Instructions: This is a 2 ½ hour exam. Please answer the following questions in the provided booklet. Ensure that your name and netid are on your exam booklet. Clearly indicate your answer to each question. Books, notes, calculators, laptops, and carrier pigeons are all disallowed. You may leave mathematical expressions unevaluated (e.g. just write 17 · 3 instead of 51). You may use results proved in class (or in the homeworks, or the prelims) without proof.

We will use \( \mathbb{N} \) to denote the set of natural numbers, i.e. \{0, 1, 2, 3, \ldots \} and \( \mathbb{Z} \) to denote the integers \{\ldots, -1, 0, 1, 2, \ldots \}.

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 \( n = 1 \).
   
   (b) **Proof that 2 = 1:** Let \( a = b \).

   \[
   \begin{align*}
   &\Rightarrow a^2 = ab \\
   &\Rightarrow a^2 - b^2 = ab - b^2 \\
   &\Rightarrow (a + b)(a - b) = b(a - b) \\
   &\Rightarrow a + b = b
   \end{align*}
   \]

   Setting \( a = b = 1 \), we get \( 2 = 1 \).
   
   (c) **Proof that** \( (a + b)(a - b) = a^2 - b^2 \):

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

   \[
   \begin{align*}
   &\Rightarrow a^2 - ab + ab - b^2 = a^2 - b^2 \\
   &\Rightarrow a^2 - b^2 = a^2 - b^2
   \end{align*}
   \]

   \( \ldots \) which is true, hence the result is proved.

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 \( P(A \cup B) \leq P(A) + P(B) \).

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.

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

5. Prove that

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

   for all positive integers \( n \).

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).

---

\(^1\)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.
7. Prove or give a counterexample: if \( L_1 \setminus L_2 \) is regular then \( L_1 \) must be regular.

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

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.

10. (a) What are the units of \( \mathbb{Z} \mod 12 \)?
    (b) What are their inverses?
    (c) What is \( \phi(12) \)?

11. (a) Let \([X \rightarrow Y]\) denote the set of all functions with domain \( X \) and codomain \( Y \). Give a function \( f \) from \([X \rightarrow Y] \times [Y \rightarrow Z]\) to \([X \rightarrow Z]\).
    (b) Is your function injective? Is it surjective? Is it bijective?
    (c) Based on your function, what can you conclude about the relationship between the cardinality of \([X \rightarrow Y] \times [Y \rightarrow Z]\) and the cardinality of \([X \rightarrow Z]\)?

12. Consider the following two graphs:

\[
G_1:
\begin{array}{ccc}
  a & b \\
  \_ & \_ \\
  c & \_ & d \\
\end{array}
\]

\[
G_2:
\begin{array}{ccc}
  x & y \\
  \_ & \_ \\
  z & w \\
\end{array}
\]

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