Problems

Problem 1

Show that the square of an even number is also an even number using both:

- A Direct Proof
- A Proof by Contradiction

Problem 2

Prove that $\forall n \in \mathbb{Z}, \ n^2 + 3n - 5$ is odd using division of cases.
Logic/Circuits

Problem 1

a. Suppose $p$ and $q$ are propositions such that $p \rightarrow q$ is False. Determine the truth values of:

(i) $\neg p \rightarrow q$
(ii) $p \lor q$
(iii) $q \rightarrow p$

b. You are now going to design a circuit that takes as input two 1-bit binary numbers $A$ and $B$ and outputs whether or not $A > B$, $A < B$, or $A = B$. Namely, the circuit should have two inputs, the bits $A$ and $B$, and three outputs $G$, $E$, and $L$. For any input, exactly one of $G$ (greater), $E$ (equal), or $L$ (less) should be 1. Note that $G$ corresponds to $A > B$.

(i) Write out a truth table equivalent to this circuit.
(ii) Draw your circuit. Please use only And, Or, and Not gates with at most two inputs per gate. Note that we care only about the correctness of the circuit, not its complexity.

Be sure to explain how your circuit works.

Problem 2

a. Add parentheses to the following expressions to make them true (1 represents true, and 0 represents false). Note also that there is no implicit ordering; that is, all ordering comes from your parentheses. State explicitly any assumptions you are making about the order of operations.

i. $0 \land 1 \lor 1 \Rightarrow 1 \land 1 \land 1 \lor 0$
ii. $0 \lor 0 \land 1 \land 0 \land 1 \lor 1$
iii. $0 \land 1 \lor 1 \leftrightarrow 0 \Rightarrow 0$
iv. $0 \lor 1 \Rightarrow 0 \land 0 \Rightarrow 1$

b. Prove the following logical equivalences:

i. $\neg (p \lor (\neg p \land q)) \equiv \neg p \land \neg q$
ii. $(p \Rightarrow r) \land (q \Rightarrow r) \equiv (p \lor q) \Rightarrow r$

b. Prove that $q \land \neg (p \Rightarrow q)$ is unsatisfiable.

d. Prove that $(p \land q) \Rightarrow (p \lor q)$ is valid.
Set Theory

Problem 1

Determine whether each of the following statements is true or false, and explain why.

a. The powerset of the empty set has the empty set as a member.
b. The empty set is an element of every set.
c. The empty set is a subset of any set that does not have the empty set as a member.
d. Any set that has the empty set as a member must be the empty set.
e. The set containing the set containing the set containing the empty set has a cardinality of zero (here, $A$ contains $B$ means $B \in A$).
f. The set of all empty sets is the same as the powerset of the empty set.

Problem 2

a. Disprove the following claim:
   For any two sets finite $A$ and $B$, there are the same number of elements in $\mathcal{P}(A \times B)$ and $\mathcal{P}(A) \times \mathcal{P}(B)$.
b. Consider two finite, non-empty sets $A$ and $B$. Suppose $\mathcal{P}(A \times B)$ and $\mathcal{P}(A) \times \mathcal{P}(B)$ were equal in size. What must be the size of $A$? What must be size of $B$? Explain your answer.
Relations

Problem 1

a. Prove or disprove that a relation that is reflexive and symmetric is necessarily transitive.
b. Prove or disprove that a relation that is reflexive and transitive is necessarily symmetric.
c. Prove or disprove that a relation that is symmetric and transitive is necessarily reflexive.

Problem 2

Let $S = \{0, 1\}$, $T = \{t|t \subseteq S \times S\}$, and $R$ be the set of all possible functions from $S$ to $S$.

a. Can an injection from $T$ to $R$ exist? If so, give one such injection and prove that this mapping is indeed injective. If not, prove why such a mapping cannot exist.
b. Can a surjection from $T$ to $R$ exist? If so, give one such surjection and prove that this mapping is indeed surjective. If not, prove why such a mapping cannot exist.
c. Can a bijection from $T$ to $R$ exist? If so, why? If not, why not?
## Induction

### Problem 1

Suppose we have a sequence defined as follows:

\[
a_1 = 1 \\
a_2 = 3 \\
a_k = a_{k-2} + 2a_{k-1}
\]

Prove by induction that \( a_n \) is odd for all positive integers \( n \).

### Problem 2

Use mathematical induction to prove the following generalization of one of DeMorgan’s laws:

\[
\bigcap_{j=1}^{n} A_j = \bigcup_{j=1}^{n} \overline{A_j}
\]

whenever \( A_1, A_2, \ldots, A_n \) are subsets of a universal set \( U \) and \( n \geq 2 \). To give you an idea of what this notation means

\[
\bigcap_{j=1}^{3} A_j = A_1 \cap A_2 \cap A_3
\]

**Note:** You must prove DeMorgan’s Law for the base case.

## 1 Number Theory

### Problem 1

Suppose \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \). Let \( n \in \mathbb{Z}^+ \). Prove the following statements:

a. \( ac \equiv bd \pmod{m} \).
b. \( a^n \equiv b^n \pmod{m} \).

**Hint:** Try induction on \( n \).
Problem 2

Use the extended Euclidean algorithm, showing your steps, find the greatest common divisor of 99 and 129 and express it as a linear combination of those values.