CSC3001 Discrete Mathematics

Midterm Examination

March 11, 2023: 9:00am - 11:30am

Name: ____________________ Student ID: ____________________

Answer ALL questions in the Answer Book.

Question	Points	Score
1	20	
2	20	
3	16	
4	16	
5	12	
6	16	
Total:	100	

1. (20 points) Let sets $A = \{\{3, 4\}, \{3, 4, \{3, 4\}\}\}$, $B = \{3, 4\}$. Find $|A|$, $A \cap B$, A^2, and find the power set of B.

Solution: $|A| = 2$; $A \cap B = \emptyset$; $A^2 = \{(\{3, 4\}, \{3, 4\}), (\{3, 4\}, \{3, 4, \{3, 4\}\}), (\{3, 4, \{3, 4\}\}, \{3, 4\}), (\{3, 4, \{3, 4\}\}, \{3, 4, \{3, 4\}\})\}$; $\text{pow}(B) = \{\emptyset, \{3\}, \{4\}, \{3, 4\}\}$.

2. (20 points) Let n be a positive integer.
   (a) (10 points) Prove that $\gcd(n, n + 1) = 1$.
   (b) (10 points) Prove that for any integer z, there exist integers s, t such that $sn + tn + t = z$.

Solution:

Part (a) Because 1 divides any integer 1 is a common divisor. Any common divisor of n and $n+1$ must divide their difference, which is 1. This indicates that 1 is the only positive common divisor. As such, $\gcd(n, n + 1) = 1$.

Part (b) Because $\gcd(n, n + 1) = 1$, we have $\text{spc}(n, n + 1) = 1$. Therefore there are integers s', t' such that $s'n + t'(n + 1) = 1$. Let $s = s'z$, $t = t'z$, we have $sn + tn + t = z$ as desired.

3. (16 points) Alice desires to prove that "For all $n \in \mathbb{Z}^+, 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.". Alice wrote the following proof:

We use induction to prove the statement. For the base case $n = 1$, both sides of the equation are 1. For the induction step, assume that the equation holds for k, then when $n = k + 1$,

$$1 + 2 + \cdots + (k + 1) = \frac{(k + 1)(k + 2)}{2} .$$

Then,

$$(1 + 2 + \cdots + k) + (k + 1) = \frac{k(k + 1)}{2} + \frac{2(k + 1)}{2} .$$

By the induction assumption, we obtain

$$(k + 1) = \frac{2(k + 1)}{2} ,$$

which is true. Therefore the statement holds for $n = k + 1$.

Point out a mistake in Alice's proof. Give a correct proof of the statement.

Solution: At the beginning of the induction step, Alice concludes the desired statement that when $n = k+1$, $1+2+\cdots+(k+1) = \frac{(k+1)(k+2)}{2}$ without justification. Therefore the proof is invalid. We now provide a correct proof.

We use induction to prove the statement. For the base case $n = 1$, both sides of the equation are 1. For the induction step, assume that the equation holds for k, then we have,

$$1+2+\cdots+k = \frac{k(k+1)}{2}\,.$$

Then, for $n = k+1$,

$$\begin{aligned}(1+2+\cdots+k)+(k+1) &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2}\,.\end{aligned}$$

Therefore the statement holds for $n = k+1$, and by induction the statement holds for all $n \in \mathbb{Z}^+$.

4. (16 points) Let $n \in \mathbb{Z}^+$ and $k \in \mathbb{Z}_4$. Let $f(n,k)$ be the number of solutions of the equation

$$a_1 + a_2 + \cdots + a_n \equiv k \pmod 4,$$

with $a_1, \ldots, a_n \in \{1,2,3\}$. For example,

$f(1,2) = 1,$ because the only solution is 2;

$f(2,3) = 2,$ because the only 2 solutions are $1+2, 2+1$;

$f(2,0) = 3,$ because the only 3 solutions are $1+3, 2+2, 3+1$.

(a) (8 points) Find a recursion for $f(n,k)$ and point out the initial conditions.

(b) (8 points) Find a closed-form expression for $f(n,k)$.

Solution:

Part (a) For any $a_1, \ldots, a_n$ and $k \in \mathbb{Z}_4$, there is a unique $a \in \mathbb{Z}_4$ such that $a_1 + \cdots + a_n + a \equiv k \pmod 4$. Because a_{n+1} must be nonzero in $\mathbb{Z}_4$, when $a_1 + \cdots + a_n \equiv k \pmod 4$ it is not possible to find such an a_{n+1}. Therefore,

$$f(n+1,k) = \sum_{j \neq k} f(n,j) \quad \forall k\,.$$

The initial condition is

$$f(1,k) = 1 \quad \forall k \in \{1,2,3\}\,; \quad f(1,0) = 0\,.$$

Part (b) We conjecture that

$$f(n,0) = \frac{3^n + 3(-1)^n}{4}\,,$$

$$f(n,1) = f(n,2) = f(n,3) = \frac{3^n - (-1)^n}{4}\,.$$

We now prove this conjecture by induction. The base case regards the initial condition. Because there is only one number a_1, there is only one solution when $k \in \{1,2,3\}$, and none otherwise. Now assume that the closed-form expression holds for n, and then for $n+1$, we have

