潘承洞《数论基础》选解

作者：韦明

时间：May 7, 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，$\sum\limits_{d|n}\mu(d)\log d=0$; 一般若 $m\geqslant 1$ 且 $\omega(n)>m$，则 $\sum\limits_{d|n}\mu(d)\log^m d=0.$

证明 由于若 d 存在平方因子，则 $\mu(d)=0$，不妨设

$$n=p_1p_2\cdots p_k$$

其中 $p_i,p_j(i\neq j)$ 为互异素因子。

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

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

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

交换求和次序，有：

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

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 $\sum\limits_{d|n}\mu(d)\log^m d=0$。

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

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

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 $\sum_{n=1}^{\infty}\mu(n!)$ 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：$\sum\limits_{\substack{1\leqslant d\leqslant n\\(n,d)=1}}d=\frac{1}{2}n\varphi(n)$；

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

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 $S = \sum_{\substack{1 \le d \le \frac{n}{2} \\ (d,n)=1}} d$，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：$24=2^3\times3$

(a). $n=p^k$

即

$$p^{k-1}(p-1)=2^3\times3$$

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

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

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

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

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 $24 = 1\times2\times12 = 1\times3\times8 = 1\times4\times6 = 2\times3\times4$

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 $n = 2\times3\times5\times7 = 210$，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).

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

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).

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

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 $\sum_{k=K+1}^{\infty} \frac{1}{p_k}$ 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 $\sum_{k=K+1}^{\infty} \frac{1}{p_k}$ 收敛（由假设），根据无穷乘积与级数的关系，无穷乘积 $\prod_{k=K+1}^{\infty} (1 - \frac{1}{p_k})$ 收敛到一个正值 $P'_K > 0$。

因此，Euler 乘积 $\sum_{m \in M_K} \frac{1}{m} = \prod_{k=K+1}^{\infty} (1 - \frac{1}{p_k})^{-1} = \frac{1}{P'_K}$ 收敛到一个有限值 V_K。

现在，令 $P_K = p_1 p_2 \cdots p_K$ 为前 K 个素数的乘积。考虑形如 $1 + qP_K$ 的整数，其中 $q = 1, 2, 3, \ldots$。

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 $\sum_{p} \frac{1}{p}$ 收敛，则级数 $\sum_{q=1}^{\infty} \frac{1}{1 + qP_K}$ 必须收敛。

然而，我们使用极限比较判别法，将级数 $\sum_{q=1}^{\infty} \frac{1}{1 + qP_K}$ 与发散的调和级数 $\sum_{q=1}^{\infty} \frac{1}{q}$ 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 $\sum_{q=1}^{\infty} \frac{1}{q}$ 发散，根据极限比较判别法，级数 $\sum_{q=1}^{\infty} \frac{1}{1 + qP_K}$ 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 $a_1 \equiv b_1 (\mathrm{mod} m), a_2 \equiv b_2 (\mathrm{mod} m)$, 则

$$a_1 a_2 \equiv b_1 b_2 (\mathrm{mod} m).$$

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 $a_1 a_2 - b_1 b_2$:

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= (b_1 + mk_1)(b_2 + mk_2) - b_1 b_2 \\ &= b_1 b_2 + b_1 mk_2 + b_2 mk_1 + m^2 k_1 k_2 - b_1 b_2 \\ &= m(b_1 k_2 + b_2 k_1 + mk_1 k_2) \end{aligned}$$

由于 b_1, k_2, b_2, k_1, m 均为整数，所以 $b_1 k_2 + b_2 k_1 + mk_1 k_2$ 也是整数。因此，$m \mid (a_1 a_2 - b_1 b_2)$。根据同余的定义，有

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

证毕。

2 若 $C \equiv d (\mathrm{mod} m), (C, m) = 1$，则

$$aC \equiv bd (\mathrm{mod} m)$$

与

$$a \equiv b (\mathrm{mod} m)$$

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：

$$N = (a_2 a_1 a_0)_{10} + (a_5 a_4 a_3)_{10} \cdot 10^3 + (a_8 a_7 a_6)_{10} \cdot 10^6 + \cdots$$

令 $A_0 = (a_2 a_1 a_0)_{10} = 100a_2 + 10a_1 + a_0$，$A_1 = (a_5 a_4 a_3)_{10} = 100a_5 + 10a_4 + a_3$，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：

$$N = (a_1 a_0)_{10} + (a_3 a_2)_{10} \cdot 10^2 + (a_5 a_4)_{10} \cdot 10^4 + \cdots$$

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。

1.3 第五周作业

第四章

7 试证：$641 \mid \left(2^{32}+1\right)$.

证明 注意到 $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$。由 $641 = 5 \cdot 2^7 + 1$，可得

$$5 \cdot 2^7 \equiv -1 \pmod{641}$$

两边取 4 次方，得

$$(5 \cdot 2^7)^4 \equiv (-1)^4 \pmod{641}$$

$$5^4 \cdot 2^{28} \equiv 1 \pmod{641}$$

又由 $641 = 5^4 + 2^4$，可得

$$5^4 \equiv -2^4 \pmod{641}$$

代入上式，得

$$(-2^4) \cdot 2^{28} \equiv 1 \pmod{641}$$

$$-2^{32} \equiv 1 \pmod{641}$$

即

$$2^{32} \equiv -1 \pmod{641}$$

因此，$2^{32}+1 \equiv 0 \pmod{641}$，即 $641 \mid (2^{32}+1)$。

8 若 a 是一奇数，则 $a^{2^n} \equiv 1 \left(\mathrm{mod} 2^{n+2}\right)$， $n \geqslant 1$.

证明 用数学归纳法证明。

奠基 当 $n = 1$ 时，需证 $a^{2^1} \equiv 1 \pmod{2^{1+2}}$，即 $a^2 \equiv 1 \pmod{8}$。因为 a 是奇数，设 $a = 2k+1$，其中 k 为整数。

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$$

由于 $k(k+1)$ 必为偶数，设 $k(k+1) = 2j$，其中 j 为整数。则 $a^2 = 4(2j) + 1 = 8j + 1 \equiv 1 \pmod{8}$。故当 $n = 1$ 时命题成立。

归纳 假设当 $n = k\,(k \geq 1)$ 时命题成立，即 $a^{2^k} \equiv 1 \pmod{2^{k+2}}$。这意味着存在整数 c，使得 $a^{2^k} = 1 + c \cdot 2^{k+2}$。需要证明当 $n = k+1$ 时命题也

成立，即 $a^{2^{k+1}} \equiv 1 \pmod{2^{(k+1)+2}}$，即 $a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$。

$$\begin{aligned} a^{2^{k+1}} &= (a^{2^k})^2 \\ &= (1 + c \cdot 2^{k+2})^2 \\ &= 1 + 2 \cdot (c \cdot 2^{k+2}) + (c \cdot 2^{k+2})^2 \\ &= 1 + c \cdot 2^{k+3} + c^2 \cdot 2^{2(k+2)} \\ &= 1 + c \cdot 2^{k+3} + c^2 \cdot 2^{2k+4} \end{aligned}$$

因为 $k \geq 1$，所以 $2k+4 = (k+3) + (k+1) \geq k+3+2 = k+5$。因此 $2^{k+3} \mid c^2 \cdot 2^{2k+4}$。故

$$a^{2^{k+1}} \equiv 1 + c \cdot 2^{k+3} \pmod{2^{k+3}}$$

$$a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$$

当 $n = k+1$ 时命题成立。

由数学归纳法原理，原命题对所有 $n \geq 1$ 成立。

9 证明：

$$x = u + p^{s-t}v, \quad u = 0, 1, 2, \cdots, p^{s-t} - 1, \quad v = 0, 1, 2, \cdots, p^t - 1, \quad t \leqslant s$$

