INSTRUCTIONS

The exam consists of nine problems worth a total of 120 points. Of these, 20 points in Problem 9 are extra-credit points. That is, a score of only 100 points is needed to receive the full 50% credit given to the final exam. Scores in excess of 100 points will compensate for the midterm exam and/or homework scores.

Write your answers in the spaces provided. Show all your work, except in the multiple choice problem and in the true/false problems. If you need extra space, please use the back of the previous page. Partial credit will be given only for substantial progress on a problem.

Good luck!
Problem 1 (4 points)

Let $x = 1010110_2$ and $y = 101_2$. Then the 10-bit two’s complement representation of $-xy$ is:

- $0110101110_2$
- $0001010010_2$
- $1001010010_2$
- $1001010001_2$

Check at most one of the four boxes. **No justification is required.** Grading: 4 points if the correct box is the only one checked, 1 point if no box is checked, and 0 points in all other cases.
Problem 2 (10 points)

Which of the following statements are true and which are false?

<table>
<thead>
<tr>
<th>True</th>
<th>False</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Note: a palindrome is a sequence, such as 1, 5, 10, 5, 1, that reads the same from right and left.

No justification is required. For each of the five statements above, grading is as follows: 2 points if the correct box is the only one checked, 1 point if no box is checked, and 0 points in all other cases.
Problem 3 (10 points)

In this problem, $X$, $Y$, and $Z$ are arbitrary finite sets. Determine whether the following statements are true or false for all functions $f: X \to Y$ and $g: Y \to Z$.

True  False

☐  ☐  $f$ is either an injection or a surjection (or both).

☐  ☐  If both $f$ and $g$ are injections, then $g \circ f$ is an injection.

☐  ☐  If $g$ is a surjection, then $g \circ f$ is a surjection.

☐  ☐  There exists a function $h: Y \to X$ such that $h \circ f$ is a bijection.

☐  ☐  If $f$ and $g$ are both bijections, then $g \circ f$ is a bijection.

No justification is required. For each of the five statements above, grading is as follows: 2 points if the correct box is the only one checked, 1 point if no box is checked, and 0 points in all other cases.
Problem 4 (17 points)

Let \( f(x, y, z) \) be the boolean function defined by the following truth table:

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( z )</th>
<th>( f(x, y, z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

a. Express the function \( f(x, y, z) \) in disjunctive normal form.

\[
f(x, y, z) =
\]

b. Design a logic circuit that implements this function. You can use any number of NOT gates, and any number of two-input AND, OR, XOR gates. However, your score will decrease by one point for each gate in your design beyond the minimum number of gates required.
c. Consider the following statement about \( f(x, y, z) \) and another boolean function \( g(x, y, z) \):

\[
S : \forall x, y, z \in \{0, 1\}, \text{ if } f(x, y, z) = 1 \text{ then } g(x, y, z) = 1
\]

What is the negation of this statement? What is its converse?

Negation:

Converse:

d. If \( f(x, y, z) \) is the function defined at the beginning of this problem, how many different boolean functions \( g(x, y, z) \) are there such that \( S \) is a true statement? For how many different boolean functions \( g(x, y, z) \) is the converse of \( S \) true?

\[
\# \text{ of boolean functions } g(x, y, z) \text{ such that } S \text{ is true:}
\]

\[
\# \text{ of boolean functions } g(x, y, z) \text{ such that the converse of } S \text{ is true:}
\]
Problem 5 (14 points)

a. Prove by induction that for all positive integers $n$, the sum $7^{2n-1} + 6^{2n-1}$ is divisible by 13.

Base:

Induction Hypothesis:

Induction Step:
b. Now prove that $7^{2n-1} + 6^{2n-1}$ is divisible by 13 for all positive integers $n$ \textit{without induction}.

Use modular arithmetic instead!
**Problem 6 (12 points)**

Alice uses the following RSA public key: modulus $N = 187$, encryption key $e = 107$. Bob chooses a message $m$ such that $\gcd(m, N) = 1$, encrypts it using the public key above, and sends to Alice the encrypted message $M = 3$. What was Bob’s original message to Alice? Show your work.

*Hint:* Factor the modulus $N$ using the test we have developed in class for divisibility by 11.
Problem 7 (14 points)

Given a positive integer $n$, let $D_n$ denote the set of all the divisors of $n$. For example, for $n = 30$, we have $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

a. List all the elements of the set $D_{336} \cap D_{210}$.

$D_{336} \cap D_{210} = \{\}$
b. Now express the elements of the same set $D_{336} \cap D_{210}$ in the binary number system, and list them in lexicographic order (with $0 < 1$).

*Note:* When writing the elements of $D_{336} \cap D_{210}$ in binary, use the minimum number of bits necessary to represent each integer. For example, the elements of $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ should be represented as \{1, 10, 11, 101, 110, 1010, 1111, 11110\}. 
Problem 8 (19 points)

Let $A$ be a finite set, and let $f: A \rightarrow A$ be a function from $A$ to $A$ with the following property:

$$\forall x \in A, \ f(f(x)) = x$$

Thus $f \circ f$ is the identity permutation of $A$; functions with this property are called involutions.

a. Prove that $f$ is an injection.

b. Using the fact that $f$ is an injection, prove that $f$ is a permutation.
c. Suppose that $|A| = 100$ and that $f$ has no fixed points, meaning that $f(x) \neq x$ for all $x \in A$. How many cycles are there in the cycle-form representation of $f$?

\[
\text{# of cycles in the cycle-form representation of } f =
\]

d. Prove that if $|A|$ is odd and $f$ is an involution of $A$, then $\exists x \in A$ such that $f(x) = x$. Such an element $x$ is called a fixed point of $f$. 
e. Now suppose that $|A| = 10$. How many different involutions $f : A \to A$ without fixed points are there?

\[
\text{# of different involutions } f : A \to A \text{ without fixed points } =
\]
Extra credit Problem 9 (20 points)

A group of \( n \) students, numbered \( 1, 2, \ldots, n \), stand in a circle, in the order of their numbers, and play the following game. Counting starts with student 1, and goes around the circle, eliminating every second student who then leaves the circle. This counting and elimination process continues around the circle until only one student remains. This student is the winner of the game and, as such, gets 20 points of extra credit on the final exam in CSE20. For example, for \( n = 7 \) students, the elimination order is 2, 4, 6, 1, 5, 3, and the winner is student number 7, as shown below:

Suppose that there are \( n = 1280 \) students playing this game, and you are one of them. The students are about to arrange themselves in a circle, thereby determining their numbers. Which number between 1 and 1280 would you pick to become the winner of this game? Show your reasoning!