Discrete Mathematics HW3

20180617 You SeungWoo

September 25, 2023

Problem 1

(a) *Solution.* Let total excution be $T(n)$. Then $T(n) = \sum_{i=1}^{n}\sum_{j=1}^{i}\sum_{k=1}^{j} 1 = \sum_{i=1}^{n}\sum_{j=1}^{i} j = \sum_{i=1}^{n} \frac{i(i+1)}{2}$. Note that $\frac{i^2}{2} \leq \frac{i(i+1)}{2} = \frac{i^2+i}{2} \leq= \frac{i^2+i^2}{2} = i^2$ for $^\forall i \in \mathbb{N}$. This follows $\sum_{i=1}^{n} \frac{i^2}{2} \leq \sum_{i=1}^{n} \frac{i(i+1)}{2} = T(n) \leq \sum_{i=1}^{n} i^2$. Since $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, $T(n) = \Theta(n^3)$.

□

(b) *Solution.* Let total excution be $T(n)$. Then $T(n) = n + \lfloor \frac{n}{3} \rfloor + \lfloor \frac{\lfloor \frac{n}{3} \rfloor}{3} \rfloor + \cdots + 1$.

i) If $n = 3^k$ for $k = 0, 1, \cdots$, then $T(n) = 3^k + 3^{k-1} + \cdots + 3 + 1 = \sum_{i=0}^{k} 3^i = \frac{3^{k+1}-1}{2} = \frac{3 \cdot 3^k - 1}{2} = \frac{3n-1}{2}$. Therefore, $T(n) = \Theta(n)$.

ii) If $n = 3^k + C$ with $0 < C < 2 \cdot 3^k$ for $k = 1, 2, \cdots$, then $\sum_{i=0}^{k} 3^i \leq T(n) \leq \sum_{i=0}^{k+1} 3^i$ from i). So we get $\frac{3n-1}{2} \leq T(n) \leq \frac{9n-1}{2}$, $T(n) = \Theta(n)$.

For any $n \in \mathbb{Z}^+$, we get $T(n) = \Theta(n)$.

□

(c) *Solution.* Let total excution be $T(n)$ and I_j be the value of i at jth iteration. Then by the *Archimedean Property*, $^\exists k$ such that $I_k < n \leq I_{k+1}$. It means $T(n) = k$. Note that the recursive relation $I_{k+1} = I_k^2$. By solving this, we get $I_{k+1} = I_1^{2^k} = 2^{2^k}$. So $2^{2^{k-1}} < n \leq 2^{2^k}$. From left inequality, $k < \lg(\lg n) + 1$. From right inequality, $\lg(\lg n) \leq k$. Since $T(n) = k$, $T(n) = \Theta(\lg(\lg n))$.

□

Problem 2

Solution. Make any increasing functions $f(n)$ and $g(n)$ such that $f(n) > g(n)$ and $g(n) \geq f(n)$ for infinitely many intervals. For example, define

$$f(n) = 2n, \quad g(n) = \begin{cases} n + 4k, & \text{if } n \in (4k, 4k+2] \\ n + 4k + 4, & \text{if } n \in (4k+2, 4k+4] \end{cases}$$

for $k = 0, 1, \cdots$. Then $f(n) > g(n)$ for $n \in (4k, 4k+2]$, $g(n) \geq f(n)$ for $n \in (4k+2, 4k+4]$. This gives the desired result.

$\square$

Problem 3

Proof. Use the definition of Riemann integral for $f(t) = \frac{1}{t}$ between $[1, x]$. Let $P = \{t_0, t_1, \cdots, t_n\}$ be a uniform partition between $t_0 = 1$ and $t_n = x$. Let $\Delta t_i = t_i - t_{i-1} = \frac{x-1}{n}$ for $i = 1, 2, \cdots, n$. By the definition of *Riemann integral*, $\sum\limits_{i=1}^{n} m_i \Delta t_i \leq \int_1^x \frac{1}{t}\, dt \leq \sum\limits_{i=1}^{n} M_i \Delta t_i$ where $m_i = \inf\limits_{t \in [t_{i-1}, t_i]} f(t)$, $M_i = \sup\limits_{t \in [t_{i-1}, t_i]} f(t)$. Since $f(t)$ is continuous and strictly decreasing function, $m_i = \frac{1}{t_i}$ and $M_i = \frac{1}{t_{i-1}}$.
Take $x = n + 1$. Then $t_i = i + 1, \Delta t_i = 1$. It follows:

