1. True/false. For each of the following statements, indicate whether the statement is true or false. Give a one or two sentence explanation for your answer.

(a) \( \{\emptyset\} = \emptyset \)

Solution  False. \( \emptyset \in \{\emptyset\} \), while \( \emptyset \notin \emptyset \).

(b) Every set is a subset of its power set

Solution  False. Every set is an element of its power set.

(c) A proof that starts “Choose an arbitrary \( y \in \mathbb{N} \), and let \( x = y^2 \)” is likely to be a proof that \( \forall y \in \mathbb{N}, \forall x \in \mathbb{N}, \ldots \)

Solution  False. This would only be a proof that \( \exists x \in \mathbb{N} \) with some property, not a proof that \( \forall x \in \mathbb{N} \) the property holds.

(d) The logical negation of “everybody can fool Mike” is “nobody can fool Mike”.

Solution  False. The negation would be “somebody can’t fool Mike”.

(e) The relation \( \leq \) is an equivalence relation

Solution  False. It is not symmetric, because (for example) \( 1 \leq 2 \) but \( 2 \nleq 1 \).

(f) If there is a bijection from \( \mathbb{Q} \) to \( X \) then \( X \) is countable.

Solution  True. We know that \( |\mathbb{Q}| = |\mathbb{N}| \). If there is a bijection from \( \mathbb{Q} \to X \), then \( |\mathbb{Q}| = |X| \). This means \( |X| = |\mathbb{N}| \), so \( X \) is countable.

(g) Recall that \( |X \to Y| \) denotes the set of functions with domain \( X \) and codomain \( Y \). Let \( f : 2^S \to [S \to \{0,1\}] \) be given by \( f(X) := h \) where \( h : S \to \{0,1\} \) is given by \( h(s) := 0 \). \( f \) is injective.

Solution  False. \( f \) always returns the same thing, so it can’t be one to one. For example, choose any two different subsets \( X_1 \) and \( X_2 \) of \( S \); then \( f(X_1) = h = f(X_2) \).

(h) \( f \) as just defined is surjective.

Solution  False. Choose any function \( h' : S \to \{0,1\} \) other than \( h \). Since \( f \) only outputs \( h \), it never outputs \( h' \).

(i) If a function has a right inverse, then the right inverse is unique.
Solution  False. Let $f : \{0, 1, 2\} \to \{a, b\}$ be given by $f(0) := a, f(1) := a$ and $f(2) := b$. Then $g_1 : \{a, b\}$ given by $g_1(a) := 0$ and $g_1(b) := 2$ is a right inverse, but so is $g_2$ given by $g_2(a) := 1$ and $g_2(b) := 2$.

2. Briefly and clearly identify the errors in each of the following proofs:

(a) Proof that 1 is the largest natural number: Let $n$ be the largest natural number. Then $n^2$, being a natural number, is less than or equal to $n$. Therefore $n^2 - n = n(n-1) \leq 0$. Hence $0 \leq n \leq 1$. Therefore $n = 1$.

Solution  The error is in the first sentence “Let $n$ be the largest natural number”. The proof is only valid if there is a largest natural number (which there isn’t).

(b) Proof that $2 = 1$: Let $a = b$.

\[ a^2 = ab \]
\[ a^2 - b^2 = ab - b^2 \]
\[ (a + b)(a - b) = b(a - b) \]
\[ a + b = b \]

Setting $a = b = 1$, we get $2 = 1$.

Solution  The error comes when we divide both sides by $(a - b)$, which is zero (division by zero is meaningless!). Just because $(a - b)x = (a - b)y$, we cannot conclude that $x = y$.

(c) Proof that $(a + b)(a - b) = a^2 - b^2$: To prove: $(a + b)(a - b) = a^2 - b^2$

\[ a^2 - ab + ab - b^2 = a^2 - b^2 \]
\[ a^2 - b^2 = a^2 - b^2 \]

...which is true, hence the result is proved.

Solution  Although the claim is actually true, the proof is backwards; it begins by assuming that the claim is true, and then derives a fact that is known to be true.

