妮可代数结构答案

En 土土

2023 年 3 月 21 日

目录

1 集合

1.1

(1) 不相等.

(2) 相等.

(3) 相等.

1.2

证明.

$$\begin{cases} A \subseteq B \Rightarrow \forall\, x \in A,\ x \in B. \\[2em] B \subset C \Rightarrow \begin{cases} \forall\, x \in B,\ x \in C \\[1em] \exists\, x \in C,\ x \notin B \end{cases} \end{cases} \Rightarrow \begin{cases} \forall\, x \in A,\ x \in C \\[1em] \exists\, x \in C,\ x \notin A \end{cases} \Rightarrow A \subset C.$$

$\square$

1.3

(1) 不成立.

(2) 不成立.

(3) 不成立.

(4) 成立.

(5) 成立.

(6) 不成立.

1.4

(1) 不成立.

(2) 成立.

(3) 成立.

1.5

证明.

  (1)
$$A \cap \left(\overline{A} \cup B\right) = \left(A \cap \overline{A}\right) \cup (A \cap B) = \varnothing \cup (A \cap B) = A \cap B.$$

  (2)
$$A \cup (A \cap B) = (A \cup A) \cap (A \cup B) = A \cap (A \cup B).$$

$$\begin{cases} A \subseteq A \cup (A \cap B) \\ A \supseteq A \cap (A \cup B) \end{cases} \Rightarrow A \cup (A \cap B) = A.$$

  (3) (a)

$$\begin{aligned} \forall\, x \in \overline{\bigcap_i A_i} &\Rightarrow x \notin \bigcap_i A_i \\ &\Rightarrow \exists 1 \le k \le n, x \notin A_k \\ &\Rightarrow \exists 1 \le k \le n, x \in \overline{A_k} \\ &\Rightarrow x \in \bigcup_i \overline{A_i} \\ &\Rightarrow \overline{\bigcap_i A_i} \subseteq \bigcup_i \overline{A_i} \end{aligned} \qquad \begin{aligned} \forall\, x \in \bigcup_i \overline{A_i} &\Rightarrow \exists 1 \le k \le n, x \in \overline{A_k} \\ &\Rightarrow \exists 1 \le k \le n, x \notin A_k \\ &\Rightarrow x \notin \bigcap_i A_i \\ &\Rightarrow x \in \overline{\bigcap_i A_i} \\ &\Rightarrow \bigcup_i \overline{A_i} \subseteq \overline{\bigcap_i A_i} \end{aligned}$$

即证 $\overline{\bigcap_i A_i} = \bigcup_i \overline{A_i}.$

    (b)

$$\begin{aligned} \forall\, x \in \overline{\bigcup_i A_i} &\Rightarrow x \notin \bigcup_i A_i \\ &\Rightarrow \forall 1 \le k \le n, x \notin A_k \\ &\Rightarrow \forall 1 \le k \le n, x \in \overline{A_k} \\ &\Rightarrow x \in \bigcap_i \overline{A_i} \\ &\Rightarrow \overline{\bigcup_i A_i} \subseteq \bigcap_i \overline{A_i} \end{aligned} \qquad \begin{aligned} \forall\, x \in \bigcap_i \overline{A_i} &\Rightarrow \forall 1 \le k \le n, x \in \overline{A_k} \\ &\Rightarrow \forall 1 \le k \le n, x \notin A_k \\ &\Rightarrow x \notin \bigcup_i A_i \\ &\Rightarrow x \in \overline{\bigcup_i A_i} \\ &\Rightarrow \bigcap_i \overline{A_i} \subseteq \overline{\bigcup_i A_i} \end{aligned}$$

即证 $\overline{\bigcup_i A_i} = \bigcap_i \overline{A_i}.$

$\square$

1.6

证明.

(1) $B \subseteq C \Rightarrow \forall x \in B, x \in C.$

$$\forall x \in (A \cap B), x \in A且 x \in B \Rightarrow x \in A且 x \in C \Rightarrow x \in (A \cap C)$$

(2)

$$
\begin{aligned}
A \subseteq C, \ B \subseteq \ C \ &\Leftrightarrow A \cup C = C, \ B \cup C = C \\
&\Leftrightarrow (A \cup B) \cup C = A \cup (B \cup C) = A \cup C = C \\
&\Leftrightarrow (A \cup B) \subseteq C.
\end{aligned}
$$

(3) 若 $|A \cup B| > |A| + |B|$, 则 $\exists x \in (A \cup B)$, 且 $x \notin A, x \notin B$, 矛盾.

   $|A \cup B| = |A| + |B| - |A \cap B|, |A \cup B| = |A| + |B|$ 当且仅当 $A \cap B = \phi$ 时.

$\square$

1.7

(1) 设所求集合为 E.

   1.（基础语句）令 $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$，若 $x \in D$，则 $x \in E$.

   2.（归纳语句）若 $x, \ y \in E$，则 x 与 y 的连接 $\overline{xy} \in E$.

   3.（终结语句）$x \in E$，当且仅当 x 是由有限次 $1, 2$ 得到的.

(2) 设所求集合为 E.

   1.（基础语句）令 $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$，若 $x \in D$，则 $x. \in E, \ .x \in E$.

   2.（归纳语句）若 $x = a.b, \ y = c.d \in E$，则 $\overline{ac}.\overline{bd} \in E$.

   3.（终结语句）$x \in E$，当且仅当 x 是由有限次 $1, 2$ 得到的.

(3) 设所求集合为 E.

   1.（基础语句）$0, \ 10 \in \ E$.

   2.（归纳语句）若 $x = \overline{A0} \in \ E \ (x \neq 0)$，则 $\overline{A00}, \ \overline{A10} \in \ E$.

   3.（终结语句）$x \in \ E$，当且仅当 x 是由有限次 $1, 2$ 得到的.

2 数论初步

2.1

证明.

(1)

$$\forall\ x|a,\ x|b \begin{cases} x > 0 & \xrightarrow{a>0,x|a} x \le a \\ x < 0 & \xrightarrow{a>0} x < a \end{cases} \Rightarrow\ x < a\ \xrightarrow{a|a,a|b} (a,b) = a.$$

(2)

$$\begin{cases} (a,b)|(a,b),\ (a,b)|b \\ \\ \forall\ x|(a,b),\ x|b,\ 有x \le (a,b).\quad (证明同(1)) \end{cases} \Rightarrow\ ((a,b),b) = (a,b).$$

$\square$

2.2

证明.

(1) 不妨假设 $\exists\, n > 0,\ (n, n+1) = d > 1$

$$\begin{aligned} (n, n+1) = d &\Rightarrow \exists\, x, y \in \mathbb{Z},\ n = xd, n+1 = yd \\ &\Rightarrow 1 = (n+1) - n = (y - x)d > 0 \\ &\Rightarrow y > x,\ (y-x)d \ge d > 1 \\ &\Rightarrow 矛盾,假设不成立. \end{aligned}$$

(2) 可取 (n, k),证明如下

由推论 2.3,取$x = 1,\ a = n,\ b = k$,有$(n, k) = (n, n+k)$.

