SOME MADMAN'S RAVINGS

GISPISQUARED

Contents

1. Introduction

If you can't be bothered reading, see the tldr here.

I'm writing this since I think that most of the resources out there that try to teach you olympiad maths have all the theory you need to solve IMO-level problems (and sometimes much more!), but it's much more rare to see people who tell you how to look at problems and figure out approaches that may, or in some cases should, work. True, much of this is an individual learning experience, but I think a lot of this can be written more explicitly.

This may reduce some of the magic of figuring this stuff out for yourself; to mitigate this effect, I have relegated the solutions to examples to the back so that you can (and I encourage you to!) try the examples before reading the solutions.

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

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

2. Theory

Now it's time to learn how proofs work.

2.1. Methods of Proof.

There are a few main methods of proof — that is, ways in which you can go from the conditions in the problem to your given condition.

2.1.1. *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.

Example 1. *Prove that the remainder when a perfect square is divided by 4 is either 0 or 1.* Solution

2.1.2. *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.

Example 2. *Prove that there are infinitely many primes.* Solution

2.1.3. *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.

Example 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

2.1.4. *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.
  - 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.

  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.

Example 4. *Prove that for all positive integers n,*

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

Solution

To conclude the Methods of Proof section, I'll include one final example that combines most of what we've covered so far.

Example 5. *The* Well-Ordering Principle *states that any set of positive integers has a least element. Prove that it's equivalent to PMI — that is, prove that PMI is true if and only if well-ordering is true.* *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.

3. Practice

4. Solutions

Example 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. □

Example 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. □

Example 3 The problem itself is not of much interest once you realise that you're meant to prove the contrapositive. However, this problem is instructive for two main reasons. First, it shows how much easier it is (in this particular instance) to prove the contrapositive than the original statement. You could be stuck for ages trying the original problem, but as soon as you ask "what if the conclusion wasn't true" the problem pretty much solves itself. The second, more subtle, takeaway here is about how to realise that you should use some kind of indirect (contrapositive or contradiction) approach. Usually, a conclusion that has some kind of "or" statement in it is a good sign that an indirect approach may be easier, since negating the conclusion turns the "or" into an "and", which is much easier to work with. The exception is when you can split the conditions into cases that naturally give you each part of the "or", like in Example 1.

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. □

Example 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 $n=k$. □

Example 5 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 every 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 first find an element that's in it. But this quickly becomes circular and it's difficult to make airtight. The trick is to utilise proof by contrapositive — start with a set of positive integers that has no smallest element, and prove it's empty using our sequential checking process. Make sure you actually use PMI somewhere, otherwise it's probably a fakesolve.

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, $n\notin S$. Clearly this is sufficient.

Base case $n = 1$: if $1 \in S$, then 1 would be the smallest element in S. So since S has no smallest element, 1 is not the smallest element in S so 1 is not in S. (Notice where I used the contrapositive here?)

Strong inductive step: Assume that for all $i = 1, 2, \ldots, k,\ i \notin S$. 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.

This completes the induction, so no integer is in S meaning that S is empty as needed.

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 $a - 1$ is a positive integer. Since $a - 1 < a$ and a is the smallest member of $\mathbb{N} \setminus S$, $a - 1 \notin \mathbb{N} \setminus S \implies a - 1 \in S$. So since $a - 1 \in S,\ a \in S$ which contradicts the assumption that $a \notin S$. $\square$

5. TLDR

This section contains some ideas about how to approach problems; basically, I've taken what I think are the most important bits and condensed them together here.

- 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
- Can you reduce a counterexample to a smaller counterexample?
- Think about what happens if the problem, or the conclusion, is wrong.