是模 p^s（p 为素数）的一个完全剩余系。

证明 首先，计算 x 的可能取值的个数。u 有 p^{s-t} 个可能的取值。v 有 p^t 个可能的取值。因此，x 的可能取值总数为 $p^{s-t} \cdot p^t = p^s$ 个。这与模 p^s 的完全剩余系的元素个数相同。接下来，证明这些值两两关于模 p^s 不同余。假设存在两组 (u_1, v_1) 和 (u_2, v_2)，其中 $0 \leq u_1, u_2 < p^{s-t}$ 且 $0 \leq v_1, v_2 < p^t$，使得

$$u_1 + p^{s-t}v_1 \equiv u_2 + p^{s-t}v_2 \pmod{p^s}$$

这意味着

$$(u_1 - u_2) + p^{s-t}(v_1 - v_2) \equiv 0 \pmod{p^s}$$

由此可知 $p^s \mid (u_1 - u_2) + p^{s-t}(v_1 - v_2)$。这也意味着

$$(u_1 - u_2) + p^{s-t}(v_1 - v_2) \equiv 0 \pmod{p^{s-t}}$$

因为 $p^{s-t}(v_1 - v_2) \equiv 0 \pmod{p^{s-t}}$，所以

$$u_1 - u_2 \equiv 0 \pmod{p^{s-t}}$$

即 $p^{s-t} \mid (u_1 - u_2)$。又因为 $0 \leq u_1, u_2 < p^{s-t}$，所以 $-(p^{s-t}) < u_1 - u_2 < p^{s-t}$。

满足 $p^{s-t} \mid (u_1 - u_2)$ 的唯一可能是 $u_1 - u_2 = 0$，即 $u_1 = u_2$。将 $u_1 = u_2$ 代入原同余式 $(u_1 - u_2) + p^{s-t}(v_1 - v_2) \equiv 0 \pmod{p^s}$，得到

$$p^{s-t}(v_1 - v_2) \equiv 0 \pmod{p^s}$$

这意味着存在整数 k，使得 $p^{s-t}(v_1 - v_2) = k \cdot p^s$。两边同除以 p^{s-t}（由于 $t \leq s, s - t \geq 0$），得到

$$v_1 - v_2 = k \cdot p^s / p^{s-t} = k \cdot p^t$$

这意味着 $p^t \mid (v_1 - v_2)$。又因为 $0 \leq v_1, v_2 < p^t$，所以 $-p^t < v_1 - v_2 < p^t$。满足 $p^t \mid (v_1 - v_2)$ 的唯一可能是 $v_1 - v_2 = 0$，即 $v_1 = v_2$。因此，如果 $u_1 + p^{s-t}v_1 \equiv u_2 + p^{s-t}v_2 \pmod{p^s}$，则必有 $u_1 = u_2$ 且 $v_1 = v_2$。这说明该集合中的 p^s 个数两两关于模 p^s 不同余。综上所述，该集合构成模 p^s 的一个完全剩余系。

10 (a). 若 $2 \nmid m$，则 $2, 4, 6, \cdots, 2m$ 是 m 的完全剩余系；

(b). 若 $m > 2$，则 $1^2, 2^2, 3^2, \cdots, m^2$ 不是 m 的完全剩余系.

证明

(a). 集合为 $S = \{2k \mid 1 \leq k \leq m\}$。该集合包含 m 个整数。我们需要证明这 m 个整数关于模 m 两两不同余。假设存在 $1 \leq k_1, k_2 \leq m$，使得 $2k_1 \equiv 2k_2 \pmod{m}$。则 $m \mid (2k_1 - 2k_2)$，即 $m \mid 2(k_1 - k_2)$。因为 m 是奇数，所以 $\gcd(2, m) = 1$。根据同余的性质，可以约去因子 2，得到

$$k_1 \equiv k_2 \pmod{m}$$

即 $m \mid (k_1 - k_2)$。又因为 $1 \leq k_1, k_2 \leq m$，所以 $|k_1 - k_2| < m$。满足 $m \mid (k_1 - k_2)$ 的唯一可能是 $k_1 - k_2 = 0$，即 $k_1 = k_2$。因此，集合 S 中的 m 个整数关于模 m 两两不同余。由于集合大小为 m，它构成模 m 的一个完全剩余系。

(b). 考虑集合 $T = \{k^2 \mid 1 \leq k \leq m\}$。我们需要证明当 $m > 2$ 时，这个集合中的数并非关于模 m 两两不同余。考虑 $k = 1$ 和 $k = m - 1$。因为 $m > 2$，所以 $m - 1 \geq 2$，且 $1 \neq m - 1$。它们都是 $\{1, 2, \ldots, m\}$ 中的不同元素。计算它们的平方模 m：

$$1^2 = 1 \equiv 1 \pmod{m}$$

$$(m-1)^2 = m^2 - 2m + 1$$

因为 $m^2 \equiv 0 \pmod{m}$ 且 $-2m \equiv 0 \pmod{m}$，所以

$$(m-1)^2 \equiv 0 - 0 + 1 \equiv 1 \pmod{m}$$

因此，我们找到了两个不同的整数 1 和 $m-1$ $(1 \leq 1, m-1 \leq m)$，它们的平方关于模 m 同余。这意味着集合 T 中至少有两个元素是相同的（模 m），所以它不能包含 m 个两两不同余的数。故 $1^2, 2^2, \cdots, m^2$ 不是模 m 的完全剩余系。

11 若 $m_1, m_2, \cdots, m_k$ 两两互素，$x_1, x_2, \cdots, x_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系，则

$$x = x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_{k-1} x_k$$

通过模 $m_1 m_2 \cdots m_k$ 的完全剩余系.

证明 令 $M = m_1 m_2 \cdots m_k$。首先，计算 x 的可能取值的个数。x_1 有 m_1 个可能的取值。x_2 有 m_2 个可能的取值。... x_k 有 m_k 个可能的取值。由于 x_i 的选择是独立的，x 的总取值个数为 $m_1 m_2 \cdots m_k = M$ 个。这与模 M 的完全剩余系的元素个数相同。接下来，证明这些值两两关于模 M 不同余。假设存在两组 $(x_1, x_2, \ldots, x_k)$ 和 $(x_1', x_2', \ldots, x_k')$，其中 x_i, x_i' 分别是模 m_i 的完全剩余系的代表元，使得

$$\begin{aligned} & x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 \cdots m_{k-1} x_k \\ \equiv & x_1' + m_1 x_2' + m_1 m_2 x_3' + \cdots + m_1 \cdots m_{k-1} x_k' \pmod{M} \end{aligned}$$

记此同余式为 $(*)$。因为 $m_1 \mid M$，所以上述同余式也意味着模 m_1 同余：

$$\begin{aligned} & x_1 + m_1 x_2 + \cdots + m_1 \cdots m_{k-1} x_k \\ \equiv & x_1' + m_1 x_2' + \cdots + m_1 \cdots m_{k-1} x_k' \pmod{m_1} \end{aligned}$$