$\square$

2.3

(1) $(314, 159) = 1$，有解。由辗转相除法

$$314 = 159 \cdot 1 + 155$$
$$159 = 155 \cdot 1 + 4$$
$$155 = 4 \cdot 38 + 3$$
$$4 = 3 \cdot 1 + 1$$

即

$$
\begin{aligned}
1 &= 4 - 3 \cdot 1 \\
&= 4 - (155 - 4 \cdot 38) \cdot 1 \\
&= (159 - 155 \cdot 1) \cdot 39 - 155 \\
&= 159 \cdot 39 - 155 \cdot 40 \\
&= 159 \cdot 39 - (314 - 159 \cdot 1) \cdot 40 \\
&= 159 \cdot 79 - 314 \cdot 40.
\end{aligned}
$$

即 $x = -40, y = 79.$

(2) $(3141, 1592) = 1$，有解。由辗转相除法

$$3141 = 1592 \cdot 1 + 1549$$
$$1592 = 1549 \cdot 1 + 43$$
$$1549 = 43 \cdot 36 + 1$$

即

$$
\begin{aligned}
1 &= 1549 - 43 \cdot 36 \\
&= 1549 - (1592 - 1549 \cdot 1) \cdot 36 \\
&= 1549 \cdot 37 - 1592 \cdot 36 \\
&= (3141 - 1592 \cdot 1) \cdot 37 - 1592 \cdot 36 \\
&= 3141 \cdot 37 - 1592 \cdot 73.
\end{aligned}
$$

即 $x = 37, y = -73.$

2.4

证明.

(0) $n = 1, n^3 - n = 0$，有 $0 = 6 \cdot 0, 6|(n^3 - n)$.

(1) $n = 2, n^3 - n = 0$，有 $6 = 6 \cdot 1, 6|(n^3 - n)$.

(2) 假设 $n = k, k \in \mathbb{N}$ 时，有 $6|(k^3 - k)$，则 $n = k + 1$ 时有

$$
\begin{aligned}
(k+1)^3 - (k+1) &= k^3 + 3k^2 + 2k \\
&= (k^3 - k) + 3k(k+1)
\end{aligned}
$$

显然有 $6|(k^3 - k)$，下证 $6|3k(k+1)$

  $1°$ $k = 1, 3k(k+1) = 6$，有 $6 = 6 \cdot 1, 6|3k(k+1)$

  $2°$ 若 $6|3k(k+1)$，则

$$3(k+1)(k+2) = 3k(k+1) + 6(k+1) \ \Rightarrow \ 6|3(k+1)(k+2)$$

即证

$$\forall \ k \in \mathbb{N} \ 6|3k(k+1) \ \Rightarrow \ 6|(k+1)^3 - (k+1)$$

综上, 即证

$$\forall \ n > 0, \ 6|(n^3 - n).$$

$\square$

2.5

证明.

$$
\begin{cases}
3^4 \equiv 1(\mathrm{mod}10) & \Rightarrow \ 3^{4n} \equiv 1(\mathrm{mod}10) \\
& \qquad\qquad\qquad\qquad\qquad \Rightarrow 3^{m+4n} \equiv (-1)(\mathrm{mod}10). \\
10|(3^m + 1) & \Rightarrow \ 3^m \equiv (-1)(\mathrm{mod}10)
\end{cases}
$$

即证

$$10|(3^{m+4n} + 1)$$

$\square$

2.6

(1)
$$2345 = 5 \cdot 7 \cdot 67$$

(2)
$$3456 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$$

2.7

证明. 不妨假设 $\exists\, n > 0$，使得 $n(n+1) = d^2$ 为平方数，则有

$$n^2 < n(n+1) = d^2 < (n+1)^2 \;\Rightarrow\; n < d < n+1$$

不存在相邻整数间的整数，d 不存在，假设不成立，即证. $\qquad\square$

2.8

证明. $\qquad n = 5! + 1 = 2 \cdot 3 \cdot 4 \cdot 5 + 1.$

(1)
$$n+1 = 2 \cdot 3 \cdot 4 \cdot 5 + 2 = 2 \cdot (3 \cdot 4 \cdot 5 + 1)$$

(2)
$$n+2 = 2 \cdot 3 \cdot 4 \cdot 5 + 3 = 3 \cdot (2 \cdot 4 \cdot 5 + 1)$$

(3)
$$n+3 = 2 \cdot 3 \cdot 4 \cdot 5 + 4 = 4 \cdot (2 \cdot 3 \cdot 5 + 1)$$

(4)
$$n+4 = 2 \cdot 3 \cdot 4 \cdot 5 + 5 = 5 \cdot (2 \cdot 3 \cdot 4 + 1)$$

$\qquad\square$

2.9

(1) $(1,1) = 1|2$，方程有解，$x_0 = 0, y_0 = 2$ 为一组特解，故通解为

$$\begin{cases} x & = \; t \quad (t \in \mathbb{Z}) \\ y & = \; 2 - t \end{cases}$$

(2) $(2,1) = 1|2$，方程有解，$x_0 = 0, y_0 = 2$ 为一组特解，故通解为

$$\begin{cases} x &= t \quad (t \in \mathbb{Z}) \\ y &= 2 - 2t \end{cases}$$

(3) $(15,16) = 1|17$，方程有解，$x_0 = -17, y_0 = 17$ 为一组特解，故通解为

$$\begin{cases} x &= 16t - 17 \quad (t \in \mathbb{Z}) \\ y &= 17 - 15t \end{cases}$$

2.10

(1) $(6, -15) = 3|51$，方程有解，$x_0 = 11, y_0 = 1$ 为一组特解，故通解为

$$\begin{cases} x &= 11 - 5t \quad (t \in \mathbb{Z}) \\ y &= 1 - 2t \end{cases}$$

又要求负整数解，故 $x, y < 0$, $t \geq 3$，即所以负整数解为

$$\begin{cases} x &= 11 - 5t \quad (t \in \mathbb{Z}, \ t \geq 3) \\ y &= 1 - 2t \end{cases}$$

(2) $(6, 15) = 3|51$，方程有解，$x_0 = 6, y_0 = 1$ 为一组特解，故通解为

$$\begin{cases} x &= 6 + 5t \quad (t \in \mathbb{Z}) \\ y &= 1 - 2t \end{cases}$$

又要求负整数解，故 $x, y < 0$, t 无解，即无负整数解.

2.11

必须要用 30 张

设需要 x 张 5 分，y 张 1 角，$z = (30 - x - y)$ 张 2 角五分. 有

$$0.05x + 0.1y + 0.25(30 - x - y) = 5 \iff x + 2y + 5(30 - x - y) = 100$$
$$\iff 4x + 3y = 50$$

$(4, 3) = 1|50$，方程有解，$x_0 = 2, y_0 = 14$ 为一组特解，故通解为

$$\begin{cases} x & = 2 + 3t \quad (t \in \mathbb{Z}) \\ y & = 14 - 4t \end{cases}$$

又 $x, y, z \in \mathbb{N}$，即

$$\begin{cases} 2 + 3t & \geq 0 \\ 14 - 4t & \geq 0 \xrightarrow{t \in \mathbb{Z}} t = 0, 1, 2, 3. \\ 14 + t & \geq 0 \end{cases}$$

即有 4 种方案，记 x 张 5 分，y 张 1 角，z 张 2 角五分，则方案为

$$\begin{cases} x & = 2 \\ y & = 14 \\ z & = 14 \end{cases} \quad \begin{cases} x & = 5 \\ y & = 10 \\ z & = 15 \end{cases} \quad \begin{cases} x & = 8 \\ y & = 6 \\ z & = 16 \end{cases} \quad \begin{cases} x & = 11 \\ y & = 2 \\ z & = 17 \end{cases}$$

不多于 30 张

即求 $a, b, c \in \mathbb{N}, 0.05a + 0.1b + 0.25c = 5$, 且 $a + b + c \leq 30$. 即解

$$\begin{cases} a + 2b + 5c = 100 \\ (a + b + c) \leq 30 \\ a, b, c \in \mathbb{N} \end{cases}$$

