Some Madman's Ravings

gispisquared

Contents

Introduction 5
General Recommendations 6

Chapter 1. Basic 7
1.1. Methods of Proof 7
1.2. Algebra 9
1.3. Combinatorics 11
1.4. Geometry 12
1.5. Number Theory 16

Chapter 2. Intermediate 19
2.1. Algebra 19
2.2. Combinatorics 20
2.3. Geometry 20
2.4. Number Theory 20

Chapter 3. Advanced 31
3.1. Algebra 31
3.2. Combinatorics 31
3.3. Geometry 31
3.4. Number Theory 31

Appendix A. Basics Solutions 43
A.1. Methods of Proof 44
A.2. Algebra 47
A.3. Combinatorics 52
A.4. Geometry 54
A.5. Number Theory 55

Appendix B. Intermediate Solutions 57
B.1. Algebra 57
B.2. Combinatorics 58
B.3. Geometry 58
B.4. Number Theory 58

Appendix C. Advanced Solutions 59
C.1. Algebra 59
C.2. Combinatorics 59
C.3. Geometry 59
C.4. Number Theory 59

Appendix D. Other free resources 61
D.1. Basics 61
D.2. NT 61
D.3. Algebra 61
D.4. Combi 61
D.5. Geo 61
D.6. Problems 61
D.7. Assorted 62
D.8. Published Books 62

Introduction

I was recently[1] asked what advice I would give to a beginner Olympiad student. Partly for your sake if you're reading this, and partly to inform how I write this, I'll copy (and punctuate) my response here:

- Don't believe people (like whoever writes hdigh) when they say methods of proof is all you should learn before spamming problems. Maybe that works if you're as smart as them, but most of us don't wanna spend most of our training reinventing the wheel.
- On the other hand, don't waste time looking up the latest crazy theorem AoPSers start mentioning; those are unlikely to ever be necessary and are probably only rarely useful because problem setters and pscs prefer problems where the easiest solution involves only canonical Olympiad knowledge.
- Most of the problems you're trying right now are gonna be pretty trivial for more advanced students, so whenever you solve or don't solve a problem figure out why it should have been trivial and hopefully this hindsight will start turning into foresight.

If I am to be consistent, then, this book's contents should be of three main types: canonical Olympiad knowledge and techniques, problems on which to practice these techniques, and solutions with motivation that try to make the problems seem as trivial as possible. I've also chosen both to include proofs to the known results (since their proofs are within Olympiad students' grasp and are often the source of canonical techniques), and to separate these proofs from the theorem statements in the same way as with problems (so that students can try to prove the theorems themselves).

There will be two main types of questions:

- *Results*, which up sporadically (or in some cases consistently) as steps in the harder problems. Every result comes with an implied "Prove that" attached. Unless specifically noted, all results are considered "well-known" and can likely be used without proof on contests. Where results are named, best practice is to quote the name when using the result; otherwise, best practice is to write "It is well known that…"
- *Problems*, which will be contest-style questions, many of which are from recent contests.

Since I refuse to rehash stuff that others have done better, I'll refer you to a couple of resources about how to write proofs properly:

- How to Write a Maths Solution
- Notes on English

[1] February 2022

Cool, hopefully now you know how to write proofs. Guess that means every time you solve a problem you'll get a 7, right?

Of course, to learn you'll need to put the required effort into maths — you're unlikely to learn too much just from reading problems and solutions. I've tried to make sure that all problems are accessible using only prior knowledge (something like high school maths up to y9 or so) and prior exposition; therefore, you should at least try to solve problems before reading the solutions.

However, there are diminishing returns when trying a single problem for ages. Opinions vary on this, but in my experience trying a problem for 15–30 minutes is enough to allow you to learn from the solution, and you'll learn from many more problems this way compared to if you try each problem for hours before giving up or moving on.

General Recommendations

This contains some general ideas about how to approach problems, or what to try when stuck.

- How are the objects referred to in the problem defined? What properties do you know them to have?
- Try small or special cases. Can you spot patterns in their structure? In how you solve them? Can you prove any of these patterns in general? Do any of these patterns help?
- Look at stuff that is extremal in some way: biggest, smallest, most connected, most disconnected, most composite, prime, whatever
- Think about what happens if the problem, or the conclusion, is wrong.
- Can you reduce any instance of the problem to a smaller instance? Can you reduce a counterexample to a smaller counterexample?
- Have you seen something similar before? Can you use the result or the method? Can you introduce some auxiliary element to make its use possible?
- Can you draw a diagram to help you understand the problem?

And some more specific recommendations:

- If you're stuck on a polynomial question, try inducting on the degree.
- If you need to prove something is unique, assume there are two things with the same properties and prove they're the same.
- If you want to prove one thing out of some set has a property, but you can't pick a "special" one, try contradiction.
- In geometry, make sure your diagrams are large and accurate. If you're stuck, try looking at a diagram and trying to guess which points look like they form similar triangles or cyclic quadrilaterals.

CHAPTER 1

Basic

1.1. Methods of Proof

If you haven't seen proofs before, chapters 4, 5, 6, and 10 of The Book of Proof provide a gentler and more complete introduction.

1.1.1. Direct Proof. This is perhaps the simplest type of proof. The idea is to start with the stuff you're given, do some logical deduction, and finish with what you want to prove.

RESULT 1. *The remainder when a perfect square is divided by 4 is either 0 or 1.* *Solution*

1.1.2. Contradiction. This is where you assume that what you're trying to prove is wrong and try to derive some kind of logical impossibility. Then the only place where the logic could have gone wrong was in the assumption so the statement you were trying to prove must be true.

RESULT 2 (Infinitude of primes). *There are infinitely many primes.* *Solution*

1.1.3. Contrapositive. It turns out that the statement $A \implies B$ is logically equivalent to the statement $\neg B \implies \neg A$. This is probably easiest to see intuitively with an example: "If x is an integer, then x is rational" is logically equivalent to "If x is not rational, then x is not an integer". Therefore, if we're asked to prove $A \implies B$, it's enough to prove $\neg B \implies \neg A$, which is sometimes easier.

PROBLEM 3. *Let $a, b \in \mathbb{R}$ such that $a + b$ is irrational. Prove that at least one of a and b is irrational.* *Solution*

1.1.4. Induction. Perhaps the hardest to understand of the basic proof techniques, this can be used to prove properties of positive integers where the property for each integer can be related to those of previous integers.

Here is the Principle of Mathematical Induction (PMI):

> Let S be a set of positive integers such that $1 \in S$ and for each $k \in S$, $k + 1 \in S$. Then S contains all positive integers.

To prove a statement for all positive integers, we let S be the set of all positive integers for which the statement is true. Then it's enough to prove:

- $1 \in S$. This is called the *base case.*
- If $k \in S$ (the *inductive hypothesis*), then $k + 1 \in S$. This is called the *inductive case.*

Then by PMI, S will contain all positive integers.

There are two ways to make induction superficially more powerful, though they're both equivalent to the usual form of induction:

- Say we want to prove a statement for all integers larger than n, for some n. Then it's enough to prove:
  - The statement is true for $n+1$.
  - If the statement is true for some integer $k > n$, then it's true for $k+1$.

  This is equivalent to the normal PMI: to see this, let S be the set of all integers m for which the statement is true for all $m+n$.
- Say we want to use not just the inductive assumption not just for k, but for smaller integers as well. Intuitively this should be fine, since we've in some sense "proved this already" by the time we get to $k+1$. Formally, to prove a statement $P(n)$ for all positive integers n, it's enough to prove:
  - $P(1)$.
  - If $P(1), \ldots, P(k)$ are all true, then $P(k+1)$ is also true.

  Once again this is equivalent to the normal PMI: let S be the set of all integers m for which $P(a)$ is true for all $a \leq m$.

  This form of proof by induction is called *strong induction*, and although most proofs by induction only explicitly use $P(k)$, there's no reason to try to make your proof inductive over strong inductive since strong induction gives you more assumptions to work with "for free".

The key idea in both of these reductions to PMI is to somehow encapsulate the extra information you're trying to assume into the framework of standard PMI.

Result 4. *For all positive integers n,*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Solution

There's also an equivalent statement to PMI — the Well-Ordering Principle.

> Let S be a nonempty set of postiive integers. Then there exists some $x \in S$ such that for all $y \in S$ we have $y \geq x$.

The Well-Ordering Principle is often used in conjunction with contradiction or contrapositive, since it is mainly "about" the existence of some element rather than the properties of the rest of the elements.

We can think of PMI as enabling us to prove something is true by building up larger cases from smaller cases, while well-ordering allows us to prove something is true by assuming there's a counterexample and finding a smaller one. It's nontrivial and instructive to prove they're actually equivalent.

First, we'll need a lemma (auxiliary result) so basic this is probably the only time we'll ever need to justify it:

Result 5. *Both PMI and well-ordering imply that if n is a positive integer then $n \geq 1$.* *Solution*

Result 6. *PMI and well-ordering imply each other.* *Solution*

I find it intriguing that induction and minimality are really just two sides of the same coin. Often you will find that a solution is much more natural to think about and write up in terms of one than the other.

1.2. Algebra

1.2.1. Factorisations. I won't have any problems attached to these, but they tend to pop up everywhere so keep an eye out. Here are some common factorisations:

- $x^2 - a^2 = (x+a)(x-a)$
- $x^2 - 2ax + a^2 = (x-a)^2$
- $x^2 + 2ax + a^2 = (x+a)^2$
- $x^3 - a^3 = (x-a)(x^2 + ax + a^2)$
- $x^3 + a^3 = (x+a)(x^2 - ax + a^2)$
- $x^3 + 3x^2a + 3xa^2 + a^3 = (x+a)^3$
- $x^3 - 3x^2a + 3xa^2 - a^3 = (x-a)^3$

Many of these are special cases of the formula

$$x^n - a^n = (x-a)(x^{n-1} + ax^{n-2} + a^2x^{n-3} + \cdots + a^{n-1}).$$

The cases $a = 1$ are especially common.

1.2.2. Systems of equations. There are a couple of ways of solving these systems — either you can isolate one variable, substitute into the rest of the equations, and repeat, or you can try and combine the equations in such a way that stuff cancels. The first method is usually fine in school maths and the AMC, but the second is more likely to be useful in harder Olympiad questions.

Sometimes these techniques won't be enough — see Section 2.1.1.

Problem 7. *The difference between two numbers is 20. When 4 is added to each number the larger is three times the smaller. What is the larger of the two original numbers? Solution*

Problem 8. *Find all triples (x, y, z) of real numbers that simultaneously satisfy the equations*

$$\begin{aligned} xy + 1 &= 2z \\ yz + 1 &= 2x \\ zx + 1 &= 2y \end{aligned}$$

Solution

1.2.3. Quadratics.

Result 9. *Let m and p be given real numbers. All real numbers x such that*

$$x^2 - 2mx + p = 0$$

are given by $x = m \pm \sqrt{m^2 - p}$. Solution

Result 10 (Quadratic Formula). *Let a, b, c be given real numbers. All real numbers x such that*

$$ax^2 + bx + c = 0$$

are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In particular, if we let $\Delta = b^2 - 4ac$, then the equation has no real roots if $\Delta < 0$, exactly one real root if $\Delta = 0$, and two real roots if $\Delta > 0$. Solution

This number Δ is called the *discriminant* of the quadratic.

Now, a couple of problems which show how useful both the results and the method are.

PROBLEM 11. *[See Section 1.5.4 if you don't know what number bases are.]*

The number x is 111 when written in base b, but it is 212 when written in base $b-2$. What is x is base 10? Solution

PROBLEM 12. *For each pair of real numbers (r, s), prove that there exists a real numer x that satisfies at least one of the following two equations.*

$$x^2 + (r+1)x + s = 0$$
$$rx^2 + 2sx + s = 0$$

Solution

PROBLEM 13. *Find all real numbers x for which $x^3 + 3x^2 + 3x + 5 = 0$.* Solution

1.2.4. Inequalities. At this level, inequalities are mostly about making stuff into squares or, well, "mostly squares". The guiding principle is to try and find an expression which you want to be always nonnegative, figure out where it's 0, and write it in terms of stuff that's 0 there and obviously nonnegative elsewhere.

RESULT 14 (2-variable AM-GM). *If a and b are real numbers, then*

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Solution

PROBLEM 15. *The set S consists of distinct integers such that the smallest is 0 and the largest is 2015. What is the minimum possible average value of the numbers in S?* Solution

1.2.5. Sums of sequences.

RESULT 16 (Sum of arithmetic sequence). *If n is a positive integer and a and b are real numbers, then*

$$\sum_{i=0}^{n} (a + bi) = \frac{(n+1)(2a + bn)}{2}.$$

Solution

RESULT 17 (Sum of geometric sequence). *If n is a positive integer and r is a real number distinct from 1, then*

$$\sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r}.$$

Solution

PROBLEM 18. *Prove that for any positive integers n and a, the sum*

$$n + (n+1) + (n+2) + \cdots + (n+a)$$

is never a power of 2. Solution

1.3. Combinatorics

Combinatorics (the branch of maths that deals with, among other things, finding smart ways to count stuff) is a field with relatively few standard techniques. Often, these are the problems that require the least technical skill and the most ingenuity. With every field, but especially with combinatorics, there is no substitute for practice.

1.3.1. Addition and Multiplication Principles. This is the most basic idea in combinatorics. If you can make one from a choices and then one from b choices, the total number of ways you can do this is ab. If you can make either one from a choices or one from b choices, the total number of ways you can do this is $a + b$.

Many combinatorics problems boil down to splitting them into cases, and then applying addition and multiplication principles to count each case.

RESULT 19 (Permutations). *The number of ways of choosing k things from n, where order matters, is*

$$n(n-1)\cdots(n-k+1) = \frac{n!}{k!}.$$

Solution

PROBLEM 20. *A hockey game between two teams is 'relatively close' if the numbers of goals scored by the two teams never differ by more than two. In how many ways can the first 12 goals of a game be scored if the game is 'relatively close'?* Solution

PROBLEM 21. *An ant's walk starts at the apex of a regular octahedron. It walks along five edges, never retracing its path. It visits each of the other five vertices exactly once. In how many ways can it do this?*

1.3.2. Combinations.

RESULT 22 (Combinations). *The number of ways of choosing k things from n, where order doesn't matter, is*

$$\frac{n!}{(n-k)!k!}.$$

Solution

PROBLEM 23. *How many pairs (a, b) of 3-digit palindromes are there with $a > b$ and $a - b$ also a 3-digit palindrome?* Solution

1.3.3. Inclusion-Exclusion. So you try to count something using the addition principle, but you realise you've counted some things twice. Obviously, the way you fix it is you subtract the stuff you doubled up. For more tedious problems this could also be overcounted, but this can be continued and hopefully the stuff you've overcounted gets easier to count each time.

