Methods of Proof in Problem Solving

Konrad Pilch

March 29, 2016

1 Direct Proof

In mathematics, there are many different types of problems. Some will ask you to find the answer to a question. Some will ask you to come up with a method that solves a type of problem. And some will ask you to prove that a certain statement is true (or indeed false)!
The first type of problem is very familiar to you. Here are some examples:

- What is the last digit of (9!) ?
- In how many ways can three people choose from 4 different hats to wear?

These types of problems may be easy or even very hard, but we know that what we need is a number at the end. [Try these problems yourself!]
The second type of problem is a bit more complex and we shall discuss such problems in the section on combinatorics. The third type of problem is what we are dealing with today. Examples of a 'proof' question include the following:

1. 10 people are at a party and some of them shake hands. If we asked each person how many times they shook hands and added all these numbers up, prove that the final answer is always even.
2. Prove that if we divide any perfect square by 4, the remainder is always 0 or 1.

How do you solve a problem like this? Well, one idea is to look at every possible case and prove that it is true in every case. This is a good place to start. However, if we look at the two above problems, it turns out that for question 1, there are **35184372088832** possible ways that the ten people could shake hands, and for question 2 there are an **infinite** number of perfect squares! There is no way we could look at all the cases here. We need a method that covers all of the (possibly infinite) possibilities.
That is a proof! A proof looks at the question in general (not looking at any particular case) and uses properties of the question to show that what you want to prove is always true.

Definition. A proof is a collection of statements that start with something definitely true and use correct logical steps to reach another truth!

Does this mean proofs are really complex and hard? Not necessarily. They need to be correct at every step and you need to make sure that you start with something that is true (do not assume anything about the question). Also, remember that proofs are the essays of mathematicians. They should not be a collection of random symbols, but something your non-mathematically inclined friend can understand. If they can't, your proof needs to be improved.
Here is an example proof, so you can see this in action.

Problem 1. 10 people are at a party and some of them shake hands. If we asked each person how many times they shook hands and added all these numbers up, prove that the final answer is always even.

Proof. It is important to realise before we start that we cannot assume all the people shook hands or indeed that all people shook hands at all! This was never stated in the question, so do not assume it.
If we add up the number of handshakes each person did, then notice that we count every handshake exactly twice (as two people are involved in every handshake). So, the number you get when you add up the number of handshakes of each person is twice the number of handshakes, which is even. QED
Note, this is true for any number of people. □

You may have noticed the little QED. Actually, the little box means the same thing. We only put one of these at the end of a proof. This is a mathematical symbol which we tend to put at the end of proofs. Here are some more handy mathematical symbols.

- $\Rightarrow$ - implies
- $\Leftarrow$ - implied by

- $\Leftrightarrow$ - is equivalent to (implies AND is implied by)
- iff - if and only if
- $\forall$ - for all
- $\exists$ - there exists
- *RTP* - required to prove
- *QED* - end of proof (Latin: quod erat demonstrandum. English: which had to be demonstrated)

Let's try one more proof. This one will be a little more complicated.

Problem 2. Prove that if we divide any perfect square by 4, the remainder is always 0 or 1.

Proof. Any whole number n is either odd or even, so we can write $n = 2k$ or $n = 2k + 1$ where k is also a whole number. If we square n, we find that

$$n^2 = (2k)^2 = 4k^2$$

or

$$n^2 = (2k+1)^2 = (2k+1)(2k+1) = 4k^2 + 2k + 2k + 1 = 4k^2 + 4k + 1.$$

In the first case, notice that $4k^2$ is divisible by 4 and so n^2 would leave a remainder of 0 when divided by 4. In the second case $4k^2 + 4k$ is divisible by 4, so n^2 would leave a remainder of 1 when divided by 4. QED □

This last proof was an example of using a variable to represent every possible case. n^2 represents every possible perfect square. Then we used what we know about whole numbers n to deduce facts about n^2. I want to stress here, that it would NOT be acceptable to check that the problem is true for $n = 0, 1, 2, 3, 4, 5, 6, \ldots$ and then say it is true because the pattern is clear. That is very bad mathematics. We must write the proof to cover all possible cases.

Now, it's time to practice this idea of proofs. Here are some tips.

- Structure the proof, so it is clear how everything flows in the proof.
- Use correct symbols, define variables and use the same names as in the question.
- Use big, neat diagrams
- Writing must be legible (big clear letters, spaces between words, sentences, line between paragraphs)
- Use your words. A proof is a story.
- Common Mistakes
  - reverse logic - you cannot start with what you want to prove.
  - division by zero - this is not allowed.
  - squaring, square roots - eg. there are **two** solutions to the equation $x^2 = 4$.
  - diagram dependence - in geometry make sure you draw your diagrams accurately, otherwise your logic will be wrong.
  - MISREADING the question
  - not checking the answer works
  - assuming things are obvious (especially patterns) - they may even be false!

