CS1800 Discrete Structures Midterm
Version C

Instructions:

1. The exam is closed book and closed notes. You may not use a calculator or any other electronic device.

2. The exam is worth 100 total points. The points for each problem are given in the problem statement and in the table below.

3. You should write your answers in the space provided; use the back sides of these sheets, if necessary.

4. You have two hours to complete the exam.

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1</td>
<td>Binary and Hexadecimal</td>
<td>15</td>
</tr>
<tr>
<td>Section 2</td>
<td>Logic</td>
<td>15</td>
</tr>
<tr>
<td>Section 3</td>
<td>Modular Arithmetic</td>
<td>15</td>
</tr>
<tr>
<td>Section 4</td>
<td>Factors and Co-Prime Numbers</td>
<td>15</td>
</tr>
<tr>
<td>Section 5</td>
<td>Sets</td>
<td>20</td>
</tr>
<tr>
<td>Section 6</td>
<td>Counting</td>
<td>20</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name: ________________________ NU ID#: ________________________

Recitation Time/Loc: ____________ Recitation TA: ________________
Section 1 [15 pts (6,4,5)]: Binary and Hexadecimal

1. Convert 00111100 to (a) decimal (b) hex and (c) octal.

2. In some programming languages, the bitshift operator “≪” takes a number’s binary representation and moves every digit to the left a number of places specified by the number that comes after the operator. So 00111100 ≪ 1 becomes 01111000, and 00111100 ≪ 2 becomes 11110000. Give a formula in terms of $m$ and $n$ (and using decimal numbers) for the value of $m ≪ n$. (Assume there are enough bits so that no 1’s “fall off the edge.”)

3. Assuming two’s complement is being used to represent negative numbers, find the sum of 11111101 and 00000001. Express the result in (a) two’s complement (binary) and (b) decimal.
Section 2 [15 pts (5, 5, 5)]: Logic

1. Draw a circuit that is equivalent to \((a \text{ NOR } b)\) using only NOT and AND gates. (Recall that NOR is NOT OR.)

2. Simplify the formula \((x_1 \lor x_2) \land (\neg x_1 \lor x_2)\) as much as possible. You can use whatever method you like. Put a box around your answer for clarity.

3. A “satisfying assignment” is a tuple that specifies the truth values for the variables in a logical formula that will make the formula true. For example, \((x_1 \land x_2) \lor (\neg x_1 \land \neg x_2)\) has two satisfying assignments, \((T,T)\) and \((F,F)\). How many satisfying assignments are there for the formula \((x_1 \lor x_2 \lor x_3) \land (\neg x_1 \lor \neg x_2 \lor \neg x_3)\)?
Section 3 [15 pts (4,5,6)]: Modular Arithmetic

1. Calculate \((123123124)^{100} \mod 3\). (It might be helpful to recall that a number is divisible by 3 if the sum of its decimal digits is divisible by 3.)

2. Calculate \(3^{23} \mod 7\) using repeated squaring. (You will not get full credit if you do not use this method.)

3. If a linear cipher has the encryption equation \(y = 3x + 7 \mod 17\), find the decryption equation. Use Extended Euclid to find the multiplicative inverse. Your final coefficients should be in the range \([0, 11]\).
Section 4 [15 pts (4,4,3)]: Factors and Co-Prime Numbers

1. Calculate the number of integers between 1 and 39 (inclusive) that are relatively prime to 39.

2. Find the (a) gcd and (b) lcm of $6 \times 10^{12}$ and $9 \times 10^6$.

3. Use Euclid’s algorithm to find the gcd of $n$ and $an + b$, where $a, n \in \mathbb{N}, a, n \geq 1, 1 \leq b < n$, and $b|n$.

4. Suppose a mathematician finds a fast way to compute $\phi(n) = (p - 1)(q - 1)$ for numbers $n$ that are the product of two primes $p$ and $q$. The method doesn’t necessarily reveal what $p$ and $q$ are – for example, running it on 77 gives the answer “60” which isn’t the same thing as saying it factors into 7 and 11. Does this fast computation of $\phi(n)$ make RSA less secure? Explain why or why not.
Section 5 [20 pts (2,3,3,4,5)]: Sets

Assume for the following questions that $A = \{1, 2, 3\}, B = \{x : x \in \mathbb{Z} \text{ and } x = 2n \text{ for some } n \in \mathbb{Z}\}, C = \{x : x \in \mathbb{Z} \text{ and } x = 2n + 1 \text{ for some } n \in \mathbb{Z}\}$

1. What is $(A \cap B)$?

2. What is $B \cup C$? (Be concise.)

3. What is $\overline{B} \cup C$?

4. What is $A - B$?

5. What is $(A \cap C) \times A$?

6. If $\mathcal{P}(A)$ is the power set of $A$, what is $\mathcal{P}(\mathcal{P}(A \cap B))$?
Section 6 [20 pts (4, 3, 3, 5, 5)]: Counting

1. How many possible 6-character license plates are there if the first 3 characters must be capital letters, the last three must be digits, and three three-letter sequences are banned because they sound like bad words?

2. How many 4-digit PINs are possible if no digit can be repeated? (You can leave your answer unsimplified.)

3. How many cards must I draw from a normal deck of cards (4 cards each of 13 values) until I must have three-of-a-kind (3 cards of the same value)?

4. How many 7-digit phone numbers have exactly 3 odd digits? (Assume no restrictions on legal phone numbers aside from this.) You can leave your answer unsimplified.

5. How many numbers between 1 and 100 inclusive are divisible by 2, 5, or 9 (inclusive or)?