PROBLEM 24. *How many integers between 1 and 1000 inclusive are divisible by at least one of 4, 6 and 10?*

1.3.4. Bijections. A bijection is simply a way of counting one set of stuff by identifying each element in the set with an element from another set that's easier to count. We've already used a bijection in our solution to Problem 23.

To come up with a bijection, it's often useful to list out the elements of each set for some small cases, and pair them up in what looks like a natural way. Often that natural way will generalise.

Result 25 (Multinomial Coefficient). *The number of ways of putting n identical things into k boxes is*

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

Problem 26. *How many paths are there from the bottom left to the top right of a 4×7 grid, if you can only go up or right?*

1.3.5. Recurrences. These are a useful way to solve problems where you're asked for the number of ways of doing something that depends on n. To set up a recurrence, we make a sequence where the ith term is the answer for $n = i$. Then, we find a way of relating each terms to previous terms.

Perhaps an example or two will serve to clarify things:

Problem 27. *How many ways are there of tiling a $2 \times n$ grid with dominoes?*

Problem 28. *How many sequences of 10 traffic lights (each green, yellow or red) are there such that a green light is always followed by a yellow light, while a red light is never followed by a red light?*

1.3.6. Pigeonhole Principle. The Pigeonhole Principle is a very simple but widely applicable idea. It is often useful in problems which ask you to prove the existence of one or more things from a set, but there's no obvious way to pick a "special" object from the set.

Result 29 (Pigeonhole Principle). *If $A_1, A_2, \ldots, A_n$ are a collection of sets whose union is A, and A has more than nk elements, then some A_i has more than k elements.*

An important special case is when A has infinitely many elements; then some A_i has infinitely many elements.

Problem 30. *Let M be a set of positive integers, none of which is larger than 100. Prove that there are two disjoint subsets of M with the same sum.*

Problem 31. *A class has 20 students. Any two of them have a common grandfather. Prove that there are 14 students all of whom have a common grandfather.*

Problem 32. *There are 101 chess players who participated in several tournaments. There was no tournament in which all of them participated. Each pair of those players met exactly once during these tournaments. Each pair of players in a tournament meet exactly once in that tournament. Prove that one of them participated in at least 11 tournaments.*

1.4. Geometry

Whenever you see a geometrical statement or problem (including everywhere in the geometry sections of this book), your first instinct should always be to draw a diagram to understand it. Diagrams should be

- Accurate — use ruler and compass
- Large — they should take up the whole page. Go landscape if it gives you more space.

This is important because your chances of solving, or even understanding, a problem are proportional to how easily you can see things in your diagram.

1.4.1. Parallels. You should know what parallel lines are: they point in the same direction and never meet.

Let ABC and DEF be points on two parallel lines (in that order, and in the same direction along each line), and let X and Y be points on BE such that $XBEY$ is in that order. Then

$$\angle ABX = \angle CBE = \angle DEX = \angle FEY,$$

the other four angles are equal, and the angles in these two sets are supplementary (add up to 180°).

RESULT 33. *For any three points A, B, C,*

$$\angle ABC + \angle BCA + \angle CAB = 180^\circ.$$

1.4.2. Congruence. Two triangles ABC and XYZ are called *congruent* if

$$AB = XY,\ AC = XZ,\ BC = YZ,$$

$$\angle BAC = \angle YXZ,\ \angle ABC = \angle XYZ,\ \angle ACB = \angle XZY.$$

We write "ABC is congruent to XYZ" as $\triangle ABC \cong \triangle XYZ$.

There are congruence tests which enable us to determine when two triangles are congruent, so that knowing some of these equalities we can deduce the others.

Triangles ABC and XYZ are congruent if any of the following hold:

- $AB = XY$, $AC = XZ$ and $BC = YZ$. (SSS)
- $AB = XY$, $AC = XZ$ and $\angle BAC = \angle YXZ$. (SAS)
- $AB = XY$ and $\angle BAC = \angle YXZ$ and $\angle ABC = \angle XYZ$. (AAS)

Note: SSA (two sides and an unincluded angle) on its own isn't enough, but we can fix it:

- $AB = XY$ and $AC = XZ$ and $\angle ABC = \angle XYZ$ and $AB < AC$. (Fixed SSA)

In the special case where $\angle ABC = \angle XYZ = 90^\circ$, this is known as RHS.

RESULT 34 (Isosceles triangle). *Let ABC be a triangle, and let M be the midpoint of BC. The following statements are equivalent:*

- $AB = AC$
- $\angle ABC = \angle ACB$
- $AM \perp BC$.

PROBLEM 35. *Let ABC be an isosceles triangle with $AB = BC$. Let D be a point on BC such that $\angle DBC = 20^\circ$. Let E be a point on AB with $AE = AD$. What is $\angle BDE$?*

RESULT 36. *Let $ABCD$ be a parallelogram (that is, $AB || CD$ and $BC || DA$). If AC intersects BD at P, then P is the midpoint of AC and of BD.*

1.4.3. Circles. A *circle* is the set of points a distance r from a central point O. Thus, any two points on the circle form an isosceles triangle with O.

The circumference (perimeter) of the circle is $2\pi r$, while the area is πr^2.

Result 37 (Thales' Theorem). *Let A, B, C, M be points in the plane such that M is the midpoint of AB. Then C lies on the circle centred at M passing through A and B if and only if $\angle ACB = 90°$.*

The next few results are generalisations of this. The proofs are linked in Section 2.3.1.

Result 38. *If A, B, C are points on a circle centred at O with A on the same side of BC as O, then $\angle BOC = 2\angle BAC$.*

Result 39. *If A, B, C are points on a circle centred at O with A and O on opposite sides of BC, then $\angle BOC = 360° - 2\angle BAC$.*

Result 40 (Bowtie Theorem). *If B and C lie on the same side of AD then there is a circle passing through all of A, B, C, D if and only if $\angle ABD = \angle ACD$.*

Result 41. *If B and D lie on opposite sides of AC, then there is a circle passing through all of A, B, C, D if and only if $\angle ABC + \angle ADC = 180°$.*

Problem 42. *For $n \geq 3$, a pattern can be made by overlapping n circles, each of circumference 1 unit, so that each circle passes through a central point and the resulting pattern has order-n rotational symmetry. For instance, the diagram shows the pattern where $n = 7$.*

If the total length of visible arcs is 60 units, what is n?

1.4.4. Similarity. We say that triangles ABC and XYZ are *similar* if for some real r (called the ratio of similitude),

$$\frac{BC}{YZ} = \frac{CA}{ZX} = \frac{AB}{XY} = r,$$

$$\angle ABC = \angle XYZ, \ \angle BCA = \angle YZX, \ \angle CAB = \angle ZXY.$$

We write "ABC is similar to XYZ" as $\triangle ABC \sim \triangle XYZ$.

Triangles ABC and XYZ are similar if any of the following hold:

- $\frac{BC}{YZ} = \frac{CA}{ZX} = \frac{AB}{XY}$ (PPP)
- $\frac{AB}{XY} = \frac{BC}{YZ}$, $\angle ABC = \angle XYZ$ (PAP)
- $\angle ABC = \angle XYZ$, $\angle BCA = \angle YZX$ (AA)

Once again, PPA (two sides and an unincluded angle) doesn't work. However, we can fix it in the same way:

- $\frac{AB}{XY} = \frac{AC}{XZ}$, $\angle ABC = \angle XYZ$ and $AB < AC$. (Fixed PPA)

In the special case where $\angle ABC = \angle XYZ = 90°$, this is known as RHS.

Result 43 (Similar Switch). *Let ABC and ADE be similar triangles with the same orientation (that is, $\triangle ABC \sim \triangle ADE$ and both triangles are labelled either clockwise or anticlockwise). Then ABD and ACE are also similar and similarly oriented.*

Problem 44. *Let A, B, C, D be points on a circle such that $\triangle ABC$ is equilateral, and D lies on minor arc BC. Prove that $AD = BD + CD$.*

1.4.5. Areas. We assign a positive real number, known as an *area*, to each polygon in the plane such that

- the area of a rectangle with sidelengths a and b is ab;
- the areas of two congruent triangles are equal; and
- if two polygons have disjoint interiors then the area of their union equals the sum of their areas.

The area of a polygon $P_1, P_2, \ldots, P_n$ is denoted $|P_1 P_2 \cdots P_n|$. We may use these properties to deduce some well-known facts about areas.

RESULT 45. *Let ABC be a triangle such that $\angle ABC = 90°$. Then,*

$$|ABC| = \frac{1}{2} \times AB \times BC.$$

RESULT 46. *Let ABC be a triangle, and let D be a point on line BC such that $AD \perp BC$. Then,*

$$|ABC| = \frac{1}{2} \times AD \times BC.$$

An important special case of this is that two triangles with the same height have areas in the same ratio as their bases, and two triangles with the same base have areas in the same ratio as their heights.

RESULT 47. *Let ABC and XYZ be similar triangles with ratio of similitude r. Then,*

$$\frac{|ABC|}{|XYZ|} = r^2.$$

PROBLEM 48. *A triangle ABC is divided into four regions by three lines parallel to BC. The lines divide AB into four equal segments. If the second largest region has area 225, what is the area of ABC?*

PROBLEM 49. *Let $ABCD$ be a parallelogram. Point P is on AB produced such that DP bisects BC at X. Point Q is on BA produced such that CQ bisects AD at M. Lines DP and CQ meet at O. If the area of parallelogram $ABCD$ is 192, find the area of triangle POQ.*

PROBLEM 50. *The area of triangle ABC is 300. In triangle ABC, Q is the midpoint of BC, P is a point on AC between C and A such that $CP = 3PA$, R is a point on side AB such that the area of $\triangle PQR$ is twice the area of $\triangle RBQ$. Find the area of $\triangle PQR$.*

RESULT 51 (Angle Bisector Theorem). *In triangle ABC, point P is on AB such that AP bisects $\angle BPC$. Then, $\frac{BP}{PC} = \frac{BA}{AC}$.*

1.4.6. Pythagoras. Pythagoras' Theorem is arguably the most famous theorem in mathematics. You should aim to find multiple proofs of it, to cement your understanding of the techniques developed in this section on geometry.

Four proofs are given in the linked solutions, with a fifth in Section 2.3.2.

RESULT 52 (Pythagoras' Theorem). *If $\angle ABC = 90°$, then $AB^2 + BC^2 = AC^2$.*

PROBLEM 53. *Let $ABCD$ be a square and let E and F be points on BC and CD, respectively, such that AEF is an equilateral triangle.*

Find the length BE.

1.4.7. Trigonometry. These concepts are easiest to define working on the coordinate plane. Let O be the origin, and let A be the point $(1, 0)$. Let $P = (x, y)$ be a point on the unit circle (that is, $x^2 + y^2 = 1$) such that the counterclockwise angle $\angle AOP$ is θ (see the diagram). We define

$$\cos(\theta) = x,\ \sin(\theta) = y,\ \tan(\theta) = \frac{y}{x}.$$

RESULT 54. *For all θ we have* $\cos(-\theta) = \cos(\theta) = \sin(90-\theta) = -\cos(180-\theta)$.

RESULT 55. *Let ABC be a triangle with $\angle ABC = 90°$. Then,*

$$\sin(\angle ACB) = \frac{AB}{AC},\ \cos(\angle ACB) = \frac{BC}{AC},\ \tan(\angle ACB) = \frac{AB}{BC}.$$

RESULT 56. *We have*

$$\sin(0) = 0,\ \sin(30) = \frac{1}{2},\ \sin(45) = \frac{\sqrt{2}}{2},\ \sin(60) = \frac{\sqrt{3}}{2},\ \sin(90) = 1.$$

For the next two results we define ABC to be a triangle with sidelengths $a = BC,\ b = CA,\ c = AB$. We use the shorthand $\angle A = \angle BAC$ and similarly for $\angle B$ and $\angle C$.

RESULT 57 (Extended Rule of Sines).

$$\frac{a}{\sin \angle A} = \frac{b}{\sin \angle B} = \frac{c}{\sin \angle C}.$$

Further, if A, B, C lie on a circle with radius R then these quantities are all equal to $2R$.

RESULT 58 (Rule of Cosines).

$$\cos \angle A = \frac{b^2 + c^2 - a^2}{2bc}.$$

PROBLEM 59. *In quadrilateral $PQRS$ we have $PS = 5,\ SR = 6,\ RQ = 4$, and $\angle P = \angle Q = 60°$. Find the length of PQ.*

PROBLEM 60. *Let $ABCD$ be a trapezium with $AB \| CD$ such that its vertices A, B, C, D lie on a circle with centre O. Let the diagonals AC and BD intersect at a point M. Assume that $\angle AMD = 60°$ and $MO = 1$.*

What is the difference between the lengths AB and CD?

1.5. Number Theory

1.5.1. Divisibility. For integers a and b, we say $a \mid b$ (read "a divides b") if there is some integer c with $b = a \times c$.

RESULT 61. *If a and b are positive integers with $a \mid b$ then $a \leq b$.*

RESULT 62. *If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for all integers x and y.*

PROBLEM 63. *Find all integers n such that $n^2 + 1 \mid n^3 + n^2 - n - 15$.*

1.5.2. Primes. We define a *prime* as a positive integer larger than 1 which is not divisible by any positive integer other than 1 and itself.

RESULT 64. *Every positive integer larger than 1 can be written as a product of primes.*

This was what allowed us to prove Result 2.

The Fundamental Theorem of Arithmetic (proved in Results 64 and 86) states that each positive integer has a unique prime factorisation; that is, we can write a positive integer n uniquely (up to permuting the p_is) as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where p_i are all prime and e_i are all positive integers.

Prime factorisations allow us to view statements about divisibility and multiplication in terms of the exponents e_i.

In what follows, let

$$a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}, \ b = q_1^{f_1} q_2^{f_2} \cdots q_k^{e_k}.$$

RESULT 65. *$a \mid b$ if and only if for each i we have that $p_i = q_j$ for some j, and that $e_i \leq f_j$.*

RESULT 66. *a is a perfect kth power if and only if $k \mid e_i$ for all i.*

RESULT 67. *Let m and n be positive integers. Then, $\sqrt[m]{n}$ is an integer or irrational.*

RESULT 68. *The lcm is found by taking the maximum power of each prime that divides either a or b; the gcd is found by taking the minimum power of each prime that divides both a and b.*

RESULT 69. $\gcd(a, b) \times \operatorname{lcm}(a, b) = ab$.

1.5.3. Factorisations. Factorisations allow us to make equations nicer to work with. For example, solving the equation $xy + x + y = 3$ over the integers becomes much easier when we express it as $(x + 1)(y + 1) = 4$.

