



潘承洞 《数论基础》

作者：韦明

时间：April 6, 2025

E-mail: wm31415926535@outlook.com

目录

第 1 章 作业	1
1.1 第三周作业	2

第 1 章 作业

1.1 第三周作业

第二章

8 试证：当 $\omega(n) > 1$ 时， $\sum_{d|n} \mu(d) \log d = 0$ ；一般若 $m \geq 1$ 且 $\omega(n) > m$ ，则

$$\sum_{d|n} \mu(d) \log^m d = 0.$$

证明 由于若 d 存在平方因子，则 $\mu(d) = 0$ ，不妨设

$$n = p_1 p_2 \cdots p_k$$

其中 $p_i, p_j (i \neq j)$ 为互异素因子。

(a). 当 $\omega(n) > 1$ 时， $\sum_{d|n} \mu(d) \log d = 0$ 。

$$k = \omega(n) > 1 \implies k > 1$$

$$\begin{aligned} \sum_{d|n} \mu(d) \log d &= \sum_{S \subseteq \{p_1, p_2, \dots, p_k\}} \mu\left(\prod_{p \in S} p\right) \log\left(\prod_{p \in S} p\right) \\ &= \sum_{S \subseteq \{p_1, p_2, \dots, p_k\}} (-1)^{|S|} \sum_{p \in S} \log p \end{aligned}$$

交换求和次序，有：

$$\sum_{d|n} \mu(d) \log d = \sum_{p|n} \log p \sum_{\substack{d|n \\ p|d}} \mu(d)$$

固定 p ，则

$$\begin{aligned} \sum_{\substack{d|n \\ p|d}} \mu(d) &= (-1) \left[(-1)^0 \binom{k-1}{0} + (-1)^1 \binom{k-1}{1} + \cdots + (-1)^{k-1} \binom{k-1}{k-1} \right] \\ &= (-1)(-1+1)^{k-1} \\ &= 0 \end{aligned}$$

因此，

$$\sum_{d|n} \mu(d) \log d = 0$$

(b). 若 $m \geq 1$ ，且 $\omega(n) > m$ ，则 $\sum_{d|n} \mu(d) \log^m d = 0$ 。

$$k = \omega(n) > m \geq 1 \implies k > 1$$

$$\sum_{d|n} \mu(d) \log^m d = \sum_{d|n} \mu(d) \sum_{\substack{p_1|d, \dots, p_m|d \\ p_i|n}} \log p_1 \cdots \log p_m$$

交换求和次序，有：

$$\sum_{d|n} \mu(d) \log^m d = \sum_{p_1|n} \cdots \sum_{p_m|n} \log p_1 \cdots \log p_m \sum_{\substack{d|n \\ p_1|d, \dots, p_m|d}} \mu(d)$$

固定 p_1, p_2, \dots, p_m ，令 $S = \{s : s = p_i, i = 1, 2, \dots, m\}$ 为其中不同素因子的集合；设 $r = |S|$ ，则 $r \leq m < k$ 。

则：

$$\begin{aligned} & \sum_{\substack{d|n \\ p_1|d, \dots, p_m|d}} \mu(d) \\ &= (-1)^r \left[(-1)^0 \binom{k-r}{0} + (-1)^1 \binom{k-r}{1} + \cdots + (-1)^{k-r} \binom{k-r}{k-r} \right] \\ &= (-1)^r (-1+1)^{k-r} \\ &= 0 \end{aligned}$$

因此，

$$\sum_{d|n} \mu(d) \log^m d = 0$$

10 求 $\sum_{n=1}^{\infty} \mu(n!)$ 之值。

解 对于 $n \geq 4$ ，有 $2^2 = 4|n$ ，故 $\mu(n) = 0$ 。

则：

$$\sum_{n=1}^{\infty} \mu(n!) = \mu(1) + \mu(2) + \mu(6) = 1 + (-1) + (-1)^2 = 1$$

11 证明： $\sum_{d|n} \mu^2(d) = 2^{\omega(n)}$ 及 $\sum_{t|n} \mu(t)d(t) = (-1)^{\omega(n)}$ 。

证明

(a). 设 $f = \mu^2 * u$ ，则 f 为积性函数，且 $f(n) = \sum_{d|n} \mu^2(d)$ 。

设 $n = p^\alpha$, 则有:

$$f(p^\alpha) = \begin{cases} 1, & \alpha = 0 \\ 2, & \alpha \geq 1 \end{cases}$$

若 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则

$$f(m) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_s^{\alpha_s}) = 2^{\omega(m)}$$

即

$$\sum_{d|n} \mu^2(d) = 2^{\omega(n)}$$

(b). 设 $g = \mu d * u$, 则 g 为积性函数, 且 $g(n) = \sum_{t|n} \mu(t) d(t)$.