$$\sum_{i=1}^{n} \frac{1}{i+1} \leq \int_1^{n+1} \frac{1}{t}\, dt = \ln(n+1) \leq \sum_{i=1}^{n} \frac{1}{i}$$

$$\Rightarrow \ln(n+1) \leq \sum_{i=1}^{n} \frac{1}{i} = \sum_{i=1}^{n} \frac{1}{i+1} + 1 - \frac{1}{n+1} \leq \ln(n+1) + 1 + 0$$

$$\Rightarrow \sum_{i=1}^{n} \frac{1}{i} = \Theta(\lg n)$$

□

Problem 4

(a) *Proof.* Using the definition of *limit* and O *notation.*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$$
$$\Rightarrow \text{for given } \epsilon > 0, ^{\exists} N \in \mathbb{Z}^+ \text{ such that } n \geq N \implies \left| \frac{f(n)}{g(n)} - 0 \right| \leq \epsilon$$
$$\Rightarrow ^{\exists} N \in \mathbb{Z}^+ \text{ such that } n \geq N \implies |f(n)| \leq \epsilon \, |g(n)| \text{ for some(exactly, any) } \epsilon > 0$$
$$\Rightarrow f(n) = O(g(n))$$

$\square$

(b) *Proof.* Using the definition of *limit* and Θ *notation.*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = c \neq 0$$
$$\Rightarrow \text{for given } \epsilon > 0, ^{\exists} N \in \mathbb{Z}^+ \text{ such that } n \geq N \implies \left| \frac{f(n)}{g(n)} - c \right| \leq \epsilon$$
$$\Rightarrow ^{\exists} N \in \mathbb{Z}^+ \text{ such that } n \geq N \implies (c - \epsilon) \, |g(n)| \leq |f(n)| \leq (c + \epsilon) \, |g(n)| \text{ for any } \epsilon > 0$$
$$\Rightarrow f(n) = \Theta(g(n))$$

Note that we can find $\epsilon > 0$ where $c - \epsilon > 0$ because of the *Archimedean Property.*

$\square$

Problem 5

(a) *Proof.* Proof by induction. Let $P(j)$ be the given statement. Consider $j = 1$. Then $\sum_{k=1}^{1} f_k^2 = f_1^2 = 1^2 = f_1 f_2$ is clearly true.
Suppose $P(j)$ is true for $j = n$. Consider $j = n + 1$. Note that the recursive relation of *Fibonacci Sequence*: $f_n = f_{n-1} + f_{n-2}$.

$$\begin{aligned}\sum_{k=1}^{n+1} f_k^2 &= \sum_{k=1}^{n} f_k^2 + f_{n+1}^2 \\ &= f_n f_{n+1} + f_{n+1}^2 \\ &= f_{n+1}(f_n + f_{n+1}) \\ &= f_{n+1} f_{n+2}\end{aligned}$$

Therefore, $P(j)$ is true for $^{\forall} j \in \mathbb{N}$.

$\square$

(b) *Proof.* Proof by induction. Note that the following:

$$\begin{aligned} f_n &= \frac{f_{n-1} + \sqrt{5f_{n-1}^2 + 4(-1)^{n+1}}}{2} \\ \Leftrightarrow & \ (2f_n - f_{n-1})^2 = 5f_{n-1}^2 + 4(-1)^{n+1} \\ \Leftrightarrow & \ 4f_n^2 - 4f_n f_{n-1} + f_{n-1}^2 = 5f_{n-1}^2 + 4(-1)^{n+1} \\ \Leftrightarrow & \ 4f_n^2 - 4f_n f_{n-1} = 4f_{n-1}^2 + 4(-1)^{n+1} \\ \Leftrightarrow & \ f_n^2 - f_n f_{n-1} = f_{n-1}^2 + (-1)^{n+1} \\ \Leftrightarrow & \ f_n^2 = f_n f_{n-1} + f_{n-1}^2 + (-1)^{n+1} \\ \Leftrightarrow & \ f_n^2 = f_{n-1}(f_n + f_{n-1}) + (-1)^{n+1} \\ \Leftrightarrow & \ f_n^2 = f_{n-1} f_{n+1} + (-1)^{n+1}\end{aligned}$$

