CS1800 Discrete Structures Midterm
Version A

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>10</td>
</tr>
<tr>
<td>Section 3</td>
<td>Modular Arithmetic</td>
<td>12</td>
</tr>
<tr>
<td>Section 4</td>
<td>Primes and GCDs</td>
<td>10</td>
</tr>
<tr>
<td>Section 5</td>
<td>Modular Arithmetic Algorithms</td>
<td>8</td>
</tr>
<tr>
<td>Section 6</td>
<td>Sets</td>
<td>20</td>
</tr>
<tr>
<td>Section 7</td>
<td>Counting</td>
<td>8</td>
</tr>
<tr>
<td>Section 8</td>
<td>Permutations and Combinations</td>
<td>17</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 (5,3,2,5)]: Binary and Hexadecimal

1. Write the number 30 (base 10) in (a) 8 digits of binary and (b) 2 digits of hexadecimal.

2. Convert the two’s complement number 11110000 to decimal.

3. How many 1’s are in the binary representation of the eight digit hex number 0xFFFFFFFFE? (You shouldn’t need to convert a large number to binary to answer this.)

4. Assume we are using two’s complement, and add 11110000 and 00001111. Express the result (again interpreted as two’s complement) in decimal.
Section 2 [10 pts (4, 2, 4)]: Logic

1. Write a truth table for the formula \((a \lor b) \land \neg(a \land b)\).

2. Give the name of the logical operator that is equivalent to the formula of the preceding question.

3. Use the truth table to construct an equivalent formula to the one in the first question in disjunctive normal form (clauses containing and’s joined by or’s).
Section 3 [12 pts (5,2,5)]: Modular Arithmetic

1. Use fast exponentiation (repeated squaring) to find $2^{30} \pmod{7}$. Show your work; if you see another method besides fast exponentiation, you may use it only to check your work.

2. Fill in the blank: $a$ has a multiplicative inverse mod $n$ if and only if $a$ and $n$ are

3. Derive a formula for $\phi(n) = |\{x : x \in \mathbb{N}, 1 \leq x \leq n, \gcd(x, n) = 1\}|$ when $n = p^k$ for some prime $p$. 


Section 4 [10 pts (4,2,4)]: Primes and GCDs

1. If the prime factorization of $m$ is $p^2q^5r^{10}$ and the prime factorization of $n$ is $pq^{10}r^2s^5$, where $p$, $q$, $r$, and $s$ are primes, find (a) gcd$(m,n)$ and (b) lcm$(m,n)$.

2. What is the prime factorization of 60?

3. Use Euclid’s algorithm to find the gcd of 143 and 121. Show your work.
Section 5 [8 pts (2, 1, 5)]: Modular Arithmetic Algorithms

1. Find two messages (numbers) whose ciphertext is the same as their plaintext for any RSA key \((e, n)\).

2. If \((e, n)\) is some RSA public key and \(d\) is the matching private key, simplify \(M^{100ed} \mod n\).

3. If an equation describing a linear cipher is \(y = 9x \mod 26\), write an equation for decryption \(x = \ldots\). You must use the Extended Euclidean algorithm and show your work for full credit.
Section 6 [20 pts (2,2,2,3,3,3,3,3)]: Sets

Assume for the following questions that \( A = \{1, 2, 3\}, B = \{3, 4, 5\}, C = \{5, 6, 7\}, \) and the universe \( U = \{x : x \in \mathbb{N}, 0 \leq x \leq 10\}. \)

1. What is \((A \cap B) \cup C\)?

2. What is \(A \cap (B \cup C)\)?

3. What is \(A \cap B \cap C\)?

4. What is \(B - A\)?

5. What is \(\overline{A} \cup B \cup C\)?

6. What is \((A \times B) \cap (B \times A)\)?

7. What is the power set \(\mathcal{P}((B - A) - C)\)?

8. What is \(|\mathcal{P}(A)|\)?
Section 7 [8 pts (4, 4)]: Counting

1. How many 8-bit numbers either start or end with a 1 in binary? (10000000 starts with a 1, but 01000000 does not.)

2. (a) How many students must be in the same room to be certain two of them share a birthday month? (b) What is the name of the specific kind of logical reasoning used here?
Section 8 [17 pts (4, 4, 5, 4)]: Permutations and Combinations

1. How many ways can five people arrange themselves so that one of them is taking a photo, and the other four are in some order from left to right that counts as a different photo for different orderings? (Calculate the number.)

2. How many 8-bit numbers have exactly half their bits set to 1? (Again, calculate the actual number; giving an expression is partial credit. Cancellation of terms will help you.)

3. How many 4-digit PINs composed of digits 0 through 9 have exactly two 9’s? (Again, calculate an exact answer for full credit.)

4. How many ways are there to merge the sorted lists (1, 2, 3, 4) and (A, B, C, D) into a sequence of 8 symbols where all elements of each list are still in the correct order? (For example, AB12C34D is such a sequence, but ABDC1234 is not, only because D and C are out of order.)