(1) $c \leq 13$

$$a + 2b + 5c < 2 \cdot (30 - c) + 5c = 3c + 60 \leq 99 < 100, \text{无解}.$$

(2) $c > 20$

$$a + 2b + 5c > 5c > 100, \text{无解}.$$

(3) 由 (1)(2) 可知 $14 \leq c \leq 20$

$$a + 2b = 100 - 5c, (1, 2) = 1|100 - 5c \Rightarrow \text{方程存在解}.$$

又 $a = 100 - 5c, b = 0$ 为一组特解，故通解为

$$\begin{cases} a = 100 - 5c - 2t; \\ b = t. \ (t \in \mathbb{N}) \end{cases}$$

10

$$
\begin{cases} a+b+c=100-4k-t & \le 30 \\ a=100-5c-2t & \ge 0 \end{cases} \Rightarrow \begin{cases} t \ge 70-4k \\ \\ t \le [\dfrac{100-5k}{2}] \end{cases}
$$

即解的组数为

$$
\begin{cases} \left[\dfrac{100-5k}{2}\right] - (70-4k) + 1; & (70-4k \ge 0) \\ \\ \left[\dfrac{100-5k}{2}\right] + 1. & (70-4k < 0) \end{cases}
$$

(a) $(c=14)$ 解的组数为 $\left[\dfrac{100-5\times14}{2}\right] - (70-4\times14) + 1 = 2$

(b) $(c=15)$ 解的组数为 $\left[\dfrac{100-5\times15}{2}\right] - (70-4\times15) + 1 = 3$

(c) $(c=16)$ 解的组数为 $\left[\dfrac{100-5\times16}{2}\right] - (70-4\times16) + 1 = 5$

(d) $(c=17)$ 解的组数为 $\left[\dfrac{100-5\times17}{2}\right] - (70-4\times17) + 1 = 6$

(e) $(c=18)$ 解的组数为 $\left[\dfrac{100-5\times18}{2}\right] + 1 = 6$

(f) $(c=19)$ 解的组数为 $\left[\dfrac{100-5\times19}{2}\right] + 1 = 3$

(g) $(c=20)$ 解的组数为 $\left[\dfrac{100-5\times20}{2}\right] + 1 = 1$

即共有 $2+3+5+6+6+3+1=26$ 种兑换方法.

2.12

设买了 x 个苹果, $12-x$ 个橘子, 每个苹果 y 分钱, 每个橘子 $y-3$ 分钱, 则有

$$
\begin{cases} 0 \le 12-x < x \\ xy+(12-x)(y-3)=99 \end{cases} \Leftrightarrow \begin{cases} 6 < x \le 12 \\ x+4y=45 \end{cases}
$$

$(1,4)=1|45$, 方程有解, $x_0=9, y_0=9$ 为一组特解, 故通解为

$$
\begin{cases} x & = 9+4t \quad (t \in \mathbb{Z}) \\ y & = 9-t \end{cases}
$$

又 $6 < x \le 12$, 即 $t=0$, $x=9, 12-x=3$, 买了 9 个苹果和 3 个橘子.

2.13

$$6k + 5 \equiv 6k + 1 (\mathrm{mod}4)$$

又 $6k \equiv 6(\mathrm{mod}4)$，有

$$6k + 5 \equiv 7(\mathrm{mod}4)$$
$$\equiv 3(\mathrm{mod}4)$$

2.14

证明.

(1) 分情况讨论 $6k, 6k+2, 6k+3, 6k+4$ $(k \geq 1)$ 即可，不再赘述.

(2) 记素数为 $p, p > 3$.

    (a) $p < 6$，则 $p = 5$，成立.

    (b) $p > 6$，有 $(6, p) = 1$，故 p 属于 6 的缩系，故 p 模 6 或与 1 或 5 同余.

$\square$

2.15

证明.

不妨设这两个连续的立方数为 k^3 与 $(k+1)^3$.

$$(k+1)^3 - k^3 \equiv 3k^2 + 3k + 1 (\mathrm{mod}3)$$
$$\equiv 1 (\mathrm{mod}3)$$

$\square$

2.16

证明.

设该数为 $A = \overline{a_n a_{n-1} \ldots a_1 a_0}$，则

$$A = \sum_{i=0}^{i=n} a_i \cdot 10^i, \quad \sum_{i=0}^{i=n} a_i \equiv 0 (\mathrm{mod}3)$$

又 $\forall\, k \in \mathbb{N},\ 10^i \equiv 1(\mathrm{mod}3)$，故

$$A \equiv \sum_{i=0}^{i=n} a_i \cdot 10^i (\mathrm{mod}3)$$
$$\equiv \sum_{i=0}^{i=n} a_i (\mathrm{mod}3)$$
$$\equiv 0(\mathrm{mod}3)$$

$\square$

2.17

证明.

(1)
$$10 \equiv -1(\mathrm{mod}11) \ \Rightarrow\ 10^k \equiv (-1)^k(\mathrm{mod}11)$$

(2) 设数为 $A = \overline{a_n a_{n-1} \ldots a_1 a_0}$，则

$$A \equiv 0(\mathrm{mod}11) \ \Leftrightarrow\ \sum_{i=0}^{n} (-1)^i \cdot a_i \equiv 0(\mathrm{mod}11)$$

即偶数位之和与奇数位之和的差能被 11 整除等价于该数也能被 11 整除.

$\square$

2.18

(1)
$$2x \equiv 1(\mathrm{mod}17) \qquad \xrightarrow{(2,17)=1}\ x \equiv 9(\mathrm{mod}17)$$
$$\equiv 18(\mathrm{mod}17)$$

(2) $(3,18) = 3|6$，故有 3 组解由 $x \equiv 2(\mathrm{mod}6)$ 得原方程解为

$$x \equiv 2 + 6t(\mathrm{mod}18) \quad (0 \le t \le 2).$$

即

$$x \equiv 2, 8, 14(\mathrm{mod}18).$$

(3) $(4, 18) = 2 | 6$，故有 2 组解解 $2x \equiv 3(\mathrm{mod}9)$

$$2x \equiv 3(\mathrm{mod}9) \atop \equiv 12(\mathrm{mod}9) \xrightarrow{(2,9)=1} x \equiv 6(\mathrm{mod}9).$$

即原方程解为

$$x \equiv 6 + 9t(\mathrm{mod}18) \quad (t = 0, 1) \ \Rightarrow \ x \equiv 6, 15(\mathrm{mod}18).$$

(4)

$$3x \equiv 1(\mathrm{mod}17) \atop \equiv 18(\mathrm{mod}17) \xrightarrow{(3,17)=1} x \equiv 6(\mathrm{mod}17).$$

2.19

(1) $(2, 3) = 1$，有解。本题中

$$M = 2 \cdot 3 = 6, M_1 = 3, M_2 = 2.$$

由

$$\begin{cases} 3b_1 & \equiv 1(\mathrm{mod}2) \\ 2b_2 & \equiv 1(\mathrm{mod}3) \end{cases} \Rightarrow \begin{cases} b_1 & = 1 \\ b_2 & = 2 \end{cases}$$

从而

$$y = 3 \cdot 1 \cdot 1 + 2 \cdot 1 \cdot 2 \atop = 7 \ \Rightarrow \ y \equiv 1(\mathrm{mod}6).$$

(2) $(41, 26) = 1$，有解。原式等价于

$$\begin{cases} x \equiv & 31(\mathrm{mod}41) \\ x \equiv & 7(\mathrm{mod}26) \end{cases}$$

本题中

$$M = 41 \cdot 26, M_1 = 26, M_2 = 41.$$

由

$$\begin{cases} 26b_1 & \equiv 1(\mathrm{mod}41) \\ 41b_2 & \equiv 1(\mathrm{mod}26) \end{cases} \Rightarrow \begin{cases} b_1 & = 30 \\ b_2 & = 7 \end{cases}$$

从而

$$y = 26 \cdot 31 \cdot 30 + 41 \cdot 7 \cdot 7$$
$$= 26819$$
$$\Rightarrow \ y \equiv 605 (\text{mod} 1066).$$

