CSC3001 Discrete Mathematics

Mid-term Examination

November 6, 2021: 9:00am - 11:30am

Name: ____________________ Student ID: ____________________

Answer ALL questions in the Answer Book.

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

1. (16 points) Let $P(x, y)$ be a predicate with variables $x, y \in \mathbb{Z}$. Let $A = \forall x \exists y : P(x, y)$ and $B = \exists y \forall x : P(x, y)$

   (a) (8 points) Let $P(x, y)$ be $x = y$. Show that $A \to B$ is false.

   (b) (8 points) Show that B implies A.

Solution:

Part (a) A is true as for every x $P(x, y)$ is true when y is x. B is false as for every x, $P(x, y)$ is false when $y = x + 1$. Therefore $A \to B$ is false.

Part (b) When B is true, we specify a y_0 such that $P(x, y_0)$ is true for an arbitrary x. This indicates that for every x we can specify $y = y_0$ such that $P(x, y)$ is true, as desired.

2. (16 points) Let n be a positive integer.

   (a) (8 points) Show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1).$$

   (b) (8 points) Find $1^2 + 3^2 + \cdots + (2n-1)^2$.

Solution:

Part (a) We prove the claim by induction. When $n = 1$, the equation holds as both sides of the equation are 1. If the equation holds when $n = k$, then when $n = k + 1$,

$$\begin{aligned} 1^2 + 2^2 + \cdots + (k+1)^2 &= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\ &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\ &= \frac{1}{6}(k+1)(k+2)(2k+3). \end{aligned}$$

By induction the equation holds for every positive integer.

Part (b)

$$\begin{aligned} 1^2 + 3^2 + \cdots + (2n-1)^2 &= (1^2 + 2^2 + \cdots + (2n)^2) - (2^2 + 4^2 + \cdots + (2n)^2) \\ &= (1^2 + 2^2 + \cdots + (2n)^2) - 4(1^2 + 2^2 + \cdots + (n)^2) \\ &= \frac{1}{6}(2n)(2n+1)(4n+1) - \frac{4}{6}n(n+1)(2n+1). \end{aligned}$$

3. (16 points) An eccentric collector of $2 \times n$ domino tilings pays 4 dollars for each vertical domino and 1 dollar for each horizontal domino. For example, the following are two examples of different $2 \times n$ tilings that are worth 6 dollars.

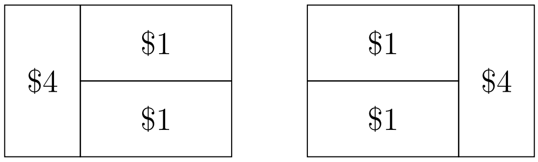

Figure 1: Examples of \$6 tilings.

Let $r_0 = 1$. For $m, n = 1, 2, \ldots$, let $r_{m,n}$ be the number of different tilings of size $2 \times n$ that are worth exactly m dollars. Define $r_m = \sum_{n=1}^{\infty} r_{m,n}$.

(a) (6 points) Find $r_1, r_2, r_3, r_4, r_5, r_6$.

(b) (10 points) Find the closed form expression for r_m.

Solution:

Part (a) $r_1 = r_3 = r_5 = 0, r_2 = 1, r_4 = 2, r_6 = 3$.

Part (b) Observe that we cannot construct a $2 \times n$ domino tiling by using an odd number of horizontal dominos. This implies that we cannot form a $2 \times n$ domino tiling that is worth an odd amount of dollars. Thus, if m is odd, $r_m = 0$.

If $m \geq 4$ is even, we have $r_m = r_{m-2} + r_{m-4}$. This is because in this case, we can form valid domino tilings of m dollars by attaching a vertical domino at the beginning of valid domino tilings of $m - 4$ dollars or by attaching a stack of two horizontal dominos at the beginning of valid domino tilings of $m - 2$ dollars. Moreover, for even m, the above recurrent relation shows that $r_0, r_2, r_4, \ldots$ form the Fibonacci sequence.

In summary, we have

$$r_m = \begin{cases} \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}, & \text{if } m = 2k, \\ 0, & \text{if } m = 2k+1, \end{cases}$$

where $k \geq 0$.

4. (16 points) The least common multiple of two positive integers m and n, denoted by $\operatorname{lcm}(m, n)$, is the smallest positive integer that is divisible by both m and n.

(a) (6 points) Find $\operatorname{lcm}(36, 60)$.

(b) (10 points) Prove or disprove: For all $a, b, c \in \mathbb{Z}^+$,

$$\operatorname{lcm}(a, \gcd(b, c)) \mid \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c)).$$

Solution:

Part (a) $\operatorname{lcm}(36, 60) = 180$.

