CS1800 Discrete Structures Practice MidTerm

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 200 total points. The points for each problem are given in the problem statement and in the table below.
3. Please look through the entire exam and verify that you have all pages numbered 1 through 14.
4. You should write your answers in the space provided; use the back sides of these sheets, if necessary.
5. You have two hours to complete the exam.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Title</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem 1</td>
<td>Colors</td>
<td>20</td>
</tr>
<tr>
<td>Problem 2</td>
<td>Two’s Complement</td>
<td>20</td>
</tr>
<tr>
<td>Problem 3</td>
<td>Circuits</td>
<td>25</td>
</tr>
<tr>
<td>Problem 4</td>
<td>Modular arithmetic and GCD</td>
<td>20</td>
</tr>
<tr>
<td>Problem 5</td>
<td>Cryptography</td>
<td>25</td>
</tr>
<tr>
<td>Problem 6</td>
<td>Sets and Set Operations</td>
<td>24</td>
</tr>
<tr>
<td>Problem 7</td>
<td>Sum Product Rules</td>
<td>24</td>
</tr>
<tr>
<td>Problem 8</td>
<td>Inclusion-Exclusion Principle</td>
<td>22</td>
</tr>
<tr>
<td>Problem 9</td>
<td>Pigeonhole Principle</td>
<td>20</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name: ____________________ NU ID#: ____________________
**Problem 1** [20 pts], (6,6,3,2,3): Colors

Colors are usually represented using the 24-bit *RGB Truecolor* scheme, which gives the red, green, and blue components (RGB) in the color. The most significant 8 bits give the red value, the middle 8 bits give the green value, and the least significant 8 bits give the blue value.

The 24-bit color representation can be written in several formats: (a) 24-bit binary format; (b) 6-digit hexadecimal format; (c) the decimal triplet format which gives the decimal values for the red, blue, and green components.

For instance, if the red, green, and blue values of a color are 200, 18, and 5, respectively, then the decimal triplet, hexadecimal, and binary formats are, respectively:

\[(200 \ 18 \ 5) \quad \text{C81205} \quad \text{110010000001001000000101}\]

To see how the hexadecimal format is obtained, note that the decimal numbers 200, 18, and 5, are C8, 12, and 05, respectively in hexadecimal.

1. Convert the hexadecimal format FFEFD5 of the color FireBrick to decimal triplet format.

2. Convert the decimal triplet format (102 205 170) of the color MediumAquamarine to hexadecimal format.
iii. Arrange the three colors BurlyWood (DEB887), RosyBrown (D2B48C), and Tan (BC8F8F) in increasing order of their green values.

iv. How many different green values can be given in the RGB Truecolor scheme?

v. Roughly how many different colors can be represented using the 24-bit format? Use the approximation $2^{10} \approx 1,000$ and express your answer as an integral number of millions, billions, trillions, or whatever is necessary; for example, an answer of the form “28 million” would be acceptable (though incorrect, in this case). Explain your answer, e.g., Why millions? Why 28?
Problem 2 [20 pts], (5,5,10): Negative Numbers and Two’s Complement

i. Give the 8-bit two’s complement representations of the following integers: 77, −88. Show your work.

ii. Give the integer (in standard base-10 notation) which is represented by each of the following 8-bit two’s complement numbers: 00010111, 10110101. Show your work.
iii. Compute the following using 8-bit two’s complement representations, as shown in class and described in the text: $-88 - 88$, $77 - 88$, $77 + 77$. In each case, indicate whether the calculation results in an overflow. Show your work.

*Note:* Use the two’s complement representations from part i above.
Problem 3 [25 pts, (5 each)]: Truth Tables, Boolean Formulae, and Circuits

i. Fill in the following table with the missing truth tables, Boolean formulae, and circuits.

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Boolean Formula</th>
<th>Truth Table</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>Out</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>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</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>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Diagram:

```
  OR
   /\   /
  AND  AND
     |   |
    A  B  C
```
ii. Using the laws of logic covered in class, show that the following two Boolean formulae are logically equivalent.

\[(A \lor \neg B) \land (\neg A \lor B)\]

\[(A \land B) \lor (\neg A \land \neg B)\]

Show your work, and indicate the particular law you are using in each step. For your convenience, we list some laws that are sufficient for showing the above equivalence. You may use any of these laws or others covered in class.