(3) $(2,3) = (2,7) = (3,7) = 1$，有解。本题中

$$M = 2 \cdot 3 \cdot 7 = 42, M_1 = 21, M_2 = 14, M_3 = 6.$$

由

$$\begin{cases} 21b_1 & \equiv 1(\text{mod} 2) \\ 14b_2 & \equiv 1(\text{mod} 3) \ \Rightarrow \\ 6b_3 & \equiv 1(\text{mod} 7) \end{cases} \begin{cases} b_1 & = 1 \\ b_2 & = 2 \\ b_3 & = 6 \end{cases}$$

从而

$$y = 21 \cdot 1 \cdot 1 + 14 \cdot 1 \cdot 2 + 6 \cdot 6 \cdot 6$$
$$= 265.$$
$$\Rightarrow \ y \equiv 13 (\text{mod} 42).$$

(4) 原式等价于

$$\begin{cases} x & \equiv 3(\text{mod} 5) \\ x & \equiv 3(\text{mod} 7) \\ x & \equiv 3(\text{mod} 11) \end{cases}$$

$(5,7) = (5,11) = (7,11) = 1$，有解。本题中

$$M = 5 \cdot 7 \cdot 11 = 385, M_1 = 77, M_2 = 55, M_3 = 35$$

由

$$\begin{cases} 77b_1 \equiv & 1(\text{mod} 5) \\ 55b_2 \equiv & 1(\text{mod} 7) \ \Rightarrow \\ 35b_3 \equiv & 1(\text{mod} 11) \end{cases} \begin{cases} b_1 & = 3 \\ b_2 & = 6 \\ b_3 & = 6 \end{cases}$$

从而

$$y = 77 \cdot 3 \cdot 3 + 55 \cdot 3 \cdot 6 + 35 \cdot 3 \cdot 6$$
$$= 2313.$$
$$\Rightarrow \ y \equiv 3 (\text{mod} 385).$$

2.20

设

$$\begin{cases} 3x \equiv m-1 & \pmod{20} \\ 5y \equiv m & \pmod{20} \qquad (1 \le m \le 18) \\ 7z \equiv m+1 & \pmod{20}. \end{cases}$$

则

$$\begin{cases} 3x & = 20(m-1)+(m-1) \\ 5y & = 20m+m \\ 7z & = 20(m+1)+(m+1). \end{cases} \Rightarrow \begin{cases} x & = 7m-7 \\ y & = \dfrac{21m}{5} \\ z & = 3m+3. \end{cases} \Rightarrow 5|m, m \in \{5,10,15\}$$

即

$$\begin{cases} x & = 28 \\ y & = 21 \\ z & = 18; \end{cases} \quad \begin{cases} x & = 63 \\ y & = 42 \\ z & = 33; \end{cases} \quad \begin{cases} x & = 98 \\ y & = 63 \\ z & = 48. \end{cases}$$

2.21

由题意有

$$\begin{cases} n & \equiv 0 \pmod 2 \\ n+1 & \equiv 0 \pmod 3 \\ n+2 & \equiv 0 \pmod 4 \iff \\ n+3 & \equiv 0 \pmod 5 \\ n+4 & \equiv 0 \pmod 6 \end{cases} \begin{cases} n & \equiv 0 \pmod 2 \\ n & \equiv 2 \pmod 3 \\ n & \equiv 2 \pmod 4 \\ n & \equiv 2 \pmod 5 \\ n & \equiv 2 \pmod 6 \end{cases}$$

由 $n=2$ 为一个特解，有模 $[2,3,4,5,6]=60$ 唯一解

$$n \equiv 2 \pmod{60}$$

故所求最小整数 $n(n>2)$ 为

$$n = 62.$$

2.22

(1)
$$\phi(42) = \phi(2 \cdot 3 \cdot 7) = \phi(2) \cdot \phi(3) \cdot \phi(7) = 1 \cdot 2 \cdot 6 = 12.$$

(2)
$$\phi(420) = \phi(2^2 \cdot 3 \cdot 5 \cdot 7) = \phi(2^2) \cdot \phi(3) \cdot \phi(5) \cdot \phi(7) = 2 \cdot 2 \cdot 4 \cdot 6 = 96.$$

(3)
$$\phi(4200) = \phi(2^3 \cdot 3 \cdot 5^2 \cdot 7) = \phi(2^3) \cdot \phi(3) \cdot \phi(5^2) \cdot \phi(7) = 4 \cdot 2 \cdot 20 \cdot 6 = 960.$$

2.23

(1) 小于 18 且与 18 互素的正整数有

$$1, 5, 7, 11, 13, 17$$

(2)

$$1 \cdot 5 \equiv 5 (\mathrm{mod} 18) \qquad 5 \cdot 5 \equiv 25 (\mathrm{mod} 18)$$
$$\equiv 7 (\mathrm{mod} 18)$$

$$7 \cdot 5 \equiv 35 (\mathrm{mod} 18) \qquad 11 \cdot 5 \equiv 55 (\mathrm{mod} 18)$$
$$\equiv 17 (\mathrm{mod} 18) \qquad \equiv 1 (\mathrm{mod} 18)$$

$$13 \cdot 5 \equiv 65 (\mathrm{mod} 18) \qquad 17 \cdot 5 \equiv 85 (\mathrm{mod} 18)$$
$$\equiv 11 (\mathrm{mod} 18) \qquad \equiv 13 (\mathrm{mod} 18)$$

仍为缩系，引理 2.1 成立.

2.24

设 m, n 有素数分解

$$m = m_1^{k_1} m_2^{k_2} \cdots m_x^{k_x} \cdot p^M, \quad n = n_1^{l_1} n_2^{l_2} \cdots n_y^{l_y} \cdot p^N$$

且

$$\forall \, 1 \leq i \leq x, 1 \leq j \leq y, 有 m_i \neq n_j. \qquad (m_i, n_j 均为素数)$$

$$\phi(mn) = \phi\left(p^{M+N} \cdot \prod_{i=1}^{x} m_i^{k_i} \cdot \prod_{j=1}^{y} n_j^{l_j}\right)$$

$$= \phi(p^{M+N}) \cdot \prod_{i=1}^{x} \phi(m_i^{k_i}) \cdot \prod_{j=1}^{y} \phi(n_j^{l_j})$$

$$= p^{M+N} \cdot (1 - \frac{1}{p}) \cdot \prod_{i=1}^{x} m_i^{k_i}(1 - \frac{1}{m_i}) \cdot \prod_{j=1}^{y} n_j^{l_j}(1 - \frac{1}{n_j})$$

$$= mn \cdot (1 - \frac{1}{p}) \cdot \prod_{i=1}^{x} (1 - \frac{1}{m_i}) \cdot \prod_{j=1}^{y} (1 - \frac{1}{n_j})$$

$$\phi(m)\phi(n) = \phi\left(p^{M} \cdot \prod_{i=1}^{x} m_i^{k_i}\right) \cdot \phi\left(p^{N} \cdot \prod_{j=1}^{y} n_j^{l_j}\right)$$

$$= \phi(p^{M}) \cdot \phi(p^{N}) \cdot \prod_{i=1}^{x} \phi(m_i^{k_i}) \cdot \prod_{j=1}^{y} \phi(n_j^{l_j})$$

$$= p^{M} \cdot (1 - \frac{1}{p}) \cdot p^{N} \cdot (1 - \frac{1}{p}) \cdot \prod_{i=1}^{x} m_i^{k_i}(1 - \frac{1}{m_i}) \cdot \prod_{j=1}^{y} n_j^{l_j}(1 - \frac{1}{n_j})$$

$$= mn \cdot (1 - \frac{1}{p})^2 \cdot \prod_{i=1}^{x} (1 - \frac{1}{m_i}) \cdot \prod_{j=1}^{y} (1 - \frac{1}{n_j})$$

即

$$\phi(m)\phi(n) = (1 - \frac{1}{p}) \cdot \phi(mn)$$

2.25

证明.

