# MATH1081 – Seminar solutions

## [Proofs & Logic]

Written by: Gerald Huang

Updated on *May 1, 2020*

The following document are full worked solutions to the questions that was discussed in the revision seminar on April 30, 2020. The solutions were written by Gerald Huang and can be used as supplement resources while preparing for final exams. Please use this resource ethically. The following document is **NOT** endorsed by the School of Mathematics and Statistics and may be prone to errors; if you spot an error, please message us here. Happy studying!

## Contents

## Part I: Seminar solutions

(2017 S2, Q3i)
Show, using truth tables, that $(p \to q) \vee (\sim p \to r)$ is a tautology.

SOLUTION.

| $p$ | $q$ | $r$ | $p \to q$ | $\sim p \to r$ | $(p \to q) \vee (\sim p \to r)$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $T$ | $T$ |
| $T$ | $T$ | $F$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ | $F$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $F$ | $T$ | $T$ |
| $F$ | $T$ | $T$ | $T$ | $T$ | $T$ |
| $F$ | $T$ | $F$ | $T$ | $F$ | $T$ |
| $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $F$ | $T$ | $F$ | $T$ |

We see that, regardless of what truth values we pick for $p$, $q$ and $r$ are, the statement holds true. Hence, the statement is a **tautology**.

(2017 S2, Q3ii)
Show, using standard logical equivalences, $(q \vee \sim r) \to p$ is logically equivalent to $(r \vee p) \wedge (q \to p)$.

SOLUTION.
Recall that

$$p \to q \equiv \sim p \vee q.$$

Then, applying this definition to the proof, we have

$$\begin{aligned}
(q \vee \sim r) \to p &\equiv \sim (q \vee \sim r) \vee p && \text{(defn of implication)}\\
&\equiv (\sim q \wedge \sim (\sim r)) \vee p && \text{(De Morgan's law)}\\
&\equiv (\sim q \wedge r) \vee p && \text{(double negation law)}\\
&\equiv p \vee (\sim q \wedge r) && \text{(commutative law)}\\
&\equiv (p \vee \sim q) \wedge (p \vee r) && \text{(distributive law)}\\
&\equiv (\sim q \vee p) \wedge (r \vee p) && \text{(commutative law)}\\
&\equiv (q \to p) \wedge (r \vee p) && \text{(defn of implication)}\\
&\equiv (r \vee p) \wedge (q \to p) && \text{(commutative law)}
\end{aligned}$$

(2018 S2, Q3iv)
Let $a_1, a_2, a_3, \cdots$ be a sequence of real numbers. The definition of the *limit* of the sequence, $\lim_{n\to\infty} a_n = \ell$, is

$$\forall \epsilon > 0 \, \exists N \in \mathbb{N} : \forall n \geq N \;\; |a_n - \ell| < \epsilon \qquad (*)$$

Write in symbolic form the negation of $(*)$, and simplify your answer so that the negation symbol is not used.

SOLUTION.
We can break this statement into two parts; the first part we shall consider is the section

$$\forall \epsilon > 0 \;\; \exists N \in \mathbb{N}.$$

Recall the following negations

$$\neg\forall \longrightarrow \exists, \quad \neg\exists \longrightarrow \forall.$$

To negate the first part, we simply swap all instances of $\forall$ to $\exists$ and vice versa. Hence, the negation is

$$\exists \epsilon > 0 \;\; \forall N \in \mathbb{N}.$$

Consider the second half of the statement. This is an implied "implication" statement. To negate this statement, we simply negate our quantifier and note that the negation of $<$ is $\geq$. Hence, we have

$$\exists n \geq N \;\; |a_n - \ell| \geq \epsilon.$$

Altogether this gives us the negation

$$\exists \epsilon > 0 \;\; \forall N \in \mathbb{N} : \;\; \exists n \geq N \;\; |a_n - \ell| \geq \epsilon.$$

In words, we're saying

> *There exists an $\epsilon > 0$ such that for all natural numbers $N$, there is an $n \geq N$ such that $|a_n - \ell| \geq \epsilon$.*

(2016 S1, Q3iv)
A function $f$ defined on the open interval $D = (a, b)$ is called **uniformly continuous on** $D$ if and only if

$$\forall \epsilon > 0 \, \exists \delta > 0 \, \forall x_0 \in D \, \forall x \in D :$$
$$|x - x_0| < \delta \to |f(x) - f(x_0)| < \epsilon.$$

Write down the negation of this definition, simplified so that it does not contain the "not" symbol.