Using this, let the last equation be $P(j = n)$. Consider $j = 2$. Then $f_2^2 = 1^2 = 0 = 1 \cdot 2 + (-1)^3 = f_{2-1} f_{2+1} + (-1)^{2+1}$ is true.
Suppose $P(j = n)$ is true. Consider $j = n + 1$.

$$\begin{aligned} f_{n+1}^2 &= f_{n+1}(f_n + f_{n-1}) \\ &= f_{n+1} f_n + f_{n+1} f_{n-1} \\ &= f_{n+1} f_n + \left(f_n^2 - (-1)^{n+1}\right) \\ &= f_n(f_{n+1} + f_n) + (-1)^{n+2} \\ &= f_n f_{n+2} + (-1)^{n+2}\end{aligned}$$

Therefore, $P(j)$ is true for $j \geq 2$.

$\square$

(c) *Proof.* Proof by strong induction. Let $P(j)$ be the given statement. Consider $j = 6$. Then $f_6 = 8 > \left(\frac{3}{2}\right)^{6-1} \simeq 7.59$ is clearly true.

Suppose $P(j)$ is true for $j = 1, 2, \cdots, n$. Consider $j = n + 1$.

$$\begin{aligned}
f_{n+1} &= f_n + f_{n-1} \\
&> \left(\frac{3}{2}\right)^{n-1} + \left(\frac{3}{2}\right)^{n-2} \\
&= \left(\frac{3}{2}\right)^{n-2} \left(\frac{3}{2} + 1\right) = \frac{5}{2} \left(\frac{3}{2}\right)^{n-2} \\
&= \frac{10}{4} \left(\frac{3}{2}\right)^{n-2} > \frac{9}{4} \left(\frac{3}{2}\right)^{n-2} \\
&= \left(\frac{3}{2}\right)^{2} \left(\frac{3}{2}\right)^{n-2} = \left(\frac{3}{2}\right)^{n}
\end{aligned}$$

Therefore, $P(j)$ is true for $j \geq 6$.

$\square$

(d) *Proof.* First, claim that $\gcd(a, b) = \gcd(a + b, b)$. Let $\gcd(a, b) = d$. Then $a = pd$, $b = qd$, $\gcd(p, q) = 1$ for some $p, q \in \mathbb{N}$. This gives $a + b = (p + q)d$. If $\gcd(p + q, q) = 1$, then $\gcd(a + b, b) = d$. Assume, if not, $\gcd(p + q, q) = c \neq 1$. Then $p + q = kc$, $q = tc$, $\gcd(k, t) = 1$ for some $k, t \in \mathbb{N}$. This gives $p = (k - t)c$, so $\gcd(p, q) \geq c$. But it contradicts to $\gcd(p, q) = 1$. Therefore, $\gcd(a + b, b) = d$. Now, $\gcd(a, b) = d \implies \gcd(a + b, b)$ is proved. We can proof the reveresed direction($\gcd(a + b, b) = d \implies \gcd(a, b)$) similarly. Therefore, the claim is true.

Proof by induction. Let $P(j)$ be the given statement. Consider $j = 1$. Then $\gcd(f_1, f_2) = 1$ is clearly true.

Suppose $P(j = n)$ is true. Consider $j = n + 1$. Then by the claim, $\gcd(f_{n+1}, f_{n+2}) = \gcd(f_{n+1}, f_n + f_{n+1}) = \gcd(f_n, f_{n+1}) = 1$. Therefore, $P(j)$ is true for ${}^{\forall} j \in \mathbb{N}$.