设 $n = p^\alpha$, 则有:

$$g(p^\alpha) = \begin{cases} 1, & \alpha = 0 \\ -1, & \alpha \geq 1 \end{cases}$$

若 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则

$$g(m) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \cdots g(p_s^{\alpha_s}) = (-1)^{\omega(m)}$$

即

$$\sum_{t|n} \mu(t) d(t) = (-1)^{\omega(n)}$$

12 试证: $\sum_{d|n} \mu(d) \sigma(d) = (-1)^{\omega(n)} \prod_{p|n} p$ 及 $\sum_{d|n} \mu(d) \varphi(d) = (-1)^{\omega(n)} \prod_{p|n} (p-2)$.

证明

(a). $\sum_{d|n} \mu(d) \sigma(d) = (-1)^{\omega(n)} \prod_{p|n} p$.

设 $f = \mu * \sigma$, 则 f 为积性函数, 且 $f(n) = \sum_{d|n} \mu(d) \sigma(d)$.

设 $n = p^\alpha$, 则有:

$$f(p^\alpha) = \begin{cases} 1, & \alpha = 0 \\ -p, & \alpha \geq 1 \end{cases}$$

若 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则

$$f(m) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_s^{\alpha_s}) = (-1)^{\omega(m)} \prod_{p|m} p$$

即

$$\sum_{d|n} \mu(d) \sigma(d) = (-1)^{\omega(n)} \prod_{p|n} p$$

(b). $\sum_{d|n} \mu(d) \varphi(d) = (-1)^{\omega(n)} \prod_{p|n} (p-2)$ 。

设 $g = \mu * \varphi$, 则 g 为积性函数, 且 $g(n) = \sum_{d|n} \mu(d) \varphi(d)$ 。

设 $n = p^\alpha$, 则有:

$$g(p^\alpha) = \begin{cases} 1, & \alpha = 0 \\ 2 - p, & \alpha \geq 1 \end{cases}$$

若 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则

$$g(m) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \cdots g(p_s^{\alpha_s}) = (-1)^{\omega(m)} \prod_{p|m} (p-2)$$

即

$$\sum_{d|n} \mu(d) \varphi(d) = (-1)^{\omega(n)} \prod_{p|n} (p-2)$$

14 (1) 设 $n > 1$, 证明: $\sum_{\substack{1 \leq d \leq n \\ (n,d)=1}} d = \frac{1}{2} n \varphi(n)$;

(2) 设 n 为奇数, 证明: $\sum_{\substack{1 \leq d \leq \frac{n}{2} \\ (d,n)=1}} d = \frac{1}{8} n \varphi(n) - \frac{1}{8} \prod_{p|n} (1-p)$ 。

证明

(a). 若 $n > 1$, 则

$$\begin{aligned} \sum_{\substack{1 \leq d \leq n \\ (n,d)=1}} d &= \frac{1}{2} \sum_{\substack{1 \leq d \leq n \\ (n,d)=1}} d + \frac{1}{2} \sum_{\substack{1 \leq d \leq n \\ (n,d)=1}} (n-d) \\ &= \frac{1}{2} \sum_{\substack{1 \leq d \leq n \\ (n,d)=1}} n \end{aligned}$$

$$= \frac{1}{2}n\varphi(n)$$

(b). 设 $S = \sum_{\substack{1 \leq d \leq \frac{n}{2} \\ (d,n)=1}} d$, 则有

$$S = \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} d \cdot I((d, n))$$

其中 $I = \mu * u$, 故

$$I((d, n)) = \sum_{k|(d, n)} \mu(k)$$

于是,

$$S = \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} d \sum_{k|(d, n)} \mu(k)$$

交换求和次序, 有

$$S = \sum_{k|n} \mu(k) \sum_{\substack{1 \leq d \leq \lfloor \frac{n}{2} \rfloor \\ k|d}} d$$

固定 k , 设 $d = km$, 则

$$\sum_{\substack{1 \leq d \leq \lfloor \frac{n}{2} \rfloor \\ k|d}} d = k \sum_{m=1}^{\lfloor \frac{n}{2k} \rfloor} m = k \cdot \frac{M(M+1)}{2}$$