This is a valid proof that if $(a + b)(a - b) = a^2 - b^2$ then $a^2 - b^2 = a^2 - b^2$, but this is not a very interesting fact (and is not what was claimed).

3. Which of these is the correct negation of $\exists x, \neg \forall y, \neg \exists z, \neg F(x, y, z)$?

(a) $\exists x, \exists y, \exists z, F(x, y, z)$
(b) $\exists x, \exists y, \exists z, \neg F(x, y, z)$
(c) $\forall x, \forall y, \forall z, F(x, y, z)$
(d) $\forall x, \forall y, \forall z, \neg F(x, y, z)$

Solution  (c).

\[ \neg (\exists x, \neg \forall y, \neg \exists z, \neg F(x, y, z)) = \forall x, \neg \neg (\forall y, \neg \exists z, \neg F(x, y, z)) \]
\[ = \forall x, \forall y, (\neg \exists z, \neg F(x, y, z)) \]
\[ = \forall x, \forall y, \forall z, (\neg \neg F(x, y, z)) \]
\[ = \forall x, \forall y, \forall z, F(x, y, z) \]
4. Complete the following diagonalization proof:

**Claim:** \( X = [\mathbb{N} \rightarrow \mathbb{N}] \) is uncountable.

**Proof:** We prove this claim by contradiction. Assume that \( X \) is countable. Then there exists a function \( F : \text{FILL IN} \) that is \text{FILL IN}.

Write \( f_0 = F(0), f_1 = F(1) \), and so on. We can write the elements of \( X \) in a table:

\[
\begin{array}{ccc}
 & 0 & 1 & 2 & \ldots \\
 f_0 & f_0(0) & f_0(1) & f_0(2) & \ldots \\
f_1 & f_1(0) & f_1(1) & f_1(2) & \ldots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
\]

Let \( f_D : \text{FILL IN} \) be given by \( f_D : x \mapsto \text{FILL IN} \)

Then \text{FILL IN}

This is a contradiction because \text{FILL IN}.

**Solution**  
**Claim:** \( X = [\mathbb{N} \rightarrow \mathbb{N}] \) is uncountable.

**Proof:** We prove this claim by contradiction. Assume that \( X \) is countable. Then there exists a function \( F : \mathbb{N} \rightarrow X \) that is \text{surjective}.

Write \( f_0 = F(0), f_1 = F(1) \), and so on. We can write the elements of \( X \) in a table:

\[
\begin{array}{ccc}
 & 0 & 1 & 2 & \ldots \\
 f_0 & f_0(0) & f_0(1) & f_0(2) & \ldots \\
f_1 & f_1(0) & f_1(1) & f_1(2) & \ldots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
\]

Let \( f_D : \mathbb{N} \rightarrow \mathbb{N} \) be given by \( f_D : x \mapsto 1 + f_x(x) \)

Then \( f_D \) is not in the table, because for any \( i \), it differs from \( f_i \) on input \( i \).

This is a contradiction because we assumed \( F \) was surjective.

5. Which of the following sets are countably infinite and which are not countably infinite? Give a one to five sentence justification for your answer.

(a) The set \( \Sigma^* \) containing all finite length strings of 0’s and 1’s.

**Solution**  This set is countable. You can list all strings of length 0, then all strings of length one, then all strings of length 2, and so on.

(b) The set \( 2^\mathbb{N} \) containing all sets of natural numbers.

**Solution**  This set is not countable. If it were, we could put all of the sets in a table:

\[
\begin{array}{ccc}
 & 0 & 1 & 2 & \ldots \\
 S_1 & \in S_1 & \notin & \in & \ldots \\
 S_2 & \notin & \notin & \notin & \ldots \\
 S_3 & \notin & \notin & \notin & \ldots
\end{array}
\]

We can then construct the set \( S_D \) by swapping everything on the diagonal (\( S_D = \{i \mid i \notin S_i\} \)). Then \( S_D \neq S_k \) for any \( k \), because \( k \in S_D \) if and only if \( k \notin S_k \). Thus \( S_D \) is not in the table, which contradicts the fact that the table contained all sets.
(c) The set $\mathbb{N} \times \mathbb{N}$ containing all pairs of natural numbers.

