CS1800 Discrete Structures Midterm
Version B

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. SHOW YOUR WORK FOR ALL PROBLEMS.

5. 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>9</td>
</tr>
<tr>
<td>Section 2</td>
<td>Logic</td>
<td>16</td>
</tr>
<tr>
<td>Section 3</td>
<td>Proofs</td>
<td>12</td>
</tr>
<tr>
<td>Section 4</td>
<td>Modular Arithmetic &amp; Algorithms</td>
<td>21</td>
</tr>
<tr>
<td>Section 5</td>
<td>Sets and Counting</td>
<td>22</td>
</tr>
<tr>
<td>Section 6</td>
<td>Permutations and Combinations</td>
<td>20</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Name: ___________________________ CS1800 (Lecture) Instructor: ___________
Section 1 [9 pts: 4,3,2]: Binary, Octal, and Hexadecimal

1. Write the number 55 in (a) hexadecimal (b) base 7.
   
   Solution: (a) 37 (b) 106

2. Find the sum of 1110000 and 0001110 in binary and in decimal, assuming an 8-bit two’s complement representation of negative numbers.

   Solution: 11111110 is -2.

3. Convert the hex number AFAF to binary.

   Solution: 1010111110101111
Section 2 [16 pts: 4,3,2,2,3]: Logic

1. Use logic rules to simplify the expression

\[ \neg (p \lor \neg (q \land r)) \lor \neg (p \lor q) \land r \]

Show each step and specify when you are applying the following rules: (1) De Morgan, (2) Distributive, (3) Double negation.

**Solution:**

\[ \neg (p \lor \neg (q \land r)) \lor \neg (p \lor q) \land r \]
\[ \equiv (\neg p \land \neg (q \land r)) \lor (\neg p \land \neg q \land r) \quad \text{De Morgan’s laws} \]
\[ \equiv (\neg p \land q \land r) \lor (\neg p \land \neg q \land r) \]
\[ \equiv ((\neg p \land r) \land q) \lor ((\neg p \land r) \land \neg q) \]
\[ \equiv (\neg p \land r) \land (q \lor \neg q) \quad \text{Double negation} \]
\[ \equiv (\neg p \land r) \land T \]
\[ \equiv \neg p \land r \quad \text{Distributive law} \]

2. (a) Write a logic expression in *Disjunctive Normal Form* with the variables \( p, q, r \) that is true exactly when \( p = r \) and \( q \neq r \).

**Solution:** \((r \land p \land \neg q) \lor (\neg r \land \neg p \land q)\)

(b) Draw a logic circuit with three input lines \( p, q, r \) that outputs 1 exactly when \( p = r \) and \( q \neq r \). Use only NOT, OR, and AND gates (OR and AND gates may have any number of input lines).

**Solution:**

[Diagram of logic circuit]
3. For each logic expression below, list all assignments of truth values to variables $q_1, q_2, q_3, q_4$ that make the expression false. Write these assignments in form of quadruples $(q_1, q_2, q_3, q_4)$. For example $(F, T, F, T)$ has the indicated format.

(a) $q_1 \rightarrow (q_2 \rightarrow (q_3 \rightarrow q_4))$

Solution: An implication $a \rightarrow b$ is false exactly when $a = T$ and $b = F$. Thus the only assignment that makes $q_1 \rightarrow (q_2 \rightarrow (q_3 \rightarrow q_4))$ false is having $q_1 = T$ and $(q_2 \rightarrow (q_3 \rightarrow q_4)) = F$. The latter is the case exactly when $q_2 = T$ and $(q_3 \rightarrow q_4) = F$ which happens exactly when $q_3 = T$ and $q_4 = F$. The only assignment is therefore $(q_1, q_2, q_3, q_4) = (T, T, T, F)$.

(b) $((q_1 \rightarrow q_2) \rightarrow q_3) \rightarrow q_4$

Solution: $((q_1 \rightarrow q_2) \rightarrow q_3) \rightarrow q_4$ is false exactly when $(q_1 \rightarrow q_2) \rightarrow q_3) = T$ and $q_4 = F$.