Don't forget that even questions where you are to provide a numerical answer often require you to prove that that number is the only answer!

Problems

1.1 Easy

1. Prove that the sum of two squares does not leave a remainder of three when divided by four.
2. Prove that a positive integer is divisible by nine, if the sum of its digits is divisible by nine.
3. Prove that the product of two consecutive integers is always even.
4. Prove that the product of three consecutive integers is always divisible by 6.
5. We have an $n \times n$ chessboard where n is odd and the lower left hand square is black. Prove that the number of black squares is one more than the number of white squares on the whole chessboard.
6. Prove that the product of four consecutive integers is always divisible by 24.

1.2 Hard

1. Prove that a repeating decimal can be written as the ratio of two whole numbers (in other words, as a fraction!).
2. Determine all integers n such that $n^4 - 3n^3 - n^2 + 4n + 1$ is a multiple of 7.
3. Prove that there is no solution to $a^2 + b^2 = 1234567$.
4. Find the number of distinct positive integers n such that
$$\frac{n^3 + 2007}{n - 19}$$
is an integer.
5. Prove that if x and y are the sum of two perfect squares then so is xy.
6. Prove that
$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 2.$$
7. Prove that
$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$
is unbounded, that is, it goes off to infinity.
8. Determine all integers m, n such that $m^2 = n! + 3$.

1.3 Very Hard

1. Take a prime number p. For any number k from the set $\{1, 2, \ldots, p-1\}$, prove that there is only one number l from the same set such that kl leaves a remainder of 1 when divided by p.
2. Using the notation from the previous question, call l the inverse of k and denote it properly as k^{-1}. Show that
$$2^{-1} = 3^{-1} + 6^{-1}.$$
3. Determine all integers n for which
$$2^n = n^2.$$

4. Determine all positive integers n for which

$$n^4 + 2n^3 + 3n^2 + 4n + 5$$

is a perfect square.

5. Determine all integers n such that

$$\sqrt{\frac{4n-1}{n+5}}$$

is rational.

2 Proof By Contradiction

Sometimes it is very hard to prove a mathematical fact directly. You learnt last week that a direct proof aims to logically use given information A to prove our result B. Or,

$$A \implies B.$$

An indirect proof (also known as a proof by contradiction) works a little differently. Instead, you take your given information A and assume the opposite of what we want to prove, B^c (the little c means complement). You then show that combining these two things gives a contradiction (a logical fallacy). This means that B^c can't be true, so B is! Or,

$$A \text{ and } B^c \implies \text{ contradiction. Hence, } B \text{ is true.}$$

The next section gives a few example indirect proofs.

2.1 Example Proofs

Problem 3. Prove that $\sqrt{2}$ is irrational.

Proof. Our given information A are all the basic facts we know about addition, multiplication and rationals. What we want to prove, B, is that $\sqrt{2}$ is irrational. So, to do a proof by contradiction, assume A and B^c, where B^c is the assumption that $\sqrt{2}$ is rational (the opposite of B).
As we are assuming $\sqrt{2}$ is rational. Let

$$\sqrt{2} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}$. We can also make sure that this fraction is in simplest form, ie. a and b are coprime (have no factors in common). So, square both sides and multiply by b^2. We get

$$2b^2 = a^2.$$

The left hand side is divisible by 2, so the right hand side must be divisible by 2. Hence, a must be even. So, call $a = 2x$ where $x \in \mathbb{Z}$. Substituting gives

$$2b^2 = 4x^2.$$

Simplifying gives

$$b^2 = 2x^2.$$

Again, this means the right hand side is even, so the left hand side must be even. So, b is even. But then a and b have a common factor of 2, which contradicts how we set up a and b. So, our original assumption that $\sqrt{2}$ is rational is false. Hence, $\sqrt{2}$ is irrational. QED

□

Problem 4 (Pigeon-Hole Principle)**.** If there are $nk + 1$ pigeons in k pigeonholes, then there exists at least one pigeonhole that contains at least $n + 1$ pigeons.

Proof. A lot of people would try and prove this using worst case scenario type ideas. But what do you define as 'a worst case scenario'? It's better to use proof by contradiction.
We can assume there are $nk + 1$ pigeons in k pigeonholes. We will also assume the opposite of what we want to prove. So, we assume that there do not exist any pigeonholes with at least $n + 1$ pigeons. We can also think of this as meaning that all pigeonholes have at most n pigeons. But then, there are at most nk pigeons. This is a contradiction because there are $nk + 1$ pigeons. Hence, our assumption that there do not exist any pigeonholes with at least $n + 1$ pigeons is false. Hence, there is at least one pigeonhole that contains at least $n + 1$ pigeons. QED □

Problems

2.2 Easy

1. If m and n are positive integers, show that $\sqrt[m]{n}$ is either an integer or irrational.
2. Prove there are infinitely many primes.
3. If a and b are integers, such that ab is even, show that either a or b must be even.
4. Prove that there is no triangular number which is one less than a multiple of 11.
5. Does there exist a pair of integers (x, y) such that $x^2 + y^2 = 7007$?
   What about a triplet of integers (x, y, z) such that $x^2 + y^2 + z^2 = 7007$?