Here are the most useful factorisations:

$$axy + bx + cy = d \iff (ax + c)(ay + b) = ad + bc$$
$$a^k - b^k = (a - b)\left(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}\right)$$

PROBLEM 70. *Find all right-angled triangles with positive integer sides such that their area and perimeter are equal.*

PROBLEM 71. *Prove that $1^k + 2^k + \cdots + n^k$ is divisible by $1 + 2 + \cdots + n$ for all positive integers n and odd positive integers k.*

PROBLEM 72. *Prove that if $2^n + 1$ is prime for a positive integer n, then n is a power of 2.*

1.5.4. Number bases.

RESULT 73 (Base n representation). *Given positive integers $n > 1$ and k, prove that there are unique nonnegative integers $m, a_0, a_1, \ldots, a_m$ such that $a_m > 0$, $0 \leq a_i < n$ for all i, and*

$$k = a_0 n^0 + a_1 n^1 + \cdots + a_m n^m.$$

This representation is often written as

$$(\overline{a_m a_{m-1} \cdots a_0})_n.$$

When the a_is are specific digits, the parentheses and the bar over the a_is are often dropped. So for example, the decimal number 16 can be expressed as 10000_2.

PROBLEM 74. *If $234_{b+1} - 234_{b-1} = 70_{10}$, what is 234_b in base 10?*

PROBLEM 75. *A sequence $\{a_i\}$ begins with $a_1 = 0$, and for each i the number a_{i+1} is the smallest integer larger than a_i which is not equal to $2a_k - a_j$ for any j, k with $1 \leq j < k \leq i$. So the sequence begins 0,1,3,4,9,...*

Find the 2000th term of this sequence.

1.5.5. Euclid's Algorithm.

RESULT 76 (Division Algorithm). *If a is an integer and b is a positive integer, there is a unique pair (q, r) of integers such that $0 \leq r < b$ and $a = qb + r$.*

RESULT 77 (Euclid's Algorithm). *If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.*

RESULT 78 (Bezout's Identity). *There are integers c and d such that $ac + bd = \gcd(a, b)$.*

PROBLEM 79. *The denominators of two irreducible fractions are x and y. Find the minimum possible value of the denominator of their sum.*

RESULT 80 (GCD Trick). *Prove that for all positive integers a, b, m, n with $a > b$ and $\gcd(a, b) = 1$ we have*

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}.$$

PROBLEM 81. *Let S be a nonempty set of integers such that if a and b are in S, then so is $2a - b$. Prove that S is an arithmetic progression.*

CHAPTER 2

Intermediate

2.1. Algebra

2.1.1. Systems of Equations.

2.1.2. Polynomials. A polynomial is just an expression of the form

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 x^0,$$

where each of the a_is is a constant and $a_n \neq 0$. The number n is called the *degree* of the polynomial. The term $a_n x^n$ is called the *leading term*. The expression $P(x) = 0$ is also a polynomial, and it's defined to have degree $-\infty$.

RESULT 82. *Let $A(x)$ and $B(x)$ be polynomials. Then,*

- $\deg(A \pm B) \leq \max(\deg A, \deg B)$. *Equality occurs unless the leading terms of A and B cancel.*
- $\deg(A \times B) = \deg(A) + \deg(B)$.

Many proofs in polynomial questions proceed by (strong) induction on the degree. The following few examples illustrate a few of the ways in which we can reduce a polynomial to a smaller-degree polynomial.

RESULT 83 (Division Algorithm). *Let $A(x)$ and $B(x)$ be polynomials with $B(x) \neq 0$. There exist unique polynomials $Q(x)$ and $R(x)$ such that* $\deg R < \deg B$ *and*

$$A(x) = Q(x)B(x) + R(x).$$

Solution

We say that a polynomial $P(x)$ divides another polynomial $Q(x)$ if there is a polynomial $R(x)$ such that $P(x) = Q(x)R(x)$. With this terminology, an important corollary is that for any real number r and any polynomial $A(x)$, the polynomial $x - r$ divides the polynomial $A(x) - A(r)$.

RESULT 84 (Vieta's Formulas). *If a polynomial*

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 x^0$$

has roots $r_1, \ldots, r_n$ then for each i,

$$a_{n-i} = (-1)^i a_n \sum_{j_1 < \cdots < j_i} \prod_{k=1}^{i} r_{j_k}.$$

Solution

2.2. Combinatorics

2.3. Geometry

2.3.1. Directed Angles.

2.3.2. The Incircle.

2.4. Number Theory

2.4.1. Fundamental Theorem of Arithmetic.

RESULT 85 (Euclid's Lemma). *If n, a, b are positive integers such that $n \mid ab$ and $\gcd(n, a) = 1$ then $n \mid b$.*

RESULT 86. *If $p_1, \ldots, p_m,\ q_1, \ldots, q_n$ are primes such that*

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n,$$

then the q_is are a permutation of the p_is.

PROBLEM 87. *We call the* main divisors *of a composite number n the two largest of its divisors other than n. Composite numbers a and b are such that their main divisors coincide. Prove that $a = b$.*

PROBLEM 88. *Let a, b, p be positive integers such that p is prime and $\operatorname{lcm}(a, a+p) = \operatorname{lcm}(b, b+p)$. Prove that $a = b$.*

PROBLEM 89. *Determine all composite integers $n > 1$ that satisfy the following property: if $d_1, d_2, \ldots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \le i \le k-2$.*

2.4.2. Arithmetic Functions. We define:

- The number of positive divisors function $d(n)$.
- The sum of positive divisors function $\sigma(n)$.
- The totient function $\varphi(n)$: the number of positive integers which are at most n and coprime to n.

PROBLEM 90. *Prove that $d(n) \le 2\sqrt{n}$.*

PROBLEM 91. *Prove that for all n,*

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) \le n^2.$$

PROBLEM 92. *Prove that for all composite n,*

$$\varphi(n) \le n - \sqrt{n}.$$

RESULT 93. *If $n = \prod p_i^{e_i}$, then $d(n) = \prod (e_i + 1)$.*

RESULT 94. *If $n = \prod p_i^{e_i}$, then*

$$\sigma(n) = \prod \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right).$$

RESULT 95 (Even perfect numbers). *Let n be an even positive integer such that $\sigma(n) = 2n$. There is a prime p such that $n = 2^{p-1}\left(2^p - 1\right)$.*

RESULT 96. *If $n = p^e$, then*

$$\varphi(n) = n \left(1 - \frac{1}{p} \right).$$

Actually, it is true that if $n = \prod p_i^{e_i}$, then
$$\varphi(n) = n \prod \left(1 - \frac{1}{p_i}\right).$$
We prove this in Result 111.

2.4.3. Modular Arithmetic. Let n be a nonzero integer. For integers a and b, we say that
$$a \equiv b \pmod{n} \iff n \mid b - a.$$
Notice that for fixed values of a and n, infinitely many values of b satisfy $a \equiv b \pmod{n}$.

The numbers $0, 1, \dots, n-1$ are called the *least residues mod n*. Every integer is congruent to a unique least residue mod n.

RESULT 97. *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then*
- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^m \equiv b^m \pmod{n}$ *for any nonnegative integer m.*

Be careful: division does not work as expected. For example, $2 \equiv 6 \pmod{4}$ but $2/2 \not\equiv 6/2 \pmod{4}$. Instead, we have the following:

RESULT 98. *If $mx \equiv my \pmod{n}$ then*
$$x \equiv y \left(\mathrm{mod}\ \frac{n}{\gcd(n,m)}\right).$$

PROBLEM 99. *Let $n > 6$ be an integer such that $n-1$ and $n+1$ are both prime. Prove that $720 \mid n^2(n^2+16)$.*

PROBLEM 100. *Let $a_1 = 20,\ a_2 = 23$. For $n \geq 1$, let a_{n+1} be the least residue of $a_n + a_{n-1}$ mod 100. Find the least residue of $a_1^2 + \cdots + a_{2023}^2 \bmod 8$.*

PROBLEM 101. *Let n be a positive integer. All numbers m which are coprime to n satisfy $m^2 \equiv 1 \pmod{n}$. Find the maximum possible value of n.*

2.4.4. Inverses.

RESULT 102. *If $\gcd(y,n) = 1$ then there exists some x such that $ax \equiv y \pmod{n}$.*

RESULT 103. *If $\gcd(a,n) = 1$ then there exists a unique least residue $a^{-1} \pmod{n}$ such that $aa^{-1} \equiv 1 \pmod{n}$.*

The least residue a^{-1} such that $aa^{-1} \equiv 1 \pmod{n}$ is called the *inverse* of a mod n.

RESULT 104. *Let $\gcd(b,n) = \gcd(d,n) = 1$. Then,*
- $b^{-1}d^{-1} \equiv (bd)^{-1} \pmod{n}$
- $(b^k)^{-1} \equiv (b^{-1})^k \pmod{n}$
- $ab^{-1} + cd^{-1} \equiv (ad+bc)(bd)^{-1} \pmod{n}$

PROBLEM 105. *Let $p = 3k-1$ be a prime. Prove that*
$$1^{-1} - 2^{-1} + 3^{-1} - 4^{-1} + \cdots + (2k-1)^{-1} \equiv 0 \pmod{p}.$$

2.4.5. Theorems About Mods.

RESULT 106 (Wilson's Theorem). $(n-1)! \equiv -1 \pmod{n}$ *if and only if n is prime.*

RESULT 107 (Chinese Remainder Theorem). *Let $a_1, a_2, \ldots, a_k$ be pairwise coprime positive integers, and let $b_1, b_2, \ldots, b_k$ be integers. Then there is exactly one least residue x mod $a_1 a_2 \cdots a_n$ such that for each i,*

$$b_i \equiv x \pmod{a_i}.$$

PROBLEM 108. *Call a lattice point "visible" if the greatest common divisor of its coordinates is 1. Prove that there exists a 100 × 100 square on the board none of whose points are visible.*

RESULT 109. *If* $\gcd(a, b) = 1$*, then* $\varphi(ab) = \varphi(a)\varphi(b)$.

PROBLEM 110. *Prove that for all composite $n > 6$, $\varphi(n) \geq \sqrt{n}$.*

RESULT 111 (Euler's Product Formula). *If $n = \prod p_i^{e_i}$, then*

$$\varphi(n) = n \prod \left(1 - \frac{1}{p_i}\right).$$

RESULT 112 (Euler's Theorem). *If* $\gcd(a, n) = 1$*, then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

The special case where $n = p$ is prime yields $a^{p-1} \equiv 1 \pmod{p}$, which is known as Fermat's Little Theorem.

PROBLEM 113. *Let p be a prime and let c be a positive integer. Prove that there exists a positive integer x such that $x^x \equiv c \pmod{p}$.*

2.4.6. Choosing Good Mods. Many number theory problems, especially Diophantine equations, can be solved by looking at them using an appropriate mod. These are especially common:

RESULT 114. *Squares are 0, 1 or 4 mod each of {5,8}, and 0 or 1 mod 3.*

RESULT 115. *Squares are 0, 1 or -1 mod each of {7,9}.*

In general, for nth powers, try looking mod m where $\varphi(m)$ is a small multiple of n. You can also try choosing a mod which divides a bunch of terms in an equation.

However, remember that if you find a single solution to a polynomial equation, then that solution is still a solution in every mod so you won't be able to find a contradiction.

PROBLEM 116. *Find all positive integers a, b such that $a^4 + b^4 = 10a^2b^2 - 2022$.*

PROBLEM 117. *Find all positive integers n such that $2^n + 7^n$ is a perfect square.*

PROBLEM 118. *Find all pairs of positive integers x, y such that $x! + 5 = y^3$.*

2.4.7. Bounding. This subsection is all about finding bounds on a variable in a problem. Once you do that, there are finitely many cases to check and those cases are usually not difficult.

Techniques:

- WLOG arguments: break symmetry to bound one of the variables.
- Bound the output of a monotonic function between consecutive values.

- If a and b are integers with $b \neq 0$ and $a \mid b$ then $|a| \leq |b|$. Thus, try to get big dividing small. Polynomial long division is helpful here.
- Look for "dominant terms" that grow larger than everything else. For sufficiently large n and any $c > 1$, we have $c \ll \log n \ll n^c \ll c^n \ll n! \ll n^n$ (Result 225).
- If you need to prove a specfic bound of the form "$f(x) > g(x)$ for $x > k$," try induction.
- If you have a factorial, $n! \equiv 0 \pmod{c}$ for $n \geq c$ so mods are often nice.

PROBLEM 119. *Find all positive integers k such that there is a positive integer n for which*

$$k = \frac{n^2 - 29}{3n + 11}.$$

PROBLEM 120. *Find all positive integers a, b, c such that $ab + bc + ca = abc + 2$.*

PROBLEM 121. *Prove that if $n > 11$ then $n^2 - 19n + 89$ is not a square.*

PROBLEM 122. *Find all positive integers n such that $2^n \leq (n + 1)^2$.*

2.4.8. Descent. Descent works like this: assign some positive integer quantity (the "size" of a solution, e.g. the sum of the absolute values of the variables) to each solution, take the solution with lowest "size" that doesn't fit your claimed pattern and derive a contradiction.

PROBLEM 123. *Find all solutions in integers to $a^3 + 2b^3 + 4c^3 = 0$.*

PROBLEM 124. *Let's say you have a set S of positive rational numbers such that $1 \in S$, and if $x \in S$ then both $x + 1$ and $\frac{1}{x}$ are in S. Prove that S contains all positive rationals.*

PROBLEM 125. *Prove that if x, y, z are integers such that $x^2 + y^2 + z^2 = (xy)^2$, then $x = y = z = 0$.*

PROBLEM 126. *A list of 2022 positive integers is given, such that if you remove any one of them, the rest can be split into two groups of equal sum. Prove that all the numbers in the list are equal.*

2.4.9. Integer Polynomials. An integer polynomial is a polynomial with integer coefficients.

RESULT 127. *In Result 83, if A and B have rational coefficients, then Q and R have rational coefficients. If A and B have integer coefficients and B is monic, then Q and R have integer coefficients.*

RESULT 128. *If p is an integer polynomial and a and b are integers, then $a - b \mid p(a) - p(b)$.*

RESULT 129 (Rational Root Theorem). *If p is an integer polynomial with leading coefficient a_0, and y and z are integers with $\gcd(y, z) = 1$ such that $p(y/z) = 0$, then $z \mid a_0$ and $y \mid p(0)$.*

PROBLEM 130. *Prove that every nonconstant integer polynomial has a composite number in its image.*

PROBLEM 131. *Let P be an integer polynomial such that if $P(x)$ is an integer then x is rational. Prove that P is linear.*

Problem 132. *Prove that for every polynomial $P(x)$ of degree at least 2 with integer coefficients, there is an infinite arithmetic progression of integers which does not contain $P(k)$ for any integer k.*

Problem 133. *Prove that if P is a polynomial with integer coefficients and leading term $a_0 n^k$ such that $m \mid P(n)$ for all n, then $m \mid k! a_0$.*

2.4.10. Assorted Problems.

Problem 134. *Prove that for each positive integer n there exist n consecutive positive integers, none of which is a prime power.*

Problem 135. *Consider a sequence of positive integers $a_1, a_2, \ldots$ which satisfies $a_n = a_{n-1}^2 + a_{n-2}^2 + a_{n-3}^2$ for all $n \geq 3$. Prove that if $a_k = 1997$ then $k \leq 4$.*

Problem 136. *Prove that for positive integers $m, n > 2$ we cannot have $2^m - 1 \mid 2^n + 1$.*

Problem 137. *For a natural number N, consider all distinct perfect squares that can be obtained from N by deleting one digit from its decimal representation. Prove that the number of such squares is bounded by some value that doesn't depend on N.*

Problem 138. *Is there a polynomial f of degree 2023 with integer coefficients such that*

$$f(n), f(f(n)), f(f(f(n))), \cdots$$

are pairwise relatively prime for any integer n?

