1 Introduction

Like every year when the AIME comes around, people begin to agonize over details: what should I guess on #15? Should I bring a granola bar or a water bottle? Will the USAMO cutoff be 211 or 211.5? Others more wisely decide to spend their time preparing for the impending doomsday, leading to the constant refrain of the AoPS forums: what should I do in the last [length of time] to prepare for AIME? Should I take my 45th practice test? Study Combinatorical Nullstellensatz? Read every prime numbered chapter in AoPS volume 2?

The purpose of this document is to provide an answer to the important question: what should I study to prepare for AIME? It is, of course, impossible to create a comprehensive list of every detail that might appear on an AIME, but I would personally be rather surprised if most of the concepts on the AIME test were not, at least in spirit, present on thi slisting. Please note that this document is not intended to *teach* all the concepts that may appear on the AIME - indeed, such an endeavor would require several volumes. Instead the intention is to provide two things: a starting point for additional study, and a reference that can be utilized to decide what to work on.

As per usual, the (mathematical) material has been split into the four major subjects: Algebra, Combinatorics, Number Theory, and Geometry. The tips and strategies suggested should not, however, be considered exclusive to the subject in which they appear; with many problems being interdisciplinary and the lines between subjects being blurred, a line in the Combinatorics section may well find greater use on a problem that is objectively categorized under Algebra. Within each subject, the material is intended to increase in difficulty, beginning with basic tips applicable to the opening problems and concluding with material that is advanced even for the end of the test. To more easily distinguish between the two, some of the later sections are marked with stars. They denote sections that, while well worth study, are likely to be impractical for the AIME exam and whose use will be limited to the last few problems.

Again, I wish to reiterate that this is intended as a starting point only. In some sections, the concept is given a brief explanation, done for one of three reasons: either because it is not feasible to understand the later results without first having a overview of the earlier ones, because examples illustrate the concept better than a description can, or because the current literature is lacking and further self-study may prove difficult without an appropriate background. Where they appear, however, they should not generally be considered sufficient to have learned the concept - such mastery comes from working on related problems and reading more detailed treatments.

I have also taken what seems to be a relatively unique approach - after detailing a concept, I have added a brief note detailing the motivations and the cues for its use. It is quite suprising to me that this approach has not found a great deal of use, as it seems that an overview of concepts is dramatically incomplete without an explanation of their functions. My hope is that this approach will catch on in future documents similar to this one.

Lastly, this work is still a rough draft - in "beta", so to speak - and I hope to improve it in the future. Specifically, one major short-term goal is to associate practice problems with the concepts and strategies laid out here, so that even if left unsolved, the reader might gain a better understanding of what problem cues suggest a certain methodology. It is also possible, if not likely, that this article contains errors - while I hope that such errors are limited to typographical ones, it is possible that some of the mathematics requires revision as well. If you notice any such mistakes, please let me know as soon as possible. Finally, if you have any suggestions for how to improve this document, including the addition of concepts currently left omitted, please let me know!

I hope that you find this useful, and wish you good luck on the upcoming AIME!

2 General

- Basic testing tips
  - Know your goal! If you know you're not going to be happy with anything lower than 15, you need to adjust your strategy to focus more on the later questions. If, like many others, your goal is to make USA(J)MO, then make sure you know what you're looking for going in. The USA(J)MO cutoffs are usually between 210 and 215, which means most of you will be coming in looking for an 8 to 10.
  - If that's you, you'll want to focus mainly on the first 10 problems. This is hardly a glamorous strategy, but if you can check over and over and over again to really make sure you've gotten the first 8-9 right, the rest is about picking off the easy ones in the last *half* of the test. Focusing on 1-10 and whichever of the last 5 you can do fairly quickly is probably your best bet towards olympiad qualification.
  - Some of you will be taking the AIME for the first or second time, with no olympiad dreams in mind. In that case you should be realistic about your expectations: while you certainly shouldn't ignore the back half of the test or be intimidated by the high question numbers, your main focus will be on problems 1-7. Adjust accordingly.
  - 3 hours may sound like a long time, but it's easy to let that time fly by while getting sucked into a wrong approach. Don't be afraid to abandon a problem if you're not making serious progress - take another look in half an hour or so, when you've cleared your head a bit and got yourself going again.
- Avoiding stupid mistakes
  - When I'm asked for AIME advice, my favorite thing to say is "make sure you get points for the problems you solve!". Once you figure out the solution to a problem, you've only won half the battle - you still have to make sure you see it through to the correct answer. A lot can happen between the correct flash of inspiration and the various computations that go into the final process, so make sure you stay alert throughout the whole process.
  - If you define auxiliary variables, scale a diagram up to avoid fractions, or anything else that might cause you to write down a number that isn't the final answer you meant, write a VERY LARGE note at the top of your paper detailing it. For example, if you write $k = n - 42$, write a rather large note to yourself to add 42 at the end. It may seem like you'll remember, but after the computation's done and you want to get to the next problem as soon as possible, it's very easy to make these kinds of errors.
  - Keep your work organized! 3 hours is plenty of time for you to come back and check your work, and it will be much easier to catch any mistakes you made if you can follow it. It's a good idea to keep work for a problem in its own self-contained box, if not its own page, and you might even want to outline your solution at the end for when you come back later.
  - Write out all nontrivial computations explicitly. Yes, everybody knows you can do $42 \cdot 16$ in your head, but when you get 684, it will be much easier to find your mistake if you've written $42 \cdot 16 = 420 + 42 \cdot 6 = 420 + 264 = 684$ than if you didn't write anything at all.
  - And, of course, READ THE PROBLEM CAREFULLY! Reading each problem **twice** before you do *any work on it* will help to cut down your reading errors significantly. It may also help you to circle key points of the problem, such as the final answer they're looking for or anything else that you think might confuse you later on (for example, if you see "compute m" on your first read-through, it will help you to circle it for when you've finished the problem and are panicing because $m+n$ is too big).
- Problem ordering
  - Every year, there's almost always at least one problem in the last 5 that actually turns out to be rather easy, and there's almost always a problem within the first 7 or so that actually turns out to be really difficult (or at least annoying). Don't be afraid to temporarily concede a problem just because it's placed early, and don't be afraid to take a crack at a harder problem you think can do just because it's a #13. In 2009 I scored a 5: problems 1, 2, 3, 4, and 13.
  - That said, you almost certainly want to be working on the problems in order - at least for the first half of the test. After you've finished 5-7 problems or so, then you can take a more detailed look around and see which problems you think you can do.
  - Keep in mind that the problems that *look* the hardest usually are more notational messes than actually hard, and the ones that seem the simplest are usually the most difficult to solve. This may sound paradoxical, but it actually makes quite a bit of sense - if you're given little information in a problem, it will seem very simply stated, but it will be difficult to work with.

3 Algebra

- General
  - Be explicit about assigning your variables. Writing a note to yourself at the beginning of your work such as "x=Bob's speed, t=time for Alice to finish first leg" may save you a headache later on.
  - When you have a word problem, the first thing to do is to convert it into equations - keeping the first point in mind!
  - Before diving into complicated algebra, take a minute or two to see if there's a simpler method. If you don't see one, feel free to bash away, but there's often a nice simplification you can make right away.
  - Keep looking for better methods throughout your algebra - it might take you a few steps to notice the key insight, and even if there isn't any key insight to be had, there are still often little tricks you can perform to make your life a bit easier.
- Solving equations
  - Watch out for extraneous solutions. If you're doing anything non-reversible, such as squaring, check your solutions at the end.
  - Also watch out for division by expressions that could possibly be 0. Usually you want to factor rather than divide - e.g. write $a^2 = ab$ as $a(a-b) = 0$ instead of dividing through by a.
  - Don't multiply out big constants until you have to; you're far more likely to recognize $\frac{3 \cdot 22 \cdot 53}{7 \cdot 11 \cdot 53}$ simplifies than you are to notice $\frac{3498}{4081}$ does.
- Useful factorizations
  - Difference of squares: $x^2 - y^2 = (x-y)(x+y)$
  - Square of sum (2-var): $x^2 \pm 2xy + y^2 = (x \pm y)^2$, 3-var: $x^2 + y^2 + z^2 + 2xy + 2yz + 2zx = (x+y+z)^2$
  - Sum of cubes: $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$, difference: $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$
  - Binomial Theorem: $(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + y^n$ - used often when expressions are "close" to $(x+y)^k$ (e.g. $x^3 + 3x^2 + 3x = 999$; find x)
- Substitutions:
  - Always consider swapping in different variables to make things easier; even auxilary variables like $y = x - 42$ can simplify your algebra a bit.
  - Use substitutions to clear out fractions or nasty radicals - work with integers whenever possible
  - If you get an equation in terms of, for example, $x+y$ and $x-y$, consider writing $x - y = n$, solving for $x + y$ in terms of n, and then expressing both x and y in terms of n - this essentially reduces the number of variables.
- Sequences/series: $a_1, a_2, a_3, \ldots, a_n$
  - Arithmetic: kth term $a_1 + (k-1)d$ where d is the common difference, sum $n \cdot \frac{a_1 + a_n}{2}$.
  - Tip: When working with arithmetic sequences, it's often better to write them as $\ldots, a-2r, a-r, a, a+r, a+2r, \ldots$ instead of $a, a+r, \ldots$.
  - Geometric: kth term $a_1 \cdot r^{k-1}$ where r is the common ratio, sum $\frac{a(1-r^n)}{1-r}$ (when $|r| < 1$ and $n \to \infty$, this becomes $\frac{a}{1-r}$).
  - General strategy for other series (e.g. arithmetico-geometric): Write the sum as S and multiply by the common ratio, e.g. $S = r + 2r^2 + 3r^3 + \ldots \implies rS = r^2 + 2r^3 + \ldots \implies S - rs = r + r^2 + r^3 + \ldots$, causing reduction to to a geometric series.
  - $0.\overline{a_1 a_2 \ldots a_n} = \frac{\overline{a_1 a_2 \ldots a_n}}{10^n - 1}$; e.g. $0.\overline{135} = \frac{135}{999} = \frac{5}{37}$
  - When given a sequence with a seemingly arbitrary rule (e.g. $a_n = a_{n-1} - a_{n-2}$), list out the first few terms to see if there's a pattern you can prove.