2.3 Hard

1. The integers a, b and c are the sides of a right angled triangle. Prove that abc is a multiple of 60.
2. Find all integer solutions to the equation $a^3 + 2b^3 = 7a^2b$.
3. Find all integers k such that
   $$k^2 + k + 1 | k^3 + 2k + 2\,.$$
4. Determine all integers n such that
   $$\sqrt{\frac{4n-1}{n+5}}$$
   is rational.
5. Find all integers a, b, c, n such that
   $$a! + b! + c! = 2^n\,.$$
6. Suppose that a and b are positive integers, and
   $$a^2 + ab + 1 | b^2 + ab + 1\,.$$
   Show that $a = b$.

3 Induction

Consider a stack of dominoes that are set up to all fall. What does this set up include? Most importantly, if any domino falls, it must knock the next one over. Given this, if one knocks the first one, then you'll get a chain reaction that guarantees that they all fall.
This idea applies to proofs about a proposition that is supposed to hold for all positive numbers. This is how to go about using a proof by induction.

1. Identify what you are trying to prove. Write down the statement for n as $P(n)$.

2. Base case: Prove $P(1)$.

3. Inductive hypothesis: Assume $P(k)$.

4. Inductive step: Prove $P(k+1)$. [You should be using your inductive hypothesis as much as possible]

5. By the principal of mathematical induction, $P(n)$ holds for all positive integers n.

This may seem a little abstract, but it's really straightforward once you get the hang of it. The only work that needs to be done is the base case and inductive step. The other steps are there to make this rigorous. Here is an example.

Problem 5. Prove that the sum of the first n integers is $\frac{n(n+1)}{2}$.

Proof. I will follow the steps outlined above.

1. Denote by $P(n)$: the sum of the first n integers is $\frac{n(n+1)}{2}$.

2. $P(1)$ says that the sum of the first 1 integer is $\frac{1\times 2}{2} = 1$, which is definitely true!

3. Assume $P(k)$. In other words, assume that the sum of the first k integers is $\frac{k(k+1)}{2}$.

4. Now, we prove $P(k+1) =$ the sum of the first $k+1$ integers is $\frac{(k+1)(k+2)}{2}$. We need to somehow include our assumption from the previous step. Here is how it goes. The sum of the first $k+1$ integers is:

   $$1 + 2 + \cdots + k + (k+1) = (1 + 2 + \cdots + k) + (k+1).$$

   The first big bracket is just the sum of the first k integers and our assumption tells us that this is $\frac{k(k+1)}{2}$. So,

   $$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2} + 1\right) = (k+1)\frac{k+2}{2} = \frac{(k+1)(k+2)}{2}$$

   as we wanted.

5. By the principle of mathematical induction we have shown that the sum of the first n integers is $\frac{n(n+1)}{2}$.

□

Remark. Note, that in the above example we started at $n = 1$. Induction however, can start at any integer, including 0. You might have to prove a statement that starts at 8 or at -2. These are perfectly fine beginning numbers to start with. I include a geometric example of this.

Problem 6. Prove that a polygon with n sides (also called an n-gon) for $n \geq 3$, has a total internal angle sum of $180(n-2)$ degrees.

Proof. This is quite a difficult problem to prove if the n-gon is not convex, so for the purpose of conveying how to use induction, we will assume the polygon is convex (think of this as meaning that if I were to put a rubber band around the polygon it would snap exactly to the polygon itself).

1. Denote by $P(n)$: the angle sum of an n-gon is $180(n-2)$ degrees for $n \geq 3$.

2. $P(3)$ says that the angle sum of a triangle is $180(3-2) = 180$ degrees, which is definitely true!

3. Assume $P(k)$. In other words, assume that the angle sum of a k-gon is $180(k-2)$ degrees.

4. Now, we prove $P(k+1) =$ the angle sum of a $(k+1)$-gon is $180(k-1)$ degrees. We need to somehow include our assumption from the previous step. Here is how it goes.

   Take the $(k+1)$-gon and draw a line segment from one vertex to a vertex that is two away. You should now have the $(k+1)$-gon divided into two parts: a k-gon and a triangle. Also, it's clear that the total angle sum is the sum of the angles of the k-gon and the triangle. Thus, the angle sum of the $(k+1)$-gon is:
   $$180(k-2) + 180 = 180(k-1).$$

   The first term is just $P(k)$ (which we assumed in the inductive hypothesis) and the second term is the angle sum of a triangle. This is what we wanted.