Problem 139. *Let a and b be positive irrational numbers such that $\frac{1}{a} + \frac{1}{b} = 1$. Let $A = \{\lfloor na \rfloor : n \in \mathbb{N}\}$, and $B = \{\lfloor nb \rfloor : n \in \mathbb{N}\}$. Prove that the sets A and B together contain each posiive integer exactly once.*

Problem 140. *Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(m + f(n)) = f(m) - n$ for all integers m and n.*

Problem 141. *Find all polynomials $P(x)$ with integer coefficients such that if $m \mid n$ then $P(m) \mid P(n)$.*

Result 142. $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Problem 143. *Solve over integers: $6(6a^2 + 3b^2 + c^2) = 5n^2$.*

Problem 144. *Let p and q be coprime. Prove that*

$$\sum_{i=1}^{q-1} \left\lfloor \frac{ip}{q} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

Problem 145. *Find all positive integers n such that $3^{n-1} + 5^{n-1} \mid 3^n + 5^n$.*

Problem 146. *Prove that for every positive integer n, there is a positive integer X such that*

$$X,\ 2X,\ 3X,\ \ldots,\ nX$$

are all nontrivial perfect powers.

Problem 147. *Let a, b, c, d be positive integers with $ab = cd$. Prove that there exist positive integers p, q, r, s such that $a = pq, b = rs, c = pr, d = qs$.*

Problem 148. *Let a, b, c be positive integers such that $a^3 + b^3 = 2^c$. Prove that $a = b$.*

Result 149 (Schur's Theorem). *For any integer polynomial p, the set of primes that divide $p(x)$ for some x is infinite.*

Problem 150. *The sequence $\{a_i\}_1^\infty$ is defined by $a_1 = 1$ and $a_{n+1} = a_n^2 + 1$ for $n \geq 1$. Prove that there are infinitely many primes which divide some a_i.*

Problem 151. *We are given a positive integer $s \geq 2$. For each positive integer k, we define its twist k' as follows: write k as $as + b$, where a, b are non-negative integers and $b < s$, then $k' = bs + a$. For the positive integer n, consider the infinite sequence $d_1, d_2, \ldots$ where $d_1 = n$ and d_{i+1} is the twist of d_i for each positive integer i. Prove that this sequence contains 1 if and only if the remainder when n is divided by $s^2 - 1$ is either 1 or s.*

Problem 152. *Does one of the first $10^8 + 1$ Fibonacci numbers end with four zeroes?*

Problem 153. *For each prime p and positive integer k, find the least residues of $\binom{p-1}{k}$ and $\frac{1}{p}\binom{p}{k}$ in mod p.*

Problem 154. *Prove that the function $f(n) = \lfloor (1 + \sqrt{2})^n \rfloor$ alternates between even and odd integers.*

Problem 155. *Prove that for any positive integer n which is not a perfect square, there is a positive integer k such that*

$$n = \left\lfloor k + \sqrt{k} + \frac{1}{2} \right\rfloor.$$

Problem 156. *Given are positive integers a, b satisfying $a \geq 2b$. Does there exist a polynomial $P(x)$ of degree at least 1 with coefficients from the set $\{0, 1, 2, \ldots, b-1\}$ such that $P(b) \mid P(a)$?*

Problem 157. *Find all positive integers a for which $1! + 2! + \cdots + a!$ is a perfect cube.*

Problem 158. *Let $S(n)$ be the sum of the digits of n. Find $S(S(S(4444^{4444})))$.*

Problem 159. *Prove that the equation $y^2 = x^3 + 7$ has no integer solutions.*

Problem 160. *Prove that for any positive integer n we have $\sigma(n) \geq d(n)\sqrt{n}$.*

Problem 161. *Prove that there are infinitely many positive integers which are not the sum of a square and a prime.*

Problem 162. *Let m and c be integers. Prove that for any infinite sequence $a_1, a_2, \ldots$ of positive integers which contains every positive integer exactly once, there are integers x, y, k such that $x < y$ and $a_x + a_{x+1} + \cdots + a_y = mk + c$.*

Problem 163. *Let x be an irrational number, and let a and b be real numbers such that $0 \leq a < b \leq 1$. Prove that there is an integer n such that $a < \{nx\} < b$. Hence prove that there is a power of 2 whose decimal representation starts with 2023.*

Result 164. *Prove that if p is an odd prime that divides n^2+1 for some integer n, then $p \equiv 1 \pmod 4$.*

PROBLEM 165. *Prove that every positive integer is a sum of one or more numbers of the form 2^r3^s, where r and s are nonnegative integers and no summand divides another.*

PROBLEM 166. *Let a and b be positive integers such that $a \mid b^2 \mid a^3 \mid b^4 \mid \cdots$ Prove that $a = b$.*

PROBLEM 167. *Find all triples (x, y, z) of integers such that*

$$x^3 + 2y^3 + 4z^3 - 6xyz = 0.$$

PROBLEM 168. *Prove that for any positive integer c and any prime p, there is a positive integer x such that $x^x \equiv c \pmod{p}$.*

PROBLEM 169. *Let m and n be positive integers. Prove that*

$$m \mid \gcd(m, n)\binom{m}{n}.$$

PROBLEM 170. *Find all positive integers a, b, c such that $a! \times b! = a! + b! + c!$.*

PROBLEM 171. *Prove that any infinite sequence of integers in arithmetic progression has an infinite subsequence in geometric progression.*

PROBLEM 172. *Find all positive integers x, y such that $x^2 - 3xy + 2y^2 = 2023$.*

PROBLEM 173. *Prove that for any two distinct polynomials P and Q with coefficients in $\{0, 1, \ldots, 9\}$, either $P(-2) \neq Q(-2)$ or $P(-5) \neq Q(-5)$.*

PROBLEM 174. *Find all positive integers a, b, c such that $a \mid b + c,\ b \mid c + a,\ c \mid a + b$.*

PROBLEM 175. *Prove that $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+1} \rfloor$.*

PROBLEM 176. *Determine all integers $n \geq 2$ such that $\sqrt{n - a^2}$ is an integer which divides n, where a is the smallest prime divisor of n.*

PROBLEM 177. *Let $p > 3$ be prime. Define $m = (4^p - 1)/3$. Prove that $2^{m-1} \equiv 1 \pmod{m}$.*

PROBLEM 178. *Find all positive integers x, y, z such that $3^x + 4^y = 5^z$.*

PROBLEM 179. *Let m be a positive integer for which there exists a positive integer n such that mn is a perfect square and $m - n$ is prime. Prove that $4m = (m - n + 1)^2$.*

PROBLEM 180. *Find all primes p, q for which $pq \mid (5^p - 2^p)(5^q - 2^q)$.*

PROBLEM 181. *Find all positive integers n such that $1 + \lfloor \sqrt{n} \rfloor$ divides n.*

PROBLEM 182. *Find all pairs of positive integers x, y such that $y^2(x - 1) = x^5 - 1$.*

PROBLEM 183. *Let $n \geq 2$ be an integer and $P(x)$ be a polynomial with nonnegative integer coefficients satisfying $P(1) = 1$ and $x^n P(1/x) = P(x)$ for all x. Prove that there exist infinitely many pairs x, y of positive integers such that $x|P(y)$ and $y|P(x)$.*

PROBLEM 184. *Prove that there is an infinite set of positive integers such that the sum of any finite subset is not a perfect power.*

PROBLEM 185. *Find all primes* p *such that* $p^{2022} + p^{2023}$ *is a perfect square.*

PROBLEM 186. *Let* S *be a subset of the set of numbers* $\{1, 2, 3, \ldots, 2023\}$ *such that if* a, b *are in* S*, then* $23 \nmid a + b$*. What is the maximum possible size of* S*?*

PROBLEM 187. *Prove that there exists a strictly increasing sequence* $\{a_n\}_1^\infty$ *of positive integers such that for any* $k \geq 0$*, the sequence* $\{k + a_n\}$ *contains only finitely many primes.*

PROBLEM 188. *Prove that every positive integer has at least as many divisors which are 1 (mod 4) as divisors which are 3 (mod 4).*

RESULT 189. *If* $a,\ b,\ c,\ x$ *are integers such that* $ax^2 + bx + c = 0$ *then* $b^2 - 4ac$ *is a perfect square.*

PROBLEM 190. *Prove that the equation* $x^3 + 3 = 4y(y + 1)$ *has no integer solutions.*

PROBLEM 191. *Does there exist an infinite sequence of integers* $a_1, a_2, \ldots$ *such that* $\gcd(a_m, a_n) = 1 \iff |m - n| = 1$*?*

PROBLEM 192. *Find all triples of positive integers* x, y, z *such that* $x^3 + y^3 + z^3 - 3xyz$ *is prime.*

PROBLEM 193. *Prove that for each positive integer* n*, there are* n *consecutive positive integers, none of which is a prime power.*

PROBLEM 194. *Find all functions* $f : \mathbb{N} \to \mathbb{N}$ *satisfying* $f(n + f(n)) = f(n)$ *for all* n *such that 1 is in the range of* f*.*

PROBLEM 195. *Show that* 30 *is the greatest common divisor of all numbers of the form* $2^{3n} + 5^{n+1} + 3^{n+2}$*, where* $n \in \mathbb{N}$*.*

RESULT 196 (Pythagorean triples). *If* $a,\ b,\ c$ *are positive integers such that* $a^2 + b^2 = c^2$*, then there exist integers* d, x, y *such that* $\{a, b\} = \{d(x^2 - y^2), 2dxy\}$ *and* $c = d(x^2 + y^2)$*.*

PROBLEM 197. *Prove that for every positive integer* n*, there is a set* S *of* n *distinct positive integers such that every subset of* S *has a geometric mean which is a positive integer.*

PROBLEM 198. *Prove that every arithmetic progression* $\{a + nb\}_{n=1}^\infty$ *where* $\gcd(a, b) = 1$ *has infinitely many terms which are not divisible by any perfect square larger than* 1*.*

PROBLEM 199. *Prove that for every positive integer* n *there is a number divisible by* n *consisting of only* 1*s and* 0*s.*

PROBLEM 200. *Prove that if* n *is not a multiple of* 5*, there is a number divisible by* n *consisting of only* 1*s and* 2*s.*

PROBLEM 201. *Prove that if* p *is prime, then* $2^p + 3^p$ *is not a nontrivial perfect power.*

PROBLEM 202. *Let* $P(x)$ *and* $Q(x)$ *be polynomials with integer coefficients such that the leading coefficient of* $P(x)$ *is 1. Suppose that* $P(n)^n$ *divides* $Q(n)^{n+1}$ *for infinitely many positive integers* n*. Prove that* $P(n)$ *divides* $Q(n)$ *for infinitely many positive integers* n*.*

PROBLEM 203. *Let f be a function defined on the nonnegative integers such that $f(2x) = 2f(x)$, $f(4x+1) = 4f(x)+3$, and $f(4x-1) = 2f(2x-1)-1$. Prove that f is injective.*

PROBLEM 204. *Prove that for every positive integer n, there are infinitely many terms of the Fibonacci sequence which are divisible by n.*

PROBLEM 205. *Find all pairs of positive integers x, y such that $x^2 - y! = 2001$.*

PROBLEM 206. *Prove that if m and n are natural numbers, then $3^m + 3^n + 1$ is not a perfect square.*

PROBLEM 207. *Let n be a positive integer. Calculate $\gcd((n-1)! + 1, n!)$.*

PROBLEM 208. *Let a, b be odd positive integers. Define the sequence c_n by choosing $c_1 = a, c_2 = b$ and for each $i > 2$ letting c_i be the largest odd divisor of $c_{i-1} + c_{i-2}$. Prove that this sequence is eventually constant.*

PROBLEM 209. *Prove that there does not exist a function $f : \mathbb{N} \to \mathbb{N}$ such that for any distinct positive integers i and j, $\gcd(f(i) + j, f(j) + i) = 1$.*

PROBLEM 210. *Find all pairs a, b of positive integers such that $2017^a = b^6 - 32b + 1$.*

PROBLEM 211. *Do there exist primes x, y, z such that $x^2 + y^3 = z^4$?*

PROBLEM 212. *The cells in a jail are numbered from 1 to 100, and there are 100 buttons also numbered from 1 to 100. For each i, the ith button opens a closed cell and closes an open cell, affecting only the multiples of i.*

For example, if the 47th cell is open and the 94th cell is closed, then pressing the 47th button will close the 47th cell and open the 94th cell.

Initially all cells are closed. The warden presses the first button, then the second, and so on, for all 100 buttons. Which cells are open at the end?

