CSC3001 Discrete Mathematics

Midterm Examination

November 4, 2023: 9:30am - 12:00pm

Name: _____ Student ID: _____

Answer ALL questions in the Answer Book.

Question	Points	Score
1	24	
2	16	
3	16	
4	16	
5	12	
6	16	
Total:	100	

1. (24 points) Let $D = \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$.
   (a) (8 points) Show that for any $x, y \in D$, $x + y \in D$.
   (b) (8 points) Show that there is a unique element $O \in D$, such that for all $x \in D$, $x = O + x$.
   (c) (8 points) Let O be the element specified from part (b). Show that for every $x \in D$, there is a unique element $y \in D$ such that $x + y = O$.

Solution:

(a) If $x, y \in D$ then there exist $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ such that $x = x_1 + \sqrt{2}x_2$ and $y = y_1 + \sqrt{2}y_2$. Then $x + y = (x_1 + y_1) + \sqrt{2}(x_2 + y_2)$. Because $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ we have $x_1 + y_1, x_2 + y_2 \in \mathbb{Z}$. Therefore $x + y \in D$.

(b) Existence: Because $0 = 0 + \sqrt{2}0 \in D$ and $x = 0 + x$ for all $x \in D$, such an element O exists.

Uniqueness: If O exists, let x be an arbitrary element in D, we must have $O = x - x = 0$. This concludes the uniqueness.

(c) Existence: If $x \in D$, x could be written into $a + \sqrt{2}b$. Because $a, b \in \mathbb{Z}$, we have $-a, -b \in \mathbb{Z}$. Therefore $-x = -a - \sqrt{2}b \in D$. As $x + (-x) = 0 = O$, we take $y = -x$ and conclude the existence.

Uniqueness: If $x + y = O = 0$, then $y = -x$. The uniqueness follows.

2. (16 points) Let X, X', Y, Y' be sets. Let $\times$ denote the Cartesian product of sets. Show that

$$X \times Y - X' \times Y' = ((X \cap X') \times (Y - Y')) \cup ((X - X') \times Y)\,.$$

Solution:

$$\begin{aligned}
(x, y) \in LHS \iff & x \in X \wedge y \in Y \wedge \neg(x \in X' \wedge y \in Y') \\
\iff & x \in X \wedge y \in Y \wedge (x \notin X' \vee y \notin Y') \\
\iff & x \in X \wedge y \in Y \wedge (x \notin X' \vee (y \notin Y' \wedge x \in X')) \\
\iff & (x \in X \wedge y \in Y \wedge x \notin X') \vee (x \in X \wedge y \in Y \wedge y \notin Y' \wedge x \in X') \\
\iff & (x \in (X - X') \wedge y \in Y) \vee (x \in X \wedge x \in X' \wedge y \in (Y - Y')) \\
\iff & (x, y) \in RHS\,.
\end{aligned}$$

3. (16 points) Let $n \geq 1$ be an integer. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be real numbers. Show that

$$(a_1 b_1 + \cdots + a_n b_n)^2 \leq (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2)\,.$$

Solution: We prove the inequality by induction. The base cases are $n = 1$ which holds trivially as $a_1^2 \le a_1^2$, and $n = 2$, which holds because $(a_1b_1 + a_2b_2)^2 - (a_1^2 + a_2^2)(b_1^2 + b_2^2) = -(a_1b_2 - a_2b_1)^2 \le 0$. Assume that the inequality is true for $n = k$. Then for $n = k + 1$, we have

$$\begin{aligned}
a_1b_1 + \cdots + a_{k+1}b_{k+1} &= (a_1b_1 + \cdots + a_kb_k) + a_{k+1}b_{k+1} \\
&\le \sqrt{a_1^2 + \cdots + a_k^2}\sqrt{b_1^2 + \cdots + b_k^2} + a_{k+1}b_{k+1} \\
&\le ((\sqrt{a_1^2 + \cdots + a_k^2})^2 + a_{k+1}^2)^{1/2}((\sqrt{b_1^2 + \cdots + b_k^2})^2 + b_{k+1}^2)^{1/2} \\
&= (a_1^2 + \cdots + a_{k+1}^2)^{1/2}(b_1^2 + \cdots + b_{k+1}^2)^{1/2}.
\end{aligned}$$

Squaring both sides concludes the inequality for $n = k + 1$. By induction the inequality holds for all $n \ge 1$.

