Year 11 Spec Week 1/2

Yape

Pre-note-note: Hi this is the first of the weekly/fortnightly/we'll see how long this lasts, notes. I hope you all find it somewhat useful.

1 Proofs

Intro

We start spec with proofs and they're quite intimidating. However, proofs - perhaps beside inequalities - are actually very much straightforward if they didn't have the word 'Prove' there. What I'm saying is that if I asked you 'a is an even number, and b is an even number. Show $a + b$ is even', then you'd be like well no shit. Proofs are mathematicians way of making the 'well no shit' more rigorous. Unfortunately that involves

Definitions

When we want to deal with, odd, even, numbers divisible by 3, rationals and irrationals, we want to make these into tangible mathematical definitions.

First, we have some notation for the type of numbers we deal with:

Type	Symbol	Example
Real	$\mathbb{R}$	$\pi, 11, 4.3$
Rational	$\mathbb{Q}$	$\frac{22}{7}$
Integer	$\mathbb{Z}$	$-1, 0, 1$
Positive integer	$\mathbb{N}$	$7, 15$

Table 1.1: Caption

- If n is even, then write "Let $n = 2k$ **for some** $k \in \mathbb{Z}$**.**"
- If n is odd, then write "Let $n = 2k + 1$ for some $k \in \mathbb{Z}$."
- If n is rational, then write "Let $n = \frac{p}{q}$ for some $(p, q) \in \mathbb{Z}$."
  - Actually, we can write $\gcd(p, q) = 1$ as well, which you'll see in contradiction proofs.

- If n is divisible by d for some integer d, then write $n = dk$, for some $k \in \mathbb{Z}$.
  - For example, If n is divisible by 3, then write "Let $n = 3k$, for some $k \in \mathbb{Z}$."

The "for some $k \in \mathbb{Z}$" part is very very important. Don't leave it out.

Direct Proofs

Direct proof takes on the form of an implication. You want to show directly, through some manipulation or chain of reasoning that a statement A implies a statement B ($A \implies B$)

Example 1.1. *Prove that if a is even and b is even, then $a + b$ is even.*

Proof. Let $a = 2m$ and $b = 2n$ for some integers m and n. Then, we have

$$a + b = 2m + 2n = 2(m + n) \dots \text{ for some } m + n \in \mathbb{Z}$$

Therefore, $a + b$ is an even number. □

The form of these even/odd type proofs is always you're given some starting numbers and an expression to prove is odd/even.

1. Define your numbers (e.g. $a = 2m$, $b = 2n$ for some integers m and n.)
2. Manipulate the expression (e.g. $a + b = 2m + 2n$)
3. Factorise the expression to get it into the form of **the definition of odd/even** (e.g. $2m + 2n = 2(m + n) \dots$ for some $m + n \in \mathbb{Z}$
4. Closing statement. (e.g. Therefore $a + b$ is an even number)

Now I recommend doing the next question following those steps.

Example 1.2. *Prove that if a and b are odd numbers, ab is also odd.*

Proof. Let $a = 2m + 1$ and $b = 2n + 1$ for some $(m, n) \in \mathbb{Z}$. Then,

$$\begin{aligned} ab &= (2m + 1)(2n + 1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1 \dots \text{ where } 2mn + m + n \in \mathbb{Z} \end{aligned}$$

Thus, ab is odd. □

Example 1.3. *Prove that $2^n - 1$ is odd for all integers $n \geq 1$.*

Proof. Let $n \in \mathbb{Z}$. Then,

$$2^n - 1 = 2(2^{n-1}) - 1 \ldots \text{ for some } 2^{n-1} \in \mathbb{Z}$$

□

Contrapositive

The contrapositive statement is the opposite of the statements in the opposite order. So if $P \implies Q$ then the contrapositive is $Q' \implies P'$ where P' and Q' are the opposite of the statements P and Q. For example, the contrapositive of

$$\text{“It is raining”} \implies \text{“The floor is wet.”}$$
$$\text{“The floor is not wet”} \implies \text{“It is not raining.”}$$

Contrapositive is useful because **if the contrapositive is true then the original is true.**[1]

An advantage of contrapositive is that it can prove statements that direct proof sometimes cannot.

Example 1.4. *Prove that if n^2 is even then n is even.*

Proof. We prove the contrapositive statement

“If n is not even (odd) then n^2 is not even (odd).”

We proceed as per our direct proof.

Let $n = 2k + 1$, for some $k \in \mathbb{Z}$. Then,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \ldots \text{ for some } 2k^2 + 2k + 1 \in \mathbb{Z}$$

□

Example 1.5. *Prove that if mn is even and $m + n$ is even, then m and n are even.*

Proof. Careful! The contrapositive of “X and Y” is “not X or not Y”. The contrapositive of the above is:

[1]Use proof by contradiction to see this is true.