PROBLEM 213. *Find all pairs of integers x, y such that $x^4 + 2x^2y + y^3 = 0$.*

PROBLEM 214. *Find all triples a, b, c of positive integers such that $a \mid bc-1$, $b \mid ca-1$ and $c \mid ab-1$.*

PROBLEM 215. *Do there exist two quadratics $ax^2 + bx + c$ and $(a+1)x^2 + (b+1)x + (c+1)$ which both have two integer roots?*

PROBLEM 216. *Find all primes p and q such that $p + q = (p-q)^3$.*

PROBLEM 217. *Find all integers a, b such that $a^3 + (a+1)^3 + \cdots + (a+6)^3 = b^4 + 1$.*

PROBLEM 218. *Define a sequence by $a_1 = n$ and $a_{i+1} = \frac{a_i(a_i-1)}{2}$ for each $i \geq 1$. For which positive integers n are all values of a_i odd?*

PROBLEM 219. *Compute the remainder when 2023^{2022} is divided by 2021.*

PROBLEM 220. *Suppose $a_1, a_2, \ldots$ is an infinite strictly increasing sequence of positive integers and $p_1, p_2, \ldots$ is a sequence of distinct primes such that $p_n \mid a_n$ for all $n \geq 1$. It turns out that $a_{n+1} - a_n = p_{n+1} - p_n$ for all $n \geq 1$. Prove that the sequence $\{a_n\}$ consists only of prime numbers.*

PROBLEM 221. *Find all monotonically increasing functions $f : \mathbb{N} \to \mathbb{Z}_{\geq 0}$ such that $f(mn) = f(m) + f(n)$ for all nonnegative integers m and n.*

PROBLEM 222. *Let n be a positive integer. Define a sequence by letting $a_1 = n$, and for each $i > 1$ choosing a_i such that $0 \leq a_i < i$ and $\frac{a_1+\cdots+a_i}{i}$ is an integer. Prove that this sequence is eventually constant.*

PROBLEM 223. *Given are positive integers $n > 20$ and $k > 1$, such that k^2 divides n. Prove that there exist positive integers a, b, c such that $n = ab + bc + ca$.*

RESULT 224 (Farey sequences). *Let n be a fixed positive integer. Let $\frac{a_1}{b_1}, \dots, \frac{a_k}{b_k}$ be the rational numbers between 0 and 1 inclusive with denominators at most n, written in increasing order and lowest terms.*

- *For each i, $a_{i+1}b_i - a_i b_{i+1} = 1$.*
- *The rational number x with smallest denominator such that $\frac{a_i}{b_i} < x < \frac{a_{i+1}}{b_{i+1}}$ is $\frac{a_i+a_{i+1}}{b_i+b_{i+1}}$.*

CHAPTER 3

Advanced

3.1. Algebra

3.2. Combinatorics

3.3. Geometry

3.4. Number Theory

3.4.1. Arithmetic functions. A function $f : \mathbb{N} \to \mathbb{R}$ is called multiplicative if for any coprime positive integers a and b, we have

$$f(a)f(b) = f(ab).$$

It's called completely multiplicative if this equation holds for *any* positive integers a and b.

- Prove that the values at the primes of a completely multiplicative function completely define the function (unless these values are all 0, in which case $f(1)$ can be 0 or 1).
- Prove that the values at prime powers of a multiplicative function completely define it.
- Find a formula for the number of solutions $1 \le x \le n$ of $n \mid x^2 - 1$.

Problems:

- Prove that $\sigma(n) < n\sqrt{2d(n)}$ for all positive integers n.
- Find all completely multiplicative functions $f : \mathbb{N} \to \mathbb{N}$ such that for all $a, b \in \mathbb{N}$, at least two of $f(a), f(b), f(a+b)$ are equal.

3.4.2. Bounding.

Result 225. *For any $c > 1$, we have $c \ll \log n \ll n^c \ll c^n \ll n! \ll n^n$.*

Result 226. *A concave down function on a closed interval achieves its minimum at an endpoint of the interval.*

Result 227 (Stirling's Approximation). $\left(\frac{n}{e}\right)^n < n! < n\left(\frac{n}{e}\right)^n$.

Result 228 (Bernoulli's Inequality). *For $r \ge 1$ and $x \ge -1$ we have $(1+x)^r \ge 1 + rx$.*

Problem 229. *Find all triples of positive integers a, b, c such that $a^2 + b + c = abc$.*

3.4.3. Descent. The following is something of a Fundamental Theorem of Vieta Jumping. Unfortunately, it doesn't seem to be well-known enough that you can use it without proof, so you should know the proof well enough that you can reproduce it in contest if necessary.

RESULT 230. *Let a, b, k be nonnegative integers such that* $\gcd(a, b) = 1$*, and let* $t = a^2 + b^2 - kab$*. If* $|t - 2| < k$ *then* $t = 1$*.*

Another important application of descent is the Pell equation:

RESULT 231. *Let d be a positive integer which is not a perfect square. There exist positive integers x_0, y_0 such that $x_0^2 - dy_0^2 = 1$ and for any pair x, y of positive integers satisfying $x^2 - dy^2 = 1$, there is a positive integer k satisfying*

$$x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^k.$$

There is an analogous version for $x^2 - dy^2 = -1$:

RESULT 232. *Let d be a positive integer which is not a perfect square. There exist positive integers x_0, y_0 such that for any pair x, y of positive integers satisfying $x^2 - dy^2 = -1$, there is an odd positive integer k satisfying*

$$x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^k.$$

Note that in this case solutions to the equation don't necessarily exist, e.g. by a mod 3 argument.

- Prove that there are infinitely many triples (a, b, c) of positive integers in arithmetic progression such that $ab + 1$, $bc + 1$ and $ca + 1$ are all perfect squares.
- Find all solutions in integers to $x^2 + y^2 + z^2 = 2xyz$.
- Find all positive integers n such that

$$\sqrt{\frac{7^n + 1}{2}}$$

  is prime.

3.4.4. Density Arguments. The technique here is to estimate how many objects (usually numbers or expressions) have a specific property and lie in a specific range. The aim is usually to apply pigeonhole.

Perhaps some examples will be clearer:

RESULT 233 (Thue's Lemma). *Let $n > 1$ be an integer, and let a be an integer coprime to n. There exist integers x, y with $0 < |x| < \sqrt{n}$, $0 < |y| < \sqrt{n}$ and $ay \equiv x \pmod{n}$.*

- Is there a positive integer which can be written as the sum of 2023 distinct 2022nd powers in at least 2021 different ways?
- Prove that every positive integer is the root of a polynomial all of whose coefficients are of the form $2^a - 2^b$ for positive integers a and b.

3.4.5. Largest exponent notation. Let p be a prime and let r be a rational number. We let $\nu_p(r)$ be the exponent of p in the prime factorisation of r.

- $\nu_p(a + b) \geq \min(\nu_p(a), \nu_p(b))$.
- If $\nu_p(a + b) > \min(\nu_p(a), \nu_p(b))$ then $\nu_p(a) = \nu_p(b)$.
- If a is a positive integer, then $\nu_p(a) \leq \log_p(a)$.
- Legendre's Formula:

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - s_p(n)}{p - 1} < \frac{n}{p - 1}.$$

- Let p be an odd prime, and let a and b be integers such that $p \mid a - b$ but $p \nmid a$. Let k be a positive integer. Then, $\nu_p\left(a^k - b^k\right) = \nu_p(a - b) + \nu_p(k)$.
- Let a and b be odd integers, and let k be a positive integer. If k is even, we have $\nu_2(a^k - b^k) = \nu_2(a - b) + \nu_2(a + b) + \nu_2(k) - 1$. If k is odd, we have $\nu_2(a^k - b^k) = \nu_2(a - b)$.
- Prove that for all positive integers n,
$$\binom{2n}{n} \mid \operatorname{lcm}(1, 2, \ldots, 2n).$$
- Let a, b, c be positive integers such that $c \mid a^c - b^c$. Prove that $c(a - b) \mid a^c - b^c$.
- Find all positive integers n and k such that
$$k! = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}).$$

3.4.6. Orders. The *order* of an invertible element a of $\mathbb{Z}_n$, denoted $\operatorname{ord}_n(a)$, is the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$.

If $\operatorname{ord}_n(a) = |Z_n^*|$, then a is said to be a *generator* mod n.

- $a^k \equiv 1 \pmod{n} \iff \operatorname{ord}_n(a) \mid k$.
- $\operatorname{ord}_n(a) \mid \varphi(n)$.
- If p is prime and $q \mid 2^p - 1$, then $q > p$.
- Every prime factor of $2^{2^n} + 1$ is congruent to 1 mod 2^{n+1}.
- If g is a generator mod n, then the least residues of $\{g^1, g^2, \ldots, g^{\varphi(n)}\}$ are $\mathbb{Z}_n^*$.
- If g is a generator mod n, and $\varphi(n) = 2k$, then
$$g^k \equiv -1 \pmod{n}.$$
- There are either 0 or $\varphi(\varphi(n))$ generators mod n.
- If $a \mid \varphi(n)$ and there exists a generator mod n, then there are $\varphi(a)$ residues x mod n such that $\operatorname{ord}_n(x) = a$.
- If there exists a generator mod n, then the product of the elements of $\mathbb{Z}_n^*$ is -1 mod n.
- For any positive integer $n < p - 1$,
$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod{p}.$$
- Assume there exists a generator mod n. An element $x \in \mathbb{Z}_n^*$ can be written as y^k for $y \in \mathbb{Z}_n^*$ iff $\operatorname{ord}_p(x) \gcd(\varphi(n), k) \mid \varphi(n)$.

Result 234. *Let p be an odd prime.*

- *There exists a generator mod p.*
- *There exists a generator mod p^k for any positive integer k.*
- *There exists a generator mod $2p^k$ for any positive integer k.*
- *There exists a generator mod 2^k iff $k \leq 2$.*
- *If $n = xy$, where x and y are coprime and larger than 2, then there does not exist a generator mod n.*

- Let $p > 10$ be a prime. Prove that there are positive integers m, n with $m + n < p$ such that p divides $5^m 7^n - 1$.
- Find all positive integers n such that $n \mid 2^n - 1$.

- Prove that if $\sigma(n) = 2n + 1$, then n is a perfect square.
- Let p be a prime. Find all nonempty sets S of residues mod p such that if the least residues of a and b are not in S, then
$$\prod_{i \in S}(a - i) \equiv \prod_{i \in S}(b - i) \pmod{p}.$$

3.4.7. Polynomials.

Result 235 (Hensel's Lemma). *Let P be an integer polynomial. Let r be an integer such that $P(r) \equiv 0 \pmod{n}$ but $\gcd(P'(r), n) = 1$. For any positive integer m, there is a unique s mod n^m such that $s \equiv r \pmod{n}$ and $P(s) \equiv 0 \pmod{n^m}$.*

- Let p be prime and let a and b be positive integers such that $p \nmid b$. Prove that there exists a positive integer n such that $p^a \mid n^n - b$.
- Let P be a nonconstant polynomial with integer coefficients. Prove that for any integer m there exist an integer n and a prime p such that $p^m \mid P(n)$.

An integer polynomial is *primitive* if its coefficients have gcd 1.

- Every nonzero rational polynomial has exactly one primitive multiple with positive leading coefficient.
- (Gauss' Lemma) The product of two primitive polynomials is primitive.
- (Gauss' Lemma, alternate form) If an integer polynomial is the product of two nonconstant rational polynomials then it is the product of two nonconstant integer polynomials.

An integer polynomial is *irreducible* over $\mathbb{Z}$ (for the rest of this handout, I'll shorten this to irreducible) if it is not the product of two nonconstant integer polynomials.

Usually, to prove irreducibility you will assume for contradiction that the polynomial is reducible. Modular arithmetic arguments on the coefficients are often useful.

- (Unique factorisation) Every integer polynomial can be factorised into a product of a constant and primitive irreducible integer polynomials. This factorisation is unique up to the permutation and sign of these polynomials.
- (Eisenstein's Criterion) If there exists a prime q such that $q^2 \nmid a_0$, $q \mid a_i$ for each i from 0 to $n - 1$, and $q \nmid a_n$, then p is irreducible.
- If an integer polynomial is irreducible mod n for any positive integer n, then it is irreducible over $\mathbb{Z}$.

Let p be prime.

- Prove that unique factorisation holds for polynomials mod p. (This is not true for all integers — for instance, $(x-1)^2 \equiv (x-3)^2 \pmod{4}$.)
- Prove that for every function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ there is a unique polynomial P in $\mathbb{Z}_p$ of degree less than $p - 1$ such that $f(x) = P(x)$ for each $x \in \mathbb{Z}_p$.
- Let g be a generator mod p, and let $ab = p - 1$. Prove that
$$\prod_{i=1}^{a}(x - g^{bi}) \equiv x^a - 1 \pmod{p}.$$
What does this tell us about the roots of the cyclotomic polynomials in mod p?

- Consider all $\binom{p-1}{k}$ products of k elements of $\mathbb{Z}_p$. Prove that their sum is divisible by p.
- For any positive integer $n < p-1$, prove that
$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod{p}.$$

Problems:

- Prove that if p is prime, then $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible.
- Find all integer polynomials p such that
  - $p(n) > n$ for all positive integers n, and
  - for each positive integer n there is a positive integer k such that $p^{(k)}(1)$ (p repeated k times) is divisible by n.
- Let p be prime. Find the least residue of the product of $(4-x)$ mod p, where x runs over all residues mod p except the quadratic residues.

3.4.8. Quadratic Residues. If x can be written as y^2 for $y \in \mathbb{Z}_n^*$, then we say that x is a *quadratic residue (QR)* mod n. Note that 0 is not a QR mod n.

Prove that x is a QR mod n iff both

- $x \equiv 1 \pmod{\gcd(8, n)}$, and
- for each odd prime $p \mid n$, x is a QR mod p.

Hence, we now restrict ourselves to considering QRs mod p. Define the *Jacobi symbol*
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ is a QR mod } p \\ -1 & \text{otherwise} \end{cases}.$$

- (Euler's criterion) Prove that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Hence, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
- (Gauss' Lemma) Let $a \in \mathbb{Z}_p^*$, and let $S \subseteq \mathbb{Z}_p^*$ such that $x \in S \iff -x \notin S$. Let $T = \{ay : y \in S\}$. Then $\left(\frac{a}{p}\right) = (-1)^{|T \setminus S|}$.
- Find $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$.

Finally, there is quadratic reciprocity. Let p and q be distinct odd primes. Then,
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Problems:

- Let p be an odd prime and let a be an integer with $\gcd(a, p) = 1$. Prove that
$$\sum_{n=1}^{p} \left(\frac{n^2+a}{p}\right) = -1.$$
- Prove that for any prime p and positive integer a with $p \nmid a$ there are at least $p-1$ solutions in $\mathbb{Z}_p$ to $x^2 + y^2 \equiv a \pmod{p}$.
- If $p > 3$ is a prime such that $\varphi(p-1) > \frac{p-1}{3}$, prove that there are two consecutive generators mod p.

3.4.9. Existence proofs. Apart from density arguments, existence proofs in number theory usually rely on actually constructing the object using theorems about the existence of numbers satisfying certain properties. These theorems include Results 2, 78, 107, 149, 231, 235, 234 and 236.

Here are a few other results that may be helpful, but whose proofs are outside the scope of Olympiad maths:

- (Dirichlet's Theorem) For any coprime positive integers a and b, there are infinitely many positive integers k such that $a + bk$ is prime.
- (Bertrand's Postulate) For any positive integer n, there is a prime in $(n, 2n]$.
- (Zsigmondy's Theorem) If $a > b > 0$ are coprime integers, then for any integer $n \geq 3$ there is a prime number p that divides $a^n - b^n$ and does not divide $a^k - b^k$ for any positive integer $k < n$, unless $(a, b, n) = (2, 1, 6)$. The same holds for $a^n + b^n$ with the exception $2^3 + 1^3 = 9$.

