潘承洞《数论基础》

作者：韦明

时间：April 13, 2025

E-mail：wm31415926535@outlook.com

目录

第 1 章 作业

1.1 第三周作业

第二章

8 试证：当 $\omega(n)>1$ 时，$\sum\limits_{d\mid n}\mu(d)\log d=0$; 一般若 $m\geqslant 1$ 且 $\omega(n)>m$，则 $\sum\limits_{d\mid n}\mu(d)\log^m d=0.$

证明 由于若 d 存在平方因子，则 $\mu(d)=0$，不妨设

$$n=p_1p_2\cdots p_k$$

其中 $p_i,p_j(i\neq j)$ 为互异素因子。

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

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

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

交换求和次序，有：

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

固定 p，则

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

因此，

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

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

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

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

交换求和次序，有：

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

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

则：

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

因此，

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

10 求 $\sum\limits_{n=1}^{\infty}\mu(n!)$ 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：$\sum\limits_{d|n}\mu^2(d)=2^{\omega(n)}$ 及 $\sum\limits_{t|n}\mu(t)d(t)=(-1)^{\omega(n)}$.

证明

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

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 $g(n)=\sum\limits_{t|n}\mu(t)d(t)$。

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：$\sum\limits_{d|n}\mu(d)\sigma(d)=(-1)^{\omega(n)}\prod\limits_{p|n}p$ 及 $\sum\limits_{d|n}\mu(d)\varphi(d)=(-1)^{\omega(n)}\prod\limits_{p|n}(p-2)$.

证明

(a). $\sum\limits_{d|n}\mu(d)\sigma(d)=(-1)^{\omega(n)}\prod\limits_{p|n}p$。

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

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：$\sum_{\substack{1 \leqslant d \leqslant n \\ (n,d)=1}} d = \frac{1}{2} n\varphi(n)$；

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

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 $S = \sum\limits_{\substack{1\le d\le \frac{n}{2}\\(d,n)=1}} d$，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

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

固定 k，设 $d = km$，则

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

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，

$$\sum_{\substack{1\le d\le \lfloor \frac{n}{2} \rfloor\\ k|d}} d = k \cdot \frac{\frac{\frac{n}{k}-1}{2}(\frac{\frac{n}{k}-1}{2} + 1)}{2}$$

$$= \frac{n^2 - k^2}{8k}$$

则

$$S=\sum_{k|n}\mu(k)\cdot\frac{n^2-k^2}{8k}$$

$$=\frac{1}{8}\left(n^2\sum_{k|n}\frac{\mu(k)}{k}-\sum_{k|n}\mu(k)k\right)$$

其中，

$$\sum_{k|n}\frac{\mu(k)}{k}=\frac{\varphi(n)}{n}$$

$$\sum_{k|n}\mu(k)k=\prod_{p|n}(1-p)$$

于是，

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

$$=\frac{1}{8}n\varphi(n)-\frac{1}{8}\prod_{p|n}(1-p)$$

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

$$\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})$$

$$=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)$$

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). $n=p^aq^b$

即

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

I. $a=1$，$b=1$，则

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

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

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

III. $a=3$，$b=1$，则

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

故

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

于是

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

IV. $a=3$，$b=2$，则

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

故

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

于是

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

V. 其他情况，均无解。

(c). $n = p^aq^br^c$

即

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

I. $a = b = c = 1$，则

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

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

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

III. $a = b = 2$，$c = 1$ 或其它情况，均无解。

(d). $n = p^aq^br^cs^t$.

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

$$4|\varphi(m)$$

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 $4|(p_i-1)(p_j-1)$，故 $4|\varphi(n)$。
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

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

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，$4 \nmid \varphi(m) \Longleftrightarrow m = 1 \Longleftrightarrow n = 4$。

(d). $a \geq 3$，则 $4|\varphi(n)$，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 $\psi(x) = \sum\limits_{n \leq x} \Lambda(n)$，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).

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

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

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

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. $d \mid n$。

而

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

故 $\sigma(n) \neq 1 + n$，矛盾。

因此，n 为素数。

(b).

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

1.2 第四周作业

第三章

1 试证 $\prod_p \frac{p^2}{p^2-1} = \frac{\pi^2}{6}$.

