1. 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 \( a = b \).

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

   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: \((a + b)(a - b) = a^2 - b^2\)

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

   ...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).

2. If \(A\) and \(B\) are any two events in a probability space \((S, P)\), prove using (only) Kolmogorov’s axioms and basic set theory that \(P(A \cup B) \leq P(A) + P(B)\).

   **Solution:** \(A \cup B = A \cup (B \setminus A)\). Since \(A\) and \(B \setminus A\) are disjoint, we can apply Kolmogorov’s third axiom to conclude that \(P(A \cup B) = P(A) + P(B \setminus A)\).

   I claim that \(P(B \setminus A) \leq P(B)\). This is because \(B\) is the union of the disjoint sets \(B \setminus A\) and \(B \cap A\), and thus \(P(B) = P(B \setminus A) + P(B \cap A)\). Since \(P(B \cap A) \geq 0\) (by axiom 2), we conclude that \(P(B \setminus A) \leq P(B)\).

   Combining this with the above statement, we conclude that \(P(A \cup B) = P(A) + P(B \setminus A) \leq P(A) + P(B)\).

3. Given a positive integer \(m\), let \(\sim_m\) be the relation on \(\mathbb{Z}\) given by \(a \sim_m b\) if and only if there exists some integer \(c\) such that \(a - b = mc\). Prove that \(\sim_m\) is an equivalence relation.

   1
Solution: We must check three things:

∼_m is reflexive: Choose any x ∈ ℤ. Then x − x = 0 = 0 · m. Thus x ∼_m x.

∼_m is symmetric: Choose any x, y ∈ ℤ, and suppose x ∼_m y. Then x − y = mc for some c. Thus y − x = m(−c), so y ∼_m x.

∼_m is transitive: Choose any x, y, z ∈ ℤ such that x ∼_m y and y ∼_m z. Since x ∼_m y, we know x − y = mc. Similarly, y − z = mc_2. Adding these together, we find x − z = x − y + y − z = m(c_1 + c_2). Thus x ∼_m z.

4. 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 ≡ 1 (mod 6), thus 7^m ≡ 1 (mod 6) for any m (applying the known result that “if a ≡ b (mod m) and c ≡ d (mod m) then ac ≡ bd (mod m)” m − 1 times), and thus 7^m − 1 ≡ 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 ≥ 1 (inductive hypothesis). Then 7^{m+1} − 1 = 7^m(7 − 1) + 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.

5. Prove that

\[ \sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1} \]

for all positive integers n.

Solution: There is a straightforward proof by induction.

Base case: For n = 1, the left-hand side is \( \frac{1}{1\cdot 2} \), and the right-hand side is \( \frac{1}{2} \), which are obviously equal.

Inductive step: Assume the statement is true for some n ≥ 1 (inductive hypothesis). Then

\[ \sum_{i=1}^{n+1} \frac{1}{i(i+1)} = \sum_{i=1}^{n} \frac{1}{i(i+1)} + \frac{1}{(n+1)(n+2)} \]

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

\[ = \frac{n(n+2)}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \]

\[ = \frac{n(n+2) + 1}{(n+1)(n+2)} \]

\[ = \frac{n^2 + 2n + 1}{(n+1)(n+2)} \]

\[ = \frac{(n+1)^2}{(n+1)(n+2)} \]

\[ = \frac{n+1}{n+2} \]

This proves the statement for n + 1. Hence proved by induction.
Note: We deducted a point for not clearly stating the inductive hypothesis. We also penalized reasoning backwards (the error of 1(c)), even though we let this pass in the prelims, since this has been extensively discussed throughout the course and there is a question in this exam to explicitly warn you against doing this.