SOLUTION.
Recall the following negations

$$\neg\forall \longrightarrow \exists, \quad \neg\exists \longrightarrow \forall, \quad \neg(p \to q) \longrightarrow p \wedge \neg q.$$

Using these pieces of information, we can then break down our original statement. Let's consider the first half of the statement. The negation of

$$\forall \epsilon > 0 \;\; \exists \delta > 0 \;\; \forall x_0 \in D \;\; \forall x \in D$$

is

$$\exists \epsilon > 0 \;\; \forall \delta > 0 \;\; \exists x_0 \in D \;\; \exists x \in D.$$

We're simply negating all of our logical quantifiers.

The second half of the statement is an implication. So we need to use our implication negation. Hence, the negation of

$$\underbrace{|x - x_0| < \delta}_{p} \to \underbrace{|f(x) - f(x_0)| < \epsilon}_{q}$$

is

$$|x - x_0| < \delta \;\wedge\; |f(x) - f(x_0)| \geq \epsilon.$$

Altogether, this is saying that the negation of our original statement is

$$\exists \epsilon > 0 \;\; \forall \delta > 0 \;\; \exists x_0 \in D \;\; \exists x \in D$$
$$|x - x_0| < \delta \;\wedge\; |f(x) - f(x_0)| \geq \epsilon.$$

In words, we're saying

> *There exists an $\epsilon > 0$ such that for all $\delta > 0$, there is an $x_0$ and $x \in D$ so that **both** $|x - x_0| < \delta$ and $|f(x) - f(x_0)| \geq \epsilon$ are true.*

(2019 T2, Q3ii)
Consider the following argument. "If I buy a new car then I will have to give up eating out and seeing movies. If I have to give up eating out then I won't give up seeing movies. Therefore, I won't buy a car."
Show that the argument is **logically valid**.

SOLUTION.
Define the following propositions:

$$\begin{aligned} p &\implies \text{"buy new car"}. \\ q &\implies \text{"give up eating"}. \\ r &\implies \text{"give up seeing movies"}. \end{aligned}$$

Construct the following hypotheses and conclusion:

- **Hypotheses**

$$p \to q \wedge r.$$
$$q \to \sim r.$$

- **Conclusion**

$$\therefore \sim p.$$

Finally, construct a truth table and reject all of the rows that reject the hypotheses (ie any of the hypotheses result in an $F$). In the following table, all of the results labelled $*$ means we don't need to consider the result.

| $p$ | $q$ | $r$ | $p \to q \wedge r$ | $q \to \sim r$ | $\sim p$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $F$ | $*$ |
| $T$ | $T$ | $F$ | $F$ | $*$ | $*$ |
| $T$ | $F$ | $T$ | $F$ | $*$ | $*$ |
| $T$ | $F$ | $F$ | $F$ | $*$ | $*$ |
| $F$ | $T$ | $T$ | $T$ | $F$ | $*$ |
| $F$ | $T$ | $F$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $F$ | $T$ | $T$ | $T$ |

From our truth table, we can see that whenever the hypotheses are both accepted, the conclusion is also accepted. This tells us that the statement is **logically valid**.

Prove that, if $n$ is odd, then $n^2$ is also odd.

Solution.
Suppose that $n$ is odd. Then, there exists some integer $k$ so that $n = 2k+1$. Then

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2m + 1, \quad \text{where } m = 2k^2 + 2k. \end{aligned}$$

Since $k$ is an integer, then so is $2k^2 + 2k$. So $m$ is also an integer. Hence, $n^2$ can be written as a sum of an even number and $1$. So $n^2$ is odd. $\square$

(2016 S2, Q3ii)

a) Prove that

$$x^{n+1} - y^{n+1} = (x+y)(x^n - y^n) - xy(x^{n-1} - y^{n-1}).$$

b) Let $\alpha = 1 + \sqrt{5}$ and $\beta = 1 - \sqrt{5}$. Use mathematical induction to prove that

$$F_n = \frac{\alpha^n - \beta^n}{2^n \sqrt{5}}$$

is an integer for $n = 1, 2, 3, \ldots$.

