomes z and $P(z)$ is the probability of that particular outcome. If the event Z has a continuous probability distribution, then $E(Z) = \int_z P(z) \cdot z \; dz$.

Lemma (Additivity)

If $Z_1, Z_2, ...Z_k$ are several events (independent or not), then:

$$E(Z_1 + Z_2 + ... + Z_k) = E(Z_1) + E(Z_2) + ... + E(Z_k)$$

Semi-Proof

We will prove the lemma if the events are independent. We will proceed by induction for the base case, we need to prove that we can sum two expected values. Also, we are assuming the events are finite. Suppose that X has m possible outcomes, which have probabilities $p_1, p_2, \dots, p_m$ and values $z_1, z_2, \dots, z_m$. This means that $p_1 + p_2 + \cdots + p_m = 1$ and that:

$$E(Z) = p_1 z_1 + p_2 z_2 + \cdots + p_m z_m = \textstyle\sum_{i=1}^m p_i z_i.$$

Similarly, suppose that Y has n possible outcomes, which have probabilities $q_1, q_2, \dots, q_n$ and values $y_1, y_2, \dots, y_n$. This means that $q_1 + q_2 + \cdots + q_n = 1$ and that:

$$E(Y) = q_1y_1 + q_2y_2 + \cdots + q_ny_n = \textstyle\sum_{j=1}^{n} q_jy_j.$$

Since Z and Y are independent events, we know that "$Z + Y$" has mn possible outcomes: value $z_i + y_j$ occurs with probability p_iq_j, for all $1 \leq i \leq m$ and $1 \leq j \leq n$. So:

$E(Z+Y) = p_1q_1(z_1+y_1)+p_1q_2(z_1+y_2)+\cdots+p_1q_n(z_1+y_n)+p_2q_1(z_2+y_1)+p_2q_2(z_2+y_2)+\cdots+$
$p_2q_n(z_2+y_n)+\ldots+p_mq_1(z_m+y_1)+p_mq_2(z_m+y_2)+\cdots+p_mq_n(z_m+y_n) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_iq_j(z_i+y_j).$

We can isolate the z terms in each row. For example, in the first row of the above equation for $E(Z + Y)$, we have:

$$p_1q_1x_1 + p_1q_2x_1 + \cdots + p_1q_nx_1 = p_1x_1(q_1 + \cdots + q_n) = p_1x_1,$$

since $q_1 + \cdots + q_n = 1$. Similarly, the z terms in the second row sum to p_2z_2, and so on. Thus all the z terms, summed over all rows, gives:

$$p_1x_1 + p_2x_2 + \cdots + p_mx_m = E(X).$$

We can also isolate the y terms, but this time by column. For example, in the first column of the above equation for $E(Z + Y)$, we have:

$$p_1q_1y_1 + p_2q_1y_1 + \cdots + p_mq_1y_1 = q_1y_1(p_1 + \cdots + p_m) = q_1y_1,$$

since $p_1 + \cdots + p_m = 1$. Similarly, the y terms in the second column sum to q_2y_2, and so on. Thus all the y terms, summed over all columns, gives:

$$q_1y_1 + q_2y_2 + \cdots + q_ny_n = E(Y).$$

This shows that $E(Z + Y) = E(Z) + E(Y)$. Now, we are essentially done. Note that we can prove $E(X + Y + Z) = E(X) + E(Y) + E(Z)$ by letting $X = Y + X$ and applying the formula for summing two values.

Example

n people's hats are randomly distributed onto n people's heads. A cycle is a minimal group of people who collectively have each other's hats. Find the expected number of cycles in terms of n.

Modular Arithmetic: An Introduction

Notations: First we say that two numbers: a and b are congruent in the same modulus m, if they both leave the same remainder when divided by m. Another way of thinking of this is to note that if a and b are congruent $(modm)$, $\mid a + b \mid$ must be divisible by m.

To denote modular congruence, we write: $a \equiv b(modm)$ or $amodm = bmodm$. Here, we say that a and b are modulands (b being the right moduland and a being the left moduland, though both modulands are interchangable [often termed the modular reflexivity principle]), whereas we say that m is the modulus. The remainder left when a moduland is divided by the modulus is called the modular residue, and two modulands that leave the same residue r in $(modm)$ are said to be in the residue class $r(modm)$. To notate that a leaves residue r in $(modm)$ we often write: $amodm = r$. For example: $5mod4 = 1$, and $100mod3 = 1$.