There is another neat proof that doesn’t require induction. Note that \( \frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1} \). Then the sum can be written as:

\[
\sum_{i=1}^{n} \frac{1}{i(i+1)} = \sum_{i=1}^{n} \left( \frac{1}{i} - \frac{1}{i+1} \right) \\
= \left( \frac{1}{1} - \frac{1}{2} \right) + \left( \frac{1}{2} - \frac{1}{3} \right) + \left( \frac{1}{3} - \frac{1}{4} \right) + \cdots + \left( \frac{1}{n} - \frac{1}{n+1} \right) \\
= \frac{1}{1} - \frac{1}{n + 1} \quad \text{(all the other terms cancel out)} \\
= \frac{n}{n + 1}
\]

6. Prove by induction that the sum of the interior angles of a convex\(^1\) polygon with \( n \) sides (and hence \( n \) vertices) is \( 180(n - 2) \) degrees. You may use the fact that the sum of the interior angles of a triangle is \( 180 \) degrees. You do not need to prove straightforward geometrical facts rigorously (check with us if unsure).

Solution: The proof rests on the observation that a polygon can be decomposed into two (or more) simpler polygons. Here’s one way to do this.

Base case: A triangle is the simplest convex polygon. It has 3 sides and its interior angles sum to \( 180 = 180(3 - 2) \) degrees (given). Hence the base case is true.

Inductive step: Assume that for some \( n \), the interior angles of a convex polygon with \( n \) sides sum to \( 180(n - 2) \)°. Consider a convex polygon with \( n + 1 \) sides. It can be decomposed into a convex polygon with \( n \) sides (\( A \)) and a triangle (\( B \)) by “chopping off” a vertex.

\[ A \quad B \]

The sum of the interior angles of the \((n + 1)\)-gon is clearly the sum of the interior angles of \( A \) and \( B \). The interior angles of \( A \) sum to \( 180(n - 2) \)° (by the inductive hypothesis), and the interior angles of the triangle \( B \) sum to \( 180 \)°. Adding up, we get \( 180(n - 2) + 180 = 180(n + 1 - 2) \) degrees, which proves the statement for \( n + 1 \). Hence proved by induction.

Note: There are many other ways to solve this problem, not all of which use induction. For instance, you could use strong induction and break the \((n + 1)\)-gon into two smaller polygons, neither of which need be a triangle. Or you could pick an arbitrary point in the center of the polygon and draw lines from it to the vertices, splitting the polygon up into \( n \) triangles whose interior angles sum to \( 180n \)°.

\(^1\)A polygon is convex if, for all vertices \( p \) and \( q \) of the polygon, the line joining \( p \) and \( q \) lies entirely within the polygon.
from which you subtract the 360° at the center. This is a correct but non-inductive proof, hence it would not get credit unless you managed to incorporate induction somehow.

For non-convex polygons, you can in fact always chop off a triangle (and hence the inductive proof still works), although this is not an obvious result. For instance, in the goat-shaped non-convex polygon below, the “ear” triangle at vertex p can be removed, although no such operation is possible at a different vertex q. This fact leads to a polygon-triangulation algorithm called “ear-clipping”.

![Goat-shaped non-convex polygon](image)

7. Prove or give a counterexample: if \( L_1 \setminus L_2 \) is regular then \( L_1 \) must be regular.

**Solution:** The claim is false. Consider \( L_1 = \{0^n1^n \mid n \in \mathbb{N}\} \) and \( L_2 = L_1 \). Then \( L_1 \setminus L_2 \) is \( \emptyset \) which is clearly regular, while \( L_1 \) is not regular.

8. Prove that the language \( L = \{0^n1^n \mid n > m\} \) is not regular.

**Solution:** Suppose for the sake of contradiction that \( L \) is regular. Then there is a DFA \( M \) with \( m \) states that recognizes \( L \). Consider the string \( x = 0^m1^{m+1} \). By definition of \( L \), \( x \in L \). Moreover, \( |x| > m \), so we can apply the pumping lemma to rewrite \( x = uvw \). The pumping lemma guarantees that \( |uv| \leq m \), so we know that \( v \) contains only zeros. Moreover, we know that \( uv^2w \in L \). Now \( uv^2w = 0^{m+|v|}1^{m+1} \). But this is a contradiction, because \( |v| \geq 1 \), so \( uv^2w \) has at least as many 0s as 1s.

Thus our original premise, that \( L \) was regular, must be faulty.

