Homework 2

1.

(1)

對於任意 $f \in S_1$，因為 f 遞增，構造函數

$$\mathcal{F}_1 : S_1 \to \mathbb{N} \times \mathbb{N}$$

其中：

$$\mathcal{F}_1(f) = (a, b), \text{where } f(x) = \begin{cases} 0 & \text{if } a \geq x \geq 0 \\ 1 & \text{if } b \geq x > a \\ 2 & \text{if } x > b \end{cases}$$

若對於某個 S_1 中的函數，這樣的數對存在相異兩組 $(a_1, b_1), (a_2, b_2)$，不失一般性令 $a_1 < a_2$，則會發現在 (a_1, a_2) 區間內將與 f 是函數定義矛盾，因此不可能存在。故可知 $\mathcal{F}_1$ 為 1-1，且：

$$\mathcal{F}_1(S_1) \subseteq \mathbb{N} \times \mathbb{N}$$

反之，若給定一組 $(a, b) = \mathbb{N} \times \mathbb{N}$ 的數對，定義：

$$\mathcal{F}_2 : \mathbb{N} \times \mathbb{N} \to S_1$$

其中：

$$[\mathcal{F}_2(a, b)](x) = \begin{cases} 0 & \text{if } a \geq x \geq 0 \\ 1 & \text{if } b \geq x > a \\ 2 & \text{if } x > b \end{cases}$$

因為一組 (a, b) 可唯一決定一個 $\mathcal{F}_2(a, b)$，故 $\mathcal{F}_2$ 為 1-1。因此：

$$\mathcal{F}_2(\mathbb{N} \times \mathbb{N}) \subseteq S_1$$

由以上兩點，可知：

$$|\mathbb{N} \times \mathbb{N}| = |S_1|$$

因此 S_1 是無限集合。又，仿照課堂時證明有理數為可數集合的方法：

0	**1**	**2**	**3**	**...**

0	1	3	6	10	15
1	2	5	9	14	
2	4	8	13		
3	7	12			
4	11				
.					

可證明 $\mathbb{N} \times \mathbb{N}$ 為可數集合。故 S_1 為可數集合。

(2)

給定任意一個 $\mathbb{N}$ 的子集合，不失一般性令該集合為：

$$B = \{b_1, b_2 \dots b_k\} \in 2^{\mathbb{N}}$$

且對於任意 $i, j \in \{1 \dots k\}$：

$$\forall i < j . b_i < b_j$$

定義函數 $\mathcal{F}$，其中：

$$\mathcal{F} : 2^{\mathbb{N}} \to S_2$$

且：

$$\mathcal{F}(B) = \begin{cases} 0 & \text{if } b_1 \geq x \geq 0 \\ 1 & \text{if } b_2 \geq x > b_1 \\ 2 & \text{if } b_3 \geq x > b_2 \\ \vdots & \\ i & \text{if } b_{i+1} \geq x > b_i \\ \vdots & \\ k-1 & \text{if } b_k \geq x > b_{k-1} \\ k & \text{if } x > b_k \end{cases}$$

且任意相異的 B ，都可構造出相異的 $\mathcal{F}(B)$，即 $\mathcal{F}$ 是 1 - 1。故可知 S_1 為無限集合，且：

$$\mathcal{F}(2^{\mathbb{N}}) \subseteq S_2$$

但 $2^{\mathbb{N}}$ 為不可數的集合，故 S_1亦不可數。

2.

1.

反證：假定 $n^2 - n \in O(n)$ 。則存在正數 C, n_0，使得：

$$\forall n > n_0.\ n^2 - n < Cn$$

但：

$$n^2 - n < Cn \Rightarrow n^2 < (C+1)n$$

當 $n > \max\{C+1, n_0\} := n'$ 時：

$$n \cdot n > (C+1)n \Rightarrow n^2 - n > Cn$$

與假定矛盾。故 $n^2 - n \notin O(n)$。

2.