由于 $m_1 x_2, m_1 m_2 x_3, \ldots$ 都是 m_1 的倍数，它们模 m_1 都同余于 0。所以 $x_1 \equiv x_1' \pmod{m_1}$。因为 x_1, x_1' 都来自模 m_1 的一个完全剩余系，所以 $x_1 = x_1'$。将 $x_1 = x_1'$ 代入 $(*)$ 并消去，得到

$$\begin{aligned} & m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 \cdots m_{k-1} x_k \\ \equiv & m_1 x_2' + m_1 m_2 x_3' + \cdots + m_1 \cdots m_{k-1} x_k' \pmod{M} \end{aligned}$$

两边同除以 m_1（这是允许的，因为 $M = m_1(m_2 \cdots m_k)$），得到

$$\begin{aligned} & x_2 + m_2 x_3 + \cdots + m_2 \cdots m_{k-1} x_k \\ \equiv & x_2' + m_2 x_3' + \cdots + m_2 \cdots m_{k-1} x_k' \pmod{m_2 \cdots m_k} \end{aligned}$$

记此同余式为 (**)。因为 $m_2 \mid (m_2 \cdots m_k)$，所以上述同余式也意味着模 m_2 同余：

$$x_2 + m_2 x_3 + \cdots \equiv x_2' + m_2 x_3' + \ldots \pmod{m_2}$$

$$x_2 \equiv x_2' \pmod{m_2}$$

因为 x_2, x_2' 都来自模 m_2 的一个完全剩余系，所以 $x_2 = x_2'$。我们可以继续这个过程。假设我们已经证明了 $x_1 = x_1', x_2 = x_2', \ldots, x_{j-1} = x_{j-1}'$。将这些代入 (*) 并消去相应的项，然后两边同除以 $m_1 m_2 \cdots m_{j-1}$，我们得到

$$\begin{aligned} & x_j + m_j x_{j+1} + \cdots + m_j \cdots m_{k-1} x_k \\ \equiv & x_j' + m_j x_{j+1}' + \cdots + m_j \cdots m_{k-1} x_k' \pmod{m_j m_{j+1} \cdots m_k} \end{aligned}$$

考虑模 m_j，得到

$$x_j \equiv x_j' \pmod{m_j}$$

因为 x_j, x_j' 都来自模 m_j 的一个完全剩余系，所以 $x_j = x_j'$。通过归纳，我们可以证明对所有的 $j = 1, 2, \ldots, k$，都有 $x_j = x_j'$。因此，如果两个 x 值关于模 M 同余，那么它们必定是由完全相同的 $(x_1, \ldots, x_k)$ 序列生成的。这证明了由不同序列生成的 M 个 x 值两两关于模 M 不同余。综上所述，这些 x 值构成了模 M 的一个完全剩余系。

22 判断下列同余方程是否有解，若有解求其解：

(a). $20x \equiv 4 (\mathrm{mod} 30)$；

(b). $15x \equiv 25 (\mathrm{mod} 35)$；

(c). $15x \equiv 0 (\mathrm{mod} 35)$.

解 线性同余方程 $ax \equiv b \pmod{m}$ 有解当且仅当 $\gcd(a, m) \mid b$。若有解，则恰有 $\gcd(a, m)$ 个模 m 的互不同余解。

(a). $20x \equiv 4 \pmod{30}$。计算 $\gcd(20, 30) = 10$。因为 $10 \nmid 4$，所以该同余方程无解。

(b). $15x \equiv 25 \pmod{35}$。计算 $\gcd(15, 35) = 5$。因为 $5 \mid 25$，所以该同余方

程有解，且恰有 5 个模 35 的互不同余解。原方程等价于 $15x = 25+35k$ 对于某个整数 k。两边同除以 $\gcd(15, 35) = 5$：

$$3x \equiv 5 \pmod 7$$

为解此方程，我们需要找到 3 模 7 的逆元。观察可知 $3 \times 5 = 15 \equiv 1 \pmod 7$。所以 3 的逆元是 5。用 5 乘以上述同余式两边：

$$5 \cdot (3x) \equiv 5 \cdot 5 \pmod 7$$

$$15x \equiv 25 \pmod 7$$

$$x \equiv 4 \pmod 7$$

所以解的形式为 $x = 4+7t$，其中 t 是整数。这些解在模 35 下为：当 $t = 0$ 时，$x = 4$。当 $t = 1$ 时，$x = 4 + 7 = 11$。当 $t = 2$ 时，$x = 4 + 14 = 18$。当 $t = 3$ 时，$x = 4 + 21 = 25$。当 $t = 4$ 时，$x = 4 + 28 = 32$。当 $t = 5$ 时，$x = 4 + 35 = 39 \equiv 4 \pmod{35}$，开始重复。因此，解为 $x \equiv 4, 11, 18, 25, 32 \pmod{35}$。

(c). $15x \equiv 0 \pmod{35}$。计算 $\gcd(15, 35) = 5$。因为 $5 \mid 0$，所以该同余方程有解，且恰有 5 个模 35 的互不同余解。原方程等价于 $15x = 35k$ 对于某个整数 k。两边同除以 $\gcd(15, 35) = 5$：

$$3x \equiv 0 \pmod 7$$

因为 $\gcd(3, 7) = 1$，我们可以约去 3，得到：

$$x \equiv 0 \pmod 7$$

所以解的形式为 $x = 7t$，其中 t 是整数。这些解在模 35 下为：当 $t = 0$ 时，$x = 0$。当 $t = 1$ 时，$x = 7$。当 $t = 2$ 时，$x = 14$。当 $t = 3$ 时，$x = 21$。当 $t = 4$ 时，$x = 28$。当 $t = 5$ 时，$x = 35 \equiv 0 \pmod{35}$，开始重复。因此，解为 $x \equiv 0, 7, 14, 21, 28 \pmod{35}$。

23 解二元一次同余方程组

$$\begin{cases} x + 4y - 29 \equiv 0 (\mathrm{mod} 143) \\ 2x - 9y + 84 \equiv 0 (\mathrm{mod} 143) \end{cases}$$

解 将方程组写为标准形式：

$$\begin{cases} x+4y \equiv 29 \pmod{143} & (1) \\ 2x-9y \equiv -84 \pmod{143} & (2) \end{cases}$$

注意到 $143 = 11 \times 13$。我们可以用消元法。将方程 (1) 乘以 2：

$$2x+8y \equiv 58 \pmod{143} \quad (3)$$

用方程 (3) 减去方程 (2)：

$$(2x+8y)-(2x-9y) \equiv 58-(-84) \pmod{143}$$
$$17y \equiv 142 \pmod{143}$$

因为 $142 \equiv -1 \pmod{143}$，所以

$$17y \equiv -1 \pmod{143}$$

我们需要解这个关于 y 的线性同余方程。首先计算 $\gcd(17, 143)$。因为 $143 = 11 \times 13$，17 是素数，且 $17 \neq 11, 17 \neq 13$，所以 $\gcd(17, 143) = 1$。这保证了方程有唯一解。我们需要找到 17 模 143 的逆元。使用扩展欧几里得算法：

$$143 = 8 \times 17 + 7$$
$$17 = 2 \times 7 + 3$$
$$7 = 2 \times 3 + 1$$

现在反向代入：

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2 \times (17 - 2 \times 7) \\ &= 7 - 2 \times 17 + 4 \times 7 \\ &= 5 \times 7 - 2 \times 17 \\ &= 5 \times (143 - 8 \times 17) - 2 \times 17 \\ &= 5 \times 143 - 40 \times 17 - 2 \times 17 \\ &= 5 \times 143 - 42 \times 17 \end{aligned}$$