Modular arithmetic is a very powerful and valuable tool for quickly solving many challenging problems that appear on current AMC's. To complete your modular toolkit, I recommend you learn the following:

- Operations in modular arithmetic (particularly exponentiation and division [which does not work the normal way in the modular world])
- Converting from Modular to Parametric forms of an equation
- Solving linear modular congruences with subtraction and division, etc.
- Solving systems of linear modular congruences with the Chinese Remainder Theorem and Parametric Visualization
- Fermat-Euler Theorem for quick ways to extract the modular residue (and how to use this in union with the Chinese Remainder Theorem)

- Quadratic and higher order residues (these aren't needed for the AMC, and rarely helpful for the AIME and beyond)
- Divisibility Rules with Modular Arithmetic
- Units digit of a large exponent by looking $(mod 10)$, tens digit by looking $(mod 100)$, hundreds digit with $(mod 1000)$, and so on...

Lastly, let's look at some helpful mod forms: For questions involving the sum of the digits, look at $(mod 9)$ and $(mod 3)$. For questions involving the n^th digit from the right (where $n = 0$ gives the units digit, $n = 1$ gives the tens digit, and so on) in the decimal representation of a number, look (mod 10^{n+1})

Fermat-Euler Totient (Phi) Theorem for Modular Arithmetic

Given the general prime factorization of $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, one can compute $\phi(n)$ using the formula

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).$$

The above is Euler's Totient function, Euler's Totient theorem states that if $\phi(n)$ is Euler's totient function and n is a positive integer, $\phi(n)$ is the number of integers in the range $\{1, 2, 3 \cdots, n\}$ which are relatively prime to n. If a is an integer and m is a positive integer relatively prime to a,Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof

Consider the set of numbers $A = n_1, n_2, ...n_{\phi(m)} \pmod{m}$ such that the elements of the set are the numbers relatively prime to m. It will now be proved that this set is the same as the set $B = an_1, an_2, ...an_{\phi(m)} \pmod{m}$ where $(a, m) = 1$. All elements of B are relatively prime to m so if all elements of B are distinct, then B has the same elements as A. In other words, each element of B is congruent to one of A.This means that $n_1 n_2 ... n_{\phi(m)} \equiv an_1 \cdot an_2 ... an_{\phi(m)} \pmod{m} \implies a^{\phi(m)} \cdot (n_1 n_2 ... n_{\phi(m)}) \equiv n_1 n_2 ... n_{\phi(m)} \pmod{m} \implies a^{\phi(m)} \equiv 1 \pmod{m}$ as desired. Note that dividing by $n_1 n_2 ... n_{\phi(m)}$ is allowed since it is relatively prime to m.

Parametric Visualization

We, so far, have looked at how we can use CRT to quickly find the solutions to a system of linear equations. However, the Introduction to Number Theory book from AoPS provides another and sometimes quicker way to analyze such systems. To set the scene, we consider the following system of two linear modular congruences:

$$x \equiv 7(mod 11) \text{and} x \equiv 4(mod 5)$$

We can convert the system of equations into a much easier to manipulate parametric format, involving two parameters (which I'll call t and u).

$$x = 11t + 7 \text{and} x = 5u + 4$$

Now it may be a good idea to equate the two:

$$11t + 7 = 5u + 4$$

We can look at both sides $(mod 5)$ at this point, in hopes of eliminating the u and "solving" for t:

$$11t + 7 mod 5 = 5u + 4 mod 5 \implies t + 2 \equiv 4(mod 5) \implies t \equiv 2(mod 5)$$