- If $q_3 = T$ then $(q_1 \rightarrow q_2) \rightarrow q_3) = T$ whatever $q_1$ and $q_2$ are, yielding the four assignments
  
  $(q_1, q_2, q_3, q_4) = (T, T, T, F)$
  $(q_1, q_2, q_3, q_4) = (T, F, T, F)$
  $(q_1, q_2, q_3, q_4) = (F, T, T, F)$
  $(q_1, q_2, q_3, q_4) = (F, F, T, F)$

- If $q_3 = F$, then $(q_1 \rightarrow q_2) \rightarrow q_3) = T$ exactly when $(q_1 \rightarrow q_2) = F$, that is, when $q_1 = T$ and $q_2 = F$, yielding the fifth assignment
  
  $(q_1, q_2, q_3, q_4) = (T, F, F, F)$

4. Assume $x$ and $y$ are integers, and either explain why the following statement is true, or provide a counterexample: “$\forall x \exists y : x^2 = y$”

Solution: True - there’s always some integer result to squaring an integer.
Section 3 [12 pts (6 each)]: Proofs

1. Prove that there must be an integer solution $x, y$ to the formula $ax + by = 2$ if $a$ and $b$ are relatively prime.

   Solution: Bezout’s identity guarantees that there is a solution $x', y'$ to $ax' + by' = 1$ if $a$ and $b$ are relatively prime. Multiplying both sides by 2, we get $2ax' + 2by' = 2$. Then $x = 2x'$ and $y = 2y'$ is a solution.

2. Consider all the unsigned 32-bit numbers with exactly 2 bits that are 1’s. Prove that at least 16 are congruent mod 31.

   Solution: There are $C(32,2) = 31*32/2 = 31*16$ such numbers, and 31 possible values mod 31. So, by the generalized pigeonhole principle, there must be some value mod 31 that at least 16 numbers share.
Section 4 [21 pts: 3,2,3,2,5,5]: Modular Arithmetic and GCD algorithms

1. (a) Use fast exponentiation (repeated squaring) to compute $11^{64} \mod 13$. Your result should be in the range $0 \ldots 12$.

Solution:

\[
11^2 \equiv (-2)^2 = 4 \pmod{13} \\
11^4 \equiv 4^2 = 16 \equiv 3 \pmod{13} \\
11^8 \equiv 3^2 = 9 \pmod{13} \\
11^{16} \equiv 9^2 \equiv (-4)^2 = 16 \equiv 3 \pmod{13} \quad \text{from here on squares repeat} \\
11^{32} \equiv 9 \pmod{13} \\
11^{64} \equiv 3 \pmod{13}
\]

(b) Use your above results to compute $11^{67} \mod 13$.

Solution: $11^{67} = 11^{64+2+1} \equiv 3 \cdot 4 \cdot 11 \equiv 12 \cdot 11 \equiv (-1) \cdot (-2) = 2 \pmod{13}$. Result is 2.

2. If $a = 6^{32} \cdot 7^{12} \cdot 10^{14}$ and $b = 3^{30} \cdot 10^9 \cdot 12^8$, what is the prime-factorization of $\gcd(a,b)$?

Solution:

\[
a = 2^{32} \cdot 3^{32} \cdot 7^{12} \cdot 2^{14} \cdot 5^{14} = 2^{46} \cdot 3^{32} \cdot 5^{14} \cdot 7^{12} \\
b = 3^{30} \cdot 2^9 \cdot 5^9 \cdot 2^{16} \cdot 3^8 = 2^{25} \cdot 3^{38} \cdot 5^9 \\
\gcd(a,b) = 2^{25} \cdot 3^{32} \cdot 5^9
\]

3. Suppose that $a$ and $b$ are integers such that $22a - 51b = 1$.

(a) What is the multiplicative inverse of $b$ mod 22?

Your answer should be in the range $[0, 21]$.

Solution: $(-51)b \equiv 1 \pmod{22}$. The inverse of $b$ is therefore $-51 \equiv 15 \pmod{22}$. Result: 15.

(b) What is the multiplicative inverse of $b$ mod 11?

Your answer should be in the range $[0, 10]$.

Solution: $(-51)b \equiv 1 \pmod{11}$. The inverse of $b$ is therefore $-51 \equiv 4 \pmod{11}$. Result: 4.
4. Use Extended Euclid to find the multiplicative inverse of 9 mod 110. (Your answer should be in the range \([0, 109]\).)

\[
\begin{array}{ccccc}
 a & b & x & y & d \\
110 & 9 & -4 & 49 & 1 \\
 9 & 2 & 1 & -4 & 1 \\
 2 & 1 & 0 & 1 & 1 \\
\end{array}
\]

\textit{Solution:}

5. If the public key used to encrypt a message using RSA was \((27, 55)\), factor \(n\), derive the private key, and decrypt “2.”