其中, $M = \lfloor \frac{n}{2k} \rfloor$ 。

而

$$\lfloor \frac{n}{2k} \rfloor = \lfloor \frac{\frac{n}{k}}{2} \rfloor = \frac{\frac{n}{k} - 1}{2}$$

因此,

$$\begin{aligned} \sum_{\substack{1 \leq d \leq \lfloor \frac{n}{2} \rfloor \\ k|d}} d &= k \cdot \frac{\frac{\frac{n}{k}-1}{2}(\frac{\frac{n}{k}-1}{2} + 1)}{2} \\ &= \frac{n^2 - k^2}{8k} \end{aligned}$$

则

$$\begin{aligned} S &= \sum_{k|n} \mu(k) \cdot \frac{n^2 - k^2}{8k} \\ &= \frac{1}{8} \left(n^2 \sum_{k|n} \frac{\mu(k)}{k} - \sum_{k|n} \mu(k)k \right) \end{aligned}$$

其中,

$$\begin{aligned} \sum_{k|n} \frac{\mu(k)}{k} &= \frac{\varphi(n)}{n} \\ \sum_{k|n} \mu(k)k &= \prod_{p|n} (1-p) \end{aligned}$$

于是,

$$\begin{aligned} S &= \frac{1}{8} \left(n^2 \cdot \frac{\varphi(n)}{n} - \prod_{p|n} (1-p) \right) \\ &= \frac{1}{8} n \varphi(n) - \frac{1}{8} \prod_{p|n} (1-p) \end{aligned}$$

16 求出所有使 $\varphi(n) = 24$ 的自然数.

解 对于 $n \in \mathbb{N}^+$, 作如下素因数分解

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

则

$$\begin{aligned} \varphi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= p_1^{\alpha_1-1} (p_1 - 1) p_2^{\alpha_2-1} (p_2 - 1) \cdots p_k^{\alpha_k-1} (p_k - 1) \end{aligned}$$

注意到: $24 = 2^3 \times 3$

(a). $n = p^k$

即

$$p^{k-1} (p - 1) = 2^3 \times 3$$

无解。

(b). $n = p^a q^b$

即

$$p^{a-1}(p-1)q^{b-1}(q-1) = 2^3 \times 3$$

I. $a = 1, b = 1$, 则

$$(p-1)(q-1) = 24$$

$$\text{而 } 24 = 1 \times 24 = 2 \times 12 = 3 \times 8 = 4 \times 6$$

又 p, q 均为素数, 故

$$(p, q) = (3, 13), (5, 7)$$

于是

$$n = pq = 39, 35$$

II. $a = 2, b = 1$, 则

$$p(p-1)(q-1) = 24$$

故

$$(p, q) = (2, 13), (3, 5)$$

于是

$$n = p^2 q = 52, 45$$

III. $a = 3, b = 1$, 则

$$p^2(p-1)(q-1) = 24$$

故

$$(p, q) = (2, 7)$$

于是

$$n = p^3 q = 56$$

IV. $a = 3, b = 2$, 则

$$p^2(p-1)q(q-1) = 24$$

故

$$(p, q) = (2, 3)$$

于是

$$n = p^3 q^2 = 72$$

V. 其他情况, 均无解。

(c). $n = p^a q^b r^c$

即

$$p^{a-1}(p-1)q^{b-1}(q-1)r^{c-1}(r-1) = 24$$

I. $a = b = c = 1$, 则

$$(p-1)(q-1)(r-1) = 24$$

$$\text{而 } 24 = 1 \times 2 \times 12 = 1 \times 3 \times 8 = 1 \times 4 \times 6 = 2 \times 3 \times 4$$

故

$$(p, q, r) = (2, 3, 13), (2, 5, 7)$$

于是

$$n = pqr = 78, 70$$

II. $a = 2, b = c = 1$, 则

$$p(p-1)(q-1)(r-1) = 24$$

故

$$(p, q, r) = (2, 3, 7), (3, 2, 5)$$

于是

$$n = p^2 qr = 84, 90$$

III. $a = b = 2, c = 1$ 或其它情况, 均无解。

(d). $n = p^a q^b r^c s^t$.

因为若 $n = 2 \times 3 \times 5 \times 7 = 210$, 则 $\varphi(n) = 48 > 24$, 故无解。

综上所述, n 所有可能的取值为

$$39, 35, 52, 45, 56, 72, 78, 70, 84, 90$$

共 10 种。

19 求出所有 $4 \nmid \varphi(n)$ 的自然数 n .