从 $5 \times 143 - 42 \times 17 = 1$，我们得到 $-42 \times 17 \equiv 1 \pmod{143}$。所以 17 模 143 的逆元是 $-42 \equiv -42 + 143 = 101 \pmod{143}$。将 $17y \equiv -1 \pmod{143}$

两边乘以 101：

$$101 \cdot (17y) \equiv 101 \cdot (-1) \pmod{143}$$

$$y \equiv -101 \pmod{143}$$

$$y \equiv -101 + 143 \equiv 42 \pmod{143}$$

将 $y = 42$ 代入方程 (1)：

$$x + 4(42) \equiv 29 \pmod{143}$$

$$x + 168 \equiv 29 \pmod{143}$$

因为 $168 = 143 + 25 \equiv 25 \pmod{143}$，所以

$$x + 25 \equiv 29 \pmod{143}$$

$$x \equiv 29 - 25 \pmod{143}$$

$$x \equiv 4 \pmod{143}$$

因此，方程组的解为 $x \equiv 4 \pmod{143}$，$y \equiv 42 \pmod{143}$。

25 判断下列同余方程组是否有解，若有解求其解：

(a). $x \equiv 1(\mathrm{mod}4)$, $x \equiv 0(\mathrm{mod}3)$, $x \equiv 5(\mathrm{mod}7)$；

(b). $x \equiv 2(\mathrm{mod}4)$, $x \equiv 7(\mathrm{mod}10)$, $x \equiv 1(\mathrm{mod}3)$；

(c). $x \equiv 2(\mathrm{mod}3)$, $x \equiv 3(\mathrm{mod}5)$, $x \equiv 5(\mathrm{mod}2)$；

(d). $x \equiv 3(\mathrm{mod}8)$, $x \equiv 11(\mathrm{mod}20)$, $x \equiv 1(\mathrm{mod}15)$.

解 使用中国剩余定理 (CRT)。若模数不互素，则先检查相容性。

(a). $x \equiv 1 \pmod 4$, $x \equiv 0 \pmod 3$, $x \equiv 5 \pmod 7$. 模数 $m_1 = 4, m_2 = 3, m_3 = 7$ 两两互素。故有唯一解模 $M = 4 \times 3 \times 7 = 84$。$M_1 = M/m_1 = 84/4 = 21$。解 $M_1 y_1 \equiv 1 \pmod{m_1}$，即 $21y_1 \equiv 1 \pmod 4 \implies y_1 \equiv 1 \pmod 4$。取 $y_1 = 1$。$M_2 = M/m_2 = 84/3 = 28$。解 $M_2 y_2 \equiv 1 \pmod{m_2}$，即 $28y_2 \equiv 1 \pmod 3 \implies y_2 \equiv 1 \pmod 3$。取 $y_2 = 1$。$M_3 = M/m_3 = 84/7 = 12$。解 $M_3 y_3 \equiv 1 \pmod{m_3}$，即 $12y_3 \equiv 1 \pmod 7 \implies 5y_3 \equiv 1 \pmod 7$。因为 $5 \times 3 = 15 \equiv 1 \pmod 7$，取 $y_3 = 3$。根据 CRT，解为 $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod M$。

$$x \equiv 1 \cdot 21 \cdot 1 + 0 \cdot 28 \cdot 1 + 5 \cdot 12 \cdot 3 \pmod{84}$$

$$x \equiv 21 + 0 + 180 \pmod{84}$$

$$x \equiv 201 \pmod{84}$$

因为 $201 = 2 \times 84 + 33$，所以 $x \equiv 33 \pmod{84}$。

(b). $x \equiv 2 \pmod 4, x \equiv 7 \pmod{10}, x \equiv 1 \pmod 3$. 模数 4 和 10 不互素，$\gcd(4, 10) = 2$。需要检查相容性。$x \equiv 2 \pmod 4 \implies x$ 是偶数。$x \equiv 7 \pmod{10}$。考虑模 2：$x \equiv 7 \equiv 1 \pmod 2 \implies x$ 是奇数。一个数不能同时是奇数和偶数。这两个条件矛盾。因此，该同余方程组无解。

(c). $x \equiv 2 \pmod 3, x \equiv 3 \pmod 5, x \equiv 5 \pmod 2$. 最后一个同余式可简化为 $x \equiv 1 \pmod 2$。方程组为 $x \equiv 2 \pmod 3, x \equiv 3 \pmod 5, x \equiv 1 \pmod 2$. 模数 $m_1 = 3, m_2 = 5, m_3 = 2$ 两两互素。故有唯一解模 $M = 3 \times 5 \times 2 = 30$。$M_1 = M/m_1 = 30/3 = 10$。解 $10y_1 \equiv 1 \pmod 3 \implies y_1 \equiv 1 \pmod 3$。取 $y_1 = 1$。$M_2 = M/m_2 = 30/5 = 6$。解 $6y_2 \equiv 1 \pmod 5 \implies y_2 \equiv 1 \pmod 5$。取 $y_2 = 1$。$M_3 = M/m_3 = 30/2 = 15$。解 $15y_3 \equiv 1 \pmod 2 \implies y_3 \equiv 1 \pmod 2$。取 $y_3 = 1$。解为 $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \pmod M$。

$$x \equiv 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 + 1 \cdot 15 \cdot 1 \pmod{30}$$

$$x \equiv 20 + 18 + 15 \pmod{30}$$

$$x \equiv 53 \pmod{30}$$

因为 $53 = 1 \times 30 + 23$，所以 $x \equiv 23 \pmod{30}$。

(d). $x \equiv 3 \pmod 8, x \equiv 11 \pmod{20}, x \equiv 1 \pmod{15}$. 模数 8, 20, 15 两两不都互素。$\gcd(8, 20) = 4, \gcd(8, 15) = 1, \gcd(20, 15) = 5$。需要检查相容性。从 $x \equiv 3 \pmod 8$ 和 $x \equiv 11 \pmod{20}$ 检查 $\gcd(8, 20) = 4$。$x \equiv 3 \pmod 8 \implies x \equiv 3 \pmod 4$。$x \equiv 11 \pmod{20} \implies x \equiv 11 \equiv 3 \pmod 4$。这两个条件相容。从 $x \equiv 11 \pmod{20}$ 和 $x \equiv 1 \pmod{15}$ 检查 $\gcd(20, 15) = 5$。$x \equiv 11 \pmod{20} \implies x \equiv 11 \equiv 1 \pmod 5$。$x \equiv 1 \pmod{15} \implies x \equiv 1 \pmod 5$。这两个条件相容。从 $x \equiv 3 \pmod 8$ 和 $x \equiv 1 \pmod{15}$ 检查 $\gcd(8, 15) = 1$。自动相容。

因为所有条件都相容，所以方程组有解。我们可以将原方程组分解为关于素数幂的模：$x \equiv 3 \pmod 8$ $x \equiv 11 \pmod{20} \implies x \equiv 11 \pmod 4$