5. By the principle of mathematical induction we have shown that the angle sum of an n-gon is $180(n-2)$ degrees.

□

In the standard induction method, we prove that the base case is true and then use the k^{th} case to prove the $(k+1)^{th}$ case. Sometimes this is not enough and it would be useful to use more than just the previous case.

3.1 Stronger Induction

The first method is to bundle a number of cases into one. For example, in the case of bundling two things together:

1. Identify what you are trying to prove. Write down the statement for n as $P(n)$. Then $Q(n)$ is the statement that $P(2n-1)$ and $P(2n)$ are both true.

2. Base case: Prove $Q(1)$. To do this, we need to show that $P(1)$ and $P(2)$ are true.

3. Inductive hypothesis: Assume $Q(k)$. Hence, we assume that $P(2k-1)$ and $P(2k)$ are both true.

4. Inductive step: Prove $Q(k+1)$ [You should be using your inductive hypothesis as much as possible]. This requires proving both $P(2k+1)$ and $P(2k+2)$.

5. By the principal of mathematical induction, $P(n)$ holds for all positive integers n.

Remark. When you prove $P(2k+1)$, you can of course use the assumptions that both $P(2k-1)$ and $P(2k)$ are true, but when you prove that $P(2k+1)$ is true, you can now assume that the previous *three* cases are true (as you just proved $P(2k+1)$)!

Remark. Again, one does not need to start at 1.

3.2 Strong Induction

This method is even more advanced, but easier to explain:

1. Identify what you are trying to prove. Write down the statement for n as $P(n)$.

2. Base case: Prove $P(1)$.

3. Inductive hypothesis: Assume $P(i)$ for $i = 1, 2, \ldots, k-1, k$.

4. Inductive step: Prove $P(k+1)$. [You should be using your inductive hypothesis as much as possible]

5. By the principal of mathematical induction, $P(n)$ holds for all positive integers n.

Essentially, in the inductive hypothesis, you can assume *all* previous cases!
Last example problem.

Problem 7. There are n lamps labeled $1, 2, \ldots, n$. Lamp 1 can be switched on or off at any time. Lamp k, where $1 < k \leq n$ can only be switched (on or off) when lamp $k-1$ is the only lamp that is on out of lamps $1, 2, \ldots, k-1$. If initially all lamps are off, how many moves does it take to switch on lamp n?

Proof. I claim, the answer is 2^{n-1}. So, $P(n)$ is that it takes at least 2^{n-1} moves to turn on lamp n. This is obviously true for lamp 1 as it takes $1 = 2^{1-1}$ move to turn on. I will use strong induction, so assume this is true for all $i = 1, 2, \ldots, k$ (ie, assume $P(1), P(2), \ldots, P(k)$). Let's show $P(k+1)$ is true. It took 2^{k-1} moves to turn on lamp k. When it turned on, by definition, lamp $k-1$ was on and no previous lamps. To turn on lamp $k+1$, we need to turn off lamp $k-1$. Turning off lamp $k-1$ is the same as turning it on when it was off, so by inductive hypothesis this takes another 2^{k-2} moves, but now we have lamp $k-2$ on and all previous lamps off (think about what needs to be happening to turn off lamp $k-1$). So, now we need to turn off lamp $k-2$, which takes 2^{k-3} moves and this continues all the way until we need to turn off lamp 1, which takes 1 move. So, we have used

$$2^{k-1} + 2^{k-2} + \cdots + 2^0 = 2^k - 1$$

moves (I used geometric series formula to calculate that). But then, you need one more move to turn on lamp $k+1$ now that only lamp k is on. So, we have used $2^k - 1 + 1 = 2^k$ moves! □

Problems

3.3 Easy

1. We need four matchsticks to make a square. Then three more of want to make two squares in a row. How many matchsticks do you need to make n connected squares in a row?

2. What if instead of one row, we are making two rows of n squares in each row. How many matchsticks are needed to make these $2n$ squares?

3. Same problem, but we have k rows of n squares. How many matchsticks do you need to make these kn squares?

4. Prove that
$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$
for every positive integer n.

5. Show that
$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$
for every positive integer n.

6. Show that
$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$
[Hint: use the previous problem]

7. Show that $n^2 < 2^n < n!$ for positive integers $n \geq 5$.

8. Prove that
$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 2.$$

9. Prove that
$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$
is unbounded, that is, it goes off to infinity.

3.4 Hard

1. A polygon is divided into triangles by diagonals of the polygon. Prove that it is possible to colour the vertices of the polygon with three colours so that each triangle has three different colours at its vertices.

2. Consider a graph (picture made up of just vertices and edges between them) such that every vertex has an even number of edges joining to it (also called an even valent graph). Show that one can draw all the edges without taking the pen off the paper and only going over every edge *exactly* once.

3. (Binary) Normally, we work in base ten, so $5436 = 5 \times 10^3 + 4 \times 10^2 + 3 \times 10^2 + 6 \times 10^0$. It turns out we can use any base. In particular, base 2 is called binary. In binary all the coefficients are 0 or 1 only and all the powers are powers of 2. Prove that every number can be *uniquely* expressed in binary form. [Hint: show every number can be written as a sum of distinct powers of two in a unique way.]