显然有 $n \geq 0$，否则 $\phi(n) \geq 0 > n$，问题无意义.

(1) $6|n$ 即 $2|n, 3|n$，不妨记 n 有素数分解

$$n = 2^p \cdot 3^q \cdot n_1^{k_1} n_2^{k_2} \cdots n_N^{k_N}. \quad (p, q \geq 1)$$

则

$$
\begin{aligned}
\phi(n) &= \phi(2^p \cdot 3^q \cdot n_1^{k_1} n_2^{k_2} \cdots n_N^{k_N}) \\
&= \phi(2^p) \cdot \phi(3^q) \cdot \prod_{i=1}^{N} \phi(n_i^{k_i}) \\
&= n \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \prod_{i=1}^{N} \left(1 - \frac{1}{n_i}\right) \\
&= \frac{n}{3} \cdot \prod_{i=1}^{N} \left(1 - \frac{1}{n_i}\right) \\
&\leq \frac{n}{3}
\end{aligned}
$$

即证，且当且仅当 $N = 0$ 时等号成立.

(2) 由 $T14$ 可知

$$
n - 1 \equiv 5 \pmod 6; \qquad n + 1 \equiv 1 \pmod 6; \qquad n \equiv 0 \pmod 6
$$

即 $6 | n$，由 (1) 即证.

<div align="right">□</div>

2.26

(1)

$$
\frac{3}{2}\phi(3) = \frac{3}{2} \cdot 2 = 3 = 1 + 2. \qquad \frac{4}{2}\phi(4) = \frac{4}{2} \cdot 2 = 4 = 1 + 3.
$$

$$
\frac{5}{2}\phi(5) = \frac{5}{2} \cdot 4 = 10 = 1 + 2 + 3 + 4. \qquad \frac{6}{2}\phi(6) = \frac{6}{2} \cdot 2 = 6 = 1 + 5.
$$

$$
\frac{7}{2}\phi(7) = \frac{7}{2} \cdot 6 = 21 = 1 + 2 + 3 + 4 + 5 + 6. \qquad \frac{8}{2}\phi(8) = \frac{8}{2} \cdot 4 = 16 = 1 + 3 + 5 + 7.
$$

(2) 对于整数 $n \geq 3$，缩系中所有数的和等于 $\frac{1}{2}n \cdot \phi(n)$. 即

$$
\sum_{\substack{(d,n)=1 \\ 1 \leq d \leq n-1}} d = \frac{1}{2}\phi(n) \cdot n.
$$

(3) 证明.

$$\forall\, 1 \le d \le n-1,\ (d,n)=1，有\ (n-d,n)=1，且\ d \ne n/2，故$$

$$\sum_{\substack{(d,n)=1 \\ 1 \le d \le n-1}} d = \sum_{\substack{(d,n)=1 \\ 1 \le d < n/2}} d + (n-d) = \frac{1}{2}n \cdot \phi(n)$$

$\square$

2.27

$$314^{159} \equiv (7 \cdot 45 - 1)^{159} \pmod 7$$
$$\equiv (-1)^{159} \pmod 7$$
$$\equiv (-1) \pmod 7$$
$$\equiv 6 \pmod 7$$

2.28

(1) 求末位即求模 10 余数

$$7^{355} \equiv \left(7^4\right)^{88} \cdot 7^3 \pmod{10}$$
$$\equiv (2400+1)^{88} \cdot (340+3) \pmod{10}$$
$$\equiv 3 \pmod{10}$$

即末位为 3. 用欧拉定理 $7^{\phi(10)} \equiv 1 \pmod{10}$ 亦可.

(2) 求末两位即求模 100 余数

$$7^{355} \equiv \left(7^4\right)^{88} \cdot 7^3 \pmod{100}$$
$$\equiv (2400+1)^{88} \cdot (300+43) \pmod{100}$$
$$\equiv 43 \pmod{100}$$

即末两位为 43. 用欧拉定理 $7^{\phi(100)} \equiv 1 \pmod{100}$ 亦可.

2.29

证明.

(1)

$$(k+1)^p - k^p \equiv 1 \pmod{p} \Leftrightarrow p \mid (k+1)^p - k^p - 1$$
$$\Leftrightarrow p \mid \sum_{i=1}^{p-1} C_p^i \cdot k^{p-i}$$

有

$$C_p^i = \frac{p(p-1)\dots(p-i+1)}{i!} \in \mathbb{N}, \ \Rightarrow \ i! \mid p(p-1)\dots(p-i+1). \quad (1 \le i \le p-1)$$

又 $\forall\, 1 \le i \le p-1,\ (p,i)=1$，故 $(p,i!)=1$，即

$$i! \mid (p-1)\dots(p-i+1) \ \Rightarrow \ \frac{(p-1)\dots(p-i+1)}{i!} \in \mathbb{N}, \ p \mid C_p^i.$$

故有

$$p \mid C_p^i \ \Rightarrow \ p \mid \sum_{i=1}^{p-1} C_p^i \cdot k^{p-i} \ \Rightarrow \ (k+1)^p - k^p \equiv 1 \pmod{p}.$$

(2) 对于任意素数 p 有 $p \nmid a$，则

$$a^p \equiv \sum_{k=0}^{a-1} \left((k+1)^p - k^p \right) \pmod{p}$$
$$\equiv \sum_{k=0}^{a-1} 1 \pmod{p}$$
$$\equiv a \pmod{p}$$

又 $(a^p, a) = a, (p,a) = 1$，故有

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

$\square$

2.30

证明.

(1)

$$\forall\, 1 \le k \le p-1,\ (k,p)=1\text{且}p \mid k \ \Rightarrow \ k^{p-1} \equiv 1 \pmod{p}$$

故

$$\sum_{i=1}^{p-1} i^{p-1} \equiv \sum_{i=1}^{p-1} 1 \pmod{p}$$
$$\equiv p-1 \pmod{p}$$
$$\equiv -1 \pmod{p}.$$

(2)

$$\forall \, 1 \le k \le p-1, \; (k,p) = 1 \text{且} p \mid k \Rightarrow k^{p-1} \equiv 1 \pmod{p}$$
$$\Rightarrow k^p \equiv k \pmod{p}$$

故

$$\sum_{i=1}^{p-1} i^{p-1} \equiv \sum_{i=1}^{p-1} i \pmod{p}$$
$$\equiv \frac{p(p-1)}{2} \pmod{p}$$
$$\equiv 0 \pmod{p}. \qquad (2|p-1)$$

$\square$

2.31

$$\begin{aligned} d(42) &= d(2 \cdot 3 \cdot 7) & d(420) &= d(2^2 \cdot 3 \cdot 5 \cdot 7) & d(4200) &= d(2^3 \cdot 3 \cdot 5^2 \cdot 7) \\ &= 2^3 & &= 3 \cdot 2^3 & &= 4 \cdot 3 \cdot 2^2 \\ &= 8. & &= 24. & &= 48. \end{aligned}$$

$$\sigma(42) = \sigma(2 \cdot 3 \cdot 7)$$
$$= \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{7^2 - 1}{7 - 1}$$
$$= 96.$$

$$\sigma(420) = \sigma(2^2 \cdot 3 \cdot 5 \cdot 7)$$
$$= \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1}$$
$$= 1344.$$

$$\sigma(4200) = \sigma(2^3 \cdot 3 \cdot 5^2 \cdot 7)$$
$$= \frac{2^4 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1}$$
$$= 14880.$$

2.32

不妨设 n 有素数分解

$$n = n_1^{k_1} n_2^{k_2} \cdots n_x^{k_x} \ \Rightarrow \ \sigma(n) = (k_1 + 1)(k_2 + 1) \ldots (k_x + 1) = 60$$

又

$$\left\lceil \log_2(10^4) \right\rceil = 13 \ \Rightarrow \ k_1 + k_2 + \cdots + k_x \leq 13$$
$$n = 2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040 \qquad \text{或} \qquad n = 2^4 \cdot 5^2 \cdot 3 \cdot 7 = 8400$$

2.33

证明.