(已包含在 $x \equiv 3 \pmod 8$ 中) 且 $x \equiv 11 \pmod 5 \implies x \equiv 1 \pmod 5$. $x \equiv 1 \pmod{15} \implies x \equiv 1 \pmod 3$ 且 $x \equiv 1 \pmod 5$ (已存在)。简化后的等价方程组为：$x \equiv 3 \pmod 8$ $x \equiv 1 \pmod 3$ $x \equiv 1 \pmod 5$ 模数 $m_1 = 8, m_2 = 3, m_3 = 5$ 两两互素。有唯一解模 $M = 8 \times 3 \times 5 = 120$。$M_1 = M/m_1 = 120/8 = 15$。解 $15y_1 \equiv 1 \pmod 8 \implies -y_1 \equiv 1 \pmod 8 \implies y_1 \equiv -1 \equiv 7 \pmod 8$。取 $y_1 = 7$。$M_2 = M/m_2 = 120/3 = 40$。解 $40y_2 \equiv 1 \pmod 3 \implies y_2 \equiv 1 \pmod 3$。取 $y_2 = 1$。$M_3 = M/m_3 = 120/5 = 24$。解 $24y_3 \equiv 1 \pmod 5 \implies 4y_3 \equiv 1 \pmod 5 \implies -y_3 \equiv 1 \pmod 5 \implies y_3 \equiv -1 \equiv 4 \pmod 5$。取 $y_3 = 4$。解为 $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \pmod M$。

$$x \equiv 3 \cdot 15 \cdot 7 + 1 \cdot 40 \cdot 1 + 1 \cdot 24 \cdot 4 \pmod{120}$$

$$x \equiv 315 + 40 + 96 \pmod{120}$$

$$x \equiv 451 \pmod{120}$$

因为 $451 = 3 \times 120 + 91$，所以 $x \equiv 91 \pmod{120}$。

27 解同余方程组：

$$2x \equiv 3(\mathrm{mod}5), \quad 3x \equiv 1(\mathrm{mod}7).$$

解 先分别解每一个线性同余方程。第一个方程：$2x \equiv 3 \pmod 5$。我们需要找到 2 模 5 的逆元。$2 \times 3 = 6 \equiv 1 \pmod 5$。逆元是 3。方程两边乘以 3：

$$3 \cdot (2x) \equiv 3 \cdot 3 \pmod 5$$

$$6x \equiv 9 \pmod 5$$

$$x \equiv 4 \pmod 5$$

第二个方程：$3x \equiv 1 \pmod 7$。我们需要找到 3 模 7 的逆元。$3 \times 5 = 15 \equiv 1 \pmod 7$。逆元是 5。方程两边乘以 5：

$$5 \cdot (3x) \equiv 5 \cdot 1 \pmod 7$$

$$15x \equiv 5 \pmod 7$$

$$x \equiv 5 \pmod 7$$

现在我们需要解联立方程组：

$$\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$

模数 $m_1 = 5, m_2 = 7$ 互素。有唯一解模 $M = 5 \times 7 = 35$。$M_1 = M/m_1 = 35/5 = 7$。解 $7y_1 \equiv 1 \pmod 5 \implies 2y_1 \equiv 1 \pmod 5$。逆元是 3，所以 $y_1 = 3$。$M_2 = M/m_2 = 35/7 = 5$。解 $5y_2 \equiv 1 \pmod 7$。逆元是 3 ($5 \times 3 = 15 \equiv 1 \pmod 7$)，所以 $y_2 = 3$。根据 **CRT**，解为 $x = a_1M_1y_1 + a_2M_2y_2 \pmod M$。

$$x \equiv 4 \cdot 7 \cdot 3 + 5 \cdot 5 \cdot 3 \pmod{35}$$

$$x \equiv 84 + 75 \pmod{35}$$

$$x \equiv 159 \pmod{35}$$

因为 $159 = 4 \times 35 + 19$，所以 $159 \equiv 19 \pmod{35}$。因此，方程组的解为 $x \equiv 19 \pmod{35}$。

1.4 第六周作业

第四章

13 (a). 求 3^{400} 的最后一位数字；

(b). 求 $\left(12371^{56}+34\right)^{28}$ 被 111 除以后所得的余数.

解

(a). $3^{400} \equiv 3^{4\times 100} \equiv (3^4)^{100} \equiv 1^{100} \equiv 1 \pmod{10}$

故其最后一位数字为 1。

(b). 注意到 $12371 \equiv 111^2 + 50$，因此

$$12371 \equiv 50 \pmod{111}$$

故

$$(12371^{56}+34)^{28} \equiv (50^{56}+34)^{28} \pmod{111}$$

我们有

$$\begin{aligned} 50^2 &\equiv 58 \pmod{111} \\ 50^4 &\equiv 34 \pmod{111} \\ 50^8 &\equiv 46 \pmod{111} \\ 50^{16} &\equiv 7 \pmod{111} \\ 50^{32} &\equiv 49 \pmod{111} \end{aligned}$$

因此

$$50^{56} \equiv 50^{32}\times 50^{16}\times 50^8 \equiv 16 \pmod{111}$$

于是

$$(50^{56}+34)^{28} \equiv 50^{28} \pmod{111}$$

而

$$50^{28} \equiv 50^{16}\times 50^8 \times 50^4 \equiv 70 \pmod{111}$$

综上，其余数为 70。

14 (a). 求 3^{400} 的最后两位数字；

(b). 求 9^{9^9} 的最后两位数字.

解

(a). $\phi(100)=\phi(2^2\times5^2)=\phi(2^2)\phi(5^2)=(4-2)\times(25-5)=40$

由 Euler 定理知

$$3^{\phi(100)}=3^{40}\equiv1 \pmod{100}$$

于是

$$3^{400}\equiv(3^{40})^{10}\equiv1 \pmod{100}$$

故其末两位为 01.

(b). 我们有

$$9^9\equiv9^{2\times4+1}\equiv(9^2)^4\times9\equiv(1)^4\times9\equiv9 \pmod{40}$$

由 Euler 定理知

$$9^{\phi(100)}=9^{40}\equiv1 \pmod{100}$$

因此

$$9^{9^9}\equiv9^9 \pmod{100}$$

对 9, 100 进行辗转相除法，有

$$9^{-1}\equiv89 \pmod{100}$$

而

$$9^9\times9=9^{10}\equiv1 \pmod{100}$$

故

$$9^9\equiv9^{-1}\equiv89 \pmod{100}$$

综上，其最后两位数字为 89

21 当 a 为何值时 $x^3\equiv a(\mathrm{mod}9)$ 有解.

解 遍历 $\mathbb{Z}/9\mathbb{Z}$, 当且仅当 $a\equiv0,1,8 \pmod 9$ 时该方程有解。

28 设 $m_1,m_2,\cdots,m_K$ 两两互素，则同余方程组 $a_ix\equiv b_i\,(\mathrm{mod}m_i)\,,1\leqslant i\leqslant K$ 有解的充要条件是每一个同余方程 $a_ix\equiv b_i\,(\mathrm{mod}m_i)$ 均可解.

证明 必要性显然，下证充分性。

假设 $a_ix\equiv b_i \pmod{m_i},1\leq i\leq k$ 的可解，则

$$(a_i,m_i)\mid b_i$$

令 $d_i=(a_i,m_i),a_i'=\dfrac{a_i}{d_i},b_i'=\dfrac{b_i}{d_i},m_i'=\dfrac{m_i}{d_i}$。

则有

$$a_ix\equiv b_i\pmod{m_i}\Leftrightarrow a_i'x\equiv b_i'\pmod{m_i'}$$

由于 $(a_i',m_i')=1$，故方程有唯一一解

$$x\equiv x_{i,0}\pmod{m_i'}$$

因此，原同余方程组等价于

$$\begin{cases}x\equiv x_{1,0}\pmod{m_1'}\\ x\equiv x_{2,0}\pmod{m_2'}\\ \cdots\\ x\equiv x_{k,0}\pmod{m_k'}\end{cases}$$

对于 $i,j\in\{1,2,\cdots,k\};i\neq j$，取素数 $p\mid(m_i',m_j')$，则 $p\mid m_i$ 且 $p\mid m_j$，而 $(m_i,m_j)=1$。故 p 不存在。

因此

$$(m_i',m_j')=1,1\leq i\neq j\leq k$$

由中国剩余定理知同余方程组有解。

29 设 $(a,b)=1,C>0$，证明一定存在整数 x，使 $(a+bx,C)=1$.