**Solution**  This set is countable. You can put all of the pairs in a table, and then map the natural numbers to the pairs by tracing diagonals of the table.

(d) The set $[\mathbb{N} \to \{0,1\}]$ containing all functions from $\mathbb{N}$ to $\{0,1\}$.

**Solution**  This set is not countable. There is a bijection between $[\mathbb{N} \to \{0,1\}]$ and $2^{\mathbb{N}}$, and we showed above that $2^{\mathbb{N}}$ is uncountable. Alternatively, you can diagonalize directly using the function $f : n \mapsto f_n(n) + 1$ or similar.

Be sure to include enough detail:

- If listing elements, be sure to clearly state how you are listing them;
- If diagonalizing, be sure it is clear what your diagonal construction is;
- If providing a function, make sure it is clear what the output is on a given input.

6. For any function $f : A \to B$ and a set $C \subseteq A$, define $f(C) = \{ f(x) \mid x \in C \}$. That is, $f(C)$ is the set of images of elements of $C$. Prove that if $f$ is injective, then $f(C_1 \cap C_2) = f(C_1) \cap f(C_2)$ for all $C_1, C_2 \subseteq A$.

(Hint: one way to prove this is from the definition of set equality: $A = B$ iff $A \subseteq B$ and $B \subseteq A$.)

**Solution**  Choose an arbitrary $b \in f(C_1 \cap C_2)$. We wish to show $b \in f(C_1) \cap f(C_2)$. Since $b \in f(C_1 \cap C_2)$, there must exist some $a \in C_1 \cap C_2$ with $f(a) = b$. Since $a \in C_1 \cap C_2$, we have $a \in C_1$ so $b = f(a) \in f(C_1)$; similarly, $b \in f(C_2)$. Therefore, $b \in f(C_1) \cap f(C_2)$.

Conversely, choose an arbitrary $b \in f(C_1) \cap f(C_2)$. We want to show $b \in f(C_1 \cap C_2)$. Now, $b = f(a_1)$ for some $a_1 \in C_1$, and $b = f(a_2)$ for some $a_2 \in C_2$. Since $f$ is injective, $a_1 = a_2$, so $a_1$ is also in $C_2$. Therefore, $a_1 \in C_1 \cap C_2$ so $b = f(a_1) \in f(C_1 \cap C_2)$ as required.

7. (a) Write the definition of “$f : A \to B$ is injective” using formal notation ($\forall, \exists$, “and”, “or”, “if . . . then . . .”, =, $\neq$, . . .).

**Solution**  $\forall x_1, x_2 \in A \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2$

(b) Similarly, write down the definition of “$f : A \to B$ is surjective”.

**Solution**  $\forall b \in B, \exists a \in A, f(a) = b$.

(c) Write down the definition of “$A$ is countable”. You may write “$f$ is surjective” or “$f$ is injective” in your expression.

**Solution**  $\exists f : \mathbb{N} \to A$ such that $f$ is surjective.

8. Recall that the composition of two functions $f : B \to C$ and $g : A \to B$ is the function $f \circ g : A \to C$ defined as $(f \circ g)(x) = f(g(x))$. Prove that if $f$ and $g$ are both injective, then $f \circ g$ is injective.

**Solution**  Assume that $f$ and $g$ are injective, and assume that $(f \circ g)(a_1) = (f \circ g)(a_2)$. By definition, we have $f(g(a_1)) = f(g(a_2))$. Since $f$ is injective, we conclude $g(a_1) = g(a_2)$; since $g$ is injective, we conclude $a_1 = a_2$.

9. For each of the following functions, indicate whether the function $f$ is injective, whether it is surjective, and whether it is bijective. Give a one sentence explanation for each answer.
10. [6 points] Recall that \([X \rightarrow Y]\) denotes the set of functions with domain \(X\) and codomain \(Y\). Let \(X\) and \(Y\) be nonempty sets, and let \(F : [X \rightarrow Y] \rightarrow [X \rightarrow (Y \times Y)]\) be given by \(F(f) := h_f\), where \(h_f : X \rightarrow (Y \times Y)\) is given by \(h_f(x) := (f(x), f(x))\) for all \(x\).