证明 考虑 Riemann zeta 函数 $\zeta(s)$ 的 Euler 乘积公式：

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

其中乘积遍历所有素数 p，该公式对于 $\mathrm{Re}(s) > 1$ 成立。

令 $s = 2$，我们知道 $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$。将 $s = 2$ 代入 Euler 乘积公式，得到：

$$\zeta(2) = \prod_p \left(1 - \frac{1}{p^2}\right)^{-1} = \frac{\pi^2}{6}$$

现在考察题目中给出的无穷乘积：

$$\begin{aligned}
\prod_p \frac{p^2}{p^2-1} &= \prod_p \frac{1}{\frac{p^2-1}{p^2}} \\
&= \prod_p \frac{1}{1 - \frac{1}{p^2}} \\
&= \prod_p \left(1 - p^{-2}\right)^{-1}
\end{aligned}$$

比较可知，该乘积正是 $\zeta(2)$ 的 Euler 乘积表示。因此，

$$\prod_p \frac{p^2}{p^2-1} = \zeta(2) = \frac{\pi^2}{6}$$

证毕。

2 试证级数 $\sum_p \frac{1}{p}$ 发散.

证明 采用反证法。假设级数 $\sum_p \frac{1}{p}$ 收敛。根据 Cauchy 准则，这意味着对于任意 $\epsilon > 0$，存在 N 使得对所有 $n > m \geq N$，有 $\sum_{k=m+1}^{n} \frac{1}{p_k} < \epsilon$。特别地，这

意味着尾项级数 $\sum\limits_{k=K+1}^{\infty}\frac{1}{p_k}$ 对于任意 K 都是收敛的（作为 $n\to\infty$ 的极限）。
设 K 为任意正整数。考虑所有素因子都大于 p_K 的正整数集合 $M_K=\{m\in\mathbb{N}\mid\forall p\text{ s.t. }p|m,p>p_K\}$。由于 $\sum\limits_{k=K+1}^{\infty}\frac{1}{p_k}$ 收敛（由假设），根据无穷乘积与级数的关系，无穷乘积 $\prod\limits_{k=K+1}^{\infty}(1-\frac{1}{p_k})$ 收敛到一个正值 $P_K'>0$。
因此，Euler 乘积 $\sum\limits_{m\in M_K}\frac{1}{m}=\prod\limits_{k=K+1}^{\infty}(1-\frac{1}{p_k})^{-1}=\frac{1}{P_K'}$ 收敛到一个有限值 V_K。
现在，令 $P_K=p_1p_2\cdots p_K$ 为前 K 个素数的乘积。考虑形如 $1+qP_K$ 的整数，其中 $q=1,2,3,\dots$。
任何 $1+qP_K$ 的素因子 p 必须满足 $p\nmid P_K$，否则 $p\mid qP_K$ 且 $p\mid(1+qP_K)$，这意味着 $p\mid 1$，这是不可能的。
因此，$1+qP_K$ 的所有素因子都大于 p_K，即 $1+qP_K\in M_K$ 对所有 $q\geq 1$ 成立。
于是，我们有级数不等式：

$$\sum_{q=1}^{\infty}\frac{1}{1+qP_K}\leq\sum_{m\in M_K}\frac{1}{m}=V_K$$

这表明，如果 $\sum\limits_{p}\frac{1}{p}$ 收敛，则级数 $\sum\limits_{q=1}^{\infty}\frac{1}{1+qP_K}$ 必须收敛。

然而，我们使用极限比较判别法，将级数 $\sum\limits_{q=1}^{\infty}\frac{1}{1+qP_K}$ 与发散的调和级数 $\sum\limits_{q=1}^{\infty}\frac{1}{q}$ 进行比较：

$$\lim_{q\to\infty}\frac{\frac{1}{1+qP_K}}{\frac{1}{q}}=\lim_{q\to\infty}\frac{q}{1+qP_K}=\frac{1}{P_K}$$

由于 $P_K=p_1\cdots p_K\geq 2$，极限值 $\frac{1}{P_K}$ 是一个正的有限常数。

因为调和级数 $\sum\limits_{q=1}^{\infty}\frac{1}{q}$ 发散，根据极限比较判别法，级数 $\sum\limits_{q=1}^{\infty}\frac{1}{1+qP_K}$ 也必须发散。

这与我们从“$\sum_p \frac{1}{p}$ 收敛”这一假设推导出的结论“$\sum_{q=1}^{\infty} \frac{1}{1+qP_K}$ 收敛”相矛盾。

因此，最初的假设“$\sum_p \frac{1}{p}$ 收敛”必定是错误的。这意味着级数 $\sum_p \frac{1}{p}$ 不满足 Cauchy 准则，故该级数发散。证毕。

3 试证数列 $\{6n-1\}$ 中包含无限个素数.