Solution.

a) Personally, this question is so much nicer logically if you begin from the right hand side because you can do a lot of algebraic manipulation from the right. But if you want to seem big brain, feel free to start from the LHS.

$$\begin{aligned} LHS &= x^{n+1} - y^{n+1} \\ &= (x^{n+1} + x^n y) - (y^{n+1} + xy^n) - x^n y + xy^n \\ &= x^n(x+y) - y^n(y+x) - xy(x^{n-1} - y^{n-1}) \\ &= (x+y)(x^n - y^n) - xy(x^{n-1} - y^{n-1}) \\ &= RHS. \end{aligned}$$

b) We need to use a variant of induction called **strong induction**, so our base cases will need to checked for $n = 1$ and $n = 2$.

When $n = 1$, we have

$$F_1 = \frac{\alpha - \beta}{2\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1.$$

When $n = 2$, we have

$$\begin{aligned} F_2 &= \frac{\alpha^2 - \beta^2}{2^2\sqrt{5}} \\ &= \frac{(\alpha - \beta)(\alpha + \beta)}{4\sqrt{5}} \\ &= \frac{2\sqrt{5} \times 2}{4\sqrt{5}} \\ &= 1. \end{aligned}$$

Since 1 is an integer, then our base cases hold. Now assume that the statement holds $n = k - 1$ and $n = k$. That is, we assume that

$$F_{k-1} = \frac{\alpha^{k-1} - \beta^{k-1}}{2^{k-1}\sqrt{5}} \quad \text{and} \quad F_k = \frac{\alpha^k - \beta^k}{2^k\sqrt{5}}$$

are both integers.

Then, we have

$$\begin{aligned} F_{k+1} &= \frac{\alpha^{k+1} - \beta^{k+1}}{2^{k+1}\sqrt{5}} \\ &= \frac{(\alpha + \beta)(\alpha^k - \beta^k) - \alpha\beta(\alpha^{k-1} - \beta^{k-1})}{2^{k+1}\sqrt{5}} && \text{(from part 1)} \\ &= \frac{2(\alpha^k - \beta^k) + 4(\alpha^{k-1} - \beta^{k-1})}{2^{k+1}\sqrt{5}} \\ &= \left(\frac{2(\alpha^k - \beta^k)}{2^{k+1}\sqrt{5}}\right) + \left(\frac{4(\alpha^{k-1} - \beta^{k-1})}{2^{k+1}\sqrt{5}}\right) \\ &= \underbrace{\left(\frac{\alpha^k - \beta^k}{2^k\sqrt{5}}\right)}_{\in\mathbb{Z}} + \underbrace{\left(\frac{\alpha^{k-1} - \beta^{k-1}}{2^{k-1}\sqrt{5}}\right)}_{\in\mathbb{Z}} && \text{(by the inductive hypotheses)} \\ &\in \mathbb{Z}. \end{aligned}$$

Hence, by strong induction, the statement holds for all $n = 1, 2, 3, \ldots$. □

(Tutorial Q53)
Prove that for all $n \in \mathbb{Z}^+$

$$21 \mid 4^{n+1} + 5^{2n-1}.$$

Solution.
Let $n = 1$. Then, we have

$$4^{1+1} + 5^{2\times1-1} = 4^2 + 5 = 21 = 21 \times 1.$$

So the statement holds for $n = 1$. Now assume that the statement holds for some integer $n = k$. That is, we assume that there exists some integer $P$ such that

$$4^{k+1} + 5^{2k-1} = 21P \iff 4^{k+1} = 21P - 5^{2k-1}.$$

Then, we have

$$\begin{aligned}
4^{(k+1)+1} + 5^{2(k+1)-1} &= 4^{k+2} + 5^{2k+1} \\
&= 4 \times 4^{k+1} + 5^{2k+1} \\
&= 4\left(21P - 5^{2k-1}\right) + 5^{2k+1} \\
&= 21(4P) - 4 \times 5^{2k-1} + 5^{2k+1} \\
&= 21(4P) - 4 \times 5^{2k-1} + 5^2 \times 5^{2k-1} \\
&= 21(4P) - 21 \times 5^{2k-1} \\
&= 21\left[4P - 5^{2k-1}\right] \\
&= 21Q, \quad \text{where } Q = 4P - 5^{2k-1}.
\end{aligned}$$

