1. Prove that if m is an even integer, then $m+7$ is odd. Do this proof in three ways: direct proof, proof by contraposition and proof by contradition.

   (a) Direct Proof: Assume that m is an even integer. Then $\exists k \in \mathbb{Z}$ such that $m = 2k$. Then $m+7 = 2k+7 = 2k+6+1 = 2k+2\times 3+1 = 2(k+3)+1$. Since k and 3 are integers, $k+3$ is an integer, so $2(k+3)$ is an even integer. Hence $m+7 = 2(k+3)+1$ is an odd integer. ■

   (b) Proof by Contraposition: We will prove that if $m+7$ is an even integer, then m is an odd integer. Proof: If $m+7$ is even, then $\exists k \in \mathbb{Z}$ such that $m+7 = 2k$. Thus $m = 2k-7 = 2k-2\times 3-1 = 2(k-3)-1$. Since k and 3 are integers, $k-3$ is an integer, so $2(k-3)$ is an even integer. Hence $m = 2(k-3)-1$ is an odd integer. ■

   (c) Proof by Contradiction: Assume $\exists m \in \mathbb{Z}$ such that m is even and $m+7$ is even. Then $\exists k, j \in \mathbb{Z}$ such that $m = 2k$ and $m+7 = 2j$. Thus $m = 2k$ and $m = 2j-7$, so that $2k = 2j-7$, or $2(k-j) = -7$. Since k and j are integers, $k-j$ is an integer, thus -7 is an even integer, a contradiction. Thus the assumption is false, and the original statement is true. ■

2. Using proof by contradiction, prove that $\forall n \in \mathbb{Z}, 4 \nmid (n^2+2)$
   Suppose that $\exists n \in \mathbb{Z}, 4|(n^2+2)$. By definition of divisibility, $\exists k \in \mathbb{Z}$, such that $4k = n^2+2$. Rewrite as $n^2 = 4k-2 = 2(k-1)$, which indicates that n^2 is even and thus n is even. By definition of even numbers, $\exists q \in \mathbb{Z}$, such that $n^2 = (2q)^2 = 4q^2$. $n^2 = 4q^2$ indicates that n^2 is divisible by 4. Previously, we assumed n^2+2 is also divisible by 4. n^2 and n^2+2 can not both be divisible by 4, hence contradiction. ■

3. Using induction, prove that for all integers $n \geq 1, 2^{2n}-1$ is divisible by 3, i.e. $3|2^{2n}-1$

   Base case: $n=1$: $2^{2\times 1}-1 = 3$ and $3|3$.
   Inductive hypothesis: assume $3|2^{2k}-1 \implies 2^{2k}-1 = 3q, q \in \mathbb{Z}$
   Prove for $k+1$:

$$\begin{aligned} 2^{2(k+1)}-1 &= 2^{2k+2}-1 \\ &= 2^{2k}\times 4-1 \\ &= 2^{2k}\times 3+2^{2k}-1 \\ &= 2^{2k}\times 3+3q \\ &= (2^{2k}+q)\times 3 \end{aligned}$$

   $q \in \mathbb{Z}$ and $2^{2k} \in \mathbb{Z}$, thus $3|2^{2(k+1)}-1$. ■

4. Given sets A, B, and C in the same universe, determine if each of the following statements is true or false. If it is true, then prove it. If it is false, then give a counter example.

   (a) $C \subseteq A \wedge C \subseteq B \rightarrow C \subseteq A \cup B$
   Proof: Let $x \in C$. Since $C \subseteq A$ and $C \subseteq B$, $x \in A$ and $x \in B$. Thus by definition, $x \in A \cap B$. ■

   (b) $C \subseteq A \cup B \rightarrow C \subseteq A \wedge C \subseteq B$
   This is false. A counter example is given for example by $A = \{1,2\}$, $B = \{3,4\}$ and $C = \{2,3\}$.

   (c) $A^c \cap (A \cup B) = B \backslash A$.
   Algbraic proof: $A^c \cap (A \cup B) = (A^c \cap A) \cup (A^c \cap B) = \emptyset \cup (A^c \cap B) = A^c \cap B = B \setminus A$. ■
   Alternatively: show that $A^c \cap (A \cup B) \subseteq A \setminus B$ and $A \setminus B \subseteq A^c \cap (A \cup B)$
   $A^c \cap (A \cup B) \subseteq A \setminus B$: Let x be an arbitrary element in $A^c \cap (A \cup B)$, by definition, $x \in A^c$ and $x \in (A \cup B)$, which is equivalent to $x \notin A$ and ($x \in A$ or $x \in B$), and it follows that $x \notin A$ and $x \in B$, which is by definition $x \in B \setminus A$