4. (16 points) Let $n \ge 3$ be a positive integer. Suppose that n prisoners are told that they will be brought to a room and seated. Hats will be placed on their heads, and each hat will be in one of the n colors (the set of possible colors is known). It is possible that some hats are of the same color. Each prisoner could see all other prisoners' hats but not their own hat. The prisoners must simultaneously submit a guess of their own hat color. They all go free if at least one prisoner guesses correctly. While no communication is allowed once the hats are placed, they will be allowed to have a strategy session before being brought to the room.

   The prisoners will execute this strategy. Number the prisoners as $0, 1, \ldots, n-1$, and the colors as $0, 1, \ldots, n-1$. When they sit down, prisoner i will calculate s_i as the sum of all $n - 1$ hat colors prisoner i could observe. Then every prisoner submits a guess, where prisoner i submits color $(i - s_i) \bmod n$. Show that these prisoners will go free.

Solution: Let h_i be the hat color of prisoner i and s be the sum of the colors of all n hats. Then prisoner i submits $(i - s_i) \bmod n = (i + h_i - s) \bmod n$. Prisoner i is correct if and only if $i + h_i - s \equiv h_i \pmod n$, which is equivalent to $s \equiv i \pmod n$. Because $s \in \{0, \ldots, n-1\} \pmod n$, one prisoner must be correct, and consequently the prisoners will go free.

5. (12 points) Let $k \ge 3$ be an integer. Alice starts with k integers, $x_1, \ldots, x_k$, where their sum is positive. These numbers are put in a circle. In every step, Alice could arbitrarily pick a negative number, x_i, among $x_1, \ldots, x_k$. Then x_i and the two neighboring numbers, namely x_{i-1}, x_i, x_{i+1}, are replaced by $x_{i-1} + x_i$, $-x_i$, $x_{i+1} + x_i$ in their respective positions (here we denote $x_0 = x_k$ and $x_{k+1} = x_1$ for simplicity because the numbers are in a circle). If at any step there is no negative number, Alice wins the game. Can Alice win this game in finitely many steps?

Solution: For simplicity write $x_j = x_{j \bmod k}$. Let $s = \sum_{j=1}^{k} \sum_{n=0}^{k-1} |x_j + \cdots + x_{j+n}|$. When Alice picks any $x_i < 0$ in one step, s is decreased by $|-x_i + \sum_{j=1}^{k} x_j| - |x_i + \sum_{j=1}^{k} x_j| > 0$ because all other terms cancel out. As s is a non-negative integer and must stay as a non-negative integer through the process, such decrease could only happen for finitely many steps. This concludes that the process must stop in finitely many steps, which means Alice wins with any strategy.

6. (16 points) Let $n \geq 3$ be an integer and write $n - 1 = d2^s$, where d is an odd integer and $s \geq 0$ is an integer. For $a \in \{2, 3, \ldots, n-2\}$, let statement $p(a)$ be "$a^d \equiv 1 \pmod{n}$ or there exists an integer $r \in \{0, 1, \ldots, s-1\}$ such that $a^{d2^r} \equiv -1 \pmod{n}$".
   (a) (8 points) Show that if there is an integer $a \in \{2, 3, \ldots, n-2\}$ such that $p(a)$ is false, then n is composite.
   (b) (8 points) Show that if n is composite then $p(a)$ is false for at least 75% of the numbers in $a \in \{2, 3, \ldots, n-2\}$.

Solution:

(a) If n is prime then by Fermat's little theorem $a^{d2^s} \equiv 1 \pmod{n}$. For prime n only $+1$ and -1 could square to 1 $\pmod{n}$. Therefore either $a^{d2^s}, a^{d2^{s-1}}, \ldots, a^d$ are all 1 $\pmod{n}$, or some of them is -1 $\pmod{n}$. Therefore for any a, $p(a)$ must be true when n is prime.

(b) See Theorem 1.1 of this notes for Miller Rabin primality test.