解 对于 $n \in \mathbb{N}^+$, 作如下素因数分解

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

则

$$\varphi(n) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_m^{k_m-1}(p_m-1)$$

设 $n = 2^a \cdot m$, 其中 $2^a \mid n$ 而 $2^{a+1} \nmid m$ 。

由于 $\varphi(n)$ 为积性函数, 于是

$$\varphi(n) = \varphi(2^a) \cdot \varphi(m)$$

(a). $a = 0$, 则 n 为奇数。

对于 m 作素因数分解

$$m = p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t}$$

其中 p_i 为奇质数。

I. 若 $p_i \equiv 1 \pmod{4}$, 则 $p_i - 1 \equiv 0 \pmod{4}$, 则

$$4 \mid \varphi(m)$$

II. 若 $p_i \equiv 3 \pmod{4}$, 则

$$\varphi(p_i^{b_i}) = p_i^{b_i-1}(p_i-1) \equiv 2 \pmod{4}$$

若 $t \leq 2$, 则存在 i, j 使得 $4 \mid (p_i-1)(p_j-1)$, 故 $4 \mid \varphi(n)$ 。

若 $t = 0$, 则 $n = 1$, $\varphi(1) = 1$, 有 $4 \nmid \varphi(1)$ 。

若 $t = 1$, 则 $n = p^b$, 其中 $p \equiv 3 \pmod{4}$, 故 $\varphi(p^b) \equiv 2 \pmod{4}$ 。

(b). $a = 1$, 则

$$\varphi(n) = \varphi(2 \cdot m) = \varphi(2)\varphi(m) = \varphi(m)$$

与上一种情况类似, 故

$$4 \nmid \varphi(n) \iff n = 2 \text{ 或 } n = 2 \cdot p^k$$

其中 $p \equiv 3 \pmod{4}$, $k \geq 1$ 。

(c). $a = 2$, 则

$$\varphi(n) = \varphi(4 \cdot m) = \varphi(4)\varphi(m) = 2\varphi(m)$$

比较可知, $4 \nmid \varphi(m) \iff m = 1 \iff n = 4$ 。

(d). $a \geq 3$, 则 $4 \mid \varphi(n)$, 无解。

综上所述, n 所有可能的取值为

$$1, 2, 4, p^k, 2 \cdot p^k$$

其中 p 为素数且 $p \equiv 3 \pmod{4}$, $k \geq 1$ 。

22 设 $\Lambda(n)$ 为 Mangoldt 函数, 且 $\psi(x) = \sum_{n \leq x} \Lambda(n)$, 则

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{n \leq x} \log n.$$

证明

(a).

$$\begin{aligned} \sum_{n \leq x} \psi\left(\frac{x}{n}\right) &= \sum_{n \leq x} \sum_{m \leq \frac{x}{n}} \Lambda(m) \\ &= \sum_{m \leq x} \Lambda(m) \sum_{n \leq \frac{x}{m}} 1 \\ &= \sum_{m \leq x} \Lambda(m) \left[\frac{x}{m}\right] \end{aligned}$$

(b).

$$\begin{aligned} \sum_{n \leq x} \log n &= \sum_{n \leq x} \sum_{d|n} \Lambda(d) \\ &= \sum_{d \leq x} \Lambda(d) \sum_{k \leq \frac{x}{d}} 1 \\ &= \sum_{d \leq x} \Lambda(d) \left[\frac{x}{d}\right] \end{aligned}$$

24 设 $\sigma(n)$ 为除数和函数, 证明:

(1) $\sigma(n) = n + 1$ 的充要条件是 n 为素数;

(2) 如果 n 为完全数, 即 $\sigma(n) = 2n$, 则

$$\sum_{d|n} \frac{1}{d} = 2$$

证明

(a). 必要性显然。

充分性:

若 $n = 1$, 则 $\sigma(1) = 1$, 而 $1 + n = 2$, 故不满足。

若 n 为合数, 则存在 d ($d \neq 1$ 且 $d \neq n$) s.t. $d|n$ 。

而

$$\sigma(n) \geq 1 + d + n > 1 + n$$

故 $\sigma(n) \neq 1 + n$ ，矛盾。

因此， n 为素数。

(b).

$$\sum_{d|n} \frac{1}{d} = \frac{1}{n} \sum_{d|n} \frac{n}{d} = \frac{1}{n} \sum_{d|n} d = \frac{\sigma(n)}{n} = \frac{2n}{n} = 2$$