Remember properties like Fermat/Euler and Wilson that allow you to control stuff. CRT is especially useful because it allows you to combine a bunch of modular conditions into one. Most of the time Dirichlet then gives you a prime for free.

- Prove that if n is not a multiple of 4, then there are positive integers a and b such that $n \mid a^2 + b^2 + 1$.
- Prove that there exist infinitely many positive integers n such that $n^2+1 \mid n!$.
- Prove that there are infinitely many positive integers n such that $d(n)$ and $\varphi(n)$ are both squares.
- Prove that there exists a positive integer m such that the equation $\varphi(n) = m$ has at least 2023 solutions n.

3.4.10. Additive number theory.

- Let n be a positive integer and $\{A, B, C\}$ a partition of $(1, 2, 3, \ldots, 3n)$ such that $|A| = |B| = |C| = n$. Prove that there exist $x \in A, y \in B, z \in C$ such that one of x, y, z is the sum of the other two.
- Suppose that every integer has been given one of the colors red, blue, green or yellow. Let x and y be odd integers so that $|x| \neq |y|$. Show that there are two integers of the same color whose difference has one of the following values: x, y, $(x + y)$ or $(x - y)$.
- Let k, m, n be integers satisfying $1 < n \leq m - 1 \leq k$. Determine the maximum size of a subset S of the set $\{1, 2, \ldots, k\}$ such that no n distinct elements of S add up to m.
- A set S of distinct integers is called sum-free if there does not exist a triple $\{x, y, z\}$ of integers in S such that $x + y = z$. Show that for any set X of distinct integers, X has a sum-free subset Y such that $|Y| > |X|/3$.
- Prove that there exists a four-coloring of the set $M = \{1, 2, \ldots, 1987\}$ such that any arithmetic progression with 10 terms in the set M is not monochro- matic.

3.4.11. Build a graph.

- Fifty numbers are chosen from the set $\{1, 2, \ldots, 99\}$, no two of which sum to 99 or 100. Prove that the numbers must be $50, 51, \ldots, 99$.

- Let p be a prime, and let $a_1, \dots, a_p$ be integers. Show that there exists an integer k such that the numbers
$$a_1 + k, a_2 + 2k, \dots, a_p + pk$$
produce at least $\frac{1}{2}p$ distinct remainders upon division by p.
- An international society has its members from six different countries. The list of members has 1978 names, numbered $1, 2, \dots, 1978$. Prove that there is at least one member whose number is the sum of the numbers of two (not necessarily distinct) members from his own country.
- A set of positive integers is called *fragrant* if it contains at least two elements and each of its elements has a prime factor in common with at least one of the other elements. Let $P(n) = n^2 + n + 1$. What is the least possible positive integer value of b such that there exists a non-negative integer a for which the set $\{P(a+1), P(a+2), \dots, P(a+b)\}$ is fragrant?
- The Fibonacci numbers $F_0, F_1, F_2, ...$ are defined inductively by $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. Given an integer $n \geq 2$, determine the smallest size of a set S of integers such that for every $k = 2, 3, \dots, n$ there exist some $x, y \in S$ such that $x - y = F_k$.
- There are $4n$ pebbles of weights $1, 2, 3, \dots, 4n$. Each pebble is coloured in one of n colours and there are four pebbles of each colour. Show that we can arrange the pebbles into two piles so that the following two conditions are both satisfied:
  - The total weights of both piles are the same.
  - Each pile contains two pebbles of each colour.
- Let k, m, n be integers satisfying $1 < n \leq m - 1 \leq k$. Determine the maximum size of a subset S of the set $\{1, 2, \dots, k\}$ such that no n distinct elements of S add up to m.
- Let n be an even positive integer. Show that there is a permutation $(x_1, x_2, \dots, x_n)$ of $(1, 2, \dots, n)$ such that for every $i \in (1, 2, \dots, n)$, the number x_{i+1} is one of the numbers $2x_i, 2x_i - 1, 2x_i - n, 2x_i - n - 1$. Here we use the cyclic subscript convention, so that x_{n+1} means x_1.

3.4.12. Problems. Less than half of the problems here require the use of the theory developed in this chapter, which is testament to how rare it is that this theory shows up in contest.

Result 236 (Fermat's Christmas Theorem). *There are positive integers a and b such that $a^2 + b^2 = n$ iff all primes which are $3 \pmod 4$ have even exponents in the prime factorisation of n. If n is prime, then such a representation is unique.*

- Let p and q be primes. Prove that there is an integer x such that $(x+1)^p \equiv x^p \pmod q$ if and only if $q \equiv 1 \pmod p$.
- Find all pairs of positive integers x, y such that $1 + 2^x + 2^{2x} = y^2$.
- Let p be an odd prime. Prove that
$$p^2 \mid 1^p + 2^p + \cdots + p^p.$$
- Four positive integers x, y, z, t satisfy $xy - zt = x + y = z + t$. Is it possible that xy and zt are both perfect squares?
- Let $P(x)$ and $Q(x)$ be polynomials whose coefficients are all equal to 1 or 7. If $P(x)$ divides $Q(x)$, prove that $1 + \deg P(x)$ divides $1 + \deg Q(x)$.

- Let a and b be positive integers such that $a^n + n \mid b^n + n$ for all positive integers n. Prove that $a = b$.
- Assume that g is a generator mod p such that $p \mid g^2 - g - 1$. Prove that if $p \equiv 3 \pmod 4$, then $g - 1$ and $g - 2$ are also generators mod p.
- Prove that for all positive integers $a > 1$ and n we have $n \mid \varphi(a^n - 1)$.
- Determine all positive integers M such that the sequence $a_0, a_1, a_2, \ldots$ defined by
$$a_0 = M + \frac{1}{2} \qquad \text{and} \qquad a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{for } k = 0, 1, 2, \ldots$$
contains at least one integer term.
- Let r be an irrational root of a polynomial $P(x)$ of degree d with integer coefficients. Prove that there is a real number C such that for any integer q we have $\{qr\} \geq \frac{C}{q^{d-1}}$.
- Find all positive integers k for which the following statement is true: if p is an integer polynomial such that $0 \leq p(i) \leq k$ for each integer $0 \leq i \leq k+1$, then all of these $p(i)$s are equal.
- Let n and z be integers greater than 1 such that $\gcd(n, z) = 1$. Prove that there is some nonnegative integer $i < n$ such that $1 + z + z^2 + \cdots + z^i$ is divisible by n.
- Find the minimum possible value of $m + n$, where m and n are distinct positive integers such that $1000 \mid 1978^m - 1978^n$.
- Prove that for some constant $C > 0$, the following statement holds:
  Let $m \geq 2$ be an integer, A a finite set of integers (not necessarily positive), and $B_1, B_2, \ldots, B_m$ subsets of A. Suppose that for every $k = 1, 2, \ldots, m$, the sum of the elements of B_k is 2^k. Then A contains at least $\frac{Cm}{\log_2 m}$ elements.
- Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that, for all integers a, b, c satsfying $a + b + c = 0$, we have
$$f(a)^2 + f(b)^2 + f(c)^2 = 2f(a)f(b) + 2f(a)f(c) + 2f(b)f(c).$$
- Let p be an integer polynomial and let a be an integer such that
$$p(p(\cdots(p(a))\cdots)) = a.$$
Prove that $p(p(a)) = a$.
- Does there exist an integer $n > 1$ such that all powers of n are base-10 palindromes?
- Given three distinct natural numbers a, b, c, show that
$$\gcd(ab + 1, bc + 1, ca + 1) \leq \frac{a + b + c}{3}.$$
- Find all integers x, y such that $(x^2 + y)(x + y^2) = (x - y)^3$.
- Prove that if $5 \nmid a$, then $x^5 - x + a$ is irreducible.
- Find all integers n such that $n^2 + 1$ divides $n^3 + n^2 - n - 15$.
- Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(f(m)f(n)) = mn$ for all positive integers m and n.
- Find all pairs x, y of positive integers such that $3^x - 8^y = 2xy + 1$.
- An infinite arithmetic progression contains a perfect ath power and a perfect bth power. Prove that it contains a perfect $\operatorname{lcm}(a, b)$th power.

- Let p be an odd prime and let m and n be natural numbers not divisible by p. Prove that if there is some integer s such that $p \mid m^{2^s} + n^{2^s}$, then $p \equiv 1 \pmod{2^{s+1}}$.
- Let $P(n)$ be the product of the digits of a positive integer n. Let n_1 be a positive integer, and define $n_{i+1} = n_i + P(n_i)$ for each $i \geq 1$. Prove that this sequence is eventually constant.
- Let p be an odd prime and r an odd natural number. Show that $pr + 1$ does not divide $p^p - 1$.
- For which positive integers r and s does there exist a positive integer n such that nr and ns have the same number of divisors?
- Let a and b be positive integers. Prove that there are infinitely many positive integers n such that $n^b - 1 \nmid a^n + 1$.
- Find all integer polynomials p such that $n \mid p(2^n)$ for all positive integers n.
- Find all pairs of positive integers x, y such that $x^3 - y^3 = xy + 61$.
- Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that for each positive integer n, $f(n) \mid n^3$ and $\displaystyle\sum_{i=1}^{n} f(i)$ is a perfect square.
- Does there exist a strictly increasing function $f : \mathbb{N} \to \mathbb{N}$ such that $f(1) = 2$ and $f(f(n)) = f(n) + n$ for all positive integers n?
- Prove that if there are two terms of an arithmetic progression which are coprime integers, then there is an infinite subset of that progression all of whose elements are coprime integers.
- We call a 5-tuple of integers *arrangeable* if its elements can be labelled a, b, c, d, e in some order such that $a - b + c - d + e = 0$. Determine all 2022-tuples of integers such that if we place them in order around a circle, then any 5-tuple of numbers in consecutive positions is arrangeable.
- Let a, b, c be pairwise coprime positive integers. Prove that there exist infinitely many triples x, y, z of distinct positive integers such that $x^a + y^b = z^c$.
- Let p be a prime with $p > 3$. Prove that there are positive integers $a < b < \sqrt{p}$ such that $p - b^2 \mid p - a^2$.
- Do there exist distinct prime numbers a, b, c such that
$$a \mid bc + b + c,\ \ b \mid ac + a + c,\ \ c \mid ab + a + b?$$
- Let x, y, z be rational numbers such that $xy,\ yz,\ zx,\ x + y + z$ are all integers.
    Prove that $x,\ y,\ z$ are all integers.
- Find all primes p, q, r such that $p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q - 1$.
- Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.
- Let p be a polynomial of dgree d. Find a linear equation that the values $p(0), p(1), \ldots, p(d + 1)$ always satisfy.
- Let k and n be positive integers such that n is odd. Prove that there is an integer a such that $a^{32} \equiv (n + 1)^3 \pmod{n^k}$.
- Find all functions $f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ such that $f(f(f(n))) = f(n+1) + 1$ for all $n \in \mathbb{Z}_{\geq 0}$.

- Find all functions $f : \mathbb{N} \to \mathbb{N}$ satisfying
$$f(n) + f(n+1) = f(n+2)f(n+3) - 2023$$
for all $n \in \mathbb{N}$.
- Prove that for any nonnegative integer n, the number $7^{7^n}+1$ is the product of at least $2n+3$ (not necessarily distinct) primes.
- Find all triples a, b, c of positive integers such that $a^3 + b^3 + c^3 = (abc)^2$.
- Find all positive integers n such that $n \mid 2^{n-1} + 1$.
- Find all positive integer solutions to $3^x + 4^y = 5^z$.
- Let n and k be positive integers. Assume that for each positive integer m, there exists a positive integer a such that $a^k \equiv n \pmod{m}$. Prove that n is a perfect kth power.
- Let a and b be two positive integers. Prove that
$$a^2 + \left\lceil \frac{4a^2}{b} \right\rceil$$
is not a square.
- Prove that there exist 2023 distinct positive integers such that each of them divides the sum of the rest.
- Let $s(n)$ be the sum of the digits of n. Prove that for each positive integer k there exists a positive integer n such that $n + s(n)$ equals either k or $k+1$.
- Find all positive integers n that satisfy the following property: for all positive integers m, relatively prime to n, we have $2n^2$ divides $m^n - 1$.
- Find all natural numbers n such that $n^2 \mid 2^n + 1$.
- What is the smallest positive integer n for which there exist positive integers $x_1, x_2, \ldots, x_n$ such that
$$x_1^3 + x_2^3 + \cdots + x_n^3 = 2002^{2002}?$$
- Prove that there are infinitely many pairs a and b of perfect squares such that they have the same number of digits in decimal, and their concatenation is also a square.
- Let $n > 1$ be an odd positive integer and let S be the set of integers x, with $1 \le x \le n$, such that both x and $x+1$ are coprime to n. Find the product of the elements of S mod n.
- Is there a sequence $a_1, \ldots$ of primes such that for each i we have $10a_i \le a_{i+1} < 10a_i + 9$?
- Let $a_1, a_2, a_3, \ldots$ be a sequence of integers, such that for any positive integers n and k, the quantity
$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$
is always the square of an integer. Prove that all a_is are equal.
- Let $p > 3$ be a prime and let a, b, c be integers with $a \neq 0$. Suppose that $ax^2 + bx + c$ is a perfect square for p consecutive integers x. Prove that $p \mid b^2 - 4ac$.
- Prove that all terms of the sequence $a_1 = a_2 = a_3 = 1$, $a_{n+1} = (1 + a_{n-1}a_n)/a_{n+2}$ are integers.
- Let a be a positive integer such that $4(a^n + 1)$ is a perfect cube for all positive integers n. Prove that $a = 1$.

- Let $n > 1$ be a positive integer and let p be a prime. Given that $n \mid p-1$ and $p \mid n^3 - 1$, prove that $4p - 3$ is a perfect square.
- Define
$$q(n) = \left\lfloor \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rfloor.$$
Determine all positive integers n for which $q(n) > q(n+1)$.
- Find all pairs of positive integers a, b such that
$$b^2 - a \mid a^2 + b \quad \text{and} \quad a^2 - b \mid b^2 + a.$$
- Is there a function $f : \mathbb{N} \to \mathbb{N}$ of positive integers such that $\gcd(a_m, a_n) = 1 \iff |m - n| = 1$?
- Show that for any fixed integers n and a, the sequence $a, a^a, a^{a^a}, \ldots$ is eventually constant mod n.
- Prove that there are infinitely many pairs of positive integers a, b such that $a \mid b^2 + 1$ and $b \mid a^2 + 1$.
- Let $k = 2^{2^n} + 1$ for some positive integer n. Prove that k is prime if and only if $k \mid 3^{(k-1)/2} + 1$.
- Let P be a polynomial of degree larger than 1 with integer coefficients. Prove that there are infinitely many positive integers which cannot be written in the form $P(x+1) + P(x+2) + \cdots + P(x+k)$ for positive integers x and k.
- Let $b \geq 5$ be a fixed positive integer. A positive integer is called a base-b palindrome if it reads the same forwards as backwards when written in base b.