4. (Fibonacci Base) In this problem, your job is to prove that there exists a Fibonacci base: where the coefficients are 0 or 1 only and instead of powers of 2, instead we use Fibonacci numbers. So, $10110 = 1 \times f_4 + 0 \times f_3 + 1 \times f_2 + 1 \times f_1 + 0 \times f_0 = 1 \times 5 + 1 \times 2 + 1 \times 1 = 8$.

    - Prove that every positive integer can be represented in Fibonacci base form.

- Prove that if we also no longer allow consecutive 1s, then every number still has a Fibonacci base form.
- Prove that if we no longer allow consecutive 1s, then the Fibonacci form is actually unique.

[Note: $f_0 = 1, f_1 = 1, f_2 = 2, f_3 = 3, f_4 = 5, f_5 = 8, \ldots$]

5. Consider all the subsets of $\{1, 2, \ldots, n\}$. For each of these subsets, consider the reciprocal of the product of its elements. What is the sum of all these numbers? (Remember, the product of the elements of the empty set is 1)

4 Proof Techniques 1

In this section, we learn about other types of proofs, important parts of proofs or commonly occurring techniques.

4.1 If and only if, and the converse

If and only if, often written as iff is a very common word in problems. For example,

Problem 8. Prove that triangle ABC is right angled at A iff $AM = MB = MC$ where M is the midpoint of BC.

I will not prove this here, but I will comment on how one proceeds with a problem such as this. You must prove the 'if' ($\Leftarrow$) and the 'only if' ($\Rightarrow$) separately.

- $\Leftarrow$: Prove that triangle ABC is right angled at A if $AM = MB = MC$ where M is the midpoint of BC.
- $\Rightarrow$: Prove that if triangle ABC is right angled at A then $AM = MB = MC$ where M is the midpoint of BC.

I changed the wording somewhat, so that you can get a better feel for what 'if' and 'only if' mean.

Remark. Once you have proved an 'iff', what you have is that the statements on either side are equivalent, like $2 + 2$ and 4 are equivalent, and can be used interchangeably everywhere.

Definition. If we prove conditions A imply a result B ($A \implies B$), then the *converse* is that the result B implies the conditions A ($B \implies A$).

Remark. VERY IMPORTANT. The converse is not the same thing and is *often* false. For example, a shape is a square $\implies$ the shape is a rectangle. But going backwards is obviously false. In an iff statement, however, the converse is true, so you need to prove one way and then the other (which is the converse). Proving the converse can often need completely different ideas.

4.2 Contrapositive

Proving the contrapositive is a proof technique very similar to proof by contradiction. I will use similar language to explain how it works. Let's say a problem asks you to prove statement B given known conditions A, or

$$A \implies B.$$

Another way one could prove this is to prove that the opposite of statement B implies the opposite of the conditions A, or

$$B^c \implies A^c.$$

This is equivalent to $A \implies B$, so if you do this you are done.

Remark. Compare this to proof by contradiction and converse. They all sound similar but they are all different.

Here is an example of proof by contrapositive:

Problem 9. If a and b are integers, such that ab is even, show that either a or b must be even.

Proof. a and b being integers is going to be taken as fact. Our given condition A is that ab is even and our result B that we want to prove is that either a or b is even. So, using the contrapositive, we ignore the condition A and take the opposite of B, which is that both a and b are odd. (Can you see how that is the opposite?) Now, if both a and b are odd, then multiplying them gives an odd number. We can see this easily by calling $a = 2k + 1$ and $b = 2\ell + 1$. Then $ab = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1$ is odd. But this is the opposite of A. So, we have proven

$$B^c \implies A^c.$$

By contrapositive, this means that $A \implies B$ and hence if ab is even, then one of a or b is even. □

4.3 Pigeonhole Principle

You may recall from the section on proof by contradiction, a little result called the pigeonhole principle. The idea is really intuitive. If I have six gifts, but only five friends, one of them will have to get more than one gift. And if I had 11 friends, one of them would have to get more than two gifts. The general statement is as follows:

Pigeonhole Principle. If there are $nk + 1$ pigeons and n pigeonholes, then at least one of the pigeonholes will have at least $k + 1$ pigeons.

Remark. Notice all of the "at leasts". They are crucial. Only in the worst case scenario (or best case depending on how you look at it), will every pigeonhole have exactly k pigeons except for one which has exactly $k + 1$ pigeons. In the vast majority of cases that pigeonhole may have more then $k + 1$ pigeons and it may not be the only pigeonhole to do so.

Remark. Note, one can replace $nk + 1$ by any number strictly bigger than nk.

There is also an infinite version:

Infinite Pigeonhole Principle. If there are an infinite number of pigeons and n pigeonholes, then at least one of the pigeonholes will have an infinite number of pigeons.