We can now once again parametrically "visualize" this resulting congruence (this time using a different parameter, called v, for 'visualizer'):

$$t = 5v + 2$$

Plugging it back into the originally parameterized version of the congruence then gives:

$$x = 11t + 7 = 11(5v + 2) + 7 = 55v + 29 \implies x \equiv 29(mod 55)$$

When the Moduli Are Not Pairwise Coprime

What happens if the moduli aren't pairwise coprime? Can you still solve the system? Well...the simple answer is "sometimes". Let's now talk a little bit about exactly when. Usually, at least for the AMC, the system is solvable. You can think of what might happen though, if two modular statements contradict each other. For example, consider the simultaneous congruence of $1(mod 2)$ and $0(mod 4)$. Clearly this is impossible, since if a number is divisible by 4, it must also be divisible by 2. And modular reduction implies: $1(mod 2)$ and $0(mod 2)$. Clearly, this is absurd, and hence the system is impossible. However, what's important for the AMC is applying modular reduction to solvable systems and potentially yielding a system that is not only linear and solvable, but also one that has the property that the moduli are pairwise coprime. Let's consider another example. Consider simultaneous congruence to $10(mod 24)$ and $18(mod 64)$. $10(mod 24)$ breaks into $10(mod 3)$ and $10(mod 8)$. But $18(mod 64)$ is $64t + 18$, and looking at $(mod 8)$ implies $10(mod 8)$. Therefore, we have $10(mod 3)$ and $10(mod 64)$ and we can proceed using any desired method. The action of breaking down a modulus into its prime decomposition similar to the above, applying parametric visualization, and showing that one modular congruence implies another with a different modulus is called Modular Reduction. If modular reduction is successful it will yield a solvable system (similar to the second example), and if not successful, it will yield two statements that contradict each other (similar to the first example).

Solving Linear Congruences

All this talk of "linear" might lead you to think, what do you mean "linear"? Well, if you recall, in algebra, "linear" means that the degree of the variable being solved for is 1. But how does this even begin to make sense in the modular realm? How can we create a modular interpretation of what it means to isolate and solve for a variable? Well, let's try using our standard knowledge of modular operations to see how far we can go with this idea. Consider the congruence $3x + 54mod2 = 1mod2$. We will try to "solve" for x by isolating it as the left moduland of the congruence. We can quite conveniently eliminate the constant term of 54 by noticing that $54mod2 = 0$. This gives $3xmod2 = 1mod2$. However, note that $3mod2 = 1$! This means $3xmod2 = xmod2 = 1mod2$. Therefore, we have isolated x: $xmod2 = 1$. Let's consider something much messier, and as a result, closer to what you might encounter on the AMC's. $4x + 3 = 14mod21$. Subtracting 3 from both sides gives: $4x = 11mod21$. We now need to divide both sides by 4, so we try to make the right moduland a multiple of 4. To do this, we add 21's to 14 until we get something congruent to $0(mod4)$: $14mod21 = 35mod21 = 56mod21$, stop here. Therefore, our congruence becomes: $4x = 56mod21$. Note that division works normally here, since $gcd(4, 21) = 1$. Therefore, $x = 14mod21$. These sorts of linear congruences in the AMC will generally be presented in the form of a word problem, so practice translating the words given into modular congruences that can be solved by such techniques.

Calculus: An Introduction

I know you've heard of it and shuddered at the very thought of it before. But yes, I recommend you have a basic idea of Calculus. Why? Because it allows you to thoroughly analyze a function in many complex ways, and in contest math, often times that's all that's needed to solve a problem. For the AMC 10 and 12, MAA states discreetly that Calculus is not required, and it's not. So this section is completely supplementary and optional. Of course, this section is in NO WAY a substitute for your regular Calculus textbook, and all of the Calculus mentioned here will be single variable.