9. Suppose that Alice sends the message \( a \) to Bob, encrypted using RSA. Suppose that Bob’s implementation of RSA is buggy, and computes \( k^{-1} \mod 4\phi(m) \) instead of \( k^{-1} \mod \phi(m) \). What decrypted message does Bob see? Justify your answer.

**Solution:** Alice transmits \( a^k \mod m \) to Bob, who then computes \((a^k)^{k^{-1}} \mod m \). Because Bob miscomputed \( k^{-1} \), we know that \( kk^{-1} \equiv 1 \mod 4\phi(m) \). In other words, \( kk^{-1} = 1 + t \cdot 4\phi(m) \) for some \( t \). Therefore Bob receives

\[
(a^k)^{k^{-1}} \equiv a^{1+4t\phi(m)} \\
\equiv a \cdot a^{4t\phi(m)} \\
\equiv a \cdot (a^{\phi(m)})^{4t} \\
\equiv a \cdot 1^{4t} \\
\equiv a \mod m
\]

10. (a) What are the units of \( \mathbb{Z} \mod 12 \)?
Solution: A unit in a set of numbers is a number that has an inverse. In the set \( \mathbb{Z}_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}, the units are [1], [5], [7], and [11]. In general, \([n]\) is a unit mod \(m\) if \(n\) and \(m\) are relatively prime.

(b) What are their inverses?


(c) What is \(\phi(12)\)?

Solution: By definition of \(\phi\), \(\phi(12)\) is the number of units mod 12. Since there are 4 units, \(\phi(12) = 4.\)

11. (a) Let \([X \to Y]\) denote the set of all functions with domain \(X\) and codomain \(Y\). Give a function \(f\) from \([X \to Y] \times [Y \to Z]\) to \([X \to Z]\).

Solution: Let \(f : [X \to Y] \times [Y \to Z] \longrightarrow [X \to Z]\) be given by \(f : (g, h) \mapsto h \circ g\). (Recall that \((h \circ g)(x) = h(g(x))\).

Note 1: This is not the only possible function — other solutions are also possible, e.g. the “constant” mapping that returns the same element of \([X \to Z]\) for all input pairs.

Note 2: \(g(x), h(x)\) etc are not in general functions! \(g(x)\) is the value output by \(g\) on input \(x\). The function itself is just \(g\). You lost points if you wrote the answer as, for instance, \(f : (g, h) \mapsto h(g(x))\) — the RHS is just the value output by the function \(h \circ g\) on a particular input \(x\) (which is undefined here).

(b) Is your function injective? Is it surjective? Is it bijective?

Solution: The function is not surjective in general. For example, if \(X = Z = Z\), but \(Y = \{\text{tires}\}\), \(f\) only outputs constant functions.

The function is not injective either (in general). For example, consider the sets \(X = \{\text{Mike, Sid}\}, Y = \{\text{fermat\_lite, fermat\_last}\}\) and \(Z = Z\). Let \(g_1 : X \to Y\) take \text{Mike} and \text{Sid} both to \text{fermat\_lite}, and let \(g_2\) take \text{Mike} and \text{Sid} both to \text{fermat\_last}. Similarly, let \(h\) take every element of \(Y\) to 0. Then \(f(g_1, h) = f(g_2, h)\) (these functions both take every element of \(X\) to 0), but \((g_1, h) \neq (g_2, h)\).

It is not bijective because it is not injective (also because it is not surjective).

(c) Based on your function, what can you conclude about the relationship between the cardinality of \([X \to Y] \times [Y \to Z]\) and the cardinality of \([X \to Z]\)?

Solution: This function does not show anything about the relative cardinalities, because it is neither injective nor surjective.

12. Consider the following two graphs:

(a) Is there a homomorphism from \(G_1\) to \(G_2\)? Justify your answer.
Solution: There is a homomorphism. For example, the function taking $a$ and $d$ to $x$ and taking $b$ and $c$ to $w$ is a homomorphism. One can check that for each of the four edges in $G_1$, the corresponding edge is an edge of $G_2$.

(b) Is there an isomorphism from $G_1$ to $G_2$? Justify your answer.

Solution: There is not. There are many possible explanations; for example, $G_1$ contains no cycle of length 3, but $G_2$ does.