- Telescoping: If you can manage to write a sequence in a form similar to $a_n = b_n - b_{n-1}$ (for some sequence b_n) - for example, $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$ - try adding up the terms from a_1 to a_n for heavy cancellation:

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \ldots + \frac{1}{n(n-1)} = \frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \ldots + \frac{1}{n-1} - \frac{1}{n} = \frac{n-1}{n}$$

- A couple common series you should know:
  - $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$
  - $1 + 3 + 5 + \ldots + 2(n-1) = n^2$
  - $2 + 4 + 6 + \ldots + 2n = n(n+1)$
  - $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$
  - $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + 3 + \ldots + n)^2$.

- Rate problems: $d = rt$
  - Make sure all your units are the same! Keep everything in miles per hour, or units per minute, or whatever is convenient - but be consistent.
  - You can often make simplifying assumptions such as "assume the length of this track is 100m" or "assume I'm moving at 1 mph" - this can simplify things a lot.
  - If things get messy, consider changing the reference frame. For example, if two people are moving at speeds of 15 and 20 mph in the same direction, you can view this from the first person's perspective of "I'm not moving, and the other person is moving away at 5 mph".

- Polynomials: $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = a_n(x - r_1)(x - r_2)\ldots(x - r_n)$
  - Useful root tidbits: There are exactly n roots (up to multiplicity). As a collollary, if $P(x) = Q(x)$ for $n + 1$ different values of x, then $P(x) = Q(x)$ for *all* x. If the coefficients are real and $a + bi$ is a root, so is $a - bi$ (and the multiplicities are the same). If the coefficients are rational and $a + b\sqrt{c}$ is a root (for squarefree c), so is $a - b\sqrt{c}$ (and, again, multiplicities are the same). Corollary: any polynomial with odd degree has at least one real root.
  - Vieta's formulas: $r_1 + r_2 + \ldots + r_n = -\frac{a_{n-1}}{a_n}$, $r_1r_2 + r_1r_3 + \ldots + r_{n-1}r_n = \frac{a_{n-2}}{a_n}$, ..., $r_1r_2\ldots r_n = (-1)^n \cdot \frac{a_0}{a_n}$.
  - Factorization: Try easy roots, such as integers dividing a_0 or rationals $\frac{m}{n}$ with $m \mid a_0, n \mid a_n$ (Rational Root Theorem).
  - Transformations: $x^n P(\frac{1}{x})$ reverses the coefficients and has reciprocal roots. $P(x - c)$ has roots $r_1 + c, r_2 + c, \ldots$; $P(cx)$ has roots $\frac{r_1}{c}, \frac{r_2}{c}, \ldots$.
  - Symmetric polynomials: Consider dividing by $x^{\lfloor \frac{n}{2} \rfloor}$ and rewriting in terms of $y = x + \frac{1}{x}$ ($x^2 + \frac{1}{x^2} = y^2 - 2, x^3 + \frac{1}{x^3} = y(y^2 - 3)$, etc.)
  - You can *usually* assume the polynomial is monic ($a_n = 1$) and fix it later if necessary; makes life a bit easier

- Logarithms: $\log_a(b) = c \iff a^c = b$
  - From definition: $a^{\log_a(b)} = b$, $\log_a(b) = \log_{a^c}(b^c)$
  - Sum: $\log_a(b) + \log_a(c) = \log_a(bc)$, Difference: $\log_a(b) - \log_a(c) = \log_a\left(\frac{b}{c}\right)$; implies $\log_a(b^c) = c\log_a(b)$
  - Change-of-base: $\log_a(b) = \frac{\log_c(b)}{\log_c(a)}$ for *any* c
  - *Always* try to make logarithms have the same base. $\log_4 x + \log_8 y$ might not look like it simplifies, but writing it as $\log_{64} x^3 + \log_{64} y^2$ makes it more obvious (by the way, 64 is usually better than 2 here to be able to work with integer powers)

- Trigonometry
  - Know common trig values! Have $\cos\theta, \sin\theta$ memorized for $\frac{\pi}{6}, \frac{\pi}{4} \mid \theta$
  - Sum/difference: $\sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \sin\beta\cos\alpha, \cos(\alpha \pm \beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta, \tan(\alpha \pm \beta) = \frac{\tan\alpha \pm \tan\beta}{1 \mp \tan\alpha\tan\beta}$
  - Useful: $e^{i\theta} = \cos\theta + i\sin\theta$ - can use to rederive above ($e^{\alpha+\beta} = e^{\alpha} \cdot e^{\beta}$)
  - Sum-to-product: $\sin\alpha + \sin\beta = 2\sin\left(\frac{\alpha+\beta}{2}\right)\cos\left(\frac{\alpha-\beta}{2}\right)$ - derive using $\sin\left(\frac{\alpha+\beta}{2} + \frac{\alpha-\beta}{2}\right) + \sin\left(\frac{\alpha+\beta}{2} - \frac{\alpha-\beta}{2}\right)$ (analogous formulas for cos follow similarly)
  - Double-angle: $\sin(2\theta) = 2\sin\theta\cos\theta, \cos(2\theta) = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta$ (special case of sum/difference above)
  - Trig substitutions: Be on the lookout for conditions like $a^2 + b^2 = r^2$ - this usually suggests substituting $a = r\cos\theta, b = r\sin\theta$ (*especially* if $r = 1$). Similarly, sequences like $a_n = 2a_{n-1}^2 - 1$ or $a_{m+n} = \frac{a_m + a_n}{1 - a_m a_n}$ suggest representing a_1 as the appropriate trig function (cosine and tangent in these examples).
- Inequalities - $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ positive reals:
  - Trivial: $x^2 \geq 0$ for real x
  - QM-AM-GM-HM:

$$\sqrt{\frac{a_1^2 + a_2^2 + \ldots + a_n^2}{n}} \geq \frac{a_1 + a_2 + \ldots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n} \geq \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}}$$

  - More generally: Define $p_k = \sqrt[k]{\frac{a_1^k + a_2^k + \ldots + a_n^k}{n}}$ (with p_0 the geometric mean) - then $a \geq b \implies p_a \geq p_b$ (the above is equivalent to $p_2 \geq p_1 \geq p_0 \geq p_{-1}$)
    Equality occurs at $a_1 = a_2 = \ldots = a_n$
  - Cauchy-Schwartz:

$$(a_1^2 + a_2^2 + \ldots + a_n^2)(b_1^2 + b_2^2 + \ldots + b_n^2) \geq (a_1 b_1 + a_2 b_2 + \ldots + a_n b_n)^2$$

    Equality occurs at $\frac{a_1}{b_1} = \frac{a_2}{b_2} = \ldots = \frac{a_n}{b_n}$.
  - Rearrangement: Suppose $a_1 \geq a_2 \geq \ldots \geq a_n$ and $b_1 \geq b_2 \geq \ldots \geq b_n$, and ϕ is a permutation of the b_i. Then

$$a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \geq a_1 b_{\phi(1)} + a_2 b_{\phi(2)} + \ldots + a_n b_{\phi(n)} \geq a_1 b_n + a_2 b_{n-1} + \ldots + a_n b_1$$

    (In other words, choose greedily)
- Roots of unity: $r^n = 1$
  - Recall $e^{i\theta} = \cos\theta + i\sin\theta$ - important here
  - $r = e^{\frac{2n\pi i}{k}} = \cos\left(\frac{2n\pi}{k}\right) + i\sin\left(\frac{2n\pi}{k}\right)$ for $k = 1, 2, \ldots, n$.
  - $r^n - 1 \implies (r-1)(r^{n-1} + r^{n-2} + \ldots + 1) = 0 \implies r^{n-1} + r^{n-2} + \ldots + 1 = 0$, as long as $r \neq 1$. For example, if ω is a third root of unity, $\omega^2 + \omega + 1 = 0$.
  - Consider cos and sin as the real/imaginary parts (respectively) of a root of unity - this will help you find sums such as

$$\begin{aligned}\sum_{k=0^\circ}^{179^\circ} \cos(2k) &= \sum_{k=0^\circ}^{179^\circ} \mathrm{Re}\left(e^{\frac{k\pi i}{90}}\right) \\ &= \mathrm{Re}\left(\sum_{k=0^\circ}^{179^\circ} e^{\frac{k\pi i}{90}}\right)\end{aligned}$$

    which is now the real part of a geometric series equal to $\frac{1(1 - (e^{\frac{\pi i}{90}})^{180})}{1 - e^{\frac{\pi i}{90}}} = 0$.