There are two basic operations in Calculus – integration (or taking the integral) and differentiation (taking the derivative) both of which are applied to a function $f(x)$. This means that we can use these two together in very clever ways to solve very complex problems. All you really need to think of them is like "magic tools" to crack a problem effectively. First, some notation: the derivative of a function $f(x)$ will be denoted as either $f'(x)$ or $\frac{d}{dx}f(x)$. For our intents and purposes, $f(x)$ will generally be a polynomial function (as are the types of functions that you typically have to analyze on the AMC). The derivative of a function tells you its "slope" or instantaneous rate of change at a certain point (which will be distinguished by its value, where the representation of a point with $x = x_0$ will be determined as $(x_0, f(x_0))$. The integral of a function tells you the area underneath the graphed curve of $f(x)$ but bounded by the x-axis and between lines $x = a$ and $x = b$ (allowing this area to be finite and calculable). The notation for integration is $\int_a^b f(x)dx$. To compute integrals and derivatives for polynomial functions, we have very-easy-to-remember formulas that I will present to you shortly. First, some more notation. Note that the derivative of a function is, indeed, another function, and to get an actual value out of it, you have to take the derivative at a very specific point, which like I also said before is determined by its x coordinate, where its y coordinate is already determined by the fact that it lies on the curve defined by $f(x)$. How we notate this is: $f'(x_0)$ or $\frac{d}{dx}f(x)\Big|_{x=x_0}$, and we will essentially just plug our x value into our derivative function to get the actual derivative at that point. Another slightly more ambiguous use of notation is when denoting the derivative of y. We clearly have no idea whether or not y is even a function of x, because if it's not, then the derivative will be . Therefore, it is important to say "the derivative of y with respect to x". This is notated as $\frac{dy}{dx}$. Keep in mind that we are trying to find the slope at a point, and normally this task requires two points. We can solve this by looking at two points that are "infinitesimally" close to each other. The notation $\frac{dy}{dx}$ makes it very clear that we are trying to take the ratio of the change in y coordinates over that of the x coordinates, but when this change becomes infinitesimal, we replace Δx with dx and do the same for y. These quantities, namely dx and dy are called differentials, and are infinitesimal (or very close to , but still not equal to) So in an essence, when we take the derivative of a function, we are giving meaning to the ratio . Anyway, enough with the notation and let's take a look at how to compute integrals and derivatives, once and for all! Let's look at derivatives first:

- Power Rule: $\frac{d}{dx}(x^n) = nx^{n-1}$(This rule holds for $n \leq 0$)
- Distributive Property: $\frac{d}{dx}(A(x) + B(x)) = \frac{d}{dx}(A(x)) + \frac{d}{dx}(B(x))$
- Scaling Property: $k\frac{d}{dx}(f(x)) = \frac{d}{dx}(kf(x))$, where k is constant
- Chain Rule: $\frac{dy}{dx} = \frac{dy}{du} \cdot \frac{du}{dx}$
- Evaluation Rule: The slope of $f(x)$ at any point $(x_0, f(x_0))$ is $f'(x_0)$
- Constant Derivative: $\frac{d}{dx}(k) = 0$ where k is a constant

These six properties, when mastered, will allow you to compute the derivative of any function that will show up on the AMC's, and in general in competition math. I won't be providing the proofs for these, as they go beyond the scope of this paper, but take my word for them. Next, let's look at some properties to compute integrals:

- Anti-derivative Property:

$$\int x^2 dx = \frac{x^{n+1}}{n+1} + C$$

  where C is any constant(this rule only works for $n \geq 0$).

- Anti-derivative Scaling Property:

$$k \int f(x)dx = \int kf(x)dx$$

- Anti-derivative Distributive Property:

$$\int (A(x) + B(x))dx = \int A(x)dx + \int B(x)dx$$

- Integral Evaluation Rule:

$$\int_a^b dx = [\int f(x)]_a^b = \int f(x)\Big|_{x=b} - \int f(x)\Big|_{x=a}$$

  (note that the C terms cancel out, as it must be the same for both anti-derivatives that are being subtracted)

An integral cannot be computed directly, and first the antiderivative of the function must be computed. Once that is done, the antiderivative can be plugged into the Integral Evaluation

Rule and the definite integral can be computed. (Note that similar to the Chain Rule for derivatives, there exists another method called substitution for integrals that is also recommended but significantly more advanced, and therefore it will be introduced later). Also, another rule concerning derivatives is called the Product Rule which is very easy to derive directly from the Chain Rule but has its own significance: $(ab)' = a'b + b'a$, where all derivatives are taken with respect to x. I will end this section by introducing one last important rule called the Fundamental Theorem of Calculus:

The Fundamental Theorem of Calculus: The antiderivative and derivative are functional inverses in Calculus. Therefore, if a derivative is taken, the antiderivative of the derivative will get you back the original function, and vice versa.