证明 采用反证法。假设形式为 $6n-1$ 的素数只有有限个，设为 $p_1, p_2, \ldots, p_r$。考虑整数 $N = 6(p_1 p_2 \cdots p_r) - 1$。

首先，$N > 1$。N 的素因子分解式中，所有素因子 p 必满足 $p \nmid 6$，即 p 不能是 2 或 3。因此，N 的任何素因子 p 必形如 $6k+1$ 或 $6k-1$。

注意到 $N = 6(p_1 p_2 \cdots p_r) - 1 \equiv -1 \pmod 6$。

如果 N 的所有素因子都形如 $6k+1$，那么它们的乘积 N 也必然形如 $6k+1$。（因为 $(6k_1+1)(6k_2+1) = 36k_1k_2 + 6k_1 + 6k_2 + 1 = 6(6k_1k_2 + k_1 + k_2) + 1 \equiv 1 \pmod 6$）这与 $N \equiv -1 \pmod 6$ 矛盾。

因此，N 必须至少有一个形如 $6k-1$ 的素因子，设为 p。

我们证明 p 不等于 $p_1, p_2, \ldots, p_r$ 中的任何一个。如果 $p = p_i$ 对于某个 $i \in \{1, 2, \ldots, r\}$ 成立，则 $p_i \mid N$ 且 $p_i \mid 6(p_1 p_2 \cdots p_r)$。因此 p_i 必须整除它们的差，即 $p_i \mid (6(p_1 p_2 \cdots p_r) - N)$，也就是 $p_i \mid 1$。这是不可能的。

所以，p 是一个形如 $6k-1$ 的素数，但它不在我们假设的有限列表 $p_1, p_2, \ldots, p_r$ 中。这与我们的初始假设（所有形如 $6n-1$ 的素数都在该列表中）矛盾。

因此，假设错误，形如 $6n-1$ 的素数有无限多个。证毕。

5 利用 $\prod_{p \leqslant x} \left(1 - \frac{1}{p}\right)^{-1} \leqslant \prod_{K=2}^{\pi(x)+1} \left(1 - \frac{1}{K}\right)^{-1}$，证明:

（1）$\pi(x) > \log x - 1$；

（2）$p_n < 3^{n+1}$（p_n 为第 n 个素数）.

证明

(a). 证明 $\pi(x) > \log x - 1$。

我们知道对于 $x \geq 1$，有 $\sum_{n \leq x} \frac{1}{n} > \log x$。

同时，我们有

$$\sum_{n \leq x} \frac{1}{n} \leq \sum_{n \in S_x} \frac{1}{n} = \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}$$

其中 S_x 是所有素因子都 $\leq x$ 的正整数集合。

结合上述不等式和题目给出的不等式，得到：

$$\log x < \sum_{n \leq x} \frac{1}{n} \leq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \leq \prod_{K=2}^{\pi(x)+1} \left(1 - \frac{1}{K}\right)^{-1}$$

计算右侧的乘积：

$$\begin{aligned}
\prod_{K=2}^{\pi(x)+1} \left(1 - \frac{1}{K}\right)^{-1} &= \prod_{K=2}^{\pi(x)+1} \left(\frac{K-1}{K}\right)^{-1} \\
&= \prod_{K=2}^{\pi(x)+1} \frac{K}{K-1} \\
&= \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdots \frac{\pi(x)+1}{\pi(x)} \\
&= \pi(x) + 1
\end{aligned}$$