- Functional equations (*)
  - Keep in mind that most functional equations are **identities**. In other words, you can plug in anything in the domain if it will help.
  - Common things to plug in: Zero, $x = y$, anything that results in cancelling an f(something) term (such as plugging in $(x, \frac{1}{x})$ in $f(x) + f(y) = (xy - 1)f(x)f(y)$).
  - Many functional equations you'll see are **cyclic**; i.e. the variables used cycle. For example, if you see $f(x) + f\left(\frac{2}{x}\right)$ or $f(x) + f(1 - x)$, you can also plug in $x \to \frac{2}{x}$ or $x \to 1 - x$ to get the same expression.
  - Some common strategies: Let $f(1) = c$ and try to describe the other values in terms of c; Plug in *another* f term (e.g. if $f(f(x)) = x^2$, plug in $f(f(f(x))) = f(x)^2 \implies f(x^2) = f(x)^2$); write $f(x) = xg(x)$ or similar - the point being to keep trying to reduce things by writing them in terms of other functions; reduce an equation to $f(x + y) = f(x) + f(y)$ which often implies $f(x) = cx$ for some constant c (the other solutions are not nice at all, and if this ever comes up on an AIME you can probably safely assume the linear solution).

4 Combinatorics

- General
  - Many early Combinatorics problems are about good bookkeeping: making sure you've accounted for all of the cases, that you've counted everyone the appropriate number of times, and so on. Be sure to work deliberately on these, and constantly be checking to make sure you've done so.
  - Combo is the biggest source of the "ugh, I was off by one" regrets that flood the forums immediately upon unlocking. Make sure this isn't you! Check the bounds in the problem, make notes of $<$ vs. $\leq$ and similar such things, and take a minute at the end of your solution to ask yourself if everything works out. Checking the extreme points (usually the smallest and/or largest solutions) can also go a long way towards avoiding this.
  - Don't forget cases where you "do nothing" - it is for this reason that $0! = 1$, and similarly why $a_0 = 1$ in many recursions rather than $a_0 = 0$.
- The basics
  - Generally, when you need to do things like "draw k marbles" or "form a committee", it's best to look at it like you're doing things *one at a time*. For example, instead of selecting 5 people to form a committee, look at the first person and think about what happens if he goes in the committee and what happens if he doesn't.
  - Don't forget about complimentary counting! It's often easier to count what you *don't* want and subtract it off from the total number of possibilities than to work constructively. For example, how many four-digit numbers don't contain a 1?
  - The principle of inclusion-exclusion (PIE) is powerful, but the important thing is to know what you're trying to do: PIE works because it counts every possbility exactly once with strategic counting and overcounting. Keeping track of how many times you're counting something will help you solve problems where PIE isn't directly applicable, e.g. "how many have *exactly* two of the three characteristics"?
- Changing perspective
  - In problems where we have to account for rotations and/or reflections, it's often simplest to **fix** one of the points - effectively looking at the entire situation from its perspective (if you're standing at a round table, and the whole room suddenly rotates, the situation looks exactly the same to you as before).
  - The same strategy of "fixing" points applies in other places as well - if you need to choose one of 9 numbers in a set, for example, and which one you choose doesn't make a difference, just abitrarily pick one and remember to multiply by 9 at the end.
  - Additionally, in problems where there's a lot going on - for example, the sum of all positive differences of two elements in some set - a good strategy is to focus on one particular element and see how its affected. For example, in the AIME problem below, focusing on what happens to each specific element quickly results in a solution.
  - Let $S = \{2^0, 2^1, \ldots, 2^{10}\}$. Consider all possible positive differences of pairs of elements in S. Let N be the sum of all those differences. Find the remainder when N is divided by 1000.
- Combinations/Permutations
  - There are $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ways to choose k members from a set of n objects, if we don't care about the order (formally: there are $\binom{n}{k}$ subsets of S, where $|S| = n$, of cardinality k. There are ${}_nP_k = \frac{n!}{(n-k)!}$ ways to choose the k members if order does matter. These are both 0 by convention if $n < k$.
  - Know basic binomial-coefficient rules: $\binom{n}{k} = \binom{n}{n-k}$ (choosing a subset is equivalent to choosing its complement), $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ (we can either put the first element in our subset or not), etc.

  - Know small common values of binomial coefficients; you should probably know the values of $\binom{n}{k}$ up through $\binom{10}{5}$ or so from experience by now.

- Symmetry
  - Always look to exploit symmetry! If you're looking for the probability of something, and its complement is the exact same scenario, you immediately know the answer is $\frac{1}{2}$ without any work.
  - Be careful for cases where there's equality however - depending on the problem, you may have to handle it different.
  - A simple example: Suppose you flip a coin 4 times. What is the probability that you get more heads than tails?
  - Solution: The probability of getting more heads than tails is symmetrically equal to the probability of getting more tails than heads... but the answer isn't immediately $\frac{1}{2}$ because we need to account for the case where the numbers of heads and tails are equal. That probability is $\frac{3}{8}$, so our answer is in fact $\frac{1-\frac{3}{8}}{2} = \frac{5}{16}$. Note that if there were an odd number of coins, the answer would indeed be exactly $\frac{1}{2}$.
  - Take also the classic: Alice flips $n+1$ coins and Bob flips n coins. What is the probability that Alice gets more heads than Bob? Well, consider the first coin Alice flips. If it's heads, she just needs to get at least as many heads as Bob gets, which has a $\frac{1+p}{2}$ chance of happening where p is the probability of them getting the same number of heads among their n coins. If it's instead tails, now she needs to get *more* heads than Bob, which has a $\frac{1-p}{2}$ chance of happening. The answer is then $\frac{1}{2}\left(\frac{1+p}{2} + \frac{1-p}{2}\right) = \frac{1}{2}$!

- Stars-and-bars or Balls-and-urns
  - If $a_1, a_2, \ldots, a_k$ are nonnegative integers satisfying $a_1 + a_2 + \ldots + a_k = n$, there are $\binom{n+k-1}{k-1}$ possible assignments of the a_i. If the a_i are necessarily positive integers, there are $\binom{n-1}{k-1}$ possible assignments.

    Proof: Consider n stars and $k-1$ bars being arranged - the number of stars between each bar (counting the start and end of the string as bars) determine one of the a_i. In the positive case, consider $n-k$ of the stars instead and add one in to each group after the assignment.
  - If instead $a_1 + a_2 + \ldots + a_k \leq n$, we can add another variable $a_{k+1} = n - a_1 - a_2 - \ldots - a_k$ to get $a_1 + a_2 + \ldots + a_{k+1} = n$, which has $\binom{n+k}{k}$ solutions. Incidentally, this proves the Hockey Stick identity.
  - Clever applications of this usually involve looking at the gaps between things we're placing down. For example, how many ways can we park two indistinguishable cars in a row of 12 parking spaces, if they both take up 3 spaces? We can look at the gaps between the start and the first car, the gap between the cars, and the gap between the last car and the end (each of which might be zero), which total 6 spaces - hence $a_1 + a_2 + a_3 = 6$ and there are $\binom{8}{2} = 28$ possible assignments.

- Binary
  - Be on the lookout for conversions to other bases, especially binary!
  - Whenever you see a lot of powers come up, whether explicitly or implied, consider looking at it in other bases.
  - Functions satisfying things such as $f(2x) = f(x)$ are prime candidates for a binary interpretation, especially if you see something like $f(2x+1) = f(x) + 1$ to go along with it.