Since $P$ and $k$ are integers, then it follows that $4P - 5^{2k-1}$ is an integer as well. Hence $Q$ is an integer. So, by the principles of mathematical induction,

$$21 \mid 4^{n+1} + 5^{2n-1}.$$

□

(2018 S2, Q3iii)
Prove by mathematical induction that for all integers $n \geq 2$,

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}.$$

SOLUTION.
Let $n = 2$. Then

$$LHS = 1 + \frac{1}{4} = 2 - \frac{3}{4} < 2 - \frac{1}{2} = RHS.$$

(**Inductive hypothesis**)
Now assume that the statement holds for some integer $n = k$. That is

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2} < 2 - \frac{1}{k}.$$

Consider the case where $n = k + 1$. We have

$$\begin{aligned}
LHS &= \underbrace{\left(1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2}\right)}_{\text{Inductive hypothesis}} + \frac{1}{(k+1)^2} \\
&< \left(2 - \frac{1}{k}\right) + \frac{1}{(k+1)^2} \\
&= 2 - \left[\frac{1}{k} - \frac{1}{(k+1)^2}\right] \\
&= 2 - \left[\frac{(k+1)^2 - k}{k(k+1)^2}\right] \\
&= 2 - \left[\frac{k^2 + 2k + 1 - k}{k(k+1)^2}\right] \\
&= 2 - \left[\frac{k^2 + k + 1}{k(k+1)^2}\right] \\
&< 2 - \frac{k^2 + k}{k(k+1)^2} \\
&= 2 - \frac{k(k+1)}{k(k+1)^2} \\
&= 2 - \frac{1}{(k+1)}.
\end{aligned}$$

Hence, by the principles of mathematical induction, the statement holds for all integers $n \geq 2$. $\square$

> (2017 S2, Q3iii)
> Prove that $\sqrt{13}$ is irrational.

SOLUTION.
Suppose that $\sqrt{13}$ is rational. Then there exist coprime integers $a, b$ such that $\sqrt{13} = \dfrac{a}{b} \implies 13b^2 = a^2$. This means that $13 \mid a^2 \implies 13 \mid a$. Let $a = 13k$ for some integer $k$. Then $13b^2 = (13k)^2 \implies b^2 = 13k^2$. This means that $13 \mid b^2 \implies 13 \mid b$. But we claimed that $a$ and $b$ are coprime so we hit a contradiction. Hence, our original statement must have been incorrect: that is, $\sqrt{13}$ is irrational. $\square$

> (2018 S1)
> Suppose that 26 integers are chosen from the set $S = \{1, 2, \ldots, 50\}$. By writing these numbers as $2^k m$ with $m$ odd, prove that one of the chosen numbers is a multiple of another of the chosen numbers.

SOLUTION.

We can write each of these numbers of $S$ as a product of $2$'s multiplied by some odd integer $m$. For example,

$$\begin{aligned} 1 &= 2^0 \times 1. \\ 5 &= 2^0 \times 5. \\ 10 &= 2^1 \times 5. \\ 25 &= 2^0 \times 25. \\ 29 &= 2^0 \times 29. \end{aligned}$$

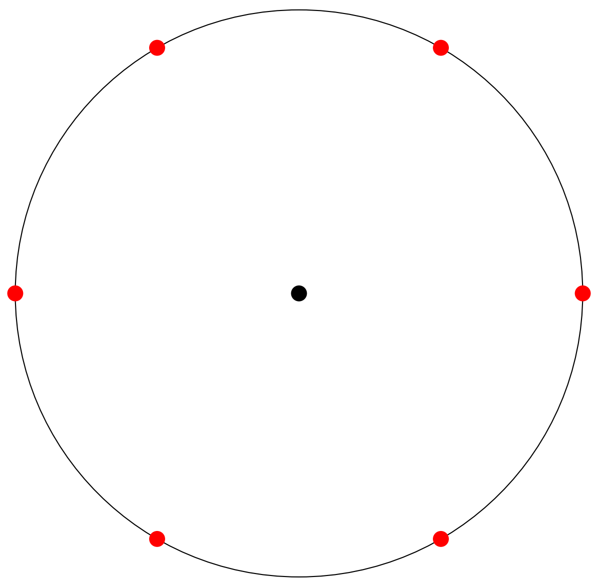
Notice that there are 25 odd integers in the set $S$; this represents our "pigeonholes" and the 26 integers represent our "pigeons". So, by the pigeonhole principle, we have *at least* two integers in the same "pigeonhole"; let's call these integers