设 $d_1, d_2, \ldots, d_k$ 为 n 的全部因子 (相同因子算两遍)，则

$$\forall \ 1 \leq i \leq k, \ \exists! \ 1 \leq j \leq k, \ d_j = n/d_i$$

不妨取一个排列使得 $i + j = k + 1$.

$$\sum_{d|n} \frac{1}{d} = \frac{1}{n} \sum_{i=1}^{k} \frac{n}{d_i}$$
$$= \frac{1}{n} \sum_{i=1}^{k} d_{k+1-i}$$
$$= \frac{1}{n} \sum_{i=1}^{k} d_i$$
$$= \frac{1}{n} \sigma(n).$$

$\square$

2.34

证明.

不妨记偶完全数为

$$n = 2^{p-1} \cdot (2^p - 1) \qquad (p, 2^p - 1\text{均为素数})$$

由题意可得

$$2^{p-1} \cdot (2^p - 1) \equiv 6 \pmod{10} \quad \text{或} \quad 2^{p-1} \cdot (2^p - 1) \equiv 8 \pmod{10}$$

等价于

$$2^{p-2} \cdot (2^p - 1) \equiv 3 \pmod 5 \quad \text{或} \quad 2^{p-2} \cdot (2^p - 1) \equiv 4 \pmod 5$$

$$\begin{cases} (2^{p-2}, 5) &= 1 \\ (2^p - 1, 5) &= 1 \end{cases} \Rightarrow \begin{cases} 2^{p-2} &\equiv a \pmod 5 \quad (a \in \{1, 2, 3, 4\}) \\ 2^p - 1 &\equiv b \pmod 5 \quad (b \in \{1, 2, 3, 4\}) \end{cases}$$

(1) $2^{p-2} \equiv 1 \pmod 5$

$$\begin{aligned} 2^p - 1 &\equiv 2^2 \cdot 1 - 1 \pmod 5 \\ &\equiv 3 \pmod 5 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 2^{p-2} \cdot (2^p - 1) &\equiv 3 \cdot 1 \pmod 5 \\ &\equiv 3 \pmod 5 \end{aligned}$$

(2) $2^{p-2} \equiv 2 \pmod 5$

$$\begin{aligned} 2^p - 1 &\equiv 2^2 \cdot 2 - 1 \pmod 5 \\ &\equiv 2 \pmod 5 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 2^{p-2} \cdot (2^p - 1) &\equiv 2 \cdot 2 \pmod 5 \\ &\equiv 4 \pmod 5 \end{aligned}$$

(3) $2^{p-2} \equiv 3 \pmod 5$

$$\begin{aligned} 2^p - 1 &\equiv 2^2 \cdot 3 - 1 \pmod 5 \\ &\equiv 1 \pmod 5 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 2^{p-2} \cdot (2^p - 1) &\equiv 3 \cdot 1 \pmod 5 \\ &\equiv 3 \pmod 5 \end{aligned}$$

(4) $2^{p-2} \equiv 4 \pmod 5$

$$2^p - 1 \equiv 2^2 \cdot 4 - 1 \pmod 5$$
$$\equiv 0 \pmod 5 \qquad \Rightarrow \quad 0 \notin \{1,2,3,4\}, \text{该情况不存在}.$$

综上，即证

$$2^{p-1} \cdot (2^p - 1) \equiv 6 \pmod{10} \quad \text{或} \quad 2^{p-1} \cdot (2^p - 1) \equiv 8 \pmod{10}$$

$\square$

2.35

证明.

由题意可得
$$n = 2^{p-1} \cdot (2^p - 1) \qquad (p,\ 2^p - 1 \text{均为素数})$$
又 $n > 6$，故 $p > 2$, $2|p-1$，不妨记 $p - 1 = 2k\ (k \in \mathbb{Z}^*)$，有
$$n = 2^{2k} \cdot (2^{2k+1} - 1) = 4^k \cdot (2 \cdot 4^k - 1)$$

又
$$\forall\ k \geq 1,\ 4^k \equiv m \pmod 9,\ \text{有} m \in \{4,7,1\}$$

(1) $4^k \equiv 4 \pmod 9$

$$2 \cdot 4^k - 1 \equiv 2 \cdot 4 - 1 \pmod 9 \qquad 4^k \cdot (2 \cdot 4^k - 1) \equiv 4 \cdot 7 \pmod 9$$
$$\equiv 7 \pmod 9 \qquad \Rightarrow \qquad \equiv 1 \pmod 9$$

(2) $4^k \equiv 7 \pmod 9$

$$2 \cdot 4^k - 1 \equiv 2 \cdot 7 - 1 \pmod 9 \qquad 4^k \cdot (2 \cdot 4^k - 1) \equiv 7 \cdot 4 \pmod 9$$
$$\equiv 4 \pmod 9 \qquad \Rightarrow \qquad \equiv 1 \pmod 9$$

(3) $4^k \equiv 1 \pmod 9$

$$2 \cdot 4^k - 1 \equiv 2 \cdot 1 - 1 \pmod 9 \qquad 4^k \cdot (2 \cdot 4^k - 1) \equiv 1 \cdot 1 \pmod 9$$
$$\equiv 1 \pmod 9 \qquad \Rightarrow \qquad \equiv 1 \pmod 9$$

综上，即证

$$n \equiv 1 \pmod 9.$$

$\square$

2.36

证明. $\forall p,\ \sigma(p) = p + 1,\ \phi(p) = p - 1,\ d(p) = 2$，有

$$\sigma(p) = \phi(p) + d(p) \quad \Rightarrow \quad \sum_{p \le x} \sigma(p) = \sum_{p \le x} \phi(p) + \sum_{p \le x} d(p).$$

$\square$

2.37

$$2^1 \equiv 2 \pmod{15} \qquad 7^1 \equiv 7 \pmod{15} \qquad 8^1 \equiv 8 \pmod{15}$$
$$2^2 \equiv 4 \pmod{15} \qquad 7^2 \equiv 4 \pmod{15} \qquad 8^2 \equiv 4 \pmod{15}$$
$$2^3 \equiv 8 \pmod{15} \qquad 7^3 \equiv 13 \pmod{15} \qquad 8^3 \equiv 2 \pmod{15}$$
$$2^4 \equiv 1 \pmod{15} \qquad 7^4 \equiv 1 \pmod{15} \qquad 8^4 \equiv 1 \pmod{15}$$

因此, 2模15的阶为4.   因此, 7模15的阶为4.   因此, 8模15的阶为4.

$$4^1 \equiv 4 \pmod{15} \qquad 11^1 \equiv 11 \pmod{15} \qquad 14^1 \equiv 14 \pmod{15}$$
$$4^2 \equiv 1 \pmod{15} \qquad 11^2 \equiv 1 \pmod{15} \qquad 14^2 \equiv 1 \pmod{15}$$

因此, 4模15的阶为2.   因此, 11模15的阶为2.   因此, 14模15的阶为2.

$$13^1 \equiv 13 \pmod{15}$$
$$13^2 \equiv 4 \pmod{15}$$
$$13^3 \equiv 7 \pmod{15}$$
$$13^4 \equiv 1 \pmod{15}$$

因此, 13模15的阶为4.