- One famous example is "A function satisfies $f(0) = 0, f(2x) = f(x), f(2x+1) = f(x) + 1$ for all nonnegative x. What is the maximum possible value of x on the interval $[0, 2015]$? The solution here is that $f(x)$ is counting the number of 1s in xs binary representation, making the answer 10 (as 1023_2 has 10 1s).

- Invariants
  - Whenever you're generating a sequence, moving around a plane, or lopping off hydra heads, look for what *doesn't* change. For example, take the classic:
  - Heracles wishes to kill the 100-headed hydra. He can only slice off *exactly* 2, 4, or 10 heads with one blow, but the hydra will grow back 5, 1, and 4 heads in those respective cases. Can Heracles ever kill the hydra? The answer is no, because the number of heads always changes by a multiple of 3, meaning it will always have a positive number of heads.
  - Similarly, if a robot can move from the point (x, y) to the points $(x+7, y+2), (x+2, y+7), (x-5, x-10)$, or $(x-10, y-5)$, note that there are two important invariants: the sum $x+y$ remains constant modulo 3, and the difference $y-x$ remains constant modulo 5.

The rest of the combinatorics section gets pretty advanced - feel free to skip this material if you don't feel confident tackling the later 5 questions yet.

- "States"
  - This concept is a somewhat difficult one to verbalize, but is also one of the most important (encompassing both recursion and expected value). So pay attention!
  - The general idea is to view situations as "states", and actions as passing between them. This sounds vague, so we'll illustrate with a simple example:
  - Alice and Bob alternately flip a coin. The winner is the player who first flips heads. What is the probability Alice wins?

    The canonical way of solving this problem involves writing out an infinite geometric series, but this doesn't scale well to harder problems and is error-prone anyway. Instead we have a much better (and generalizable) method using the concept of states. Suppose p is the desired probability. There is a $\frac{1}{2}$ chance that Alice wins on her first turn, and a $\frac{1}{2}$ chance that *we pass to the state of it being Bob's turn.* From the state of Bob's turn, there is a probability of p that he wins - meaning there's a $1-p$ chance of Alice winning from this state.
  - As a result, we can write $p = \frac{1}{2}(1) + \frac{1}{2}(1-p) \implies p = \frac{2}{3}$.
  - The key is to account for all possible states, which was easy in this case as there were only two - it was Alice's turn, or it was Bob's turn - and to account for how we pass between those states. Let's see a slightly more difficult example:
  - Alice and Bob continuously roll a die. Alice wins when a sum of 12 appears, and Bob wins when two consecutive sums of 7 appear. What is the probability Alice wins?

    We enumerate the states beforehand: Either the previous roll was neither a 7 nor a 12 or the previous roll was a 7 (or, of course, the game is over). Denote the probability that Alice wins from these states to be p_0 and p_7 respectively. From the first state, we can either roll a 12 - immediately ending the game in Alice's favor, roll a 7 thus moving to the p_7 state, or roll something else - thus staying in the same state. As a result, we have the equation

    $$p_0 = \frac{1}{6}p_7 + \frac{1}{36}(1) + \frac{29}{36}p_0$$

    From the p_7 state, there's a $\frac{1}{6}$ chance that we roll a 7, thus ending the game in Bob's favor, a $\frac{1}{36}$ chance of rolling a 12, thus ending the game in Alice's favor, and a $\frac{29}{36}$ chance of rolling something else, thus bringing us back to p_0. As a result, we have

    $$p_7 = \frac{1}{6}(0) + \frac{1}{36}(1) + \frac{29}{36}p_0$$

    solving these equations gives us $p_0 = \frac{7}{13}$, which is what we want as the game starts from the p_0 position.

- Recursion
  - Recursion is a very special case of the "states" concept above, where we only care about passing to *smaller* states.
  - Tip-offs to use recursion: We're building something iteratively, such as a string; we're representing some number as a sum or product of others (e.g. writing n as the sum of powers of two); people are rearranging themselves in some manner; we're looking for some subset of a larger set with a certain property; etc.
  - These all boil down to the same thing: if we can remove a couple chairs/people/stairs/etc. and end up with essentially the same problem (just different numbers), the solution is almost certainly recursion.
  - If we have a linear recurrence $a_n = c_{n-1}a_{n-1} + c_{n-2}a_{n-2} + \ldots + c_0a_0$ where the c_i are constants (possibly zero), then we can find the roots $r_1, r_2, \ldots, r_k$ of $x^n - c_{n-1}x^{n-1} - \ldots - c_0 = 0$, and the general solution to the recurrance will be $b_1r_1^n + b_2r_2^n + \ldots + b_kr_k^n$ for some appropriate constants b_i (there are caveats with double roots, but they don't come up very often). For example, suppose we have $a_n = a_{n-1} + 2a_{n-2}$. Then the roots of $x^2 - x - 2 = 0$ are 2 and -1, so the general solution is $c_1 \cdot 2^n + c_2 \cdot (-1)^n$ for some constants c_1, c_2 (we'd need to know some values of a_i, such as a_0 and a_1, to determine them).
  - Don't be shy about using multiple co-dependent recurrances. It can be easier to work with things such as $a_n = a_{n-1}+b_{n-1}, b_n = b_{n-1}+c_{n-1}, c_n = a_{n-1}+c_{n-1}$ than whatever single-variable recurrance this solves to.
  - For example, how many sequences of As and Bs have the property that every run of As has even length and every row of Bs has odd length? Well, let A_n denote the number of such sequences that begin with A and denote B_n similarly; then $A_n = A_{n-2} + B_{n-2}$ and $B_n = A_{n-1} + B_{n-2}$. Note that we can "reduce" this to $F(n) = 2F(n-2) + F(n-3) - F(n-4)$ were we so inclined, but this is unlikely to be particularly helpful (since the characteric polynomial is a mess).
  - If you're working with a circle (which has become very common lately), break it into a line first by considering one specific chair/person/etc. and work from there - lines are much nicer to work with than circles!
- Expected value
  - This is the more interesting version of the states concept, and can be thought of as a generalized recursion.
  - The trick here is exactly the same as how we handled the "states" problems: focus on the possible states and how we pass through them. Instead of the base cases being probabilities though, now they're expected values.
  - An illustrative example: What is the expected number of flips before we flip two consecutive heads? There are only two states here: we just flipped a tail, or we just flipped a head (of course, there is the usual state of "game over"). Call the expected number of flips from the tail state E_T, and the expected number of flips from the head state E_H. We then have the following relationships (make sure you see why):
$$E_T = \frac{1}{2}(E_T + 1) + \frac{1}{2}(E_H + 1)$$
$$E_H = \frac{1}{2}(E_T + 1) + \frac{1}{2}(1)$$
    which solves to $E_T = 6$, our answer as the starting position is equivalent to E_T.
- Roots of unity filter (*)
  - Given a polynomial $P(x)$, the sum of the coefficients to the terms with degree divisible by k is given by
$$\frac{1}{k}\left(P(\omega^0) + P(\omega^1) + \ldots + P(\omega)^{k-1}\right)$$
    where ω denotes a primitive kth root of unity.
  - The above may look scary, but the principle isn't actually that complicated. How would we, for example, find the sum of the coefficients to the terms with even degree? The method for that is well-known: we want $\frac{P(1) + P(-1)}{2}$, as all the terms with odd degree cancel out in the sum. The general method takes advantage of the fact that $1 + \omega + \omega^2 + \ldots + \omega^{k-1} = 0$ *unless* $\omega = 1$, which occurs precisely when the term has degree divisible by k!

- One application: find $\binom{2013}{0} + \binom{2013}{3} + \ldots + \binom{2013}{2013}$.

  Solution: Let $P(x) = (x+1)^{2013}$. Then

$$\frac{1}{3}(P(1) + P(\omega) + P(\omega^2)) = \frac{2^{2013} + (\omega+1)^{2013} + (\omega^2+1)^{2013}}{3}$$
$$= \frac{2^{2013} + (-\omega^2)^{2013} + (-\omega)^{2013}}{3}$$
$$= \frac{2^{2013} - \omega - \omega^2}{3} = \frac{2^{2013}+1}{3}$$

  where we used $\omega^2 + \omega + 1 = 0, \omega^3 = 1$.