  Prove that there are infinitely many pairs (x, y) of distinct perfect squares such that for any base-b palindrome p, we have $(x-p)(y-p) > 0$.
- Prove that if a sequence $\{a_n\}_0^\infty$ of nonnegative integers satisfies $a_0 = 0$ and $a_n = n - a_{a_n}$ for all n, then $a_{n+2} > a_n$ for all n.
- Let S be the set of ordered pairs of integers. We say that two elements (a, b) and (c, d) of S are k-friends if there is an element (e, f) of S such that the area of the triangle formed by these three points is k. Find the smallest positive integer k such that there exists a set of 200 elements of S such that any pair of them are k-friends.
- Given an integer $k \geq 2$, determine all functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(x_1)! + f(x_2)! + \cdots f(x_k)!$ is divisible by $x_1! + x_2! + \cdots x_k!$ for all positive integers $x_1, x_2, \cdots x_k$.
- Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(n+1) > f(f(n))$ for all positive integers n.
- Find all positive integers k such that for all positive integers n, there exist a prime p and positive integers x and y for which $\gcd(x, y) = 1$ and $p^n \mid \frac{x^k - y^k}{x - y}$.
- Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $m^2 + f(n) \mid mf(m) + n$ for all positive integers m and n.
- Let x be an irrational number. Prove that there are infinitely many positive integers n such that $\{nx\} < \frac{1}{n}$.
- Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

- Let $p \geq 7$ be prime. Prove that for any integer n there are integers a and b, both not divisible by p, such that $p \mid a^2 - b^2 - n$.
- Given a positive integer k, show that there exists a prime p such that one can choose distinct integers $a_1, a_2, \ldots, a_{k+3} \in \{1, 2, \ldots, p-1\}$ such that p divides $a_i a_{i+1} a_{i+2} a_{i+3} - i$ for all $i = 1, 2, \ldots, k$.
- Find all completely multiplicative functions $f : \mathbb{N} \to \mathbb{Z}$ such that for all $a, b \in \mathbb{N}$, at least two of $f(a), f(b), f(a+b)$ are equal.
- Let n be a positive integer, and let S be a set of n positive integers all at most n^2. Prove that there is a set T of n positive integers such that the set $\{s + t : s \in S, t \in T\}$ covers at least half of the residues mod n^2.
- Let a, b, c be integers such that $a/b + b/c + c/a$ and $a/c + c/b + b/a$ are both integers. Prove that $|a| = |b| = |c|$.
- Let a, b, n be positive integers such that $a > b > 1$ and b is odd. If $b^n \mid a^n - 1$, prove that $na^b > 3^n$.
- Let x and y be positive integers and let p be prime. Assume there are coprime positive integers m and n such that $x^m \equiv y^n \pmod{p}$. Prove that there is a unique positive integer z with $0 \leq z < p$ such that
$$x \equiv z^n \pmod{p}, \qquad y \equiv z^m \pmod{p}.$$
- Find all positive integers x, y, n such that $\gcd(x, n+1) = 1$ and $x^n + 1 = y^{n+1}$.
- Prove that every positive integer can be uniquely represented as a sum of one or more Fibonacci numbers such that the sum does not include two consecutive Fibonacci numbers.
- Let n and k be positive integers such that $\varphi^k(n) = 1$ (that is, φ iterated k times). Prove that $n \leq 3^k$.
- Find all pairs of positive integers x, y such that $1 + 2^x + 2^{2x+1} = y^2$.
- Find all pairs of positive integers x, p such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.
- Find all pairs of positive integers x, y such that $xy^2 + y + 7 \mid x^2 y + x + y$.
- Let p be an irreducible integer polynomial. Prove that p does not have multiple roots.
- Prove that if a and b are positive integers, then $4ab - a - b$ is not a perfect square.

APPENDIX A

Basics Solutions

A.1. Methods of Proof

Result 1. If you start trying some small cases, what you'll eventually find is that if n is an even integer, then n^2 leaves a remainder of 0 when divided by 4, and if n is an odd integer, then n^2 leaves a remainder of 1 when divided by 4. Once you've conjectured this, all that's left is to recall what it means for a number to be even or odd, and then the proof falls out quite naturally:

Proof. Let the perfect square be n^2. We split into cases depending on the parity of n.

- If n is even, let $n = 2m$ for some integer m. Then
$$n^2 = (2m)^2 = 4m^2,$$
which leaves a remainder of 0 when divided by 4.
- If n is odd, let $n = 2m + 1$ for some integer m. Then
$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1,$$
which leaves a remainder of 1 when divided by 4.

In either case, the remainder left when dividing n^2 by 4 is either 0 or 1, which is what we wanted to prove. $\square$

Result 2. The key here is to assume, for contradiction, that there are only finitely many primes. Then we want to prove a suitable contradiction — a nice way of doing this is to find a number that isn't 1 but isn't divisible by any of our finitely many primes. The idea of constructing such a number by multiplying everything and adding 1 is surprisingly common in Olympiad maths.

Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Then, consider the number $A = p_1 p_2 \cdots p_n + 1$. Clearly A is a positive integer larger than 1, so it must have a prime factor, which means that for some i, $p_i \mid A$. But $p_i \mid A - 1$, so $p_i \mid A - (A-1) = 1$, which is our contradiction. $\square$

Problem 3. This is more an exercise in logic than in maths. You could be stuck for ages trying to prove the problem directly, but as soon as you try to use some indirect approach (like contrapositive, contradiction, or assuming one part of the conclusion is false and proving the other is true) the problem pretty much solves itself. I think the cleanest solution in this particular case uses the contrapositive.

Proof. We prove the contrapositive: that if a and b are both rational, then so is $a + b$.

Let $a = \frac{w}{x}$, $b = \frac{y}{z}$. Then
$$a + b = \frac{w}{x} + \frac{y}{z} = \frac{wz + xy}{xz},$$
which is clearly rational. $\square$

Result 4. This is a classic induction problem. Apart from being instructive because it isolates the idea of induction, it does highlight a minor point. In the inductive step, it's just as acceptable to assume the problem is true for k and prove it for $k + 1$ as to assume the problem is true for $k - 1$ and prove it for k. In this particular case, the latter is somewhat easier.

PROOF. We prove this by induction on n.

Base case $n = 1$: We have LHS $= 1 = \frac{1\times 2}{2} =$ RHS.

Inductive step: Assume the problem is true for $n = k - 1$. Then,

$$\begin{aligned} 1 + 2 + \cdots + k &= (1 + 2 + \cdots + k - 1) + k \\ &= \frac{k(k-1)}{2} + k \\ &= \frac{k(k-1) + 2k}{2} \\ &= \frac{k(k+1)}{2}, \end{aligned}$$

so the problem is true for $n = k$. □

Result 5. This is a good example of how solutions to the same problem can look quite different when written up with PMI or with well-ordering.

First assume PMI. A direct induction will prove the statement quite easily.

Now we can try assuming well-ordering. Looking for a contradiction, assume there is some positive integer $a < 1$. A contradiction is easiest to find by applying well-ordering to the set of all positive integers.

Let's write this up.

PROOF. First, assume PMI.

Base case $n = 1$: clearly $1 \geq 1$.

Inductive step: assume that $k \geq 1$. Then $k + 1 > k \geq 1$, completing the induction.

Now, assume well-ordering. Assume there's some $a \in \mathbb{N}$ with $a < 1$. Since $\mathbb{N}$ is nonempty, we may let b be its smallest element. Since ab is a positive integer, we have $b \leq ab$. On the other hand, since $a < 1$ we get that $ab < b$. This contradiction concludes the proof. □

Result 6. Since this is an "if and only if" problem, we will probably need to find separate proofs in each direction.

First, let's use induction to prove well-ordering. Our desired conclusion is that any nonempty set of positive integers has a smallest element. Intuitively, what we would like to do is to check if 1 is in it, then if 2 is in it, and so on until we find an element that's in it. Once we've found that element, we wish to prove that it's the smallest element. However, this is hard to write up because we'd like our process to "finish" after a finite number of steps, while induction only talks about things that are true for all positive integers. To make our lives easier, we instead try to prove the contrapositive of well-ordering: that if S is a set of positive integers with no smallest element then S is empty.

Now, our argument looks similar: we claim that 1 is not in S, that 2 is not in S, and so on forever. To make sure that we can actually keep repeating this argument, we need to show that if we found an element in S it must be the smallest element. Proving this requires tweaking our inductive assumption.

Now, let's use well-ordering to prove PMI. You'll probably get nowhere if you aren't completely clear about what you're trying to prove (you may as well replace PMI by gibberish), so let's write out PMI in full:

Let S be a set of positive integers. If $1 \in S$, and if the statement $\forall a \in S,\ a+1 \in S$ is true, then S contains all positive integers.

Once again we use indirect proof — this time it's proof by contradiction (contrapositive also works). Let's assume that there is a set S that satisfies both conditions but doesn't contain all positive integers. We hope to use well-ordering to find a contradiction.

The key idea is to consider the smallest integer that isn't in S, which is possible by well-ordering. Then the condition implies that either it's not the smallest, or $1 \notin S$ — a contradiction either way.

Let's write it up.

PROOF. First we prove that if PMI is true, then so is well-ordering. Assume PMI, and we'll prove the contrapositive of well-ordering: that if S is a set of positive integers with no smallest element, then it is empty.

I prove by strong induction that for each positive integer n, if $m \in S$ then $m \geq n+1$.

Base case $n = 1$: if $1 \in S$, then 1 would be the smallest element in S (since if $m \in S$ then m is a positive integer so $m \geq 1$). So since S has no smallest element, 1 is not the smallest element in S so taking the contrapositive we get that 1 is not in S.

Inductive step: Assume that for any $m \in S$ we know that $m \geq k+1$. I claim that $k+1 \notin S$. Indeed, if $k+1$ were in S, then it would be the smallest element of S. But since S has no smallest element, $k+1$ can't be in S. Therefore, if $m \in S$ we know $m-(k+1)$ is a positive integer so $m-(k+1) \geq 1$, so $m \geq k+2$, as required for the inductive step.

This completes the induction. Now if $n \in S$ we've proven that $n \geq n+1$, a contradiction so S must be empty.

Now I prove that if well-ordering is true, then so is PMI. Assume for contradiction that well-ordering is true but PMI is not. Then, there is a set S of positive integers that contains 1 and such that for each $a \in S$, $a+1 \in S$ but that does not contain all positive integers. Then, the set $\mathbb{N} \setminus S$ is nonempty so by well-ordering it contains a smallest element a.

Since we know that $1 \in S$, we know that $a \neq 1$. So since $a \geq 1$, $a-1$ is a positive integer. Since $a-1 < a$ and a is the smallest member of $\mathbb{N} \setminus S$, $a-1$ is not in $\mathbb{N} \setminus S$ so $a-1 \in S$. So $(a-1)+1 = a \in S$, which contradicts the assumption that $a \notin S$. $\square$

A.2. Algebra

Problem 7. Not much to say here — interpret as a system of linear equations and solve however you like.

Answer: 26.

Proof. Let the two numbers be a and b, with $a > b$. Then, $b = a - 20$ so

$$\begin{aligned} a + 4 &= 3(a - 20 + 4) \\ &= 3a - 48 \\ 2a &= 52 \\ a &= 26, \end{aligned}$$

so the larger of the two numbers is 26.

To prove that this actually works, note that if $a = 26$ and $b = 6$, then $a - b = 20$ and $a + 4 = 30 = 3 \times 10 = 3(b + 4)$ as needed. $\square$

Problem 8. Since we don't like the 1s in our equations, we subtract two equations to get rid of them. Alternatively, we subtract two equations because that's one of the most obvious things to do with a system of equations. Either way, once we've done that the rest of the problem is pretty routine.

Answer: $(x, y, z) = (1, 1, 1), \left(-2, -2, \frac{5}{2}\right), \left(-2, \frac{5}{2}, -2\right), \left(\frac{5}{2}, -2, -2\right)$.

Proof. Subtract the third equation from the first:

$$\begin{aligned} xy - xz &= 2z - 2y \\ x(y - z) + 2(y - z) &= 0 \\ (x + 2)(y - z) &= 0 \end{aligned}$$

So either $x = -2$ or $y = z$. Similarly we can deduce that either $z = -2$ or $x = y$. Now we split into four cases:

- $x = -2,\ z = -2$. Then $2y = zx + 1 = 5 \implies y = \frac{5}{2}$.
- $x = -2,\ x = y$. Then similar to the above we get $z = \frac{5}{2}$.
- $y = z\ z = -2$. In the same way we get $x = \frac{5}{2}$.
- $y = z,\ x = y$. Then $x^2 + 1 = 2x \implies (x - 1)^2 = 0 \implies x = 1$, so $x = y = z = 1$.

So the only solutions are what we claim they are. It is easy to check that these solutions all satisfy the original equations. $\square$

Result 9. First, there are a few ways of seeing that this is the answer.

One way is to try to factorise $x^2 - 2mx + p$ as $(x - a)(x - b)$. Then $a + b = 2m$ and $ab = p$, and a and b are the values of x we want. Then the key idea is that the way of using the $a + b = 2m$ condition is to let $a = m + c,\ b = m - c$ so that

$$p = ab = (m + c)(m - c) = m^2 - c^2,$$

so that $c = \sqrt{m^2 - p}$.

Another way is to notice that $x^2 - 2mx + p$ looks a lot like $x^2 - 2mx + m^2 = (x - m)^2$. I'll do the rest in the proof.

PROOF. We have

$$\begin{aligned} x^2 - 2mx + p &= x^2 - 2mx + m^2 + p - m^2 \\ &= (x-m)^2 - \left(m^2 - p\right) \end{aligned}$$

If $m^2 - p < 0$ then clearly there are no solutions. Otherwise, we have

$$\begin{aligned} x^2 - 2mx + p &= (x-m)^2 - \left(\sqrt{m^2-p}\right)^2 \\ &= \left(x - m - \sqrt{m^2-p}\right)\left(x - m + \sqrt{m^2-p}\right), \end{aligned}$$

so it equals 0 if and only if $x = m \pm \sqrt{m^2 - p}$. □

Result 10. The key here is to get this equation into a form such that we can apply the previous result.

PROOF. We have

$$\begin{aligned} 0 &= ax^2 + bx + c \\ 0 &= x^2 + \frac{b}{a}x + \frac{c}{a} \\ &= x^2 - 2\frac{-b}{2a}x + \frac{c}{a} \\ x &= \frac{-b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} \\ &= \frac{-b \pm \sqrt{4a^2\left(\frac{b^2}{4a^2} - \frac{c}{a}\right)}}{2a} \\ &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

as needed.