"If one of m or n are not even then one of mn or $m+n$ is not even."

Case 1: Exactly one of m or n are odd, and the other is even. Let $m = 2a+1$ and $n = 2b$ for some $(a, b) \in \mathbb{Z}$ then

$$m + n = 2a + 2b + 1 = 2(a + b) + 1 \ldots \text{ for some } a + b \in \mathbb{Z}$$

If $m = 2a$ and $n = 2b + 1$ for some $(a, b) \in \mathbb{Z}$ then

$$m + n = 2a + 2b + 1 = 2(a + b) + 1 \ldots \text{ for some } a + b \in \mathbb{Z}$$

Thus, $a + b$ is odd.

Case 2: Both m and n are odd. Let $m = 2a + 1$ and $n = 2b + 1$ for $(a, b) \in \mathbb{Z}$. Then,

$$mn = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1 \ldots \text{ for some } 2ab + a + b \in \mathbb{Z}$$

Thus, mn is odd. □

Casework

Example 1.6. *Show the product of six consecutive odd numbers is divisible by 9.*

In examples like this, we can't define n like we did in odd even proofs. For example, to say n is not divisible by 3, I will have to split this argument into two cases; one where $n = 3m + 1$ and one where $n = 3m + 2$, for some $m \in \mathbb{N}$.

Proof. Let the first of the six consecutive odd numbers be n. We split the proof into cases.

Case 1: $n = 6m + 1$. Then, the six consecutive odds are:

$$6m + 1, 6m + 3, 6m + 5, 6m + 7, 6m + 9, 6m + 11$$

Their product is

$$\begin{aligned}
&(6m + 1)(6m + 3)(6m + 5)(6m + 7)(6m + 9)(6m + 11) \\
&= (6m + 1) \times 3(2m + 1) \times (6m + 5)(6m + 7) \times 3 \times (2m + 3) \times (6m + 11) \\
&= 9(6m + 1)(2m + 1)(6m + 5)(6m + 7)(2m + 3)(6m + 11) \\
&= 9k \ldots \text{ for some } k \in \mathbb{Z}
\end{aligned}$$

Case 2: $n = 6m + 3$. Observe the six consecutive odds still contain $6m + 3$ and $6m + 9$. Thus, the product will still be divisible by 9.

Case 3: $n = 6m + 5$. Observe the six consecutive odds are $6m + 5, 6m + 7, 6m + 9, 6m + 11, 6m + 13, 6m + 15$. Then,

$$\begin{aligned}
&(6m + 5)(6m + 7)(6m + 9)(6m + 11)(6m + 13)(6m + 15) \\
&= (6m + 5)(6m + 7)(3 \cdot (2m + 3))(6m + 11)(6m + 13)(3 \cdot (2m + 5)) \\
&= 9k \ldots \text{ for some } k \in \mathbb{Z}
\end{aligned}$$

□

Converse

When we switch the direction of the statement from $P \implies Q$ to $Q \implies P$ this is the converse. This is NOT the contrapositive, don't mix them up. Here's an example Do be careful though. The

Statement	Converse
If $a \in \mathbb{R}$ and $a = 0$ then $a^2 = 0$	If $a \in \mathbb{R}$ and $a^2 = 0$ then $a = 0$.

converse is not necessarily true. In the example above, it is. Another converse statement example is the Pythagorean theorem.

Statement	Converse
If $\angle ABC = 90°$ then $AB^2 + BC^2 = AC^2$	If $AB^2 + BC^2 = AC^2$ then $\angle ABC = 90°$

When the converse and statement are true, we use the notation $P \iff Q$ (reads P is true **if and only if** Q is true). What this means is that $P \implies Q$ and $Q \implies P$.

If you are asked to prove $P \iff Q$, split the proof into two parts; showing $P \implies Q$ and $Q \implies P$.

Inequalities

Inequalities really deserve their own topic, but in the scheme of Year 11 proofs this tactic suffices:

$$\text{If } x \in \mathbb{R} \text{ then } x^2 \geq 0.$$

Say you wish to prove for some expressions A, B that $A \geq B$. You start of by trying to show $A - B \geq 0$. From there, you want to show $A - B$ is a square of some expression or a sum of those squares.

Example 1.7. *Prove that for any real numbers x and y that $x^2 + y^2 \geq 2xy$.*

Working Out

I wish to show that $x^2 + y^2 - 2xy \geq 0$ so I want $x^2 + y^2 - 2xy$ to be a square. Luckily, we see (or maybe not) that $(x - y)^2 = x^2 - 2xy + y^2$.