$$x = 2^a m, \quad y = 2^b m.$$

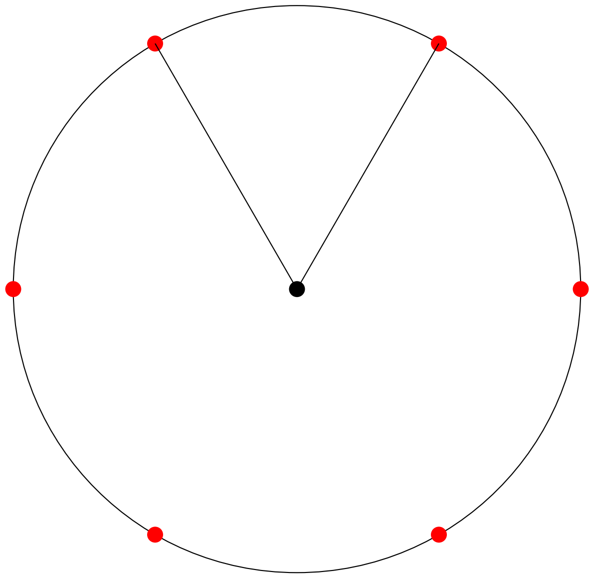
Then, because $x \neq y$ (otherwise our proof is complete), either $a < b$ or $b < a$. If $a < b$, then $x$ divides $y$. If $b < a$, then $y$ divides $x$. In either case, we have the case where either one of the integers divides the other. $\square$

(2017 S1)
Prove that given any 7 points on a circle of radius 1, there exist at least two that are less than 1 unit away from each other.

SOLUTION.
Distribute $6$ points evenly on the unit circle. This can be pictured below.



By considering any two adjacent points, connect a line from the centre to the these two points.



The angle between these two points is $\frac{2\pi}{6} = \frac{\pi}{3}$. Since the line from the centre to these two points are the same, the triangle that is formed by these three points creates an **equilateral triangle**.

Hence, the distance between any two points evenly distributed on the unit circle is $1$ unit. This means that placing the seventh point on the unit circle will be guaranteed to have a distance less than $1$ unit from any point already distributed on the unit circle. $\square$

(2019 T1)
Let $b_1, b_2, \ldots, b_{14}$ be integers, with repetition allowed. Define

$$S = \{(i, j) \in \mathbb{Z}^2 \mid 1 \leq i, j \leq 14,\ i < j\}.$$

Prove that, for some $r \in \{0, 1, \ldots, 44\}$, there exist at least *three* pairs $(i, j) \in S$ such that

$$b_i + b_j \equiv r \pmod{45}.$$

Solution.
To find the size of set $S$, consider how many terms exist for $j$ as $i$ varies.

$$\begin{aligned}
i = 1, \quad & j = |\{2, 3, \dots, 14\}| = 13. \\
i = 2, \quad & j = |\{3, 4, \dots, 14\}| = 12. \\
i = 3, \quad & j = |\{4, 5, \dots, 14\}| = 11. \\
& \vdots \\
i = 14 \quad & j = |\{\}| = 0.
\end{aligned}$$

Hence, we see that there are $0+1+2+3+\cdots+13 = 91$ total pairs that exist in $S$; these are the "pigeons". The pigeonholes are the residue class of 45. Hence, there are 45 pigeonholes and 91 pigeons. Applying the pigeonhole principle, we see that there are at least

$$\left\lceil \frac{91}{45} \right\rceil = 3$$

pigeons for some residue class of 45. In other words, for some $r \in \{0, 1, \dots, 44\}$, there exist at least three pairs such that

$$b_i + b_j \equiv r \pmod{45}.$$ □

(2018 S2)
For all integers $n$, prove that 9 does not divide $n^2 - 3$.

Solution.
We shall commence with a **proof by contradiction**.