因此，我们得到 $\log x < \pi(x) + 1$。

整理可得 $\pi(x) > \log x - 1$。

(b). 证明 $p_n < 3^{n+1}$。

由（1）可知 $\pi(x) > \log x - 1$。

令 $x = p_n$，其中 p_n 是第 n 个素数。则 $\pi(x) = \pi(p_n) = n$。

代入不等式，得到：

$$n > \log p_n - 1$$

整理得：

$$\log p_n < n + 1$$

两边取指数（以自然对数底 e）：

$$p_n < e^{n+1}$$

由于 $e \approx 2.718 < 3$，我们有 $e^{n+1} < 3^{n+1}$。

因此，

$$p_n < 3^{n+1}$$

证毕。

第四章

1 若 $a_1 \equiv b_1(\bmod m), a_2 \equiv b_2(\bmod m)$, 则

$$a_1a_2 \equiv b_1b_2(\bmod m).$$

证明 由题设 $a_1 \equiv b_1 \pmod m$ 和 $a_2 \equiv b_2 \pmod m$，根据同余的定义，可知 $m \mid (a_1 - b_1)$ 且 $m \mid (a_2 - b_2)$。因此，存在整数 k_1, k_2 使得

$$a_1 - b_1 = mk_1$$
$$a_2 - b_2 = mk_2$$

即 $a_1 = b_1 + mk_1$ 且 $a_2 = b_2 + mk_2$。
考察 $a_1a_2 - b_1b_2$：

$$\begin{aligned} a_1a_2 - b_1b_2 &= (b_1 + mk_1)(b_2 + mk_2) - b_1b_2 \\ &= b_1b_2 + b_1mk_2 + b_2mk_1 + m^2k_1k_2 - b_1b_2 \\ &= m(b_1k_2 + b_2k_1 + mk_1k_2) \end{aligned}$$

由于 b_1, k_2, b_2, k_1, m 均为整数，所以 $b_1k_2 + b_2k_1 + mk_1k_2$ 也是整数。因此，$m \mid (a_1a_2 - b_1b_2)$。根据同余的定义，有

$$a_1a_2 \equiv b_1b_2 \pmod m$$

证毕。

2 若 $C \equiv d(\bmod m), (C, m) = 1$ ，则

$$aC \equiv bd(\bmod m)$$

与

$$a \equiv b(\bmod m)$$

等价。

证明 $(\Longrightarrow)$ 假设 $a \equiv b \pmod m$。由题设 $C \equiv d \pmod m$。根据上一题的结论（同余式的乘法性质），将 $a \equiv b \pmod m$ 与 $C \equiv d \pmod m$ 两式相乘，得到：

$$aC \equiv bd \pmod m$$

$(\Longleftarrow)$ 假设 $aC \equiv bd \pmod m$。由题设 $C \equiv d \pmod m$，可知 $m \mid (C-d)$，即

$d = C - mk$ 对于某个整数 k 成立。将 $d = C - mk$ 代入 $aC \equiv bd \pmod{m}$：

$$aC \equiv b(C - mk) \pmod{m}$$
$$aC \equiv bC - bmk \pmod{m}$$

由于 $bmk \equiv 0 \pmod{m}$，上式简化为：

$$aC \equiv bC \pmod{m}$$

这意味着 $m \mid (aC - bC)$，即 $m \mid (a-b)C$。

因为 $\gcd(C, m) = 1$，根据 **Euclid** 引理，可得 $m \mid (a - b)$。根据同余的定义，有

$$a \equiv b \pmod{m}$$

综上所述，两个同余式等价。证毕。

4 设素数 $p \geqslant 3$，若 $a^2 \equiv b^2 (\mathrm{mod} p), p \nmid a$，则 $a \equiv b (\mathrm{mod} p)$ 或 $a \equiv -b (\mathrm{mod} p)$ 且仅有一个成立.

证明 由 $a^2 \equiv b^2 \pmod{p}$，可得 $a^2 - b^2 \equiv 0 \pmod{p}$，即

$$(a-b)(a+b) \equiv 0 \pmod{p}$$

因为 p 是素数，根据 **Euclid** 引理，必有 $p \mid (a-b)$ 或 $p \mid (a+b)$。

- 若 $p \mid (a-b)$，则 $a \equiv b \pmod{p}$。
- 若 $p \mid (a+b)$，则 $a \equiv -b \pmod{p}$。

