This examination document contains 6 pages, including this cover page, and 5 problems. You must verify whether there any pages missing, in which case you should let the instructor know. Fill in all the requested information on the top of this page, and put your initials on the top of every page, in case the pages become separated.

You may not use your books, notes, or any calculator on this exam.

You are required to show your work on each problem on this exam. The following rules apply:

(A) If you use a lemma, proposition or theorem which we have seen in the class or in the book, you must indicate this and explain why the theorem may be applied.

(B) Organize your work, in a reasonably neat and coherent way, in the space provided. Work scattered all over the page without a clear ordering will receive little credit.

(C) Mysterious or unsupported answers will not receive full credit. A correct answer, unsupported by calculations, explanation, or algebraic work will receive little credit; an incorrect answer supported by substantially correct calculations and explanations will receive partial credit.

(D) If you need more space, use the back of the pages; clearly indicate when you have done this.

Do not write in the table to the right.
1. (20 points) Show that there are infinitely primes of the form $4k - 1$, for $k \in \mathbb{N}$.

Let us argue by contradiction. Suppose that there are only finitely many primes

$$A = \{p_1, \ldots, p_N\}$$

of the form $4k - 1$, with $k \in \mathbb{N}$. Then consider the natural odd number

$$P = 4(p_1 \cdot \ldots \cdot p_N) - 1 \in \mathbb{N}.$$

First, let us show that none of the $p_i \in A$ divide $P$, for any $1 \leq i \leq N$. By contradiction again, suppose there exists an $i \in \mathbb{N}$ such that $p_i \mid P$, then

$$p_i \mid P - 4(p_1 \cdot \ldots \cdot p_N),$$

since $p_i$ divides each summand. However $P - 4(p_1 \cdot \ldots \cdot p_N) = -1$ and thus $p_i$ divides $-1$, which is a contradiction since $p_i$ is prime for $1 \leq i \leq N$. In consequence, none of the primes $p_i \in A$ divide $P$, and in particular $P \notin A$.

Second, either $P$ is a prime itself or it is not. In the former case, where we assume $P$ is prime, we have that $P$ is of the form $4k - 1$, and then we get a contradiction with the fact that $P \notin A$ but $A$ contained all primes of the form $4k - 1$. In the later case, where $P$ is not prime, then we know that $P$ is divisible by at least one prime $\rho \in \mathbb{N}$ of the form $4k - 1$, because otherwise $P$ would be itself of the form $4k + 1$. This is also a contradiction since $\rho$ is a prime of the form $4k - 1$ but $\rho \notin A$, since $\rho$ divides $P$.  

2. (20 points) Prove the following two statements.

(a) (10 points) Show that for all \( n \in \mathbb{Z}, n \geq 1 \), the following inequality holds
\[
2^{n-1} \leq n!
\]
The base case \( n = 1 \) is true since \( 2^{0} \leq 1! \) is the correct inequality \( 1 \leq 1 \). By induction, let us assume that the inequality \( 2^{n-1} \leq n! \) holds, and we want to prove that \( 2^{n} \leq (n + 1)! \). Indeed,
\[
2^{n} = 2 \cdot 2^{n-1} \leq 2 \cdot n! \leq (n + 1) \cdot n! = (n + 1)!,
\]
where in the first inequality we use the induction step \( 2^{n-1} \leq n! \) and in the second we use \( 2 \leq (n + 1) \), which is true for all \( n \in \mathbb{N} \).

(b) (10 points) Prove that for all \( n \in \mathbb{Z}, n \geq 1 \), the following equality holds
\[
\sum_{k=0}^{n} 7 \cdot 2^{k} = 7 \cdot 2^{n+1} - 7.
\]
The base case \( n = 1 \) states \( 7 \cdot 2^{0} + 7 \cdot 2^{1} = 7 \cdot 2^{2} - 7 \), which is true since both sides equal 21. By induction, let us assume that the formula
\[
\sum_{k=0}^{n} 7 \cdot 2^{k} = 7 \cdot 2^{n+1} - 7,
\]
holds, and we want to prove \( \sum_{k=0}^{n+1} 7 \cdot 2^{k} = 7 \cdot 2^{n+2} - 7 \). Indeed, let us develop the left hand side of this equality:
\[
\sum_{k=0}^{n+1} 7 \cdot 2^{k} = \left( \sum_{k=0}^{n} 7 \cdot 2^{k} \right) + 7 \cdot 2^{n+1} = (7 \cdot 2^{n+1} - 7) + 7 \cdot 2^{n+1} = (7 \cdot 2^{n+2} - 7),
\]
where we have split the \( 2^{n+1} \) factor in the first equality, applied the inductive hypothesis in the second equality and just rearranged the number in the third equality. Alternatively, this problem can be solved by directly using the closed formula for the geometric series
\[
\sum_{k=0}^{n} 2^{k} = \frac{2^{n+1} - 1}{2 - 1},
\]
and multiplying the equality by 7.
3. (20 points) Provide correct mathematical proofs of the following two statements.

(a) (10 points) Prove that for any \( k, n \in \mathbb{N} \) with \( k \leq n \), the following equality is true:

\[
\binom{n}{k} k = n \cdot \binom{n-1}{k-1}.
\]

By writing the definition of the binomial coefficients, the equality becomes

\[
k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1} \iff k \cdot \frac{n!}{k!(n-k)!} = n \cdot \frac{(n-1)!}{(k-1)!(n-k)!}.
\]

The equality on the right hand side is true since, by definition of the factorial, we can rewrite \( n(n-1)! = n! \) on its right hand side, and \( \frac{k}{k!} = \frac{1}{(k-1)!} \) on its left hand side.