Suppose that 9 divides $n^2 - 3$. Then there exists some integer $m$ such that

$$n^2 - 3 = 9m \iff n^2 = 9m + 3.$$

Consider the residue of $n^2 \pmod 9$. We have

$$\begin{aligned}
n \equiv 0 \pmod 9 &\implies n^2 \equiv 0 \pmod 9 \\
n \equiv 1 \pmod 9 &\implies n^2 \equiv 1 \pmod 9 \\
n \equiv 2 \pmod 9 &\implies n^2 \equiv 4 \pmod 9 \\
n \equiv 3 \pmod 9 &\implies n^2 \equiv 0 \pmod 9 \\
n \equiv 4 \pmod 9 &\implies n^2 \equiv 7 \pmod 9 \\
n \equiv 5 \pmod 9 &\implies n^2 \equiv 7 \pmod 9 \\
n \equiv 6 \pmod 9 &\implies n^2 \equiv 0 \pmod 9 \\
n \equiv 7 \pmod 9 &\implies n^2 \equiv 4 \pmod 9 \\
n \equiv 8 \pmod 9 &\implies n^2 \equiv 1 \pmod 9
\end{aligned}$$

We see that the residue classes of $n^2 \pmod 9$ are $0, 1, 4, 7$, meaning that there cannot exist an integer such that $n^2 = 9m + 3$. Hence, we have a contradiction and the proof is complete. $\square$

(2016 S1)
If $p$ and $q$ are distinct primes, then $\sqrt{pq}$ is irrational.

SOLUTION.
Suppose that $\sqrt{pq}$ is rational. Then there exist coprime integers $a, b$ such that $\sqrt{pq} = \dfrac{a}{b} \implies pqb^2 = a^2$. Since $qb^2 \in \mathbb{Z}$, then it follows that $p \mid a^2 \implies p \mid a$. Let $a = pk$ for some integer $k$. Then we have $pqb^2 = (pk)^2 \implies qb^2 = pk^2$. This means that $p \mid qb^2$. But since $p$ and $q$ are distinct primes, then it follows that $p \nmid q$. Hence, $p \mid b^2 \implies p \mid b$.

But this is a contradiction since $a$ and $b$ are coprime integers. Hence, $\sqrt{pq}$ must be irrational. $\square$

# Part II: Supplementary content

The following section are some supplementary resources in the topic; it will cover some tips on proof writing and some extra content that wasn't covered in the seminar.

## Standard logical equivalence laws

**Standard logical equivalence laws** are essentially a tool for us to be able to show that two compound propositions are equivalent without having to show it using the truth table. While truth tables are a useful visual representation, they can be quite tedious to construct, particularly when we begin to deal with more than three variables. As such, we have to deal with a new way to show that two statements are *logically equivalent*.

We can think of these laws synonymously with set algebra laws and I will highlight the sheer similarities between two with the following table (along with the names of the laws).

| Logical equivalency | Set equivalency | Name of law |
|---|---|---|
| $(p \land q) \land r \equiv p \land (q \land r)$<br>$(p \lor q) \lor r \equiv p \lor (q \lor r)$ | $(A \cap B) \cap C \equiv A \cap (B \cap C)$<br>$(A \cup B) \cup C \equiv A \cup (B \cup C)$ | Associative law |
| $p \land q \equiv q \land p$<br>$p \lor q \equiv q \lor p$ | $A \cap B \equiv B \cap A$<br>$A \cup B \equiv B \cup A$ | Commutative law |
| $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$<br>$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$ | $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$<br>$A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$ | Distributive law |
| $\neg(p \land q) \equiv \neg p \lor \neg q$<br>$\neg(p \lor q) \equiv \neg p \land \neg q$ | $(A \cap B)^c \equiv A^c \cup B^c$<br>$(A \cup B)^c \equiv A^c \cap B^c$ | De Morgan's law |
| $\neg(\neg p) \equiv p$ | $(A^c)^c \equiv A$ | Double negation law |
| $p \lor p \equiv p$<br>$p \land p \equiv p$ | $A \cup A \equiv A$<br>$A \cap A \equiv A$ | Idempotent law |
| $p \lor T \equiv T$<br>$p \land F \equiv F$ | $A \cup \mathcal{U} \equiv \mathcal{U}$<br>$A \cap \varnothing \equiv \varnothing$ | Domination law |
| $p \land T \equiv p$<br>$p \lor F \equiv p$ | $A \cap \mathcal{U} \equiv A$<br>$A \cup \varnothing \equiv A$ | Identity law |
| $p \lor (p \land q) \equiv p$<br>$p \land (p \lor q) \equiv p$ | $A \cup (A \cap B) \equiv A$<br>$A \cap (A \cup B) \equiv A$ | Absorption law |
| $p \lor \neg p \equiv T$<br>$p \land \neg p \equiv F$ | $A \cup A^c \equiv \mathcal{U}$<br>$A \cap A^c \equiv \varnothing$ | Negation law |