$$\begin{aligned} f(n+1,0) &= f(n,1) + f(n,2) + f(n,3) \\ &= 3 \cdot \frac{3^n - (-1)^n}{4} \\ &= \frac{3^{n+1} + 3(-1)^{n+1}}{4}\,, \end{aligned}$$

and for $k \in \{1,2,3\}$,

$$\begin{aligned} f(n+1,k) &= f(n,0) + 2f(n,1) \\ &= \frac{3^n + 3(-1)^n}{4} + 2 \cdot \frac{3^n - (-1)^n}{4} \\ &= \frac{3^{n+1} - (-1)^{n+1}}{4}\,. \end{aligned}$$

By induction, our conjecture is indeed the closed-form expression of $f(n,k)$.

5. (12 points) A sequence a_n satisfies $a_1 = 0$, $a_2 = 1$, and for $n \in \mathbb{Z}^+$, $a_{n+2} = \frac{1}{2}a_{n+1} + \frac{1}{2}a_n + 1$. Find a closed-form solution of a_n.

Solution: Let $a_0 = 0$. Let $F(x)$ be the generating function of the sequence $\{a_n\}_{n\geq 0}$. We have the following one-to-one correspondences between sequences and their respective generating functions:

$$\begin{array}{lccccccl} (& a_0, & a_1, & a_2, & a_3, & \dots &) \leftrightarrow & F(x)\,, \\ (& 0, & \frac{1}{2}a_0, & \frac{1}{2}a_1, & \frac{1}{2}a_2, & \dots &) \leftrightarrow & \frac{1}{2}xF(x)\,, \\ (& 0, & 0, & \frac{1}{2}a_0, & \frac{1}{2}a_1, & \dots &) \leftrightarrow & \frac{1}{2}x^2F(x)\,, \\ (& 0, & 0, & 1, & 1, & \dots &) \leftrightarrow & x^2/(1-x)\,. \end{array}$$

Therefore, $F(x) = \frac{1}{2}xF(x) + \frac{1}{2}x^2F(x) + \frac{x^2}{1-x}$, which indicates that

$$\begin{aligned} F(x) = \frac{2x^2}{(1-x)(2-x-x^2)} &= \frac{2}{3}\cdot\frac{x^2}{(1-x)^2} + \frac{2}{9}\cdot\frac{x^2}{(1-x)} + \frac{2}{9}\cdot\frac{x^2}{2+x} \\ &= \frac{2}{3}x^2(1 + 2x + 3x^2 + 4x^3 + \dots) \\ &\quad + \frac{2}{9}x^2(1 + x + x^2 + x^3 + \dots) \\ &\quad + \frac{1}{9}x^2(1 - \frac{1}{2}x + \frac{1}{4}x^2 - \frac{1}{8}x^3 + \dots)\,. \end{aligned}$$

Therefore, the coefficient of x^n in $F(x)$ is

$$a_n = -\frac{4}{9} + \frac{2}{3}n + \frac{4}{9}(-\frac{1}{2})^n .$$

6. (16 points) Let p be a prime. A residue m modulo p is a square if there is a residue x such that $x^2 \equiv m \pmod{p}$.
   (a) (6 points) Prove that $x^2 \equiv y^2 \pmod{p}$ if and only if $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$.
   (b) (6 points) Prove that there are exactly 51 residues that are squares (mod 101).
   (c) (4 points) Prove that if a and b are not squares $\pmod{p}$ then ab is a square $\pmod{p}$.

Solution:

Part (a) $(x-y)(x+y) \equiv 0 \pmod{p}$. If a product of two numbers is divisible by prime p, then at least one of $(x-y) \equiv 0 \pmod{p}$ and $(x+y) \equiv 0 \pmod{p}$ must hold.

Part (b) We take all 100 non-zero residues. By the previous part only pairs $x, -x$ give the same residue when squared. Hence we get $100/2 = 50$ different residues. We also have $0^2 = 0$, which results in 51 different residues.

Part (c) Multiplication by a non-zero residue c maps $1, \ldots, p-1$ to a permutation of $1, \ldots, p-1$. Clearly multiplying a square by a square is still a square $\pmod{p}$. Hence if c is a square, multiplication by c maps all $(p-1)/2$ squares to $(p-1)/2$ squares $\pmod{p}$. It follows that it maps $(p-1)/2$ non-squares to $(p-1)/2$ non-squares $\pmod{p}$. Hence if c is a square and d is not, then cd is not a square.

Now fix a non-square d. Multiplication by d maps $(p-1)/2$ squares to $(p-1)/2$ non-squares. It follows that it must map all $(p-1)/2$ non-squares to squares.