Distributivity: (a) \(X \land (Y \lor Z) = (X \land Y) \lor (X \land Z)\); (b) \(X \lor (Y \land Z) = (X \lor Y) \land (X \lor Z)\).

Commutativity: (a) \(X \land Y = Y \land X\); (b) \(X \lor Y = Y \lor X\).

Complement: (a) \(X \land \neg X = F\); (b) \(X \lor \neg X = T\).

Identity: (a) \(X \land T = X\); (b) \(X \lor F = X\).
Problem 4 [20 pts, (2,2,3,3,5,5)]: Modular arithmetic and gcd

Evaluate the following.

i. $39 \mod 17$.

ii. $17 \mod 39$.

iii. $-13 \mod 17$.

iv. $(39 \cdot 3 - 13) \mod 17$. Show your work.

v. $39^{13} \mod 17$. Show your work.

vi. $\gcd(525, 315)$, using Euclid’s algorithm. Show your work.
Problem 5 [25 pts, (11,[7,7])]. Cryptography

i. What is the decryption function for the following linear cipher? Show your work.

\[ m \rightarrow 7m + 5 \mod 15 \]

ii. Consider an RSA system with the public key given by \( n = 55 \), and \( e = 3 \).

What is the encryption of the message 9? Show your work.

What is the private key \( d \) of this RSA system? Show your work.
Problem 6 [24 pts, (4 each)]: Sets and Set Operations

(a) List the elements in the set described in each part. Recall that $\mathbb{Z}$ is the set of all integers (nonnegative integers and negative integers).

i. $R = \{n \mid n \in \mathbb{Z}, 4 \leq n^2 + 3 \leq 8\}$

ii. $S = \{n \mid n \in \mathbb{Z}, 4 \leq n/2 < 6\}$

Let $A = \{a, b, c, d\}$ and $B = \{1, 2\}$.

(b) Show each of the sets indicated.

i. $A \times B =$

ii. The power set $2^B$ (also denoted $\mathcal{P}(B)$) =

(c) Give each of the cardinalities below as a single integer. You do not have to show the sets; just give their size.

i. $|A \times A| =$

ii. $|\mathcal{P}(\mathcal{P}(B)) \times \mathcal{P}(A)| =$
Problem 7 [24 pts, (10,6,8)]: Sum Product Rules

(a) How many different PINs (Personal Identification Numbers) consisting of numeric characters are there of length at least 6 and at most 12, and with at least two different digits?

(b) A class has 100 students. How many ways are there to pick 6 students, one after another, to answer a question at the board?

(c) A class has 50 boys and 50 girls. How many ways are there to pick 6 students, one after another, to answer a question on the board, if boys and girls must alternate?
Problem 8 [22 pts, (5,5,5,7)]: Inclusion Exclusion Principle

Three headache drugs - A, B, and C - were tested on 50 subjects. The results of tests were as follows:

- 27 reported relief from drug A;
- 22 reported relief from drug B;
- 35 reported relief from drug C;
- 13 reported relief from both drugs A and B;
- 21 reported relief from both drugs A and C;
- 16 reported relief from both drugs B and C;
- 44 reported relief from at least one of the drugs.

Answer the following questions. (It may help to draw a Venn diagram to capture the above data.)

1. How many people got relief from none of the drugs?
2. How many people got relief from all 3 drugs?

3. How many people got relief from B only?

4. How many different pairs of people are there that got relief from B, but not from A?
Problem 9 [20 pts, (12,8)]: Pigeonhole Principle
(a) Prove that there exist (at least) two distinct powers of 3 whose difference is a multiple of 2014.

(b) What is the minimum number of cards you need to draw from a deck to be assured of getting two cards from the same suit? (A deck has 52 cards split equally among 4 suits) Explain how you used the Pigeonhole Principle to arrive at your answer.