Similarly, we also have logical equivalences for implication statements. The following table illustrates these logical equivalences that may be useful in the exam.

| Original statement | Logical equivalence | Name (if applicable) |
|---|---|---|
| $p \implies q$ | $\neg p \lor q$ | |
| $p \implies q$ | $\neg q \implies \neg p$ | Contraposition |
| $p \iff q$ | $(p \implies q) \land (q \implies p)$ | Defn. of biconditional |

## Proof writing

*Useful reads*:

- [An answer on proof writing]
- [Another answer on proof writing — using quantifiers]

Although there is no *set* method to writing and setting out proofs, there are some basic guidelines that a student should follow to ensure that they produce a proof that is clear to the reader.

1. **Be clear and concise with your argument**. Make sure you *clearly* define any symbols that you are going to introduce. The reader should be able to pick up your proof and understand the derivation of the problem. For example, if you're introducing $\phi(n)$ to be *Euler's totient function*, make that distinction clear; you don't necessarily need to explain what it does, that's left to the reader to read in their own time. But if you only introduce this symbol without stating what it is or what it does, how do you expect the reader to follow? As an example, I have highlighted some unclear arguments in red and added an example that you should follow in green.

   *Example 1.* Let $n = 30$. Then $\phi(n) = 8$.

   This example uses unclear notation with no further explanation. It's unclear what $\phi(n)$ is, or what it even does.

   *Example 2.* Define $\phi(n)$ to be the *Euler totient function* of $n$. Then, if $n = 30$, we have that $\phi(30) = 8$.

   Although the author is clear in their argument, the "if" statement is redundant. Hence, the author has added some extra information that proved meaningless to their argument. This process is described as **waffling** and it's something that proofs tend to avoid. Make sure each of your statements provide *some* meaning to your proof, even if it's not necessarily evident at the time of writing.

   *Example 3.* Define $\phi(n)$ to be the number of positive integers that are relatively prime to $n$. Then $\phi(30) = 8$.

   In this example, the author has clearly defined their notation. There are no redundant fillers in this example. So it's concise and clear; the reader should be able to follow from here.

2. **Stick to a consistent scheme of notation**. Yeah, just don't skip around when defining notation.

3. **Plan out your argument**. Draft up $2 - 3$ plans before proceeding with a full written proof. You may not have that long in the exam, so when it comes to exams, write out all of the necessary pieces of information as well as an outline on the side of your exam

paper. Then begin to write out your proof by stating all of the necessary variables that you are going to use in your proof.

4. **Avoid using logical symbols**. This is a huge red herring for many students first starting out with proof writing. While it is taught in this course, avoid using logical symbols and quantifiers in your proof. A proof is typically an **expository prose**, with an intention of presenting a logical and mathematically sound explanation for why a statement is correct. It should be easy for the reader to follow (hence, clear and concise). Mixing logical quantifiers with words is a great way for readers to get confused. As an example, think about which of the following statements is easier to digest at first glance?

   *Example 1.* Let $f : X \to Y$ such that $y = f(x)$ and suppose that $\lim_{x\to a} f(x) = L$. Then
   $$\forall \epsilon > 0\ \exists \delta > 0 :\ |x - a| < \delta \implies |f(x) - L| < \epsilon.$$

   *Example 2.* Let $f : X \to Y$ such that $y = f(x)$ and suppose that $\lim_{x\to a} f(x) = L$. Then, for all $\epsilon > 0$, there exists a $\delta > 0$ such that
   $$|x - a| < \delta \implies |f(x) - L| < \epsilon.$$

   Although these two statements are equivalent, the first statement is a lot more difficult to decipher. Sometimes less is more, and the same can be said about proof writing. Use less symbols rather than more where you can.