2.38

(1) 2 为 28 的原根.

$$n = ind_2\ k \ \Leftrightarrow\ 2^n \equiv k \pmod{29}$$

26

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
n	0	1	5	2	22	6	12	3	10	23	25	7	18	13
k	15	16	17	18	19	20	21	22	23	24	25	26	27	28
n	27	4	21	11	9	24	17	26	20	8	16	19	15	14

(2) 由 2 为 28 的原根可知

$$ind_2 9 + ind_2 x = ind_2 2 \quad (\mathrm{mod}\ ()28)$$

又由 (1) 得 $ind_2 9 = 10,\ ind_2 2 = 1$，有

$$ind_2 x = -9 \equiv 19 \quad (\mathrm{mod}\ 28) \ \Rightarrow \ x \equiv 19 \quad (\mathrm{mod}\ 29).$$

(3) 由 2 为 28 的原根可知

$$9 \cdot ind_2 x = ind_2 2 \quad (\mathrm{mod}\ 28)$$

又由 (1) 得 $ind_2 2 = 1$，有

$$9 \cdot ind_2 x = 1 \quad (\mathrm{mod}\ 28) \Rightarrow \ ind_2 x \equiv 25 \quad (\mathrm{mod}\ 28)$$
$$\Rightarrow \ x \equiv 11 \quad (\mathrm{mod}\ 29).$$

2.39

证明.

不对，证明如下:

$$457^{911} \equiv 1 \quad (\mathrm{mod}\ 10021) \quad \Leftrightarrow \quad \begin{cases} 457^{911} \equiv 1 \quad (\mathrm{mod}\ 11) \\ 457^{911} \equiv 1 \quad (\mathrm{mod}\ 911) \end{cases}$$

又

$$\begin{cases} 457^{10} \equiv 1 \quad (\mathrm{mod}\ 11) \\ 457^{910} \equiv 1 \quad (\mathrm{mod}\ 911) \end{cases} \Rightarrow \begin{cases} 457^{911} \equiv 6 \quad (\mathrm{mod}\ 11) \\ 457^{911} \equiv 1457 \quad (\mathrm{mod}\ 911) \end{cases}$$

故不对.

$\square$

2.40

$\phi(\phi(37)) = 12$，即 37 有 12 个原根.

又 $2^{36} \equiv 1 \pmod{37}$，且

$$\begin{cases} 2^1 \equiv \quad \pmod{37}; \qquad 2^2 \equiv \quad \pmod{37}; \\ 2^3 \equiv \quad \pmod{37}; \qquad 2^4 \equiv \quad \pmod{37}; \\ 2^6 \equiv \quad \pmod{37}; \qquad 2^9 \equiv \quad \pmod{37}; \\ 2^{12} \equiv \quad \pmod{37}; \qquad 2^{18} \equiv \quad \pmod{37}; \end{cases} \qquad \Rightarrow \ 2\text{为}37\text{最小原根}.$$

由推论 2.7，对于 $a = 2^i \ ((i, 36) = 1)$, a 模 37 的阶为 36. 即原根集合为

$\{ \, x \mid 1 \leq x \leq 36, \ x \equiv 2^i \pmod{37}\}$，且 $i \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$

经计算

$2^1 \equiv 2 \pmod{37}, \ 2^5 \equiv 32 \pmod{37}, \ 2^7 \equiv 17 \pmod{37}, \ 2^{11} \equiv 13 \pmod{37},$

$2^{13} \equiv 15 \pmod{37}, \ 2^{17} \equiv 18 \pmod{37}, \ 2^{19} \equiv 35 \pmod{37}, \ 2^{23} \equiv 5 \pmod{37},$

$2^{25} \equiv 20 \pmod{37}, \ 2^{29} \equiv 24 \pmod{37}, \ 2^{31} \equiv 22 \pmod{37}, \ 2^{35} \equiv 19 \pmod{37},$

即 37 的原根集合为

$$\{2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35\}$$

2.41

证明.

设 $(-a)$ 模 q 的阶为 d.

$$\begin{aligned} q \mid (a^p + 1) \Rightarrow \ & a^p \equiv -1 \pmod{q} \\ \Rightarrow \ & -a^p \equiv 1 \pmod{q} \qquad \Rightarrow \quad d \mid p, \ d = 1\text{或}p. \\ \Rightarrow \ & (-a)^p \equiv 1 \pmod{q} \end{aligned}$$

(1) $d = 1$

$$-a \equiv 1 \pmod{q} \Rightarrow a + 1 \equiv 0 \pmod{q}$$
$$\Rightarrow q \mid (a+1).$$

(2) $d = p$

$$(-a)^p \equiv 1 \pmod{q} \Rightarrow p \mid \phi(q),\ p \mid (q-1)$$
$$\Rightarrow 2p \mid (q-1)$$
$$\Rightarrow \exists\, k \in \mathbb{Z},\ 2kp = q-1,\ q \mid (2kp+1)$$

即证

$$q \mid (a+1)\ \text{或}\ q \mid (2kp+1) \qquad (k\text{为某个整数}).$$

$\square$

2.42

证明.

6 的正因子为 $1, 2, 3, 6$，则 $(a+1)$ 模 p 的阶为 6 等价于

$$\begin{cases} (a+1) \not\equiv 1 \pmod{p} \qquad (a+1)^2 \not\equiv 1 \pmod{p} \\ (a+1)^3 \not\equiv 1 \pmod{p} \qquad (a+1)^6 \equiv 1 \pmod{p} \end{cases}$$

(1)
$$(a, p) = 1 \quad \Rightarrow \quad (a+1) \not\equiv 1 \pmod{p} \quad \Rightarrow p \nmid (a-1).$$

(2) 由 $a^3 \equiv 1 \pmod{p}, a \not\equiv 1 \pmod{p}, a^2 \not\equiv 1 \pmod{p}$，得

$$a^3 - 1 = (a-1)(a^2 + a + 1) \equiv 0 \pmod{p} \Rightarrow p \mid (a^2 + a + 1)$$

$$(a+1)^2 = a^2 + 2a + 1 \equiv a \not\equiv 1 \pmod{p}.$$

(3)
$$(a+1)^3 \equiv a(a+1) \equiv -a^3 \equiv -1 \pmod{p}.$$

(4)
$$(a+1)^6 \equiv 1 \pmod{p}.$$

即证 $(a+1)$ 模 p 的阶为 6.

$\square$

3

3.1

(1) 不能构成映射，如 $x_1 = 0$，则 $x_2 = 0, 1, \ldots, 9$ 均满足.

(2) 能构成映射，$\forall \, y_1 \in \mathbb{R},\ \exists! \, y_2 = y_1^2$.

(3) 不能构成映射，如 $y_1 = 1$，则 $y_2 = \pm 1$ 均满足.

3.2

(1)

$$R_f = \{2, -2, 0\}$$

(2)

$$\begin{cases} |A| = 9 \\ |R_f| = 3 \end{cases} \Rightarrow \ n = 3^9.$$

3.3

(1) 满射

$$\forall \, y \in \mathbb{Z}^+,\ \exists \, x = \pm(y-1) \in \mathbb{Z},\ f(x) = y.$$

(2) 既不是单射，又不是满射. 值域为 $\{0, 1, 2\} \subseteq \mathbb{Z} \cup \{0\}$

$$\forall \, y \in \mathbb{Z} \cup \{0\} \begin{cases} y \in \{0, 1, 2\},\ \exists \, x = 3k + y (k \in \mathbb{Z}),\ f(x) = y. \\ y \notin \{0, 1, 2\},\ \forall \, x \in \mathbb{Z},\ f(x) \neq y. \end{cases}$$

(3) f, g 均是双射.

$$\begin{cases} \forall \, y \in \mathbb{Z},\ \exists! \, x = y - 1 \in \mathbb{Z}, f(x) = y. \\ \forall \, y \in \mathbb{Z},\ \exists! \, x = y + 1 \in \mathbb{Z}, g(x) = y. \end{cases}$$

(4) 满射.

$$\forall \, y \in \{0, 1\},\ \exists \, x = 2k + y + 1 (k \in \mathbb{Z}),\ f(x) = y.$$

(5) 既不是单射，又不是满射.

$$\begin{cases} \forall \, y \in \mathbb{Z},\ y < -16,\ \forall \, x \in \mathbb{Z},\ f(x) > y. \\ \exists \, y = -15,\ f(0) = f(-2) = y. \end{cases}$$

3.4

证明.

$$\begin{cases} f : A \times B \to B \times A, \ (a,b) \mapsto (b,a) \\ g : B \times A \to A \times B, \ (b,a) \mapsto (a,b) \end{cases}$$

则

$$f \circ g = I_{A \times B}, \quad g \circ f = I_{B \times A}, \quad g = f^{-1}.$$

即 f 为双射，即证 $|A \times B| = |B \times A|$. $\qquad\square$

3.5

证明.