(a) Show that \(F\) is injective. Note: \(g_1 = g_2\) if and only if, for all \(x\), \(g_1(x) = g_2(x)\).

Solution Assume \(F(f_1) = F(f_2)\). Then \(h_{f_1}(x) = h_{f_2}(x)\) for all \(x\). That means that for all \(x\), \((f_1(x), f_1(x)) = (f_2(x), f_2(x))\). This in turn implies that \(f_1(x) = f_2(x)\). Since this is true for all \(x\), \(f_1 = f_2\), as required.

(b) Show that \(F\) is not necessarily bijective.

Solution \(F\) only outputs functions that output pairs with the same first and second components. Any function that outputs a pair with different first and second component will not be in the image of \(F\).

For example, let \(X = \{0, 1\}\) and \(Y = \{a, b\}\), and let \(g : X \rightarrow Y \times Y\) be given by \(g(x) = (a, b)\). Then \(g\) is not in the image of \(F\).

11. Prove that \(7^m - 1\) is divisible by 6 for all positive integers \(m\).

Solution There are two ways to do this. One way: notice that 7 \(\equiv 1\) mod 6, thus \(7^m \equiv 1\) mod 6 for any \(m\) (applying the known result that “if \(a \equiv b\) (mod \(m\)) and \(c \equiv d\) (mod \(m\)) then \(ac \equiv bd\) (mod \(m\))” \(m - 1\) times), and thus \(7^m - 1 \equiv 0\) mod 6. This implies \(7^m - 1\) is divisible by 6.

Alternatively you can do a direct proof by induction:

Base case: \(m = 1\), \(7^1 - 1 = 6\) which is obviously divisible by 6.

Inductive step: Assume \(7^m - 1\) is divisible by 6 for some \(m \geq 1\) (inductive hypothesis). Then \(7^{m+1} - 1 = 7^{m+1} - 7 + 6 = 7(7^m - 1) + 6\). But \(7^m - 1\) is divisible by 6 (by the inductive hypothesis) and so is 6, so \(7^{m+1} - 1\) is also divisible by 6. Hence proved by induction.
12. [6 points] Pascal’s triangle is a sequence of rows, where each entry is formed by adding the two adjacent entries from the previous row:

\[
\begin{array}{ccccccc}
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1 \\
1 & 4 & 6 & 4 & 1 \\
\cdots
\end{array}
\]

If we let \( P_{n,k} \) stand for the \( k \)th entry in the \( n \)th row of Pascal’s triangle, then \( P_{n,k} \) is given by the formulas

\[
P_{1,1} := 1, \quad P_{n,0} := 0 \quad \text{for all } n, \quad \text{and } \quad P_{n+1,k} := P_{n,k-1} + P_{n,k} \text{ if } n \geq 1.
\]

Prove by induction on \( n \) that for all \( n \geq 1 \), for all \( k \) with \( 1 \leq k \leq n \), \( P_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!} \).

Note: The definition of \( n! \) is \( 0! := 1 \) and \( n! := n \cdot (n-1)! \) for all \( n \geq 1 \).

**Solution**  Proof by induction. Let \( P(n) \) be the statement \( P_{n,k} = \binom{n}{k} \).

\( P(1) \) is true, because \( P_{1,1} = 1 \) and \( \binom{1}{1} = 1! / 0! = 1 \).

Now, assume \( P(n) \); we wish to show \( P(n+1) \). Well,

\[
P_{n+1,k} = P_{n,k-1} + P_{n,k} \quad \text{by definition}
\]

\[
= \binom{n}{k-1} + \binom{n}{k} \quad \text{by induction hypothesis}
\]

\[
= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \quad \text{by definition}
\]

\[
= \frac{n!(k+n-k+1)}{k!(n+1-k)!} \quad \text{putting things over a common denominator}
\]

\[
= \frac{n!(n+1)}{k!(n+1-k)!} \quad \text{algebra}
\]

\[
= \binom{n+1}{k} \quad \text{by definition}
\]

as required.