4.4 Telescoping Series

This is more of a technique than a proof style. You may in your work reduce the problem to a summation. For example, to the sum of the first n odd integers. How do you calculate the sum? Telescoping series is about rewriting each term of the sum as the difference of two terms where the one being subtracted from becomes the one subtracted in the next term. The idea being that all of the terms except the first and last cancel and the calculation becomes easy. Here is an example:

Problem 10. Find the sum of the first n odd integers:

$$\sum_{i=0}^{n-1} 2i + 1$$

Proof. Notice that $2i + 1 = (i + 1)^2 - i^2$. In other words, every odd integer is the difference of consecutive squares. Then, expanding the summation yields

$$\begin{aligned}\sum_{i=0}^{n-1} 2i + 1 = \sum_{i=0}^{n-1} (i+1)^2 - i^2 &= n^2 - (n-1)^2 \\ &\quad + (n-1)^2 - (n-2)^2 \\ &\qquad + (n-2)^2 - (n-3)^2 \\ &\qquad\quad + (n-3)^2 - \cdots \\ &\qquad\qquad + 2^2 - 1^2 \\ &\qquad\qquad\quad + 1^2 - 0^2 \\ &= n^2 - 0^2 = n^2\end{aligned}$$

□

Notice, how things in the same column cancel each other out. It is more standard to expand the sum from 0 to $n - 1$, but the reverse was done to exhibit the telescoping series much better.

Problems

4.5 Easy

1. (Contrapositive) Why is the contrapositive ($B^c \implies A^c$), the same as a direct proof ($A \implies B$)?

2. (Pigeon Hole Principle)There are n people in a room. Prove that there must exist two of them who have the same number of acquaintances in the room.

3. (Pigeon Hole Principle) Show that if we take $n+1$ numbers from the set $\{1, 2, 3, \ldots, 2n\}$, there exist two which are relatively prime.

4. (Pigeon Hole Principle)If knowing is mutual, prove that among every six people you can find three that either all know each other or all don't.

5. Using Pythagoras's theorem and congruent triangles, prove the converse of Pythagoras's Theorem.

6. (Telescoping Series) What is
$$\sum_{i=0}^{n} (i+2)2^i?$$

7. (Contrapositive) Prove $\sqrt{2}$ is irrational.

4.6 Hard

1. What is
$$\sum_{i=1}^{n} \frac{1}{i \times (i+1)}?$$

2. Prove that from a set of ten distinct two-digit numbers, it is possible to select two disjoint subsets whose members have the same sum.

3. If there are five points in a square with side length 1 metre, prove that two of them are less than 75 centimetres apart.

4. If there are seven points in a circle with radius 1 metre, prove that two of them are less than 1 metre apart. What if there are only six points?

5. Let n be a given positive integer. Prove that the sequence $a, a^a, a^{a^a}, a^{a^{a^a}}, \ldots$ is eventually constant modulo n for any positive integer a.

5 Proof Techniques 2

In this section, we learn about more difficult proof techniques. This is definitely more advanced than Proof Techniques 1, however, keep this as a reference for future use and do your best to understand these ideas.

5.1 Extremal Principle

The extremal principle is the idea of looking at an extremal object. This means looking at something that is the smallest or largest when it comes to some important feature. For example, if it is a question about a graph, it might be worth considering the vertex with the greatest valency (number of edges connected to it). Or if it is a question about roads between towns, it might be worth considering the shortest road. Here is an example problem, which is a really important example in graph theory.

Problem 11. If we have n vertices, prove that the maximum number of edges one can draw between these vertices, so that there are no cycles, is $n-1$. In fact, such a graph with n vertices, $n-1$ edges and no cycles is called a *spanning tree*.

Proof. Consider a graph with n vertices and no cycles. I want to consider a vertex with smallest valency. I claim this vertex has valency 0 or 1. Suppose the contrary; suppose each vertex has valency at least 2. Start with any vertex. Since the valency is at least 2, there is an edge connected to it, so travel along this edge to another vertex. Since this vertex has valency at least 2, there is a different edge connected to this vertex, so travel along it. If you continue this way you must reach a vertex you have already been on, otherwise you would be able to iterate infinitely and hence have an infinite number of vertices, which is obviously false. (This is actually an application of infinite pigeonhole principle.) But since you've reached a vertex you have already been on, you have a cycle! This is a contradiction, so not all of the edges can have valency at least 2. Therefore, the vertex with smallest valency has valency 0 or 1.
If the valency of this smallest valency vertex is 0, it is an isolated vertex, so remove it. If the valency is 1, it has one edge connected to it, so remove the vertex and the edge. Either way we are left with a graph that still has no cycles. So, again the vertex with smallest valency in this smaller graph must have valency 0 or 1. So, do the same removal process. Continue until you have removed all the vertices but one. This last graph has a single vertex. There are no edges since it would otherwise be an edge from this vertex to itself and hence a cycle.
So we removed $n-1$ vertices and with each vertex either 0 or 1 edges, so we removed at most $n-1$ edges. And then there are no edges left. So, originally there must have been at most $n-1$ edges.
It is actually possible to draw $n-1$ edges without making a cycle. Choose a random vertex and draw one edge to every other vertex. This has no cycles and $n-1$ edges! □