Part (b) Observe that $a \mid \text{lcm}(a, b)$ and $a \mid \text{lcm}(a, c)$. So a is a common divisor of $\text{lcm}(a, b)$ and $\text{lcm}(a, c)$. It follows that

$$a \mid \gcd(\text{lcm}(a, b), \text{lcm}(a, c)).$$

Now consider $\gcd(b, c)$. Since $\gcd(b, c) \mid b$, we have $\gcd(b, c) \mid \text{lcm}(a, b)$. Similarly, we also have $\gcd(b, c) \mid \text{lcm}(a, c)$. So $\gcd(b, c)$ is a common divisor of $\text{lcm}(a, b)$ and $\text{lcm}(a, c)$. It follows that

$$\gcd(b, c) \mid \gcd(\text{lcm}(a, b), \text{lcm}(a, c)).$$

Therefore, both a and $\gcd(b, c)$ divide $\gcd(\text{lcm}(a, b), \text{lcm}(a, c))$. By definition of the least common multiple, we conclude that

$$\text{lcm}(a, \gcd(b, c)) \mid \gcd(\text{lcm}(a, b), \text{lcm}(a, c)).$$

5. (16 points) Let $S_{p,k} = \sum_{n=1}^{p-1} n^k$ where p is prime and k is a positive multiple of $p-1$.
   (a) (6 points) Show that $2 \mid S_{2,k} + 1$.
   (b) (10 points) Prove that
   $$S_{p,k} \equiv -1 \pmod{p}.$$
   (*Hint: Fermat's little theorem might be helpful.*)

Solution:

Part (a) Since $S_{2,k} = 1$ we have $2 \mid S_{2,k} + 1$.

Part (b) By Fermat's little theorem, we have $n^{p-1} \equiv 1 \pmod{p}$ for $n = 1, \ldots, p-1$. Moreover, since $p - 1 \mid k$ we have $n^{(p-1)\frac{k}{p-1}} \equiv 1 \pmod{p}$ for $n = 1, \ldots, p-1$. Therefore,

$$\begin{aligned} S_{p,k} &\equiv \sum_{n=1}^{p-1} n^k \pmod{p} \\ &\equiv \sum_{n=1}^{p-1} 1 \pmod{p} \\ &\equiv p - 1 \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$

6. (20 points) For $x \in \mathbb{R}$, define the set $A(x) = \{px + q \mid p, q \in \mathbb{Q}\}$.

(a) (8 points) Let $x \in \mathbb{R} - \mathbb{Q}$ and $s \in A(x)$. Show that there exists a unique pair $p, q \in \mathbb{Q}$ of rational numbers such that $s = px + q$.

(b) (8 points) Let $s, t \in \mathbb{R} - \mathbb{Q}$. Show that $A(s) = A(t)$ if and only if $s \in A(t)$.

(c) (4 points) Let $B \subseteq \mathbb{R}$. Assume that for every $s \in \mathbb{R} - \mathbb{Q}$ there exists a unique element $x \in B$ such that $s \in A(x)$. Show that there exist at least two different functions $f : \mathbb{R} \to \mathbb{Q}$ such that $f(s+t) = f(s) + f(t)$ for $s \in \mathbb{R}, t \in \mathbb{Q}$.

Solution:

Part (a) By the definition of $A(x)$ such a pair exists. If $s = p_1 x + q_1$ and $s = p_2 x + q_2$ hold then $(p_1 - p_2)x = q_2 - q_1 \in \mathbb{Q}$. As $x \notin \mathbb{Q}$, $p_1 - p_2$ must be 0, which indicates that $q_2 - q_1 = 0$. This guarantees the uniqueness.

Part (b) If $s \in A(t)$ then $s = p_0 t + q_0$ for some $p_0 \neq 0, q_0$. For every $u \in A(s)$, $u = p_1 s + q_1 = (p_0 p_1)t + (p_1 q_0 + q_1) \in A(t)$ by specifying p_1, q_1. For every $v \in A(t)$, $v = p_2 t + q_2 = (p_2/p_0)s + (q_2 - p_2 q_0/p_0) \in A(s)$, by specifying p_2, q_2. Thus, $A(s) = A(t)$; If $A(s) = A(t)$, then $s = 1 \cdot s + 0 \in A(s) = A(t)$; Therefore, $A(s) = A(t)$ if and only if $s \in A(t)$.

Part (c) $f(s) = 0$ satisfies the property, as $0 = 0 + 0$. It amounts to finding a non-zero function g that satisfies the property.

When $s \notin \mathbb{Q}$, by the assumption, s can be mapped to the unique element $x \in B$ such that $s \in A(x)$. By (b), we have $x \notin \mathbb{Q}$. Then by (a) we write s into the unique representation $s = px + q$ for $p, q \in \mathbb{Q}$, $x \in B$. Then we define $g(s) = q$ for an irrational s. When $s \in \mathbb{Q}$, define $g(s) = s$. As the mapping is unique, this definition of g is a function from $\mathbb{R}$ to $\mathbb{Q}$. g is non-zero as $g(1) = 1$.

It is up to verify that $g(s+t) = g(s) + g(t)$ for $s \in \mathbb{R}, t \in \mathbb{Q}$. This is immediate when $s, t \in \mathbb{Q}$ as $(s+t) = s+t$. When s is irrational, we have that for some $x \notin \mathbb{Q}$, $s+t, s \in A(x)$. Writing $s+t, s$ into their unique representations $s+t = p_1 x + q_1$, $s = p_2 x + q_2$, we have $t = (p_1 - p_2)x + q_1 - q_2$. As $x \notin \mathbb{Q}$, we have $p_1 - p_2 = 0$ and subsequently $t = q_1 - q_2$. Therefore, $g(s+t) - g(s) = q_1 - q_2 = t = g(t)$.

Remark:

When we write s into the unique representation $s = px + q$ for $p, q \in \mathbb{Q}$, $x \in B$, we can instead define $g(s) = p$ for an irrational s. For $s \in \mathbb{Q}$ it is defined as $g(s) = 0$.

An alternative solution is to define $f(s)$ to be q when s is irrational for some arbitrary $q \in \mathbb{Q}$, and 0 when s is rational. This family of infinitely many functions f satisfies the property as desired.

This problem is known as Cauchy's functional equation.