If $\Delta < 0$ there are clearly no solutions. If $\Delta = 0$ the unique solution is $x = \frac{-b}{2a}$. If $\Delta > 0$ there are two solutions given by our equation. □

Problem 11. Once again not much to say here — interpret the number bases in the usual way and solve the resulting quadratic.

Answer: 57.

PROOF. We have

$$\begin{aligned} 111_b &= 212_{b-2} \\ b^2 + b + 1 &= 2(b-2)^2 + (b-2) + 2 \\ &= 2b^2 - 7b + 8 \\ 0 &= b^2 - 8b + 7 \\ b &= 4 \pm \sqrt{4^2 - 7} \\ &= 4 \pm 3 \end{aligned}$$

Therefore, since $b > 2$ we get $b = 7 \implies x = 7^2 + 7 + 1 = 57$.

Finally, 57 is indeed 111 in base 7 and 212 in base 5. □

Problem 12. The key here is to use the discriminant (Δ in Result 10). In particular, it's enough to prove that at least one of the two Δs is nonnegative. The easiest way of doing this is to assume that the first is negative and prove that the second isn't.

Proof. Assume that there is no real number x such that $x^2+(r+1)x+s=0$. Then the discriminant $(r+1)^2-4s$ is negative, so $4s>(r+1)^2$.

Since $(r+1)^2 \geq 0$, we know that $s>0$. Also, $4(s-r)>(r+1)^2-4r=(r-1)^2 \geq 0$. So since $s>0$ and $4(s-r)>0$, their product $4s^2-4sr$ is also positive so the discriminant of the second quadratic is positive, meaning that it has at least one real solution. ☐

Problem 13. At first glance, this looks like our methods can't help since we have a cubic not a quadratic. However, the same trick used in Result 9 of recognising a common factorisation does in fact work.

Answer: $x=-1-\sqrt[3]{4}$.

Proof. We subtract 4 from both sides to make the LHS into something we recognise:

$$\begin{aligned} x^3+3x^2+3x+1 &= -4 \\ (x+1)^3 &= -4 \\ x+1 &= -\sqrt[3]{4} \\ x &= -1-\sqrt[3]{4}. \end{aligned}$$

To show that this number works, we can either substitute it in and do the algebra, or notice that each step above was actually an equivalence so the implications run backwards as well. ☐

Result 14. Since we want to use the fact that squares are nonnegative, we collect all the terms on one side. The rest is recognition, which can be helped by noticing that we want equality to occur when $a=b$.

Proof.

$$\text{RHS}-\text{LHS}=\frac{a+b}{2}-\sqrt{ab}=\frac{a+b-2\sqrt{ab}}{2}=\frac{(\sqrt{a}-\sqrt{b})^2}{2} \geq 0,$$

as needed. ☐

Problem 15. We have to have a 0 and a 2015 in the set, but apart from them the rest of the terms should be as small as possible. This means that we can apply Result 4 to get a function we want to minimise. A little algebraic trickery means it's enough to minimise

$$n+\frac{4032}{n}.$$

Then, by Result 14, the minimum of this over $\mathbb{R}$ is $2\sqrt{4032}$ at $n=\sqrt{4032} \approx 63.5$, which means either 63 or 64 should minimise the expression over $\mathbb{N}$. In fact both do, so we should try to force the expression into something that looks like $(n-63)(n-64)$, and indeed doing that solves the problem.

Answer: 62.

PROOF. Let n be the number of elements in S, and let $S = \{s_1, s_2, \ldots, s_n\}$, where the s_is are in increasing order. Then

$$s_i \geq i - 1 \,\forall\, i < n,$$

and $s_n = 2015$, so the average is at least

$$\begin{aligned}
\frac{0 + 1 + \cdots + n - 2 + 2015}{n} &= \frac{\frac{(n-2)(n-1)}{2} + 2015}{n} \\
&= \frac{n^2 - 3n + 4032}{2n} \\
&= \frac{n^2 - 127n + 4032}{2n} + 62 \\
&= \frac{(n-63)(n-64)}{2n} + 62.
\end{aligned}$$

Since n is an integer, the first term is 0 if n is either 63 or 64 and positive otherwise, which means that the minimum value is 62, achieved when S is either $\{0, 1, \ldots, 61, 2015\}$ or $\{0, 1, \ldots, 61, 62, 2015\}$. $\square$

Result 16. There are three ways I know of doing this. One of them is a standard induction, but the other two are more interesting.

For the first way, we notice that we already know the special case (see Result 4) where $a = 0$ and $b = 1$. A little algebra allows us to reduce the whole problem to this particular case.

PROOF. We have

$$\begin{aligned}
\sum_{i=0}^{n}(a + bi) &= \sum_{i=0}^{n} a + \sum_{i=0}^{n} bi \\
&= a(n+1) + b\sum_{i=0}^{n} i \\
&= a(n+1) + b\frac{n(n+1)}{2} \\
&= \frac{(2a + bn)(n+1)}{2},
\end{aligned}$$

as needed. $\square$

For the second way, we use a trick called *Gaussian pairing* — we pair the first term with the last term and so on — so that each pair has the same sum.

PROOF. We have

$$\begin{aligned}\sum_{i=0}^{n}(a+bi) &= \sum_{i=0}^{n}(a+b(n-i))\\ &= \frac{1}{2}\left(\sum_{i=0}^{n}(a+bi)+\sum_{i=0}^{n}(a+b(n-i))\right)\\ &= \frac{1}{2}\left(\sum_{i=0}^{n}(2a+bn)\right)\\ &= \frac{(n+1)(2a+bn)}{2},\end{aligned}$$

as needed. □

Result 17. The main idea here comes from extending a couple of the common factorisations:

- $1-r^2=(1-r)(1+r)$
- $1-r^3=(1-r)(1+r+r^2)$

We get the $a=1$ case of the general formula given in 1.2.1. Let's write it up.

PROOF. We have

$$1-r^{n+1}=(1-r)(1+r+r^2+\cdots+r^n),$$

since all the middle terms cancel. Dividing both sides by $1-r$ yields the desired result. □

Problem 18. So you sum your sequence using Result 16, which gets you a closed form.

Then you're left having to prove that $a+1$ and $2n+a$ cannot both be powers of 2. Playing around with special cases tells you at least one is odd, and from there it's easy to finish.

PROOF. From Result 16, we have that the given sum is equal to

$$\frac{(a+1)(2n+a)}{2}.$$

So assume, for contradiction, that this is a power of 2. Then we have that twice the sum is also a power of 2, so $(a+1)(2n+a)$ is a power of 2. Since $a+1$ and $2n+a$ both divide powers of 2, they must each be a power of 2. Since a and n are positive integers, both $a+1$ and $2n+a$ are at least 2 so they're even. So their difference, $2n-1$, must also be even, which is a contradiction. □

A.3. Combinatorics

Result 19. Not much to say here: just apply the multiplication principle.

Proof. There are n ways to choose the first thing, $n-1$ ways to choose the second (since the first has been chosen), $n-2$ to choose the third, and so on up to $n-k+1$ for the kth. Thus the total number of ways is

$$n(n-1)\cdots(n-k+1),$$

as claimed. □

Problem 20. So you try some small cases because of course you do, and you notice that every 2 goals apart from the first 2, the number of ways is multiplied by 3. With the help of like, a tree diagram, it's easy to see that after an odd number of goals there are 3 ways of scoring the next 2. The rest is easy:

Answer: 972.

Proof. There are 2 ways for the first goal to be scored.

Assume an odd number of goals has been scored. Then the difference between the two teams' goals is 1, so we can WLOG team A has one more goal than team B. Then the next two goals can be AB, BA, BB so there are 3 ways for the next two goals to be scored.

Finally, there are 2 ways for the last 2 goals to be scored.

Thus, the total number of ways for 12 goals to be scored is $2 \times 3^5 \times 2 = 972$. □

Result 22. The key to proving this is to notice that we have already proven Result 19 where order does matter. To go from order mattering to order not mattering, we need to find out how much we've overcounted by: that is, how many permutations, where order matters, go to the same combination, where order doesn't.

Proof. By Result 19, there are $\frac{n!}{k!}$ ways of choosing k things from n, where order matters.

Let there be x ways of choosing k things from n, where order doesn't matter. Then for each such way, each permutation of those k things is counted in our $\frac{n!}{(n-k)!}$ from above. Applying Result 19 again, we have that $k! \times x = \frac{n!}{(n-k)!}$, which rearranges to the claimed formula. □

Problem 23. So upon reading the problem we can let our palindromes be $\overline{xyx}$ and $\overline{ztz}$. Clearly, $x > z$, after which it's clear why $y \geq t$.

So by the multiplication principle, it suffices to count two things:

- The number of ways of choosing digits x and z with $x > z > 0$
- The number of ways of choosing digits y and t with $y \geq t$.

Both these things are quite easy to count using this section's formula.

Answer: 1980.

Proof. Let the palindromes be $\overline{xyx}$ and $\overline{ztz}$. Since their difference is 3 digits and $a > b$, we have $x > z$.

Since the second digit of our subtraction can't carry, we must have $y \geq t$. So it's enough to count the number of ways we can choose x and z, and separately the number of ways we can choose y and t.

Since x and z are distinct digits from 1 to 9, the number of choosing them is $\binom{9}{2} = 36$. Since y and t are not-necessarily-distinct digits from 0 to 9, the number of ways of choosing them is $\binom{10}{2} + 10 = 55$. Thus, the answer is $36 \times 55 = 1980$. $\square$

A.4. Geometry

A.5. Number Theory

APPENDIX B

Intermediate Solutions

B.1. Algebra

B.1.1. Polynomials.

Result 83. It is natural to split the proof into two parts: existence and uniqueness. Uniqueness is the easier part: it can be proven by the usual method of assuming two representations exist, and proving they are in fact the same.

The proof of existence proceeds by induction on the degree. The key is to reduce $A(x)$ to a polynomial with smaller degree by cancelling the leading term. If we do this in a way that lets us control $Q(x)$ and $R(x)$, the induction will work.

Proof. First we prove such a representation exists, by strong induction on the degree of A. Let $d = \deg B$.

Base cases $\deg A < d$: clearly $Q(x) = 0,\ R(x) = B(x)$ satisfies all the conditions.

Inductive step: let $a_n x^n$ be the leading term of A, and let $b_d x^d$ be the leading term of B. We may write

$$A(x) = \frac{a_n}{b_d} x^{n-d} B(x) + A_1(x)$$

for some polynomial A_1. Since the first term on the RHS cancels the $a_n x^n$, this polynomial $A_1(x)$ can be represented as $Q_1(x)B(x) + R_1(x)$. But then choosing $Q(x) = Q_1(x) + \frac{a_n}{b_3} x^{n-d} B(x),\ R(x) = R_1(x)$ provides a representation for A.

Now we prove the representation is unique. Assume there are polynomials Q_1, R_1, Q_2, R_2 such that

$$A(x) = B(x)Q_1(x) + R_1(x) = B(x)Q_2(x) + R_2(x).$$

Then, $B(x)(Q_1(x) - Q_2(x)) = R_2(x) - R_1(x)$. The degree of the RHS is less than d; therefore, so is the degree of the LHS. But since the degree of the LHS is at least D unless $Q_1 = Q_2$, we get $Q_1 = Q_2$ and therefore $R_1 = R_2$. $\square$

Result 84. First we need to understand what the problem is saying. Try special cases: $i = 0,\ i = n,\ n = 1,\ n = 2$ and so on, until you know what it's saying.

The idea here is to use the corollary from the previous result multiple times to factorise our polynomial fully, then expand it again. Then when we extract the x^{n-i} coefficient, each term that contributes to it is a product where x appears $n - i$ times, and the rest is a product of i (r_i)s and a constant term. Since each combination of i $(-r_i)$s appears exactly once in the expansion, we get the claimed formula.

The neatest way of writing this up is to use induction.

Proof. By induction on the degree.

Base case $n = 0$: there are no r_is so all that we have to prove is $a_0 = a_0$, which is obvious.

Inductive step: Since r_n is a root of $P(x)$, we can write $P(x) = (x - r_n)Q(x)$ for some polynomial $Q(x)$ of degree $n - 1$. Then we know that $Q(x)$ has roots $r_1, \ldots, r_{n-1}$ so by the inductive hypothesis, we know that in $Q(x)$:

- The coefficient of x^{n-i} is
$$(-1)^{i-1} a_n \sum_{j_1 < \cdots < j_{i-1}} \prod_{k=1}^{i-1} r_{j_k}.$$
- The coefficient of x^{n-i-1} is
$$(-1)^{i} a_n \sum_{j_1 < \cdots < j_{i}} \prod_{k=1}^{i} r_{j_k}.$$

Since the coefficient of x^{n-i} in $P(x)$ is the coefficient of x^{n-i-1} in $Q(x)$ minus r_n times the coefficient of x^{n-i} in $Q(x)$, it's what we claim it is. Since this argument works for each i, the induction is complete. □

B.2. Combinatorics

B.3. Geometry

B.4. Number Theory

APPENDIX C

Advanced Solutions

C.1. Algebra

C.2. Combinatorics

C.3. Geometry

C.4. Number Theory

APPENDIX D

Other free resources

D.1. Basics

- AOPS Resources
- The Book of Proof
- Methods of Proof
- How to write a solution
- OTIS Excerpts, chapter 1

D.2. NT

- Intermediate Number Theory
- Olympiad Number Theory through Challenging Problems
- Modern Olympiad Number Theory

D.3. Algebra

- OTIS Excerpts, chapters 2 to 5
- Polynomials
- Sequences

D.4. Combi

- Combinatorics
- Olympiad Combinatorics
- Combinatorics and Combinatorial Geometry
- Generatingfunctionology

D.5. Geo

- EGMO Chapters 1 to 3
- EGMO Chapter 8
- A Beautiful Journey through Olympiad Geometry
- Lemmas in Olympiad Geometry

D.6. Problems

- AMC Problems and Solutions
- Melbourne Uni Maths Comp past papers
- AOPS contest collections (This is the most important link on the page. See especially the pages for national olympiads, team selection tests and international contests. However, note that solutions are user contributed and can be incorrect.)

D.7. Assorted

- MO Problem Journal
- OTIS Excerpts
- HDIGH Olympiad page
- HDIGH Olympiad resources
- Evan Chen's page
- Po-Shen Loh's page
- CJ Quines' page
- Yufei Zhao's page
- Alexander Remonov's page
- Konrad Pilch's page

D.8. Published Books

Free with access to a Springer subscription:

- The IMO Compendium
- Problem Solving Strategies
- Problem-Solving Through Problems

Todos.

- Diagram for problem 42 and for trigonometry definition