Alternatively, we can prove the equality by giving it a combinatorial interpretation, as follows. Let us consider a set \( N \) with \( n \) elements, we want to choose a subset \( K \) of \( k \) elements and then a distinguished element inside of \( K \). This can be done in the following two ways:

(i) First, choose the subset \( K \subseteq N \). By the combinatorial interpretation of \( \binom{n}{k} \) as the number of subsets of size \( k \) inside a set of size \( n \), there are \( \binom{n}{k} \) choice for \( K \). Then we choose the distinguished element inside of \( K \). Since \( K \) has \( k \) elements, there are \( k \) choices, for \( k \in K \). Given that we are choosing \( K \) and the distinguished element, we must multiply, and thus we have \( k \cdot \binom{n}{k} \) choices. This is the left hand side of the equality.

(ii) We can also do this as follows. First, choose a distinguished element inside of \( N \), there are \( n \) choices for that. Now, as a second step, choose a subset \( K \) inside of \( N \) which contains \( k \) elements and also this distinguished element. For this second step we have \( \binom{n-1}{k-1} \) choices since we have to choose \( (k-1) \) elements (the distinguished one has already been chosen) out of \( n-1 \) elements, since we cannot pick again the distinguished element. Given that we are choosing the distinguished element and then subset \( K \) containing it, we must multiply, and thus we have \( n \cdot \binom{n-1}{k-1} \) choices. This is the right hand side of the equality.

(b) (10 points) Prove that for all \( n \in \mathbb{Z}, n \geq 1 \), the following formula holds:

\[
\sum_{k=0}^{n} \binom{n}{k} 8^k = 9^n.
\]

The Binomial Theorem states that for any \( a, b \in \mathbb{N} \)

\[
\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = (a + b)^n.
\]

By substituting \( a = 8 \) and \( b = 1 \) we obtain the desired equality.
4. (20 points) Let \((a_n), n \in \mathbb{N}\), be a sequence of natural numbers that satisfies the recursion
\[ a_{n+1} = a_n + 12a_{n-1}, \]
with the initial values \(a_1 = 1\) and \(a_2 = 1\).

(a) (5 points) Write the first 5 terms of the sequence.

The sequence starts with \((a_1, a_2, a_3, a_4, a_5, a_6, \ldots) = (1, 1, 13, 25, 181, 481, \ldots)\).

(b) (5 points) Find the two roots \(r_1, r_2 \in \mathbb{Z}\) of the characteristic polynomial \(p(x)\) associated to the recursion \(a_{n+1} = a_n + 12a_{n-1}\).

The characteristic polynomial of the recursion \(a_{n+1} = a_n + 12a_{n-1}\) is
\[ p(x) = x^2 - x - 12. \]

Its two distinct zeroes \(r_1, r_2 \in \mathbb{Z}\) are \(r_1 = -3\) and \(r_2 = 4\).

(c) (10 points) Find a closed formula for the \(n\)th term \(a_n\).

The general expression for the \(n\)th term \(a_n\) is of the form
\[ a_n = C \cdot (-3)^n + D \cdot 4^n. \]

It suffices to determine \(C\) and \(D\) from the initial conditions. By inserting \(a_1 = 1\) and \(a_2 = 1\) in the above expression we get the equations
\[ 1 = C \cdot (-3) + D \cdot 4, \]
\[ 1 = C \cdot (-3)^2 + D \cdot 4^2 \]
which have the unique solution \(C = -1/7\) and \(D = 1/7\). Hence the closed formula for the \(n\)th term of the sequence \((a_n)\) is
\[ a_n = \left(\frac{-1}{7}\right) (-3)^n + \left(\frac{1}{7}\right) \cdot 4^n. \]

This recovers the initial terms as in Part (a) and even more:
\[(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \ldots) = (1, 1, 13, 25, 181, 481, 2653, 8425, \ldots)\]
5. (20 points) Solve the following two problems.

(a) (10 points) Find the last digit of $19^{31}$. (Explain your reasoning.)

This is asking for a representative $k$ of the equivalence class of 19 under the equivalence relation \( \text{mod} \ 10 \), with $0 \leq k \leq 9$. Let us work modulo 10, and find a representative $19^{31}$. First, we have the equivalence

\[
19 \equiv (-1) \mod 10,
\]

and thus by taking powers we obtain $19^{31} \equiv (-1)^{31} \equiv -1 \equiv 9 \mod 10$. In consequence, the answer is that the last digit is 9.

Alternatively, observe that $9^2 \equiv 81 \equiv 1 \mod 10$, and thus we can write

\[
19^{31} \equiv 9^{31} \equiv 9^{30} \cdot 9 \equiv (9^2)^{15} \cdot 9 \equiv 1^{15} \cdot 9 \equiv 9 \mod 10,
\]

and we obtain again that the last digit is 9.

(b) (10 points) Show that there do not exist two integers $x, y \in \mathbb{Z}$ such that

\[
x^2 + 4x + 1 = 4y^2.
\]

Consider the equation

\[
x^2 + 4x + 1 = 4y^2,
\]

modulo 4, where it becomes

\[
x^2 + 1 \equiv 0 \mod 4.
\]

Now, any equivalence class $x \mod 4$ satisfies either

\[
x^2 \equiv 0 \mod 4, \quad \text{or} \quad x^2 \equiv 1 \mod 4,
\]

depending on whether $x \in \mathbb{N}$ is either even or odd. In consequence, the above equation reads

\[
1 \equiv 0 \mod 4, \quad \text{or} \quad 2 \equiv 0 \mod 4,
\]

which is impossible, and so no solution can exist. In other terms, we have shown that the left hand side of

\[
x^2 + 4x + 1 = 4y^2,
\]

is never divisible by 4, whereas the right hand side is divisible by 4. Hence no solution can exist since this would lead to a contradiction.