- Generating functions (*)
  - Generating functions are about modeling situations with polynomials. For obvious reasons, we often combine this with the roots of unity filter above.
  - Generating functions are most useful when we're moving about, by which we literally mean moving about. For example, we can model walking on a number line with a generating function, as well as around a polygon, a circle, and so on. We can also, with a bit of creativity, extend this concept to things like rolling dice, building numbers (such as partitions), and so on. In fact, this is quite similar to the "states" concept as well.
  - Let's take an illustrative example - a rather famous one, in fact. Suppose we want to travel from $(0,0)$ to (m,n) using a sequence of moves, each of which are either one unit up or one unit to the right. In how many ways is this possible? Well, let's look at one particular move: we can either increase our x coordinate or increase our y coordinate - this is equivalent to multiplying by $x+y$! If we do this $m+n$ times, we can model the situation with the generating function $(x+y)^{m+n}$.
  - The coefficient of the $x^a y^b$ term is thus the number of paths to get from $(0,0)$ to (a,b); this makes our answer $\binom{m+n}{m}$ by the Binomial Theorem.
  - The key here is that, when two moves are modeled by generating functions $G_1(x), G_2(x)$, we can model the two steps with $G_1(x)G_2(x)$.
  - For example, one roll of a die can be modeled by the function $x^1 + x^2 + x^3 + x^4 + x^5 + x^6$, one random move on a number line can be modeled by the function $x^1 + x^{-1}$, one random diagonal move on a plane by $x + \frac{1}{x} + y + \frac{1}{y}$, and so on.

5 Number Theory

- General
  - Like in Algebra, the first step is usually to convert a word problem into equations. But here, it's even more important to choose your variables wisely: do we want to let x be an odd integer, or write it as $2k+1$? The choices here are less clear and largely depend on the problem, but make sure you're at least conscious of your options.
  - Remember that you're dealing with **integers**. If there's any possibility that your variables aren't integers, it probably isn't actually a number theory problem. This is a blessing!
  - One of the most basic things you can do is look at **parity** (odd or even). It's usually easy to do, and it can often reveal a lot about a problem!
- Divisibility rules
  - Know the basics: a number is a multiple of 2 iff its last digit is, a multiple of 3 or 9 if the sum of its digits is, a multiple of 4 if its last two digits is, a multiple of 5 if its last digit is, and a multiple of 11 if the alternating sum of its digits is.
  - Keep in mind that both sides of an equality must be divisible by the same numbers. This sounds obvious, but if you have something like $3b^3 = 2a^2$, it means that a must be a multiple of 3 and b must be a multiple of 2 (and, repeating this process, a a multiple of 18 and b a multiple of 6).
  - When looking for divisibility, try breaking up your number into smaller, relatively prime parts. For example, divisibility by 10 is the same thing as divisibility by 2 and 5; similarly, divisibility by 1001 is equivalent to divisibility by 7, 11, and 13.
  - A note of warning in the above: Don't make the mistake of saying $a \mid n, b \mid n \implies ab \mid n$ - this only holds when a, b are relatively prime!
- Prime factorization
  - In a lot of cases, the first thing you want to do is to consider the prime factorizations of numbers.
  - We can interpret multiples and divisors more easily in terms of prime factorization: b is a multiple of a (and a a divisor of b) if, for every prime p dividing a, the exponent of p in b is at least the exponent of p in a. For example, $2^{88} \cdot 5^{92}$ is a multiple of $10^{88} = 2^{88} \cdot 5^{88}$, but $2^{99} \cdot 5^{87}$ is not.
  - It's also much easier to notice cancellations when working with prime factors - you'll notice 17 should be canceled out in $2 \cdot 13 \cdot 17n = 11 \cdot 17 \cdot 23m$ easily, but not so much in $442n = 4301m$.
  - A basic but effective method of prime factorizing numbers: start with 2, and divide your number by 2 as many times as you can (possibly not at all). Move on to 3, then 5, then 7, and so on. You can stop when the number you're trying to divide by is more than the square root of the number you're trying to divide, because otherwise you would have already found your answer.
  - For example, prime factorizing 22176 might seem difficult, but let's go through our method: $22176 = 2 \cdot 11088 = 2^2 \cdot 5544 = 2^3 \cdot 2772 = 2^4 \cdot 1386 = 2^5 \cdot 693$ - now we move on to 3 - $= 2^5 \cdot 3 \cdot 231 = 2^5 \cdot 3^2 \cdot 77$ - now to 5, which doesn't work, so on to 7 - $= 2^5 \cdot 3^2 \cdot 7 \cdot 11$ - and we're done (you might have noticed the factor of 11 much earlier, such as at 11088).
- Difference of squares, completing the square, and SFFT
  - One of the simplest ways to solve Diophantines (equations with integer solutions) is to write a product of numbers equal to a constant, allowing us to analyze its factors. For example, if $ab = 80$, we know that a must be a factor of 80.
  - One common usage of this is difference of squares. If we know two squares differ by 80, we can write $a^2 = b^2 + 80 \implies a^2 - b^2 = 80 \implies (a-b)(a+b) = 80$. Additionally, we might as well assume b is positive, so $a - b < a + b$. This means we only have a few factor pairs to check, which we can reduce even further since $a - b, a + b$ are of the same parity. Hence we'd only need to check $(2, 40), (4, 20), (8, 10)$, leading to the solutions $9^2 = 1^2 + 80, 12^2 = 8^2 + 80, 21^2 = 19^2 + 80$.
  - Oftentimes this isn't written out so plainly for us: in those cases we complete the square instead. For example, if $a^2 + 84a + 2008 = b^2$, we have $(a+42)^2 + 254 = b^2$, so letting $c = a + 42$ we have $(b-c)(b+c) = 244 \implies b - c = 2, b + c = 122 \implies b = 62, a = 16$.
  - In some cases, instead of completing the square, we complete the *rectangle* - better known as Simon's Favorite Favoring Trick (SFFT). When we have an equation such as $xy + 6x + 6y = 0$, we can write this as $xy + 6x + 6y + 36 = 0 \implies (x+6)(y+6) = 36$, leading to the various solutions. These often arise as a result of equations like $\frac{1}{x} + \frac{1}{y} = 4$.

- Modular arithmetic: $a \equiv b \pmod{m} \iff m \mid a - b$. We'll denote by $a \pmod{m}$ the unique $b \in \{0, 1, 2, \ldots, m-1\}$ such that $a \equiv b \pmod{m}$; i.e. the remainder upon dividing a by m extended to negative a.
  - Know basic modular rules: if $a_1 \equiv b_1 \pmod{c}$ and $a_2 \equiv b_2 \pmod{c}$, then $a_1 + a_2 \equiv b_1 + b_2 \pmod{c}$, $a_1 a_2 \equiv b_1 b_2 \pmod{c}$, etc.
  - Corollary: $a^n \equiv (a \pmod{m})^n \pmod{m}$.
  - You can use modular arithmetic to reduce your search space when solving Diophantines. For example, if you want the number of [positive integer] solutions to $2a + 5b = 2013$, you know $2a \equiv 3 \pmod{5}$, so $a \equiv 4 \pmod{5}$ (and $a < 1006$), meaning there are 201 solutions (alternatively, b must be odd leading to the same result).
  - Chinese Remainder Theorem (CRT): Given a set of linear congruences $x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_n \pmod{m_n}$, there either exists no solution (due to contradictory things such as $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{4}$) or there exists a *unique* r such that $x \equiv r \pmod{M}$, where M is the least common multiple of $m_1, m_2, \ldots, m_n$.
  - Power residues: There are only so many possible residues that can be expressed as a square in some modulus - for example, there is no n for which $n^2 \equiv 2 \pmod{3}$. In a modulus m, we only need to check $1^2, 2^2, \ldots, (m-1)^2$ (0, of course, is always a residue) - and, in fact, since $1 \equiv -(m-1) \pmod{m}$, we only need to check half of these.
  - Some excellent moduli to work with when analyzing Diophantines involving squares are 3 and 4 - in both these moduli, the only quadratic residues are 0 and 1. This immediately tells us, for example, that $x^2 - y^2 \equiv 2 \pmod{4}$ has no solutions. 8 is also an excellent modulus to use, particularly because all odd squares are $1 \pmod{4}$. For cubes, checking modulo 9 is usually a good start, since the only cubic residues are $-1, 0, 1$.
- Working with squares and other powers
  - Suppose ab is a square. Then there exists some k, x, y so that $a = kx^2, b = ky^2$. In other words, if a and b are relatively prime, they must both be squares (otherwise write out their gcd and then apply this result).
  - Similarly, if pab is a square (for some prime p) and a, b are relatively prime, either $a = px^2, b = y^2$ or vice versa.
  - This is useful for many reasons. For example, if we know $3(a^2 - 80)(a^2 + 80)$ is a square where a is odd, then we know one of $a^2 - 80, a^2 + 80$ has to be thrice a perfect square and the other a perfect square itself. But $a^2 - 80 \equiv a^2 + 1 \pmod{3}$ can't be a multiple of 3, so $a^2 - 80$ is the perfect square - allowing us to write $(a-k)(a+k) = 80$ and find solutions that way.
  - Of course, though we mainly focus on squares, all this applies to other powers as well - if ab is a perfect cube and a, b are relatively prime, both a and b must themselves be cubes, and so on.
- Bounding
  - Bounding gets a well-deserved bad reputation, but it can be a very useful tool when properly used. One common usage is to bound some expression between two consecutive squares, thus showing it cannot itself be a perfect square. For example, $n^2 < n^2 + n < n^2 + 2n + 1 = (n+1)^2$ (for positive n), so $n^2 + n$ is never a perfect square.
  - Similarly, $n^2 < n^2 + n + 8 < n^2 + 2n + 1$ for $n > 7$ (and n positive), so we only need to check $n \leq 7$ when finding whether $n^2 + n + 8$ is a perfect square. In fact, for $n = 7$, we have $n^2 + n + 8 = 64 = 8^2$, so $n^2 + n + 8$ is a perfect square only when $n = 7$.
  - On the AIME, we can also use it to reduce our search space when bashing - keep in mind that the answer is at most three digits! This means that, for example, if we want the largest n such that $2n + 79$ is a perfect square and n can be expressed as a difference of consecutive cubes, we "only" need to check the perfect squares from 9^2 to 45^2. If we couple this with some number theoretic observations, such as $n = 3a^2 + 3a + 1 \implies n \equiv 1 \pmod{3} \implies 3 \mid 2n + 79$, we can reduce this to only check perfect squares that are multiples of 3 - only about 12 numbers to check! This still is hardly a pretty method, but it can earn you points.
- Euclidean Algorithm and Phi: Denote by (a, b) the greatest common divisor of a and b - i.e. the largest d such that $d \mid a, d \mid b$.
  - The Euclidean Algorithm: We will find (a, b). If $a = 0$ or $b = 0$, then the GCD is the nonzero one, and stop. Otherwise $(a, b) = (a, b - a) = (a - b, b)$ (depending on which of a, b is greater).