证明 证明：对 C 进行素因子分解

$$C=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

构造如下的同余方程组

$$x\equiv d_i\pmod{p_i},i=1,2,\cdots,k$$

其中，

$$d_i=\begin{cases}0, & p_i\nmid b\\ -ab^{-1}+1\pmod{p_i}, & p_i\mid b\end{cases}$$

由于 $p_1,p_2,\cdots,p_k$ 两两互素，由中国剩余定理知其有唯一解 x_0。

由方程组的构造知

$$a+bx_0\not\equiv 0\pmod{p_i},i=1,2,\cdots,k$$

因此

$$(a+bx_0, C)=1$$

第五章

1 设整数 $\alpha \geqslant 1, p$ 是奇素数，若 $p^{\alpha} \nmid a$，求

$$x^2 \equiv a \pmod{p^{\alpha}}$$

的一切解.

解 (1) 若 $\left(\frac{a}{p}\right)=-1$，则 $x^2 \equiv a \pmod{p}$ 无解，故 $x^2 \equiv a \pmod{p^{\alpha}}$ 无解。

(2) 若 $\left(\frac{a}{p}\right)=1$，则 $x^2 \equiv a \pmod{p}$ 有解，由 Hensel 引理知 $x^2 \equiv a \pmod{p^{\alpha}}$ 恰有两解且在模 p^{α} 意义下互为相反数。

(3) 若 $\left(\frac{a}{p}\right)=0$，设 $a=p^k b$，其中 $1 \leq k < \alpha$ 且 $p \nmid b$

1) 若 $2 \nmid k$，则方程无解。

2) 若 $2 \mid k$，设 $k=2m$，令 $x=p^m y$，则

$$\begin{aligned} & x^2 \equiv a \pmod{p^{\alpha}} \\ \Longleftrightarrow\ & p^{2m} y^2 \equiv p^{2m} b \pmod{p^{\alpha}} \\ \Longleftrightarrow\ & y^2 \equiv b \pmod{p^{\alpha-2m}} \end{aligned}$$

同上，若 $\left(\frac{b}{p}\right)=1$，则恰有两解，设 $y_0^2 \equiv b \pmod{p^{\alpha-2m}}$，则 $x_1 \equiv p^m y_0 \pmod{p^{\alpha}}$，$x_2 \equiv p^m (p^{\alpha-2m}-y_0) \pmod{p^{\alpha}}$。

若 $\left(\frac{b}{p}\right)=-1$，则方程无解。

3 分别写出 $7, 13, 29, 37$ 的全体二次剩余和非剩余.

解

	二次剩余	二次非剩余
7	1, 2, 4	3, 5, 6
13	1, 3, 4, 9, 10, 12	2, 5, 6, 7, 8, 11
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36	2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35

4 设 $p>2$ 为奇素数，证明：

(a). $\left(\dfrac{-1}{p}\right)=1$ 的充要条件是 $p=4n+1$；

(b). $\left(\dfrac{2}{p}\right)=1$ 的充要条件是 $p=8n\pm1$；

(c). $\left(\dfrac{-2}{p}\right)=1$ 的充要条件是 $p=8n+1,8n+3$；并由此进一步证明对任意素数 $p,-1,-2,2$ 中必有一个是 p 的平方剩余.

证明

(a). $\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=1\Leftrightarrow p=4n+1$

(b). $\left(\dfrac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=1\Leftrightarrow p=8n\pm1$

(c). $\left(\dfrac{-2}{p}\right)=\left(\dfrac{-1}{p}\right)\left(\dfrac{2}{p}\right)=(-1)^{\frac{(p-1)(p+5)}{8}}$

$\left(\dfrac{-2}{p}\right)=1\Leftrightarrow p=8n+1,8n+3$

因此，对于任意奇素数 $p,-1,-2,2$ 中必有一个是 p 的二次剩余。

7 设 x,y 为整数，$(x,y)=1$，问：x^2+y^2 的大于 2 的素因子一定具有什么形式？x^2+2y^2 的大于 2 的素因子一定具有什么形式？

解 (1)

$$\begin{aligned}&x^2\equiv-y^2\pmod p\\&\Leftrightarrow\left(\frac{-1}{p}\right)=1\\&\Leftrightarrow p=4n+1\end{aligned}$$

(2)

$$\begin{aligned}&x^2\equiv-2y^2\pmod p\\&\Leftrightarrow\left(\frac{-2}{p}\right)=1\\&\Leftrightarrow p=8n+1,8n+3\end{aligned}$$

1.5 第七周作业

第五章

5 利用上题证明：对任意素数 p，必有整数 x，使

$$p \mid x^8 - 16$$

证明 若 $\left(\frac{2}{p}\right) = 1$ 或 $\left(\frac{-2}{p}\right) = 1$，则有

$$x^2 \equiv 2 \pmod{p} \text{ 或} x^2 \equiv -2 \pmod{p}$$

故

$$x^8 \equiv 16 \pmod{p}$$

若 $\left(\frac{-1}{p}\right) = 1$，则有

$$t^2 \equiv -1 \pmod{p}$$

设 $x = 1 + t$，有

$$\begin{aligned} x^2 &= t^2 + 2t + 1 \equiv 2t \pmod{p} \\ x^4 &\equiv -4 \pmod{p} \\ x^8 &\equiv 16 \pmod{p} \end{aligned}$$

6 证明：同余式 $x^2 + 1 \equiv 0 (\mathrm{mod} p), p = 4m + 1$ 的解是

$$x \equiv (2m)! (\mathrm{mod} p).$$

证明 由 Wilson 定理，知

$$(p-1)! \equiv -1 \pmod{p}$$

即

$$\begin{aligned} [(2m)!]^2 &= 1 \times 2 \times \cdots \times 2m \times (-2m) \times \cdots \times (-1) \\ &= 1 \times 2 \times \cdots \times 2m \times (2m+1) \times \cdots \times (4m) \\ &= (4m)! \\ &\equiv -1 \pmod{p} \end{aligned}$$

8 计算：$\left(\frac{-23}{83}\right), \left(\frac{51}{71}\right), \left(\frac{71}{73}\right), \left(\frac{-35}{97}\right)$.