Proof

Proof. Observe that

$$\begin{aligned} (x-y)^2 &\geq 0 \\ \implies x^2 - 2xy + y^2 &\geq 0 \\ \implies x^2 + y^2 &\geq 2xy \end{aligned}$$

□

See how I wrote the proof in the logically consistent order? I start with a true statement (square is non-negative) and through a chain of implies symbols I get to the statement I want to prove. This is the "morally" right way to do inequalities.

Three Important Symbols

The symbol $\forall$ means "for all" and is used like this $\forall x \in \mathbb{R}$. This means "for all real numbers x".
The symbol $\exists$ means "there exists" and is used like this $\exists x \in \mathbb{R}$ such that $x^2 = 0$ meaning "there exists a real number x such that $x^2 = 0$."
We can also write $\nexists$ to mean "there doesn't exist". For example, "$\nexists x \in \mathbb{R}$ such that $x^2 = -1$.
Mathematicians like compact notation that makes shit look 100 times smarter, when it really isn't.

Contradiction

A proof by contradiction begins by assuming the statement we wish to prove is false. Then, with a series of deductions we arrive at the conclusion that this assumption leads to some nonsense (e.g. $0 = 1$, [2] or odd = even).

So, if the statement you want to prove is $P \implies Q$, assume that $P \implies Q'$, and obtain a contradiction.

There's no explicit pattern to how these type of problems go, **just play around and try to poke at things you think would seem "off" if the contradiction assumption is true.**

I'll just try give as many example problems here as possible

> **Example 1.8.** *Show $\sqrt{2}$ is irrational.*

Proof. Assume for a contradiction $\sqrt{2} = \frac{p}{q}$, for some $(p, q) \in \mathbb{Z}$ where p **and** q **don't share any common factors** Then,

$$\begin{aligned}
\sqrt{2} &= \frac{p}{q} \\
2 &= \frac{p^2}{q^2} \\
p^2 &= 2q^2 \\
&\implies p^2 \text{ is divisible by } 2 \\
&\implies p \text{ is divisible by } 2 \\
\text{Let } p = 2a, \text{ for some } n \in \mathbb{Z}, \\
(2a)^2 &= q^2 \\
\therefore 2a^2 &= q^2
\end{aligned}$$

[2]seriously I have got this before

A similar argument yields q is divisible by 2. However, now p and q are both divisible by 2, contradicting the bolded claim that p and q don't share any factors. $\square$

Example 1.9. *Given the fact that x^2 can only have a remainder of 0 or 1 on division by 4, for all $x \in \mathbb{Z}$ prove that:*

If $a^2 + b^2 = c^2$, for some $a, b, c \in \mathbb{Z}$ then one of a or b are even.

Proof. Assume for contradiction that $a^2 + b^2 = c^2$ for some $a, b, c \in \mathbb{Z}$ and both a and b are odd. Then, let $a = 2m + 1$ and $b = 2n + 1$, for some $m, n \in \mathbb{Z}$. We obtain

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2m+1)^2 + (2n+1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\ &= 4(m^2 + m + n^2 + n) + 2 \end{aligned}$$

We are given that x^2 can only have remainder of 0 or 1 on division by 4, however c^2 leaves a remainder of 2 on division by 4... $\lightning$ $\square$

Example 1.10. *(Most difficult question in spec) Let $a, b, c \in \mathbb{Z}$ all be odd numbers. Show $ax^2 + bx + c = 0$ has no rational roots.*

Proof. Assume for contradiction $x = \frac{p}{q}$ is a root, for some $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$. Then,

$$\begin{aligned} 0 &= ax^2 + bx + c \\ &= a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c \\ \therefore 0 &= ap^2 + bpq + cq^2 \ldots \text{multiply through by } q^2 \end{aligned}$$

We now employ casework.

Case 1: Let p and q be odd. Then, ap^2 is odd, bpq is odd and cq^2 are all odd. Thus, $0 = ap^2 + bpq + cq^2$ is odd... $\lightning$

Case 2: Let p be even and q be odd. Then, ap^2 is even, bpq is even and cq^2 is odd so $0 = ap^2 + bpq + cq^2$ is odd... $\lightning$

Case 3: Let p be odd and q be even. Then, cq^2 is even, bpq is even and ap^2 is odd. Thus, $0 = ap^2 + bpq + cq^2$ is odd... $\lightning$

Case 4: Let p, q be even. But then 2 divides p and q, contradicting $\gcd(p, q) = 1 \ldots$ ↯

$\therefore$ Our assumption must be false, and $ax^2 + bx + c = 0$ has no rational roots, when $a, b, c \in \mathbb{Z}$ are all odd. $\square$