Repeating this gives us $(a,b) = (a \pmod b, b) = (a, b \pmod a)$. Repeat until termination. For example, $(16,56) = (16, 56 \pmod{16}) = (16,8) = (16 \pmod 8, 8) = (0,8) \implies (16,56) = 8$. If $(a,b) = 1$, we say a, b are **relatively prime**.

- How many $a < n$ are there for which $(a,n) = 1$? We go about this using a counting strategy: PIE. Suppose p divides n - then $a = p, 2p, \ldots$ don't satisfy $(a,n) = 1$. There are $\frac{n}{p} - 1$ of those. Similarly, we can do this for all the primes, and account for our overcounting using PIE.
- The phi function: if $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, we have $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$. For example, $\phi(1000) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$.
- Example: For how many $0 < n < 500$ is $\frac{n}{1000-n}$ in lowest terms? Solution: We need $(n, 1000-n) = 1$, which by the Euclidean algorithm is equivalent to $(n, 1000) = 1$. There are $\phi(1000) = 400$ such n less than 1000, exactly half of which are less than 500 (because if k works, so does $1000 - k$), making our answer 200.

- Fermat, Euler, and order
  - Fermat's Little Theorem (FLT): $a^p \equiv a \pmod p$, where p is a prime. If $p \nmid a$, this can be rewritten as $a^{p-1} \equiv 1 \pmod p$. For example, $2^{36} \equiv 1 \pmod{37}$.
  - Euler's Theorem: $a^{\phi(n)} \equiv 1 \pmod n$ if a and n are relatively prime. Note that this is a generalization of the above.
  - When using Euler's, first try splitting up n into its prime components. For example, it's usually better to look at $a^k \pmod 8$ and $a^k \pmod{125}$ than directly looking at $a^k \pmod{1000}$. We can then back-construct the remainder modulo 1000 (guaranteed by CRT), and this also has the advantage of being able to look at even a (normally impossible as $(a, 1000) \neq 1$).
  - The *order* of a modulo n, $\text{ord}_a(n)$, is the smallest positive k so that $a^k \equiv 1 \pmod n$ - again, this only makes sense when $(a,n) = 1$. Important: if $a^x \equiv 1 \pmod n$, then $\text{ord}_a(n) \mid x$. For example, $\text{ord}_a(p) \mid p - 1$. Unfortunately, there's no easy way to find the order - we have to start checking divisors of $\phi(n)$ to see if there is a smaller order.

- Inverses and "Fractions"
  - Given a modulus m and a nonzero residue a, we denote by a^{-1} the residue such that $aa^{-1} \equiv 1 \pmod m$. Obviously, this doesn't always exist - there's only one when $(a,m) = 1$. Most often, we only work with inverses with prime moduli, which are guaranteed to have inverses.
  - In a modulus p: $a + b \equiv ab(a^{-1} + b^{-1}) \pmod p \implies ab^{-1}(a+b) \equiv a^{-1} + b^{-1} \pmod p$; this essentially means we can pretend we're working with fractions: $\frac{1}{a} + \frac{1}{b} = \frac{a+b}{ab} \pmod p$.
  - Example: Let p be a prime greater than 5. Show that there exists an n with $p \mid 20^n + 15^n - 12^n$. Solution: We have $20^{p-1} \equiv 15^{p-1} \equiv 12^{p-1} \equiv 1 \pmod p$, so $20^{p-3} + 15^{p-3} - 12^{p-3} \equiv \frac{1}{20^2} + \frac{1}{15^2} - \frac{1}{12^2} \equiv 0 \pmod p$, so $n = p - 3$ works.
  - Make sure you see why we could abuse notation a bit above - $\frac{1}{20^2}$ is really the same as $(20^{-1})^2$.

- Lifting the Exponent (*)
  - First, a definition: the p-adic valuation $v_p(n)$ is the highest power of p dividing n. For example, $v_3(54) = 3$ as $3^3 \mid 54$, but $3^4 \nmid 54$. One obvious property: $v_p(ab) = v_p(a) + v_p(b)$
  - Now the theorem: Suppose p is an odd prime dividing $a - b$ but neither a nor b. Then $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$. The proof of this isn't too complicated at all, but this is a very useful result.
  - For example, suppose N is a number consisting of 2015 9s. What is the largest power of 3 dividing N? Solution: $v_3(10^{2015} - 1) = v_3(2015) + v_3(9) = 0 + 2 = 2$. Rather straightforward!
  - Suppose $a_1 = 2011$ and $a_n = 2012^{a_{n-1}} - 1$ for all $n > 1$. What is the largest power of 2011 dividing a_{2012}? Solution: We have $v_{2011}(a_n) = v_{2011}(2012^{a_{n-1}} - 1) = v_{2011}(2012 - 1) + v_{2011}(a_{n-1}) = 1 + v_{2011}(a_{n-1})$. As a result, since $v_{2011}(a_1) = 1$, we have $v_{2011}(a_{2012}) = 2012$.
  - A warning: Do not try to blindly apply this without first checking that $p \mid a - b$ and $p \nmid a, b$. It is very easy to fall into this trap and be completely wrong - make sure you understand why saying $v_3(2^{2014} - 1) = v_3(2-1) + v_3(2014) = 0$ is not valid (and see if you can figure out how to fix it).

- A second warning: Be very careful about applying this theorem to $p = 2$! If $4 \mid a - b$ then the theorem works as expected, but otherwise we have to introduce a second version: $v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1$. Of course, a, b are still odd since $p \nmid a, b$.

- Zsigmondy's theorem (*)
  - Another useful result about $a^n - b^n$: there (usually) exists some p dividing $a^n - b^n$ that does not divide $a^k - b^k$ for any $1 \leq k \leq n - 1$.
  - This doesn't seem particularly helpful, but it allows us to easily murder some Diophantines: specifically those in the form $a^n - b^n = p_1^{e_1} p_2^{e_2} \ldots$ where the p_i are fixed. This is because once we find any small solutions that use up all the primes, we immediately know there are no higher solutions! For example, take $5^k - 1 = 2^a$. Clearly, $k = 1$ is a solution. Suppose there were a bigger one, x. Then there would be some prime p dividing $5^x - 1$ but not $5^k - 1$, impossible as the only prime dividing $5^x - 1$ would be 2.
  - Similarly, cases like $2^a - 1 = 3 \cdot 5^b$ are trivialized: $a = 4$ is a solution for which $3, 5 \mid 2^a - 1$, as a result there are no higher solutions.
  - There a couple of exceptions to be careful of: if $a = 2$ and $b = 1$ (so we're working with $2^n - 1$), we have to manually check $n = 6$ as $2^6 - 1 = 63$ and $3 \mid 2^2 - 1, 7 \mid 2^3 - 1$. Additionally, if $a + b$ is a power of two and $n = 2$, we'd have $a^2 - b^2 = (a - b)(a + b)$ which fails as $a + b$ is a power of two (so no new prime) and $a - b$ is the only other smaller n, so no new primes from that factor either. Fortunately, these are usually both pretty trivial exceptions, and as long as we don't forget them we can apply this rather overpowered result.