$A \setminus B \subseteq A^c \cap (A \cup B)$: Let x be an arbitrary element in $A \setminus B$. by definition, $x \in B$ and $x \notin A$. $x \in B \rightarrow x \in (A \cup B)$ and $x \notin A \rightarrow x \in A^c$. Thus $x \in (A \cup B)$ and $x \in A^c$, by definition, $x \in A^c \cap (A \cup B)$. ■

5. Prove that give a set S, the cardinality of its power set is $2^{|S|}$.
   Do an induction on $|S|$.
   Base case: $|S| = 0$, which means S is the empty set. The power set of the empty set contains one element, the empty set itself. Thus $|P(\varnothing)| = 1 = 2^0 = 2^{|\varnothing|}$.
   Inductive hypothesis: $|S| = k$, and $|P(S)| = 2^k$
   Prove for $|S| = k + 1$:
   For the first k elements in S, we construct their power set, say $P(S_k)$, which by the inductive hypothesis, has 2^k elements. All these elements must be in the power set of $P(S)$. The rest of the power set consist of all possible subsets that contain the $(k + 1)$-th elemement, and we form these subsets by adding the $(k + 1)$-th element to every set found in $P(S_k)$. And there are 2^k of these subsets. Therefore $|P(S)| = 2^k + 2^k = 2^{k+1}$. ■

6. Prove that if $a_1, a_2, ..., a_n$ are n distinct real numbers, exactly $n - 1$ multiplications are needed to compute the product of these n numbers, no matter how parentheses are inserted into their product.
   Proof by strong induction:
   Base case: $n = 1$: The product a_1 requires $1 - 1 = 0$ multiplication.
   Inductive hypothesis: assume that $a_1 \times a_2 \times \ldots \times a_k$ require $k - 1$ multiplications, $\forall k, 1 \leq k \leq n$.
   Inductive step: Consider the last multiplication (any last multiplication no matter how the parentheses are inserted) used to compute the product of $a_1 \times a_2 \times \ldots \times a_{n+1}$. It must be the product of k of these numbers and $n + 1 - k$ of these numbers, for some k, $1 \leq k \leq n$. By the inductive hypothesis, those two products requires $k - 1$ and $n - k$ multiplications, respectively. Counting the last multiplication, the total multiplications needed for $a_1 \times a_2 \times \ldots \times a_{n+1}$ is thus $(k - 1) + (n - k) + 1 = n = (n + 1) - 1$.
   ■

7. For each of the following, give a *recursive* definition. Remember to indicate the initial terms or base:
   (a) $a_n = \sum_{i=0}^{n} i$
       $a_0 = 0$, $a_k = a_{k-1} + k$
   (b) The sequence that generates the terms 3, 6, 12, 24, 48, 96, 192, ...
       $a_0 = 3$, $a_k = 2a_{k-1}$
   (c) The set of non-negative even numbers
       $0 \in S$, $x \in S \rightarrow x + 2 \in S$, nothing else is in S.
   (d) The set of all even numbers
       $0 \in S$, $x \in S \rightarrow x + 2 \in S \wedge x \in S \rightarrow x - 2 \in S$, nothing else is in S.

8. Find explicit formulae for the following recursively defined sequences, and prove correctness using induction.
   (a) $a_k = k - a_{k-1}$, $\forall k \geq 1$, $a_0 = 0$.

$$
\begin{aligned}
a_0 &= 0 \\
a_1 &= 1 - a_0 = 1 - 0 = 1 \\
a_2 &= 2 - a_1 = 2 - 1 = 1 \\
a_3 &= 3 - a_2 = 3 - 1 = 2 \\
a_4 &= 4 - a_3 = 4 - 2 = 2 \\
a_5 &= 5 - a_4 = 5 - 2 = 3 \\
a_6 &= 6 - a_5 = 6 - 3 = 3
\end{aligned}
$$

   Guess: $a_k = \lceil \frac{k}{2} \rceil$

Proof by strong induction:
Base case: $a_0 = 0 = \lceil \frac{0}{2} \rceil$
Inductive hypothesis: $a_i = \lceil \frac{i}{2} \rceil, \forall i, 0 \leq i \leq k$
Inductive step:

$$\begin{aligned}
a_{k+1} &= k + 1 - a_k && \text{by definition} \\
&= k + 1 - \lceil \frac{k}{2} \rceil && \text{by inductive hypothesis} \\
&= \begin{cases} k+1-\frac{k+1}{2} & \text{if } k+1 \text{ is even } (k \text{ is odd}) \\ k+1-\frac{k}{2} & \text{if } k+1 \text{ is odd } (k \text{ is even}) \end{cases} && \text{by definition of ceiling} \\
&= \begin{cases} \frac{2(k+1)-(k+1)}{2} & \text{if } k+1 \text{ is even} \\ \frac{2(k+1)-k}{2} & \text{if } k+1 \text{ is odd} \end{cases} \\
&= \begin{cases} \frac{k+1}{2} & \text{if } k+1 \text{ is even} \\ \frac{k+2}{2} & \text{if } k+1 \text{ is odd} \end{cases} \\
&= \lceil \frac{k+1}{2} \rceil && \text{by definition of ceiling}
\end{aligned}$$