考慮以下函數：

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ n^2 & \text{otherwise} \end{cases}$$

以及：

$$g(n) = 1$$

則顯然 $f(n) \notin \omega(g(n))$，因 $\lim_{n\to\infty} \frac{g(n)}{f(n)}$ 並不存在，且 $f(n) \in \Omega(g(n))$，因 $n > 0$ 時 $f(n) \geq 1 \cdot 1$。

但 $f(n) \notin O(g(n))$。假定存在 c, n_0 ，使 $n > n_0$ 時：

$$f(n) < c$$

則選取任何大於 $\max\{c, n_0\}$ 的偶數，立刻得到矛盾：

$$f(n) = \max\{c, n_0\} \cdot \max\{c, n_0\} \geq c$$

故：$f(n) \notin O(g(n))$，即 $f(n) \notin \Theta(g(n))$。

3.

已知 $g(n) \in \omega(h(n))$，故：

$$\lim_{n\to\infty} \frac{g(n)}{h(n)} \to \infty$$

另外一方面，$f(n) \in O(h(n))$，故：

$$\exists c_2, n_2. \forall n > n_2. \frac{f(n)}{h(n)} \leq c_2$$

而當 $n > n_2$ 時：

$$\frac{g(n)}{h(n)} \geq \frac{g(n) - f(n)}{h(n)} = \frac{g(n)}{h(n)} - \frac{f(n)}{h(n)} \geq \frac{g(n)}{h(n)} - c_2$$

因此當 $n \to \infty$，由夾擠定理：

$$\lim_{n \to \infty} \frac{g(n) - f(n)}{h(n)} = \infty$$

即：

$$g(n) - f(n) \in \omega(h(n))$$

4.

反例：考慮

$$f_i(n) = i \cdot n$$

則對於任意 $f_i(n)$：

$$\forall n > 0. \left(\frac{1}{2} i\right) n < f_i(n) = in < (2 \cdot i)\, n$$

故：

$$f_i(n) \in \Theta(n)$$

但：

$$g(n) = \sum_{i=1}^{n} f_i(n) = \sum_{i=1}^{n} in = \frac{n^2(n+1)}{2} = \frac{n^3 + n^2}{2}$$

反證：假定：

$$g(n) = \frac{n^3 + n^2}{2} \in \Theta(n^2)$$

並且 c_1, c_2, n_0 任意該定義保證的常數：

$$n > n_0 \Rightarrow c_1 n^2 \leq \frac{n^3 + n^2}{2} \leq c_2 n^2$$

則當：

$$\frac{n+1}{2} > c_2 \Rightarrow n > 2c_2 - 1$$

時，有：

$$\frac{n^3 + n^2}{2} = \frac{n+1}{2} \cdot n^2 > c_2 n^2$$

矛盾。

3.

1.

由費馬小定理知：

$$\begin{aligned} 23^{7-1} &\equiv 1 (\mathrm{mod}\ 7) \\ 23^{5-1} &\equiv 1 (\mathrm{mod}\ 5) \end{aligned}$$

故：

$$23^{12} \equiv 1 (\mathrm{mod}\ 7)$$

及：

$$23^{12} \equiv 1 (\mathrm{mod}\ 5)$$

假定：

$$\begin{aligned} 23^{12} &= 7n_1 + 1 \\ &= 5n_2 + 1 \end{aligned}$$

故可知：

$$7n_1 = 5n_2 \Rightarrow 5 | 7n_1$$

但因 $5 \nmid 7$，故：

$$5 \mid n_1$$

令 $n_1 = 5n'$，則：

$$23^{12} = 35n' + 1 \Rightarrow 23^{12} \equiv 1 (\mathrm{mod}\ 35)$$

故：

$$\begin{aligned} 23^{4800017} &\equiv (23^{12})^{2400001} \cdot 23^5 (\mathrm{mod}\ 35) \\ &\equiv 23^5 (\mathrm{mod}\ 35) \end{aligned}$$

手動計算 $23^5 \bmod 35$：

$$23 \cdot (23^2)^2 \bmod 35 = 23 \cdot 4^2 \bmod 5 = 368 \bmod 35 = 18$$

2.