Remark. Please be really careful. There isn't always a largest or smallest object. For example, consider an infinite line of people each one metre apart from the next person. If the first person is given the number 1, the next person, the number $\frac{1}{2}$, the third person, the number $\frac{1}{3}$ and so on; then it turns out that there is no person with the smallest number! Whoever, you pick the person one metre further always has a smallest number.

5.2 Infinite Descent

Infinite Descent is an alternative to the extremal principle. Rather than using, say, a smallest object, we use any object and from it find a smaller object. We continue this infinitely showing that there is no smallest object, which hopefully is a contradiction (note, the remark in the extremal principle section mentioned that it is sometimes possible to have no smallest object). Here are the steps in order:

- Consider an object that satisfies the properties in the problem.
- Find a method to construct another 'smaller' object from the first object, using a method we can hopefully iterate.
- Iterate this method infinitely, and conclude there is no smallest object.

- Show that there is a smallest object, so we have a contradiction and there are in fact no such objects at all!

This should still be somewhat unclear. We have two things to discuss: what does it mean to be smaller and when is there a smallest object? I shall try to illuminate the answers to these questions with an example problem.

Problem 12. Show that $\sqrt{2}$ is irrational.

How is this an infinite descent problem? Well, suppose $\sqrt{2}$ is rational. Then there is a solution to the equation

$$\sqrt{2} = \frac{x}{y}$$

in integers x and y. So, our objects can be pairs (x, y) which are solutions to this equation. How can we define the size of a solution and what does it mean to be smaller? Well, there are many things one could do here. We could consider the size of a solution (x, y) to be the sum $x + y$ or the product xy. In our case, we will define the size of a solution to be the greatest common divisor of the numerator and denominator, or $\gcd(x, y)$. So, if $\frac{x}{y}$ is more reduced, it's a smaller solution! We are ready to solve the problem.

Proof. As above, suppose $\sqrt{2}$ is rational and consider solutions (x, y) to the equation

$$\sqrt{2} = \frac{x}{y}.$$

Define the size of a solution to be $\gcd(x, y)$. Now, squaring both sides and multiplying through by y^2 yields

$$2y^2 = x^2.$$

Since the left hand side is even, so must the right hand side be and therefore x is even. Let $x = 2x_1$. Expanding out and dividing by 2 gives

$$y^2 = 2x_1^2$$

and the same argument implies y is even, so let it be $y = 2y_1$, substitute and divide by 2, to get

$$2y_1^2 = x_1^2.$$

This of course, rearranges to $\sqrt{2} = \frac{x_1}{y_1}$ and so (x_1, y_1) is another solution. Is it smaller? Well, x_1 and y_1 are both exactly half of x and y, so their gcd is now half of the original gcd. We have that the size of (x_1, y_1) is half the size of (x, y). We have found a smaller solution! Notice, however, that we can just do the same working again to get a new solution (x_2, y_2) which is half the size of (x_1, y_1).

The crux of the proof is that we can iterate infinitely, so there is no smallest solution! But this is a contradiction, because any two numbers only have a finite number of factors of 2, so you cannot do this infinitely. This means that there wasn't a solution to begin with and therefore, $\sqrt{2}$ is not rational. □

Remark. The contradiction at the end requires there to be a smallest object/solution. One way to try and guarantee such a smallest object is to define the size of the objects in such a way that they are always positive integers, because then you can use this famous axiom of the natural numbers:

Well-Ordering Principle. Every non-empty set of positive integers, has a smallest element.

It applied to our problem, because we kept taking out a power of two from both x and y. Since the possibilities for the power of two that is common to both x and y is any positive integer or zero, when we keep taking one away, it will eventually reach zero and then you cannot go any further!

5.3 Without Loss of Generality

If you have three real numbers whose average is 1, why is it obvious that one of the numbers is at least 1? It's because the situation is completely symmetric in the three numbers and we can assume *without loss of generality* (or WLOG) that one of the numbers is the biggest. So, if the three numbers are a, b and c, then WLOG assume a is the biggest. In other words $a \geq b$ and $a \geq c$. Since $a + b + c = 3$, it follows that $3a \geq a + b + c = 3$ and so $a \geq 1$ as we thought!

Be careful, this can only be used if the situation really is symmetric. If $2a + b + c = 4$, it is clear that a is special; it does not behave like b or c. However, b and c behave symmetrically, so one could WLOG that $b \geq c$, for example.