6 Geometry

- General
  - It's a geometry problem - why haven't you drawn a diagram yet?
  - Choose your diagram wisely: drawing things that are too close to special cases (e.g. drawing a triangle that's very close to right, or one that's very close to isosceles) might cause you to spend time trying to prove things that aren't true - or, more disasterously, accidentally assuming something is true when it really isn't!
  - When you see a relationship you think might be true, such as two lines being perpendicular or two similar triangles, a good test is to draw a completely different diagram and see if it still looks true. If you can reproduce the same result with more than one different diagram, the chances of it being true go up significantly.
  - Don't just sit and stare! The solution isn't going to pop up magically. Assign variables to angles or lengths, draw auxiliary lines, draw another diagram and see what sticks, even jump into using coordinates - but the worst thing you can do is sit around for fifteen minutes waiting for a flash of inspiration. Yes, you sometimes need to just look and analyze your diagram, but if you've been doing that for more than 3 minutes or so it's time to try something new.
  - These next two are true for all problems, but especially for Geometry: if you're stuck, look back at the problem and ask yourself what information you haven't used yet?
  - Don't be afraid to work backwards! If you see something you can't quite figure out how to prove, start with what you'd like to be true and see if you can work backwards to what you know.
- Parallel lines and angles - suppose the line AB is parallel to the line CD, and E, F lie on AB, CD respectively.
  - Know the basics: $\angle AEF = \angle DFE$ and $\angle BEF = \angle CFE$.
  - There are 180° in a straight angle (i.e. a line), and by the above this is also the sum of the angles in a triangle.
  - Vertical angles are equal - if AB and CD intersect at E, we have $\angle AEC = \angle BED$ and $\angle AED = \angle BEC$.
- Similarity and Congruency
  - Two triangles are similar if they share the same angles; since the sum of the angles in a triangle is constant, it suffices to find two equal angle pairs. Equivalent, two triangles ABC and DEF are similar if $\frac{AB}{DE} = \frac{BC}{EF} = \frac{CA}{FD}$; determining similarity by either condition lets you conclude the other.
  - Two triangles are congruent by SSS (their sides have the same length), SAS (two sides and the angle they form are equal), or AAS (two angles and some side are equal). Note that SSA (two sides and an a different angle) could specify one of two different triangles.
  - Parallel lines almost always result in some similar triangles - be on the lookout for them. In fact, similar triangles are so useful that we often draw in parallel lines specifically to create them.
  - Also be on the lookout for right angles - they make it much easier to find similar triangles.
- Area/Perimeter and Volume/Surface area formulas
  - The area of a rectangle is ℓw, and its perimeter is $2(\ell + w)$. A special case is the square, which has area s^2 and perimeter $4s$.
  - The area of a parallelogram is bh, the area of a trapezoid is $\frac{h(b_1 + b_2)}{2}$, and the area of a rhombus is $\frac{d_1 d_2}{2}$.
  - The area of a circle is πr^2, and its circumference is $2\pi r$. The area of an ellipse is πab (the perimeter is not usually reasonable) where a, b are the length of the axes - note that a circle is a special case where $a = b = r$.
  - The volume of a sphere is $\frac{4}{3}\pi r^3$, and its surface area is $4\pi r^2$.
  - The volume of a cone or pyramid is $\frac{bh}{3}$, where b denotes the area of its base. The surface area of a cone is $\pi rs + \pi r^2$ where s is the slant height - the important point to rederive this is that the circumerence of the lateral surface area if $2\pi r$, because it's also the circumference of the base. The area of a cylinder or prism is bh. The surface area of a cylinder is $2\pi r^2 + 2\pi rh$.

- Triangle area formulas
  - All of these are useful under various circumstances. The most basic is $\frac{bh}{2}$ where h is the altitude to the base b.
  - Heron's: $[ABC] = \sqrt{s(s-a)(s-b)(s-c)}$, where $s = \frac{a+b+c}{2}$.
  - Trig: $[ABC] = \frac{1}{2}ab\sin C = \frac{1}{2}ac\sin B = \frac{1}{2}bc\sin A$. Note the corollary here: if D lies on AB and E on AC, then $\frac{[ADE]}{[ABC]} = \frac{AD}{DB}\cdot\frac{AE}{EC}$.
  - Using circumradius: $[ABC] = \frac{abc}{4R}$.
  - Using inradius: $[ABC] = sr$, where $s = \frac{a+b+c}{2}$.
  - Using coordinates: If the coordinates are $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, then the area is
$$\frac{|x_1y_2 + x_2y_3 + x_3y_1 - y_1x_2 - y_2x_3 - y_3x_1|}{2}$$
  - The above, the **Shoelace theorem**, extends to higher-order polygons as well, so long as we keep the coordinates in [counter]clockwise order.
- Useful triangle results: ABC is a triangle with $a = BC, b = CA, c = AB$.
  - In a right triangle, $a^2 = b^2 + c^2$ (Pythagorean triples). Common Pythagorean triples include $(3,4,5), (5,12,13), (8,15,17), (7,24,25), \left(n, \frac{n^2-1}{2}, \frac{n^2+1}{2}\right)$ for odd n, and their multiples.
  - Median splitting: The 3 medians split $[ABC]$ into six triangles of equal area. Additionally, the centroid G satisfies $AG = 2GM_a, BG = 2GM_b, CG = 2GM_c$ where M_a, M_b, M_c are the midpoints.
  - Angle bisectors: The 3 angle bisectors meet at the incenter. Additionally, if D lies on BC such that AD is the angle bisector, we have $\frac{AB}{AC} = \frac{BD}{CD}$.
  - Altitudes: The altitudes meet at the orthocenter, H. H has the useful property that, when reflected over any of the sides, it lies on the circumcircle of ABC.
  - Cirumcenter: The 3 perpendicular bisectors intersect at the orthocenter, O. O is, predictably, the center of the circumcircle.
  - Area ratios: If D lies on BC, then $\frac{[ABC]}{[ACD]} = \frac{BC}{CD}$ (since the two triangles share the same height).
  - Law of Cosines: $c^2 = a^2 + b^2 - 2ab\cos C, b^2 = a^2 + c^2 - 2ac\cos B, a^2 = b^2 + c^2 - 2bc\cos A$
  - (Extended) Law of Sines: $\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R$
  - Stewarts: Suppose X lies on BC and $AX = p, BX = m, CX = n$. Then $man + dad = bmb + cnc$ ("a man and his dad put a bomb in the sink").
  - Sometimes useful: $\sqrt{R(R-2r)}$ is the distance between the incenter and circumcenter; as a corollary, $R \geq 2r$.
  - One trick that's come up a bit recently: $\frac{1}{r} = \frac{1}{h_A} + \frac{1}{h_B} + \frac{1}{h_C}$, where h_A, h_B, h_C are the lengths of the altitudes and r is the inradius.
- Cyclic quadrilaterals
  - If A, B, C lie on a circle, then $\angle ABC$ is half the arc AC. In other words, an inscribed angle is half its subtended angle.
  - A, B, C, D are cyclic if they all lie on a single circle. Cyclic quadrilaterals have a ton of useful properties:
  - $\angle ABC + \angle CDA = \angle BCD + \angle DAB = 180°$.
  - $\angle ABD = \angle ACD$; analogously $\angle BCA = \angle BDA, \angle CDB = \angle CAB, \angle DAC = \angle DBC$. These are due to subtending the same arc.
  - Power of a point: if AC intersects BD at E, then $AE \cdot EC = BE \cdot ED$ (note this doesn't rely on the ordering of A, B, C, D - E might be outside the circle and $A = C$ is even possible).

- Ptolemy's theorem: $AB \cdot CD + BC \cdot DA = AC \cdot BD$.
- Area: The area of a cyclic quadrilateral is $\sqrt{(s-a)(s-b)(s-c)(s-d)}$ where $s = \frac{a+b+c+d}{2}$ - note what happens when $a = 0$!
- Simson's theorem: Let ABC be a triangle and D some point. Denote by X, Y, Z the feet of the altitudes from D to AB, BC, CA respectively. Then X, Y, Z are collinear if and only if D lies on the circumcircle of ABC.
- Cyclic quadrilaterals are like similar triangles on steroids: we get a ton of angle equalities and even some length relationships. If we manage to find one, it's almost always a sign that we're on the right track.
- Not entirely relevant: A quadrilateral has an inscribed circle if and only if $AB + CD = BC + DA$ (due to equal tangents).