解

(a).

$$\begin{aligned}\left(\frac{-23}{83}\right) &= \left(\frac{-1}{83}\right)\cdot\left(\frac{23}{83}\right)\\ &= (-1)^{\frac{83-1}{2}}\cdot(-1)\cdot\left(\frac{83}{23}\right)\\ &= \left(\frac{83}{23}\right)\\ &= \left(\frac{-9}{23}\right)\\ &= \left(\frac{-1}{23}\right)\cdot\left(\frac{9}{23}\right)\\ &= (-1)^{\frac{23-1}{2}}\cdot(-1)\cdot\left(\frac{23}{9}\right)\\ &= -1\cdot 1\end{aligned}$$

因此 $\left(\frac{-23}{83}\right) = -1$

(b).

$$\begin{aligned}\left(\frac{51}{71}\right) &= \left(\frac{3}{71}\right)\cdot\left(\frac{17}{71}\right)\\ &= (-1)\cdot\left(\frac{71}{3}\right)\cdot\left(\frac{71}{17}\right)\\ &= (-1)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{3}{17}\right)\\ &= (-1)\cdot(-1)^{\frac{9-1}{8}}\cdot\left(\frac{17}{3}\right)\\ &= (-1)\cdot\left(\frac{2}{3}\right)\\ &= -1\end{aligned}$$

(c).

$$\begin{aligned}\left(\frac{71}{73}\right) &= \left(\frac{73}{71}\right)\\ &= \left(\frac{2}{71}\right)\\ &= (-1)^{\frac{71^2-1}{8}}\\ &= 1\end{aligned}$$

(d).

$$\begin{aligned}\left(\frac{-35}{97}\right) &= \left(\frac{-1}{97}\right)\cdot\left(\frac{35}{97}\right)\\ &= \left(\frac{-1}{97}\right)\cdot\left(\frac{97}{35}\right)\\ &= (-1)^{\frac{97-1}{2}}\cdot(\frac{-1}{35})\cdot(\frac{2}{35})\cdot(\frac{4}{35})\\ &= (-1)^{\frac{35-1}{2}}\cdot(-1)^{\frac{35^2-1}{8}}\cdot 1\\ &= (-1)\cdot(-1)\cdot 1\\ &= 1\end{aligned}$$

9 设 $p>3$ 为素数，证明：

(a). $\left(\frac{3}{p}\right)=1$ 之充要条件为 $p=12n\pm 1$；

(b). $\left(\frac{-3}{p}\right)=1$ 之充要条件为 $p=6n+1$.

证明

(a).

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}\frac{3-1}{2}}=(-1)^{\frac{p-1}{2}}$$

于是

$$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

其中

$$\begin{aligned}\left(\frac{p}{3}\right)=1 &\iff p\equiv 1 \pmod 3\\ \left(\frac{p}{3}\right)=-1 &\iff p\equiv 2 \pmod 3\end{aligned}$$

故

$$\begin{aligned}
&\left(\frac{3}{p}\right)=1\\
\iff\ & p\equiv 3 \pmod 4 \wedge p\equiv 2 \pmod 3\\
\text{或}\ & p\equiv 1 \pmod 4 \wedge p\equiv 1 \pmod 3\\
\iff\ & p\equiv \pm 1 \pmod{12}\\
\iff\ & p=12n\pm 1
\end{aligned}$$

(b).

$$\begin{aligned}
\left(\frac{-3}{p}\right)&=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\\
&=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)\\
&=(-1)^{p-1}\left(\frac{p}{3}\right)
\end{aligned}$$

于是

$$\begin{aligned}
\left(\frac{-3}{p}\right)=1 \Leftrightarrow\ & p\equiv 1 \pmod 2 \wedge p\equiv 1 \pmod 3\\
&\vee p\equiv 0 \pmod 2 \wedge p\equiv 2 \pmod 3\\
&\Leftrightarrow p\equiv 1 \pmod 6\\
&\Leftrightarrow p=6n+1.
\end{aligned}$$

12 设 $p>2$ 为素数，$(a,p)=1$，则

$$\sum_{x=1}^{p}\left(\frac{ax+b}{p}\right)=0.$$

证明

$$\sum_{x=1}^{p}\left(\frac{ax+b}{p}\right)=\sum_{y=1}^{p}\left(\frac{y}{p}\right)=\frac{p-1}{2}-\frac{p-1}{2}+0=0$$

第六章

1 写出模 $3,5,11,13,19$ 的指数表，并指出它们的所有原根.

解

(a). 3 的指数表

$(\mathbb{Z}/3\mathbb{Z})^*$ 的元素 a 及其阶 $\mathrm{ord}_3(a)$ 如下：

$a=1$	$a=2$
$\mathrm{ord}_3(1)=1$	$\mathrm{ord}_3(2)=2$

原根: 2.

(b). 5 的指数表

$(\mathbb{Z}/5\mathbb{Z})^*$ 的元素 a 及其阶 $\mathrm{ord}_5(a)$ 如下：

$a=1$	$a=2$	$a=3$	$a=4$
$\mathrm{ord}_5(1)=1$	$\mathrm{ord}_5(2)=4$	$\mathrm{ord}_5(3)=4$	$\mathrm{ord}_5(4)=2$

原根: 2, 3.

(c). 11 的指数表

$(\mathbb{Z}/11\mathbb{Z})^*$ 的元素 a 及其阶 $\mathrm{ord}_{11}(a)$ 如下：

1	2	3	4	5	6	7	8	9	10
1	10	5	5	5	10	10	10	5	2

原根: 2, 6, 7, 8.

(d). 13 的指数表

$(\mathbb{Z}/13\mathbb{Z})^*$ 的元素 a 及其阶 $\mathrm{ord}_{13}(a)$ 如下：

1	2	3	4	5	6	7
1	12	3	6	4	12	12

8	9	10	11	12
4	3	6	12	2

原根: 2, 6, 7, 11.

(e). 19 的指数表

$(\mathbb{Z}/19\mathbb{Z})^*$ 的元素 a 及其阶 $\mathrm{ord}_{19}(a)$ 如下：

1	2	3	4	5	6	7	8	9
1	18	18	9	9	9	3	6	9

10	11	12	13	14	15	16	17	18
18	3	6	18	18	18	9	9	2

原根: 2, 3, 10, 13, 14, 15.

2 求 $\delta_{43}(7), \delta_{41}(10)$.

解 $\delta_{43}(7) = 6, \delta_{41}(10) = 5$

3 设 p 为素数，$n \geqslant 1, (n, p-1) = 1$. 证明：当 x 通过模 p 的完全系时，x^n 亦通过模 p 的完全系。

证明 证明

设 $f : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*, \quad x \mapsto x^n$.

即证 f 为双射.

取 $(\mathbb{Z}/p\mathbb{Z})^*$ 的一个原根 g, 则

$$f(g^k) = (g^k)^n = g^{kn}$$

由于 $(n, p-1) = 1$, 设

$$h : \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}, \quad k \mapsto kn$$

则 $h \in \mathbf{Aut}(\mathbb{Z}/(p-1)\mathbb{Z})$.

因此, f 为双射. 证毕.

5 设素数 $p > 2$ ，证明：$\delta_p(a) = 2$ 的充要条件是 $a \equiv -1 (\mathrm{mod} p)$.

证明

(a). “ $\Longrightarrow$ ”

若 $\delta_p(a) = 2$, 则

$$\begin{aligned} & a^2 \equiv 1 \pmod{p} \\ \Longleftrightarrow \quad & (a-1)(a+1) \equiv 0 \pmod{p} \\ \Longleftrightarrow \quad & p \mid (a-1) \vee p \mid (a+1) \end{aligned}$$

若 $p \nmid (a+1)$, 则 $\delta_p(a) = 1$, 矛盾, 故

$$p \mid a-1$$

即

$$a \equiv -1 \pmod{p}$$

(b). “$\Longleftarrow$”

若 $a \equiv -1 \pmod{p}$, 则

$$a^2 \equiv 1 \pmod{p}$$

故

$$\delta_p(a) = 2$$

9 设 $n = 2^k, k > 3$，证明：$\delta_n(a) = 2^{k-2}$ 的充要条件是 $a \equiv \pm 3 (\mathrm{mod} 8)$.