5. **State all axioms and theorems you plan to use throughout your proof**. Instead of just writing the result, you should reference the name of the theorem or axiom that you have used, especially if a result isn't exactly clear from. This makes it easier for the reader to follow your proof.

6. **Know your target audience**. Depending on the nature of the reader, you may feel inclined to skip over *some* trivial steps. You know your audience best, so make the judgement to include certain elements in the proof. However, in the exam, you shouldn't have to omit any steps in your proof unless it's really trivial.

## Strong induction

One of the main forms of proof is a generalised $n$-case proof called **mathematical induction**. However, this is a fairly weaker induction because our inductive hypothesis hinges on the fact that we assume the statement holds for some integer $n = k$. However, it doesn't tell us the nature about any other case that is not $k$. In cases where we consider two different hypotheses to hold, we need to use a variant of induction called **strong induction**.

In this scenario, our inductive hypothesis *slightly* varies. Instead of assuming that ONLY $n = k$ holds, we assume that **all cases preceding** $n = k$ also holds. In other words, we assume that $n = k - 1$ also satisfies the equation or inequality. This is especially useful for proving recurrence relations where the induction must satisfy two base cases.

This also means that we **must** check that the two base cases also hold. Typically that would be in the form of $n = 1$ AND $n = 2$, but that may vary depending on the nature of the question. To see this in action, there is a written solution that uses **strong induction** in the seminar solutions.

SUMMARY.

1. Prove the **two** base cases.
2. Assume that the statement holds true for $n = k - 1$ and $n = k$.
3. Use these inductive hypotheses to prove that the statement also holds for $n = k + 1$.

## Pigeonhole principle

One of the more difficult forms of proofs are applications of the **pigeonhole principle**; this section will hopefully help students ease into pigeonhole principle type questions. To begin, let's recall what the pigeonhole principle states.

Let's suppose you have $k+1$ pigeons and $k$ pigeonholes with $k > 0$. Then we can distribute the first $k$ pigeons into each of these pigeonholes. The last remaining pigeon must lie in any one of these pigeonholes. So consequently, we say that *at least* one pigeonhole will contain $2$ pigeons. Even if we distribute all $k + 1$ pigeons into one hole, the statement is satisfied since the one hole will have $k + 1 \geq 2$ pigeons.

We now move to a more general statement. Let's suppose you have $n$ pigeons and $k$ pigeonholes with $n \geq k$ and $k > 0$. Then we can distribute any multiple of $k$ pigeons into these $k$ pigeonholes. We should now be left with some number (less than $k$) of pigeons. We can distribute that freely into any of the $k$ pigeonholes. But we see that *at least* one of these pigeonholes will contain *slightly* more than $n/k$ pigeons. In other words, at least one pigeonhole will contain $\left\lceil \frac{n}{k} \right\rceil$ pigeons. This is the **pigeonhole principle**.

So how do we use this statement in proofs? Well, the idea behind pigeonhole principle allows us to prove these "at least X" type questions. We simply have to reframe the question and identify our *pigeons* and *pigeonholes*. If you observe the solutions that use pigeonhole principle, you will see that I have attempted to reframe the question so that we have "pigeons" and "pigeonholes". The application of this is then clear and the use of the pigeonhole principle completes the proof.

## Final tips

Proofs are difficult. They require heavy rigour and aren't really a topic that many lecturers place heavy emphasis on. However, they are really fundamental to the construction of mathematical statements. Without proofs, mathematics is meaningless; we'd just have statements that may not be true (ie propositions).

However, with a little bit of perseverance, anyone can improve in typesetting proofs. All it takes is a lot of practice and heavy reading. Wherever you can, read how lecturers set out proofs. Observe how they introduce variables, does their working out make sense?

From there, build a toolbox of techniques that you may like to employ when constructing proofs. Does this statement seem like a "proof by contradiction" type question? Would "induction" be feasible?

Finally, keep drafting up simpler cases. Generalisations often become apparent once you look at a few cases. Verify that the statement holds for small values and then observe the field of outputs. Do they hold any similarities? Are they contrasting?