令：

$$m = 5 \cdot 7 \cdot 11$$

以及：

$$\begin{cases} M_5 = m/5 = 77 \\ M_7 = m/7 = 55 \\ M_{11} = m/11 = 35 \end{cases}$$

解：

$$\begin{cases} 77y_5 = 1 \bmod 5 \\ 55y_7 = 1 \bmod 7 \\ 35y_{11} = 1 \bmod 11 \end{cases}$$

其中 y_5：

$$\begin{cases} 77 &= 5 \cdot 15 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{cases} \Rightarrow \begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - (77 - 5 \cdot 15) \cdot 2 \\ &= 31 \cdot 5 - 2 \cdot 77 \end{aligned}$$

故：

$$y_5 = (-2) + 5 = 3$$

y_7 直接從 $7 \cdot 8 = 56$ 觀察出來：

$$55 \cdot (-1) + 7 \cdot (8) = 1 \Rightarrow y_7 = -1 + 7 = 6$$

而 y_{11}：

$$\begin{cases} 35 &= 11 \cdot 3 + 2 \\ 11 &= 2 \cdot 5 + 1 \end{cases} \Rightarrow \begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - (35 - 11 \cdot 3) \cdot 5 \\ &= 16 \cdot 11 - 5 \cdot 35 \end{aligned}$$

因此：

$$y_3 = -5 + 11 = 6$$

令：

$$\begin{aligned} x' &= 2 \cdot y_5 M_5 + 6 \cdot y_7 M_7 + 3 \cdot y_{11} M_{11} \\ &= 2 \cdot 3 \cdot 77 + 6 \cdot 6 \cdot 55 + 6 \cdot 3 \cdot 35 \\ &= 3072 \end{aligned}$$

故：

$$x = x' \bmod (5 \cdot 7 \cdot 11) = 377$$

> Reference : 這大題我有使用 python3 進行模數驗算，但並沒有使用程式進行直接爆破或解題。

4.

仿照費馬小定理的證明。

因爲 p 是質數，故對於任意 $0 < k < p - 1$：

$$p - k \nmid p$$

因此：

$$\gcd(p-k,p)=1$$

又對於 1，顯然有 $\gcd(1,p)=1$，可將 $\gcd(p-k,p)=1$ 延伸至 $0<k<p$。定義：

$$p_k=p-k\quad\forall 0<k<p$$

則可知：

$$\forall p_k.\,\exists!\bar{p_k}.0<\bar{p_k}<p \text{ and } p_k\bar{p_k}\equiv 1 \bmod p$$

Claim：

$$\{1,2,\dots p-1\}=\{\bar{p_1}\dots\bar{p_k}\}$$

由於已知 $\forall\bar{p_k}.0<\bar{p_k}<p$，僅證 $\forall i\neq j.\,\bar{p_i}\neq\bar{p_j}$ 即可。利用反證法：假定 $i\neq j$，且存在：

$$\bar{p_i}=\bar{p_j}=:q$$

使得：

$$q(p-i)=q(p-j)\Rightarrow q(i-j)=0$$

則 $q=0$ ，或 $i=j$。前者將導致 $p_i\bar{p_i}\equiv 0(\bmod p)$，與一開始對 q 的假設矛盾; 後者與證明一開始假定 $i\neq j$ 矛盾。故得證 $\{1,2,\dots p-1\}=\{\bar{p_1}\dots\bar{p_k}\}$ 。因此：

$$\begin{aligned}\prod_{i=1}^{p-1}p_k\bar{p_k}&\equiv 1 &\pmod p\\&\equiv[(p-1)!]^2 &\pmod p\end{aligned}$$

由此得證。

5.

$$n^n,n!,2^{3n},2^n,3n^3+1,\sqrt{n}+3,2^{\log_4 n},n^{0.01},(\log_2 n)!,\log_2 n,\ln n$$

其中：

$$\sqrt{n}+3=\Theta(\sqrt{n}+3),\log_2 n=\Theta(\ln n)$$

Reference

Ceiba 上的課程筆記