INSTRUCTIONS

The exam consists of five problems worth a total of 130 points. Of these, 30 points in Problem 5 are extra-credit points. That is, a score of only 100 points is needed to receive the full 30% credit given to the midterm exam. Scores in excess of 100 points will compensate for the final exam and/or homework scores.

Write your answers in the spaces provided. Show all your work, except in the multiple choice problem and 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 (22 points)

a. In the following statements, \( \mathbb{P} \) is the set of primes, \( \mathbb{N} \) is the set of nonnegative integers, and \( \mathbb{R}^+ \) is the set of positive real numbers. Which of these 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>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**No justification is required.** Grading: for each of the four statements above, 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.
b. Let \( x = 2AF_{16} \). Represent \(-x\) in 12-bit binary two’s complement notation. Then, use the octal number system to represent the resulting 12-bit binary string. The result of these operations is:

- \( 6512_8 \)
- \( 6522_8 \)
- \( 6251_8 \)
- \( 6521_8 \)
- None of the above

Check at most one of the five boxes. **No justification is required.** Grading: 8 points if the correct box is the only one checked, 2 points if no box is checked, and 0 points in all other cases.
Problem 2 (33 points)

One of the goals in this problem is to design a logic circuit that multiplies an arbitrary 4-bit binary integer by 6. You may assume that all integers in this problem are positive, so you do not need to worry about signs or (two’s complement) representation of negative integers.

a. Carry out the calculation $11 \times 6$ in the binary number system.

b. Suppose that the number $x$ is represented in the binary number system by a string of 4 bits $a_3, a_2, a_1, a_0$, so that $x = a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0$.

What is the largest possible value of $x$? Let $m$ be the number of bits needed to represent $6x$ in the binary number system. What is $m$?

Largest value of $x$:  

$m =$
c. Let $b_{m-1}, \ldots, b_1, b_0$ be the $m$-bit representation of $6x$, where $x$ is represented by the 4-bit binary string $a_3, a_2, a_1, a_0$ as before. Then $b_3$ is a boolean function of $a_2, a_1, a_0$. Write down the truth table for this function, then express this function in disjunctive normal form.

<table>
<thead>
<tr>
<th>$a_2$</th>
<th>$a_1$</th>
<th>$a_0$</th>
<th>$a_1 \land a_0$</th>
<th>$b_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

$b_3(a_2, a_1, a_0) =$
d. Design a logic circuit that multiplies an arbitrary 4-bit binary integer, represented by the binary string \(a_3, a_2, a_1, a_0\), by 6. The circuit should have four inputs: \(a_3, a_2, a_1, a_0\) and \(m\) outputs \(b_{m-1}, \ldots, b_1, b_0\). The circuit should consist **solely** of full-adders and half-adders. You do not need to show how the full-adders and half-adders are implemented, but you do need to specify all their inputs and outputs (sum, carry) and how they are connected.

**Note:** It is OK to duplicate inputs to the circuit. For example, if you need to use the bit \(a_3\) as input in two different places in the circuit, you are allowed to do that.
Problem 3 (33 points)

Integers $x$ and $y$ are said to be additive inverses of each other if $x + y = 0$. Let $\mathcal{P}(x, y)$ and $\mathcal{Q}(x, y)$ be two predicates with domain $\mathbb{Z}$, the set of all integers, defined as follows:

\[
\mathcal{Q}(x, y) \overset{\text{def}}{=} "x = y"
\]
\[
\mathcal{P}(x, y) \overset{\text{def}}{=} "x \text{ and } y \text{ are additive inverses of each other}"
\]

a. Express the following statements in predicate logic, using the set $\mathbb{Z}$ (and no other sets!) along with the predicates $\mathcal{P}(x, y)$ and $\mathcal{Q}(x, y)$. You can also use the implication $\to$ connective (as many times as you like) in each statement.

$S_1$: Every integer has an additive inverse.
$S_2$: For all integers $x$ and $y$, if both $x$ and $y$ are additive inverses of 5, then $x = y$.
$S_3$: Every integer has at most one additive inverse.

**Hint:** You can regard $S_2$ as the statement that 5 has at most one additive inverse.
b. Let \( S_4 \) be the negation of \( S_3 \), and let \( S_5 \) be the inverse of the converse of \( S_3 \). Express the statements \( S_4 \) and \( S_5 \) in predicate logic, \textit{without} using the implication connective.

Moreover, you should not use negation, unless it is negation of a predicate. For example, it is OK to use something like \( \neg \neg \neg \neg \) \( x \wedge y \vee \neg \neg \neg \neg \) \( x \wedge z \), but not \( \neg (p(x, y) \wedge p(x, z)) \).

\[
S_4: \\
S_5:
\]
c. Express in predicate logic the statement $S$: Every integer has exactly one additive inverse. Use only the predicates $P(x, y)$, $Q(x, y)$, the quantifiers $\forall$, $\exists$ over $\mathbb{Z}$ (but not the quantifier $\forall!$), and the logical connectives $\land$, $\lor$, $\neg$. Be sure to parse the statement clearly with parentheses.

$S$: 

---
Problem 4 (22 points)

a. Compute $\gcd(78, 35)$ using the Euclidean algorithm

\[ \gcd(78, 35) = \]

b. Find integers $a$ and $b$ such that $\gcd(78, 35) = 35a + 78b$.

\[ a = \quad b = \]
c. Find an integer \( x \in \{0, 1, \ldots, 77\} \) such that \( 35x \equiv 1 \pmod{78} \).
Extra-credit Problem 5 (30 points)

What is the largest integer $d$ such that for all primes $p$ and $q$ with $p > q > 3$, the difference $p^2 - q^2$ is divisible by $d$? Prove your answer!

The largest integer $d$ with this property is