$\square$

Problem 6

Proof. ($\Rightarrow$) Using negation. Suppose $\gcd(m,n) = c \neq 1$. Note that $\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = \frac{mn}{c}$. Let $x_1 = 0$, $x_2 = \frac{\text{lcm}(m,n)}{n} = \frac{m}{c}$. Since $1 \leq \text{lcm}(m,n) < mn$, $1 < \frac{\text{lcm}(m,n)}{n} = x_2 < m$. So $x_1 \neq x_2$. But $f(x_1) = 0$, $f(x_2) = n\frac{m}{c} \mod m = 0$. Therefore, $f(x_1) = f(x_2)$, f is not one-to-one.
($\Leftarrow$) First, if $m = 1$, then it is trivial. So consider $m > 1$. Using negation. Suppose f is not one-to-one. This implies ${}^\exists x_1, x_2$ such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$. WOLG, $x_1 > x_2$. Note that $x_1, x_2 \in X$. i.e. $0 \leq x_2 < x_1 \leq m - 1$.

$$
\begin{aligned}
f(x_1) = nx_1 \mod m, \quad f(x_2) = nx_2 \mod m \\
&\Rightarrow n(x_1 - x_2) \equiv 0 \mod m \\
&\Rightarrow m \mid n \text{ or } m \mid (x_1 - x_2) \text{ but } m \nmid (x_1 - x_2) \\
&\Rightarrow m \mid n \\
&\Rightarrow gcd(m,n) = m > 1
\end{aligned}
$$

□

Problem 7

Solution. Since 5, 6, 7 are relatively prime, by the *CRT*, $^{\exists!}x \in \mathbb{Z}_{5\times6\times7}$. Find $9(3\times3)$ values:

- a_i: dividend value
- M_i: product of divisors except the self divisor m_i. $M_i = \frac{m_1 m_2 \cdots m_n}{m_i}$
- y_i: multiplicative inverse of $M_i \mod m_i$

$a_1 = 3$, $a_2 = 4$, $a_3 = 5$, $M_1 = \frac{5\cdot6\cdot7}{5} = 42$, $M_2 = \frac{5\cdot6\cdot7}{6} = 35$, $M_3 = \frac{5\cdot6\cdot7}{7} = 30$. Find any y_i which satisfies $M_i y_i \equiv 1 \mod m_i$. $y_1 = 3$, $y_2 = 5$, $y_3 = 4$.

Therefore, $x \equiv \sum_{i=1}^{3} a_i M_i y_i = 1678 \equiv 208 \mod 210$.

$\square$

Problem 8

Proof. Let $x \in \mathbb{Z}_n$. i.e. we prove $x = 1$ or $x = n - 1$. If $n = 2$, then it is true by brute-force calculate. Consider $n > 2$. Note that the *Euclid's lemma*: if prime $p \mid ab$, then $p \mid a$ or $p \mid b$.

$$\begin{aligned} & x^2 \equiv 1 \mod n \\ \Rightarrow\ & x^2 - 1 \equiv 0 \mod n \\ \Rightarrow\ & (x-1)(x+1) \equiv 0 \mod n \\ \Rightarrow\ & n \mid (x-1) \text{ or } n \mid (x+1) \end{aligned}$$

But n can divide only one of them, not both. If n can divide both, then $\gcd(x-1, x+1) = n > 2$. However, $\gcd(x-1, x+1) \leq 2$. To prove this, let $\gcd(x-1, x+1) = d$. Then $d \mid (x-1)$ and $d \mid (x+1)$, so $x - 1 \equiv 0 \mod d$ and $x + 1 \equiv 0 \mod d$. This follows $(x-1) + (x+1) = 2x \equiv 0 \mod d$ and $(x+1) - (x-1) = 2 \equiv 0 \mod d$. Therefore, $\gcd(2x, 2) = d \leq 2$.
By the above statement, we have only 2 cases:

i) Suppose $n \mid (x-1)$.

$$\begin{aligned} & n \mid (x-1) \\ \Rightarrow\ & x - 1 \equiv 0 \mod n \\ \Rightarrow\ & x \equiv 1 \mod n \end{aligned}$$

Since $x \in \mathbb{Z}_n$, $x = 1$.

ii) Suppose $n \mid (x+1)$.

$$\begin{aligned} & n \mid (x+1) \\ \Rightarrow\ & x + 1 \equiv 0 \mod n \\ \Rightarrow\ & x \equiv -1 \mod n \end{aligned}$$

Since $x \in \mathbb{Z}_n$, $x = n - 1$.

□