To see how powerful this technique can be, I provide the following very difficult problem that appeared in the 1992 International Mathematical Olympiad:

Problem 13. Find all integers a, b, c greater than 1, such that

$$(a-1)(b-1)(c-1) \text{ is a divisor of } abc - 1.$$

Proof. I will not complete the entire proof, but I will leave a few hints as to how to finish it off at the end. What I will do is show you how using WLOG will greatly simplify the problem for me.

Since the problem is completely symmetric in a, b and c, WLOG that $a \geq b \geq c$. This gives us that $ab + bc + ac \leq ab + ab + ab = 3ab$. We also have very obviously that $a + b + c - 1 > -\frac{1}{2}$. So, if $c \geq 6$, we have

$$\begin{aligned}(a-1)(b-1)(c-1) = abc - ab - ac - bc + a + b + c - 1 &> abc - 3ab - \frac{1}{2} \\ &\geq abc - \frac{1}{2}abc - \frac{1}{2} \\ &= \frac{1}{2}(abc - 1).\end{aligned}$$

This gives us $(a-1)(b-1)(c-1) > \frac{1}{2}(abc-1)$, which we cannot have, since $(a-1)(b-1)(c-1)$ is a divisor of $abc - 1$ and they are clearly not equal. So, $c < 6$. We can now try $c = 2$, $c = 3$, $c = 4$ and $c = 5$ separately. This is really good, because in each case we have simplified the problem down to two variables only. In fact, an identical idea will produce a maximal value for b in each case and so it will be a matter of simply substituting this in and seeing what values a can take. [Try it!] □

Remark. The problem as it appeared on the 1992 IMO actually specified that a, b, c should all be distinct, but this isn't necessary to my point above. The WLOG meant we could bound $ab + bc + ac$, which meant we got a maximum value for c!

5.4 Reverse Reconstruction

The idea of reverse reconstruction is a very simple one. If the situation described in the problem is unique and you can construct a situation that satisfies the problem, then that is the only situation the problem is describing and you can use every fact about what you constructed. This is most often applied in geometry problems, since it is more common that diagrams are unique. This problem illustrates this.

Problem 14. Given a square $ABCD$, consider the point P such that P is inside the square and $\angle BAP = \angle ABP = 15°$. Prove that PCD is equilateral.

Proof. I won't draw the diagram as it is a useful exercise for you. The really interesting thing about this problem is that it is very difficult to prove directly. But consider this: since $\angle BAP = 15°$, P lies on the line defined by the 15 degree angle. Similarly, P lies on the line defined by the other 15 degree angle. As these lines are not parallel they meet in only one point, so P is uniquely defined. There is only one diagram!

Since there is only one diagram, draw the following: draw square $ABCD$ and construct an equilateral triangle CDQ with Q on the interior of the square. Draw QA and QB. Now lets find some angles. $\angle CDQ = 60°$, so $\angle QDA = 30°$. Since $\triangle QCD$ is equilateral and $ABCD$ is a square, $QD = DC = DA$, so $\triangle QDA$ is isosceles and hence, $\angle QAD = 75°$. And then $\angle QAB = 15°$. Similarly, $\angle QBA = 15°$. Since these angles are $15°$, we have the unique diagram described in the problem. So $Q = P$. So, PCD is equilateral. □

Problems

5.5 Easy

1. (Extremal Principle) In every square in a rectangular grid, a number has been written such that each number is the average of the numbers in the neighbouring squares. Show that all of the numbers must be equal.

2. (*WLOG*) Determine all triplets (x, y, z) of positive integers such that the following 3 conditions all hold.

$$x|y+z,\ y|z+x,\ z|x+y$$

3. (Extremal Principle) There are $2n$ points in the plane with no three collinear. Exactly n of these points are farms and the remaining n points are wells. We would like to join each farm to a well with a straight road, with no two farms sharing a well. Show that this can be accomplished so that no two of the roads intersect.

5.6 Hard

1. Show that there are no positive solutions to the equation $a^2 + b^2 = 3c^2$.

2. Show there are no solutions to $a^3 + 3b^3 = 9c^3$ in positive integers.

3. There are n petrol stations along a road circuit. The total petrol from all the stations is just enough for David's car to go around the circuit once. Prove that David can start at one of the petrol stations with an empty tank, and do a complete lap of the circuit.

4. Prove that in any polyhedron, there are two faces with the same number of vertices. [Hint: you may want to use the fact that $v - e + f = 2$ where v is the number of vertices, e the number of edges and f the number of faces.

5. (Fermat's Last Theorem, $n = 4$) Show that there is no solution in positive integers of the equation

$$x^4 + y^4 = z^4$$

by showing there is actually no solution in positive integers of the equation

$$x^2 + y^4 = z^4.$$

[Hint: you will need to use the fact that integer solutions to Pythagoras' Theorem are of the form $(k(a^2 - b^2), 2kab, k(a^2 + b^2))$]