证明 对于 $(\mathbb{Z}/2^k\mathbb{Z})^*, k \geq 3$, 有

$$(\mathbb{Z}/2^k\mathbb{Z})^* = \{(-1)^a 5^b \mid a = 0, 1, 0 \leq b < 2^{k-2}\}$$

即

$$(\mathbb{Z}/2^k\mathbb{Z})^* \cong C_2 \times C_{2^{k-2}}$$

对于 $\forall a \in (\mathbb{Z}/2^k\mathbb{Z})^*$, 设

$$a \equiv (-1)^u 5^v \pmod{2^k}$$

其中 $u = 0, 1, 0 \leq v < 2^{k-2}$.

于是

$$\delta_{2^k}(a) = \left[2^u, \frac{2^{k-2}}{(v, 2^{k-2})}\right]$$

(a). “$\Longrightarrow$”

I. 若 $u = 0$, 则 $\delta_{2^k}(a) = \dfrac{2^{k-2}}{(v, 2^{k-2})} = 2^{k-2}$

故 $v \equiv 1 \pmod 2$.

II. 若 $u = 1$, 则 $\delta_{2^k}(a) = \left[2, \dfrac{2^{k-2}}{(v, 2^{k-2})}\right] = 2^{k-2}$. 故 $v \equiv 1 \pmod 2$.

由于 $v \equiv 1 \pmod 2$, 因此

$$5^v \equiv 5 \pmod 8$$

于是

$$a \equiv (-1)^u 5^v \equiv (-1)^u 5 \equiv \pm 5 \equiv \pm 3 \pmod 8$$

(b). “$\Longleftarrow$”

若 $a \equiv \pm 3 \pmod 8$, 则 $v \equiv 1 \pmod 2$, 于是

$$\delta_{2^k}(a) = \left[2^u, \frac{2^{k-2}}{(v, 2^{k-2})}\right] = \left[2^u, 2^{k-2}\right] = 2^{k-2}$$

10 设 $m > 2$ 并有原根存在，证明：

(a). a 是模 m 的二次剩余的充要条件是

$$a^{\varphi(m)/2} \equiv 1 (\mathrm{mod} m);$$

(b). 若 a 是 m 的二次剩余，则 $x^2 \equiv a (\mathrm{mod} m)$ 恰有二解；

(c). 模 m 恰有 $\frac{1}{2}\varphi(m)$ 个二次剩余.

证明 设 g 为 m 的一个原根, 则 $(\mathbb{Z}/m\mathbb{Z})^* = \langle g \rangle$.

(a). 设 $a \equiv g^k \pmod m, 0 < k \leq \varphi(m)$.

则

$$\begin{aligned}
&\exists x : x^2 \equiv a \pmod m \\
\Longleftrightarrow\ &\exists 0 < j \leq \varphi(m) : g^{2j} \equiv g^k \pmod m \\
\Longleftrightarrow\ &\exists 0 < j \leq \varphi(m) : 2j \equiv k \pmod{\varphi(m)} \\
\Longleftrightarrow\ &(2, \varphi(m)) \mid k
\end{aligned}$$

而 $2 \mid \varphi(m)$, 故 $2 \mid k$. 设 $k = 2t$, 于是

$$a^{\frac{\varphi(m)}{2}} \equiv (g^{2t})^{\frac{\varphi(m)}{2}} \equiv g^{t\varphi(m)} \equiv (g^{\varphi(m)})^t \equiv 1 \pmod m$$

(b). 设 $a = g^{2t}, x = g^j \pmod m$ 为其中一解, 则

$$\begin{aligned}
&x^2 \equiv a \pmod m \\
\Longleftrightarrow\ &\exists 0 < j \leq \varphi(m) : j \equiv t \pmod{\frac{\varphi(m)}{2}} \\
\Longleftrightarrow\ &x \equiv g^j \pmod m \vee x \equiv g^{j+\frac{\varphi(m)}{2}} \pmod m
\end{aligned}$$

恰有二解.

(c). 即在 $1, 2, 3, \ldots, \varphi(m)$ 中的偶数个数

$$\frac{\varphi(m)}{2}$$

11 设素数 $p > 2$，若 g 为模 p 的原根，且

$$g^{p-1} \equiv 1 \left(\mathrm{mod} p^2\right)$$

则 g 不是 p^k 的原根，$k \geqslant 2$.

证明 使用反证法.

若 g 为 p^k 的原根, 则 $g + p$ 亦为 p^k 的原根. g 为 p 的原根.

若 $g^{p-1} \equiv 1 \pmod{p^2}$, 则

$$\begin{aligned}(g+p)^{p-1} &\equiv g^{p-1} + \binom{p-1}{1} g^{p-2} p \pmod{p^2} \\ &\equiv 1 + (p-1) g^{p-2} p \pmod{p^2}\end{aligned}$$

由于 $p^2 \nmid (p-1) g^{p-2} p$, 故

$$(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$$

因此存在 p^k 的原根 g 使之为 p 的原根且 $g^{p-1} \not\equiv 1 \pmod{p^2}$.

12 (a). 若 $q = 4k+1, p = 2q+1$ 均为素数，则 2 是 p 的原根；

(b). 若 $q = 2k+1 (k > 1), p = 2q+1$ 均为素数，则 $-3, -4$ 均为 p 的原根.

证明

(a). 对于 2^2, 由于 $p = 2q+1 = 8k+3 \geq 11$, 故 $2^2 \not\equiv 1 \pmod{p}$.

而

$$2^q \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

其中

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$$

故

$$2^q \not\equiv 1 \pmod{p}$$

又由 Lagrange 定理知 $\operatorname{ord}(2) \mid \varphi(p) = 2q$, 故 $\operatorname{ord}(2) = 2q$.

故 2 是 p 的原根.

(b). I. -3 为 p 的原根.

对于 $(-3)^2$, 由于 $p = 2q+1 = 4k+3 \geq 11$, 故 $(-3)^2 \not\equiv 1 \pmod{p}$.

若 $(-3)^q \equiv (-3)^{\frac{p-1}{2}} \equiv \left(\frac{-3}{p}\right) \equiv 1 \pmod{p}$, 则 $p \equiv 1 \pmod{6}$.

而 $p = 4k+3 \not\equiv 1 \pmod{6}$.

故 $\left(\frac{-3}{p}\right) \not\equiv 1 \pmod{p}$.

由 Lagrange 定理知 $\operatorname{ord}(-3) \mid \varphi(p) = 2q$, 故 $\operatorname{ord}(-3) = 2q$.

即 -3 为 p 的原根.

II. -4 为 p 的原根.

对于 $(-4)^2$, 由于 $p = 2q+1 = 4k+3 \geq 11, \ldots$, 故 $(-4)^2 \not\equiv 1$

$(\mathrm{mod}\ p)$.

若 $(-4)^q \equiv (-4)^{\frac{p-1}{2}} \equiv \left(\dfrac{-4}{p}\right) \equiv 1\ (\mathrm{mod}\ p)$.

而

$$\begin{aligned}\left(\frac{-4}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2 \\ &= (-1)^{\frac{p-1}{2}} \cdot 1 \\ &= (-1)^q \cdot 1 \\ &= -1\end{aligned}$$

故 $(-4)^q \not\equiv 1\ (\mathrm{mod}\ p)$.

由 **Lagrange** 定理知 $\mathrm{ord}(-4) \mid \varphi(p) = 2q$, 故 $\mathrm{ord}(-4) = 2q$.

即 -4 为 p 的原根.