因此，至少有 $a \equiv b \pmod{p}$ 或 $a \equiv -b \pmod{p}$ 中的一个成立。

接下来证明仅有一个成立。假设 $a \equiv b \pmod{p}$ 和 $a \equiv -b \pmod{p}$ 同时成立。则 $b \equiv -b \pmod{p}$，即 $2b \equiv 0 \pmod{p}$。因为 p 是素数且 $p \geq 3$，所以 $\gcd(2, p) = 1$。根据同余的性质，由 $2b \equiv 0 \pmod{p}$ 可得 $b \equiv 0 \pmod{p}$。又因为 $a \equiv b \pmod{p}$，所以 $a \equiv 0 \pmod{p}$，即 $p \mid a$。这与题目条件 $p \nmid a$ 矛盾。

因此，$a \equiv b \pmod{p}$ 和 $a \equiv -b \pmod{p}$ 不能同时成立。

综上所述，$a \equiv b \pmod{p}$ 或 $a \equiv -b \pmod{p}$ 且仅有一个成立。证毕。

5 设正整数

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0, \quad 0 \leqslant a_i < 10$$

则 11 整除 a 的充要条件是

$$11 \mid \sum_{i=1}^{n}(-1)^{i}a_i$$

证明 考虑整数 a 模 11 的余数。我们注意到 $10 \equiv -1 \pmod{11}$。根据同余的性质，对于任意非负整数 i，有

$$10^i \equiv (-1)^i \pmod{11}$$

现在考察 a 模 11：

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10^1 + a_0 \\ &\equiv a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots + a_1(-1)^1 + a_0(-1)^0 \pmod{11} \\ &\equiv \sum_{i=0}^{n} a_i(-1)^i \pmod{11} \end{aligned}$$

因此，$a \equiv 0 \pmod{11}$ 当且仅当 $\sum_{i=0}^{n}(-1)^i a_i \equiv 0 \pmod{11}$。

证毕。

6 试找出整数能被 37，101 整除的判别条件来。

解 设整数 N 的十进制表示为 $a_k a_{k-1}\cdots a_1 a_0 = \sum_{i=0}^{k} a_i 10^i$。

能被 **37** 整除的判别条件：我们注意到 $1000 = 27 \times 37 + 1$，因此 $1000 \equiv 1 \pmod{37}$。将整数 N 从右往左每三位分为一组：

$$N = (a_2a_1a_0)_{10} + (a_5a_4a_3)_{10} \cdot 10^3 + (a_8a_7a_6)_{10} \cdot 10^6 + \cdots$$

令 $A_0 = (a_2a_1a_0)_{10} = 100a_2 + 10a_1 + a_0$，$A_1 = (a_5a_4a_3)_{10} = 100a_5 + 10a_4 + a_3$，以此类推。则 $N = A_0 + A_1 \cdot 10^3 + A_2 \cdot (10^3)^2 + \cdots$。考虑 N 模 37：

$$\begin{aligned} N &\equiv A_0 + A_1 \cdot 1 + A_2 \cdot 1^2 + \cdots \pmod{37} \\ &\equiv A_0 + A_1 + A_2 + \cdots \pmod{37} \end{aligned}$$

因此，一个整数能被 37 整除的充要条件是：将其从右往左每三位分为一组，这些组所表示的数之和能被 37 整除。

能被 **101** 整除的判别条件：我们注意到 $100 = 1 \times 101 - 1$，因此 $100 \equiv -1 \pmod{101}$。将整数 N 从右往左每两位分为一组：

$$N = (a_1a_0)_{10} + (a_3a_2)_{10} \cdot 10^2 + (a_5a_4)_{10} \cdot 10^4 + \cdots$$

令 $B_0 = (a_1a_0)_{10} = 10a_1 + a_0$，$B_1 = (a_3a_2)_{10} = 10a_3 + a_2$，以此类推。则 $N = B_0 + B_1 \cdot 10^2 + B_2 \cdot (10^2)^2 + \cdots$。考虑 N 模 101：

$$\begin{aligned} N &\equiv B_0 + B_1 \cdot (-1) + B_2 \cdot (-1)^2 + B_3 \cdot (-1)^3 + \cdots \pmod{101} \\ &\equiv B_0 - B_1 + B_2 - B_3 + \cdots \pmod{101} \end{aligned}$$

因此，一个整数能被 101 整除的充要条件是：将其从右往左每两位分为一组，这些组所表示的数的交错和（从右往左，符号为 $+-+-\cdots$）能被 101 整除。