■

(b) $a_k = 2a_{k-2}$, $\forall k \geq 2$, $a_0 = 1, a_1 = 2$.

$$\begin{aligned}
a_0 &= 1 = 2^0 \\
a_1 &= 2 = 2^1 \\
a_2 &= 2a_0 = 2 \times 2^1 = 2^1 \\
a_3 &= 2a_1 = 2 \times 2^1 = 2^2 \\
a_4 &= 2a_2 = 2 \times 2^1 = 2^2 \\
a_5 &= 2a_3 = 2 \times 2^2 = 2^3 \\
a_6 &= 2a_4 = 2 \times 2^2 = 2^3
\end{aligned}$$

Guess: $a_k = 2^{\lceil \frac{k}{2} \rceil}$
Proof by strong induction:
Base case: $a_0 = 1 = 2^0 = 2^{\lceil \frac{0}{2} \rceil}$ and $a_1 = 2 = 2^1 = 2^{\lceil \frac{1}{2} \rceil}$
Inductive hypothesis: $a_i = 2^{\lceil \frac{i}{2} \rceil}, \forall i, 0 \leq i \leq k$
Inductive step:

$$\begin{aligned}
a_{k+1} &= 2a_{k-1} && \text{by definition} \\
&= 2 \times 2^{\lceil \frac{k-1}{2} \rceil} && \text{by inductive hypothesis} \\
&= \begin{cases} 2 \times 2^{\frac{k-1}{2}} & \text{if } k-1 \text{ is even} \\ 2 \times 2^{\frac{k-1+1}{2}} & \text{if } k-1 \text{ is odd} \end{cases} && \text{by definition of ceiling} \\
&= \begin{cases} 2^{\frac{k-1}{2}+1} & \text{if } k-1 \text{ is even} \\ 2^{\frac{k}{2}+1} & \text{if } k-1 \text{ is odd} \end{cases} \\
&= \begin{cases} 2^{\frac{k+1}{2}} & \text{if } k-1 \text{ is even} \\ 2^{\frac{k+2}{2}} & \text{if } k-1 \text{ is odd} \end{cases} \\
&= \begin{cases} 2^{\frac{k+1}{2}} & \text{if } k+1 \text{ is even} \\ 2^{\frac{k+2}{2}} & \text{if } k+1 \text{ is odd} \end{cases} && k+1 \text{ and } k-1 \text{ have the same parity} \\
&= 2^{\lceil \frac{k+1}{2} \rceil} && \text{by definition of ceiling}
\end{aligned}$$

■

9. Prove the correctness of the following algorithm:

```
[Pre-condition: i=1 and sum=0]
while(i<=100)
  sum := sum + i
  i := i + 1
end while
[Post-condition: sum = 1 + 2 + ... + 100]
```

State your loop invariant clearly.

Loop invariant: $I(n) : i = n + 1$ and $sum = 1 + ... + n$

(a) Base case:
$$I(0) : n = 0 \Rightarrow \begin{cases} i = 0 + 1 = 1 & \text{by the loop invariant} \\ sum = 0 & \text{no addition performed, } 0 < 1 \end{cases}$$
which matches the pre-condition

(b) Inductive: Assume that before an arbitrary iteration $k + 1$, $I(k)$ is true, i.e. $i = k + 1$ and $sum = 1 + ... + k$
loop iteration execution:
`sum := sum + i` $\Rightarrow sum = 1 + ... + k + (k + 1)$
`i := i + 1` $\Rightarrow i = k + 2$
Thus $I(k + 1)$ is true after one loop iteration

(c) Eventual falsity of guard: i starts at 1 and is incremented at each iteration until ≤ 100 is violated, which is at $I(100)$.

(d) Correctness of post-condition: $I(100) : i = 101$ and $sum = 1 + ... + 100$, which matches the post-condition.

10. Given the following recursive definition of a set S:

- Basis: $\lambda \in S$
- Recursive: $x \in S \rightarrow axa \in S$

Prove using structural induction, that $\forall s \in S, |s|$ is even.

Base case: $|\lambda| = 0$, 0 is even.
Inductive hypothesis: assume all strings of length n in S have even length, thus n is even.
Recursive step:
We construct $s = axa$, by the recursive definition, where $|x| = n$. Thus $|s| = 1 + |x| + 1 = n + 2$. By the inductive hypothesis, n is even, $n + 2$ is also even, thus $|s|$ is even.