\textit{Solution:} \(n = 5 \times 11, \phi(n) = 4 \times 10 = 40\)

d is thus the multiplicative inverse of 27 mod 40:

\[
\begin{array}{ccccc}
 a & b & x & y & d \\
40 & 27 & -2 & 3 & 1 \\
27 & 13 & 1 & -2 & 1 \\
13 & 1 & 0 & 1 & 1 \\
\end{array}
\]

The multiplicative inverse \(d\) is 3, so we just need to compute \(2^3 \mod 40 = 8\).
Section 5 [22 pts: 2,2,2,3,3,3,3,4]: Sets and Counting

1. Consider sets $A = \{1, 5, 7, 11\}$ and $B = \{5, 11, 13, 17\}$. Use the listing method to describe the following sets (that is, list their elements between braces).

(a) $A \cup B$

Solution: \{1, 5, 7, 11, 13, 17\}

(b) $A \cap B$

Solution: \{5, 11\}

(c) $A - B$

Solution: \{1, 7\}

(d) $(A \cap B) \times (A - B)$

Solution: \{5, 11\} \times \{1, 7\} = \{(5, 1), (5, 7), (11, 1), (11, 7)\}

(e) $\{x \in A \mid 2x + 1 \in A\}$

Solution: \{5\}

2. If $X = \{x \mid x \in \mathbb{Z}, -1 \leq x \leq 1\}$, what is the cardinality of the power set of $X$?

Solution: $2^3 = 8$

3. Every student enrolled at Northeastern has two initials, such as AA in Alice Atwood or AB in Alice Brentwood. How many students have to be enrolled for us to be sure that at least three have the same initials (in the same order)? You may give your answer as a formula (without evaluation).

Solution: There are $h = 26^2$ possible two-letter initials. We can view these as pigeon holes. The maximum number of pigeons we can have with at most two per hole is $2h$. Thus the minimum number of pigeons to ensure that three are in the same hole is $2h + 1 = 2 \cdot 26^2 + 1$.

4. In a class of 28 students every student has learned at least one of the programming languages Macron, Python, and Zonnon. In fact, 13 know Macron, 20 know Python, 14 know Zonnon, 7 know Macron and Python, 5 know Macron and Zonnon, 5 know Macron and Zonnon, and 11 know Python and Zonnon. How many of the students know all three programming languages?

Solution:

\[28 = |M \cup P \cup Z| = |M| + |P| + |Z| - |M \cap P| - |M \cap Z| - |P \cap Z| + |M \cap P \cap Z|\]
\[= 13 + 20 + 14 - 7 - 5 - 11 + |M \cap P \cap Z|\]
\[= 24 + |M \cap P \cap Z|\]

Therefore $|M \cap P \cap Z| = 28 - 24 = 4$.  

Section 6 [20 pts 4,3,4,4,5]: Permutations and Combinations

Please complete your computations to arrive at a single integer answer for each problem.

1. How many 3-digit positive integers (that is, integers in the range $100 \ldots 999$) have neither a digit 8 nor a digit 9?

   Solution: Suppose we write all these integers systematically: there are 7 choices for the first digit (as also 0 is excluded), 8 choices for the second and 8 choices for the third. Thus there are $7 \cdot 8 \cdot 8 = 448$ possible integers.

2. You own 3 songs by Lady Gaga and 4 songs by Katy Perry that you wish to arrange in a playlist of 7 songs (with no repetition).

   (a) How many playlists are possible?

   Solution: $7! = 5040$

   (b) How many playlists are possible in which all Lady Gaga songs are together?

   Solution: The four Perry songs determine 5 slots in which the Gaga songs can be placed:

   $P \quad P \quad P \quad P \quad P$

   Sort 4 Perry songs  |  Sort 3 Gaga songs  |  Select one slot for Gaga songs
   $4! = 24$          |  $3! = 6$          |  5

   There are $24 \cdot 6 \cdot 5 = 720$ playlists with all Gaga songs together.

   (c) How many playlists are possible that have no two consecutive songs by Lady Gaga?

   Solution: For this question, each slot may contain at most one Gaga song. Suppose that the Gaga songs are Gaga1, Gaga2, Gaga3. The tasks are now:

   Sort 4 Perry songs  |  Place Gaga1  |  Place Gaga2  |  Place Gaga3
   $4! = 24$          |  5            |  4            |  3

   There are $24 \cdot 5 \cdot 4 \cdot 3 = 1440$ playlists with no two Gaga songs consecutive.

3. How many different strings can you form with the letters in “LADYGAGA”

   Solution: There are 8 letters consisting of 3 As, 2 Gs, and one each of L, D, Y.

<table>
<thead>
<tr>
<th>Positions for 3 As</th>
<th>Positions for 2 Gs</th>
<th>Place L, D, Y in remaining 3 positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^3P_3 = 56$</td>
<td>$^2P_2 = 10$</td>
<td>$3! = 6$</td>
</tr>
</tbody>
</table>

   There are $56 \cdot 10 \cdot 6 = 3360$ possible strings.