- Collinearity and Concurrency
  - Ceva: If X lies on BC, Y lies on CA, and Z lies on AB, then AX, BY, CZ are concurrent if and only if $\frac{AZ}{ZB} \cdot \frac{BX}{XC} \cdot \frac{CY}{YA} = 1$.
  - Trig Ceva: AX, BY, CZ are concurrent if and only if $\frac{\sin BAX}{\sin CAX} \cdot \frac{\sin ACZ}{\sin BCZ} \cdot \frac{\sin CBY}{\sin ABY} = 1$.
  - If D lies on BC, E lies on CA, and F lies on AB, then D, E, F are collinear if and only if $\frac{AF}{BF} \cdot \frac{BD}{CD} \cdot \frac{CE}{AE} = 1$ (or -1, should you be comfortable with directed segments).
- 3-D geometry
  - This section is short, despite the subject's high importance, because there's very few formulae and strategies for 3-D geometry - the main point is finding the right 2-D cross-sections to take.
  - Some common configurations: A cube inscribed in a cone - take the cross section through two opposite face diagonals of the cube. The 2-D analogue is then a rectangle (NOT a square!) inscribed in a triangle; four externally tangent spheres - consider the pyramid formed by joining the centers and find its centroid; a sphere inscribed in a square pyramid - like before, consider a cross section through the vertex and a diagonal of the base, which gives a 2-D analogue of a semicircle inscribed in a triangle.
  - In general, these questions require a lot of practice and intuition development, and there's no general strategy that applies to this class.
- Coordinates and special cases
  - We can often fraud geometry problems by assigning the appropriate coordinate system and bashing away.
  - Some important results: The slope between the points (a, b) and (c, d) is $\frac{d-b}{c-a}$; this gives us equations of lines. The distance between the two is $\sqrt{(d-b)^2 + (c-a)^2}$. The slopes of perpendicular lines multiply to -1, and the slopes of parallel lines are equal.
  - The distance from (p, q) to a line $ax + by + c = 0$ is $\frac{|ap + bq + c|}{\sqrt{a^2 + b^2}}$.
  - The general coordinate form for a circle is $(x-h)^2 + (y-k)^2 = r^2$ - this is centered at (h, k) and has radius r. That said, if you are finding yourself needing to use circles in coordinate bashes, you are probably going down the wrong path.
  - Coordinates are generally good options when there are a lot of lines involved - like mentioned above, circles don't tend to play nicely with coordinates. Also very important is the choice of the origin and how to orient the coordinate axes. We almost always want a base of a triangle to lie on the x-axis, and usually want the origin to be the foot of the altitude from the other point. This makes it work out very nicely with 13-14-15 triangles (or others that are combinations of right triangles).
  - Coordinates also work out nicely with right angles - right angles mean we can place the coordinate axes along *two* bases, which makes it much more likely to be a clean solution. Therefore, whenever we're coordinate bashing on an arbitrary triangle, we almost always want to assume it's right.
  - In fact, when we're talking about arbitrary triangles, **we can often assume they're special**. This means that if the question is asking about something that doesn't depend on how the triangle looks, we can make life easier on ourselves by assuming it's right, or equilateral, or whatever happens to be convenient.

- This also applies to higher-order polygons: we can often assume a quadrilateral is a rectangle, or my personal favorite: that a parallelogram is a line. Be very careful trying to do this when lengths are given in the problem however - it may be the case that the polygon is implicitly determined. Don't try to assume a 13-14-15 triangle is right!

- Complex numbers in Geometry
  - We first define what we actually mean: the complex number $a + bi$, in the complex plane, is the Cartesian analogue of the point (a, b). The modulus of z is $|z| = \sqrt{a^2 + b^2}$, or the distance to the origin.
  - Note that complex numbers are very similar to vectors - indeed, the same "parallelogram rule" applies to summing two points, among other things.
  - Rotating about the origin θ clockwise takes z to $ze^{i\theta}$. Note that when $\theta = \dfrac{2\pi}{k}$ this looks suspiciously like roots of unity - and indeed, this is one of the biggest tip-offs to use complex numbers. A regular n-side polygon in the complex plane can be placed with vertices at $1, \omega, \omega^2, \ldots, \omega^{n-1}$ where ω is an nth root of unity.
  - Incidentally, note that this immediately proves $\cos 2^\circ + \cos 4^\circ + \ldots + \cos 360^\circ$ from before - these correspond to the x-coordinates of the vertices of a polygon whose centroid is 0, so the sum is immediately 0.
  - Another useful result: w and z are perpendicular if and only if $\dfrac{z}{w}$ is pure imaginary (this refers to the lines from 0 to w and from 0 to z). Analogously, the lines from a to b and c to d are perpendicular if and only if $\dfrac{d-c}{b-a}$ is pure imaginary.
  - An application: A square in the coordinate plane has vertices whose y coordinates are $0, 1, 4$, and 5. What is the area of the square? Solution: Place the square in the complex place. We want the origin to be the center, and we'd like to work with integers, so scale everything up by a factor of 2 and then shift it 5 units downward - this makes the square have y-coordinates $-5, -3, 3, 5$. Suppose one of the points is $a + 5i$. Then $(a + 5i)e^{\frac{\pi i}{2}} = (a + 5i)i = -5 + ai$ is the result of rotating the point 90 degrees clockwise about the origin, which coincides with the vertex on $y = 3$ (or possibly $y = -3$, but the difference is academic) - this implies that $a = 3$. As a result, the magnitude of $3 + 5i$ is $\sqrt{34}$, so the diagonal of the square is $2\sqrt{34}$, making the area of the original square (remember we scaled up by a factor of two at the beginning) $\boxed{17}$. Note how little work we had to do!
  - Hints to use complex geometry: Regular polygons work excellently with complex numbers, because (if we can make the origin the centroid), multiplying the points by ω results in the same polygon. Note how we did this in the previous problem, multiplying by a 4th root of unity (i). Any sort of rotation also suggests using complex geometry, since this is very easy to do using complex geometry. Finally, points on a circle suggest making the origin the center of that circle, since this again results in a rotational analogue. Summarizing: Lines - use coordinates, Circles - use complex numbers. Remember that we almost always want the origin to be the center of whatever we're considering, usually a regular polygon.

- Radical axes (*)
  - Define the *power* of a point P with respect to a circle O, $f(P, O)$, as follows: draw an arbitrary line through P that intersects O at the points A, B (not necessarily distinct) - then $f(P, O) = PA \cdot PB$. Define the *radical axis* of two circles O_1 and O_2 to be the set of points P satisfying $f(P, O_1) = f(P, O_2)$.
  - The radical axis theorem: the radical axis is a line. This is most commonly used with two circles intersecting at points A and B - then the radical axis is AB (as the powers from A and B are 0 to both circles). This implies a couple of things: If we have another point C whose powers to both circles are equal, then A, B, C are collinear. Conversely, if C lies on AB, the powers from C to the two circles are equal.
  - One important configuration: If ℓ is the external tangent of two circles that intersect at A and B, and is tangent at T_1, T_2, then AB intersects ℓ at the midpoint of T_1T_2.
  - The radical center: Given 3 circles O_1, O_2, O_3, the 3 radical axes ℓ_1, ℓ_2, ℓ_3 concur at the **radical center** T. This is primarily useful for showing 3 lines intersect. There is one potential pitfall to watch out for: If the centers of O_1, O_2, O_3 are collinear, the 3 radical axes are actually all parallel (and thus intersect at the point at infinity, not useful for most purposes). Fortunately, this is a rather trivial case, but it has tripped up many a 2009 USAMO contestant.

- Ratio lemma and Symmedians (*)
  - Ratio lemma: Let D be a point on BC. Then $\frac{AB}{\sin\angle BDA} = \frac{BD}{\sin\angle BAD}$ and $\frac{AC}{\sin\angle CDA} = \frac{CD}{\sin\angle CAD}$, so $\frac{AB}{BD} \cdot \sin\angle BAD = \frac{AC}{CD} \cdot \sin\angle CAD$, hence $\frac{AB}{AC} \cdot \frac{\sin\angle BAD}{\sin\angle CAD} = \frac{BD}{CD}$.
  - The *isogonal conjugate* of a point P is the intersection of AP, BP, CP reflected over the A-angle bisector, B-angle bisector, and C-angle bisector, respectively.
  - The circumcenter and orthocenter are isogonal conjugates, and the incenter is its own isogonal conjugate.
  - The **A-symmedian** is the reflection of the A-median over the A-angle bisector.
  - For any point X on the A-symmedian, $\frac{d(X, AB)}{d(X, AC)} = \frac{AB}{BC}$.
  - For any point X on the A-symmedian, $\frac{XB}{XC} = \frac{AB^2}{AC^2}$.
  - Let D lie on AB and E lie on AC such that $\triangle ADE \sim \triangle ACB$. Then the midpoint of DE lies on the A-symmedian.
  - An illustrative configuration: Suppose $ACUV, ABST$ are squares erected on the sides of ABC directed outside of ABC. Then the circumcenter of ATV lies on the A-symmedian.
  - Symmedians are not generally useful in computational problems by themselves (they're more for olympiad-level problems), but there have been a few AIME/AIME-esque problems lately that essentially take a known symmedian-configuration and assign numbers to them. As such they're worth noting, if only briefly.