13. Prove the following claim using induction: for any \( n \geq 0 \), \( \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \)

**Solution**  Base case: when \( n = 0 \), the left hand side is \( 2^0 = 1 \) and the right hand side is \( 2^2 - 1 = 1 \), and they are clearly the same.

Inductive step: Choose an arbitrary \( n \) and assume that \( \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \) (this is the inductive hypothesis).

We wish to show that \( \sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1 \). We compute:

\[
\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1} \quad \text{arithmetic}
\]

\[
= (2^{n+1} - 1) + 2^{n+1} \quad \text{by the inductive hypothesis}
\]

\[
= 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1
\]
as required.

14. The Fibonacci numbers $F_0, F_1, F_2, \ldots$ are defined inductively as follows:

$$
F_0 = 1 \\
F_1 = 1 \\
F_n = F_{n-1} + F_{n-2} \quad \text{for } n \geq 2
$$

That is, each Fibonacci number is the sum of the previous two numbers in the sequence. Prove by induction that for all natural numbers $n$ (including 0):

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

**Solution** Let $P(n)$ be the statement “$\sum_{i=0}^{n} F_i = F_{n+2} - 1$.” We must show $P(0)$ and $P(n+1)$ assuming $P(n)$.

To see $P(0)$, note that $\sum_{i=0}^{0} F_i = F_0 = 1$, while $F_{0+2} - 1 = F_0 + F_1 - 1 = 1 + 1 - 1 = 1$. Since they are the same, $P(0)$ holds.

To see $P(n+1)$, first assume $P(n)$. We have

$$
\sum_{i=0}^{n+1} F_i = \sum_{i=0}^{n} F_i + F_{n+1} \\
= F_{n+2} - 1 + F_{n+1} \quad \text{by } P(n) \\
= F_{n+1+2} - 1 \quad \text{by definition of } F_{n+1+2}
$$

as required.

15. Prove by induction that for any integer $n \geq 3$, $n^2 - 7n + 12$ is non-negative.

**Solution** Let $P(n)$ be the statement “$n^2 - 7n + 12$ is non-negative.” We must show $P(3)$, and for any $n \geq 3$, $P(n+1)$ assuming $P(n)$.

To see $P(3)$, note that $3^2 - 7 \cdot 3 + 12 = 0 \geq 0$.

Now, assume $n \geq 3$ and $P(n)$; we want to show $P(n+1)$. Well,

$$
(n+1)^2 - 7(n+1) + 12 = n^2 + 2n + 1 - 7n - 7 + 12 \\
= (n^2 - 7n + 12) + (2n + 1 - 7) \\
\geq 2n + 1 - 7 \quad \text{by } P(n) \\
\geq 0 \quad \text{since } n \geq 3
$$

16. Chapter 5 of MCS has a bunch of good induction exercises (and you can find even more by searching)

17. Find the Bézout coefficients of 5 and 12. Show your work.
**Solution**

To find the gcd of $a$ and $b$, we divide to find $a = qb + r$.

Using $s'$ and $t'$ from the row below, we compute $s = t'$ and $t = s' - t'q$, and check that $1 = sa + tb$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$q$</th>
<th>$r$</th>
<th>$s$</th>
<th>$t$</th>
<th>$1 = sa + tb$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>12</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>-2</td>
<td>$1 = 5 \cdot 5 + -2 \cdot 12$</td>
</tr>
<tr>
<td>12</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>-2</td>
<td>5</td>
<td>$1 = -2 \cdot 12 + 5 \cdot 5$</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>-2</td>
<td>$1 = 1 \cdot 5 + -2 \cdot 2$</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$1 = 0 \cdot 2 + 1 \cdot 1$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$1 = 1 \cdot 1 + 0 \cdot 0$</td>
</tr>
</tbody>
</table>