(1)

$$\forall \ f(x) = \sum_{i=0}^{n} a_i \cdot x^i, \ \exists! \ g(x) = \sum_{i=1}^{n} i \cdot a_i \cdot x^{i-1}, \ \frac{d}{dx} f(x) = g(x). \ (a_i \in \mathbb{R})$$

值域为 $R[x]$，是满射不是双射.

$$\forall \ g(x) = \sum_{i=0}^{n} a_i \cdot x^i, \ \exists \ f(x) = a + \sum_{i=0}^{n} \frac{a_i}{i+1} \cdot x^{i+1}, \ \frac{d}{dx} f(x) = g(x). \ (a, a_i \in \mathbb{R})$$

(2)

$$\forall \ f(x) = \sum_{i=0}^{n} a_i \cdot x^i, \ \exists! \ g(x) = \sum_{i=0}^{n} \frac{a_i}{i+1} \cdot x^{i+1}, \ I(f(x)) = g(x). \ (a_i \in \mathbb{R})$$

值域为常数项为 0 的实系数多项式，既不是满射，也不是双射.

$$\forall \ g(x) = a \ (0 \neq a \in \mathbb{R}), \ \text{若} \exists \ f(x) \in R[x], \text{满足} I(f(x)) = g(x) = a \ I(f(x)) = g(x).$$

则

$$a = g(x) = \int_0^x f(t)\,dt \ \xrightarrow{x=0} \ g(0) = \int_0^0 f(t)\,dt = 0 \neq a.$$

矛盾.

$\qquad\square$

3.6

证明. $\forall\,(b_{i1}, b_{i2}, \ldots, b_{in}) \in S(B)$,

$$\exists!\ f \in F,\ f : A \to B,\ a_j \mapsto b_{ij}.\text{满足}g(f) = (b_{i1}, b_{i2}, \ldots, b_{in}).$$

即证 g 即是单射，又是满射，即 g 是从 F 到 $S(B)$ 的双射.

$$|F| = |S(B)| = |B|^n = m^n.$$

$\square$

3.7

证明.

(1) $f(A \cup B) = f(A) \cup f(B)$

   (a) $\forall\,y \in f(A \cup B),\ \exists\,x \in A \cup B,\ f(x) = y$.

$$\begin{cases} x \in A, y = f(x) \in f(A) \\ x \in B, y = f(x) \in f(B) \end{cases} \Rightarrow\ y \in f(A) \cup f(B) \ \Rightarrow\ f(A \cup B) \subseteq f(A) \cup f(B).$$

   (b) $\forall\,y \in f(A) \cup f(B),\ y \in f(A)\text{或}y \in f(B)$.

$$\begin{cases} y \in f(A), \exists\,x \in A, f(x) = y \\ y \in f(B), \exists\,x \in B, f(x) = y \end{cases} \Rightarrow\ y \in f(A \cup B) \ \Rightarrow\ f(A) \cup f(B) \subseteq f(A \cup B).$$

综上，即证

$$f(A \cup B) = f(A) \cup f(B).$$

(2) $f(A \cap B) \subseteq f(A) \cap f(B)$

$$\forall\,y \in f(A \cap B),\ \exists\,x \in A \cap B,\ f(x) = y.$$

由 $x \in A \cap B$ 有 $x \in A, x \in B$，即

$$\begin{cases} x \in A,\ y = f(x) \in f(A) \\ x \in B,\ y = f(x) \in f(B) \end{cases} \Rightarrow\ y \in f(A) \cap f(B) \ \Rightarrow\ f(A \cap B) \subseteq f(A) \cap f(B).$$

(3)
$$S = \mathbb{Z}, T = \{1\}, A = \{2k+1 | k \in \mathbb{Z}\}, B = \{2k | k \in \mathbb{Z}\}$$

取 $f : S \to T, n \mapsto 1$，则

$$\begin{cases} f(A \cap B) = f(\phi) = \phi. \\ f(A) \cap f(B) = \{1\} \end{cases} \quad \Rightarrow \quad f(A \cap B) \neq f(A) \cap f(B).$$

$\square$

3.8

(1) f 为单射：$f(\widetilde{A}) \subseteq \widetilde{f(A)}$.

$$\forall y \in f(\widetilde{A}) \subseteq S, \ \exists! \ x \in S 且 x \in \widetilde{A}, \ f(x) = y.$$

有

$$\forall x \in A, \ f(x) \neq y, \ y \notin f(A) \ \Rightarrow \ y \in \widetilde{f(A)}.$$

即

$$\forall y \in f(\widetilde{A}) \subseteq S, \ y \in \widetilde{f(A)} \ \Rightarrow \ f(\widetilde{A}) \subseteq \widetilde{f(A)}.$$

(2) f 为满射：$\widetilde{f(A)} \subseteq f(\widetilde{A})$.

$$\forall y \in \widetilde{f(A)}, \ \exists \ x \in S, f(x) = y.$$

若 $x \in A, \ y = f(x) \in f(A)$，矛盾. 故 $x \in \widetilde{A}$.

$$y = f(x) \in f(\widetilde{A}) \ \Rightarrow \ \widetilde{f(A)} \subseteq f(\widetilde{A}).$$

3.9

(1)
$$f \circ g = 3(3x+1) = 9x + 3.$$

(2)
$$f \circ g = 3$$

(3)
$$g \circ f = 3(3x) + 1 = 9x + 1.$$

(4)

$$g \circ h = 3(3x + 2) + 1 = 9x + 7.$$

(5)

$$f \circ g \circ h = 3(3(3x + 2) + 1) = 27x + 21.$$

3.10

证明.

先证 $g \circ f$ 是从 A 到 C 的映射.

$$\forall\, x \in A,\ \exists!\ y = f(x) \in B,\ \exists!\ z = g(y) \in C.$$

假设 $g \circ f$ 不是从 A 到 C 的单射,则等价于

$$\exists\, c \in C,\ \exists\, a_1, a_2 \in A,\ a_1 \neq a_2,\ g \circ f(a_1) = g \circ f(a_2) = c.$$

即

$$g(f(a_1)) = g(f(a_2)) = c \in C \xrightarrow{\ g\ } \exists!\ b \in B,\ g(b) = c,\ f(a_1) = f(a_2) = b \in B.$$

又

$$f为单射\ \Rightarrow\ \exists\, a \in A,\ f(a) = b.$$

即 $a_1 = a_2 = a$,矛盾,即证 $g \circ f$ 是从 A 到 C 的单射.

$\square$

3.11

会发生矛盾.

(1) 先证 g 为满射

$$若\exists\, y \in S,\ \forall\, x \in S,\ g(x) \neq y,$$

(2) 再证 g 为单射

3.12

(1)

(2)

(3)

(4)

3.13

(1)

(2)

3.14

(1)

(2)

(3)

3.15

(1)

(2)

3.16

证明. □

3.17

(1)

(2)

3.18

(1)

(2)

(3)

3.19

(1)

(2)

4 二元关系

5　群论初步

6　商群

7　环和域

8　格和布尔代数

8　格和布尔代数