1 数论初步

1.1

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)

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

□

1.2

证明.

(1) 不妨假设 $\exists\ n>0,\ (n,n+1)=d>1$

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

(2) 可取 (n,k)，证明如下

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

□

1.3

(1) $(314, 159) = 1$，有解。由辗转相除法

$$\begin{aligned}
314 &= 159 \cdot 1 + 155 \\
159 &= 155 \cdot 1 + 4 \\
155 &= 4 \cdot 38 + 3 \\
4 &= 3 \cdot 1 + 1
\end{aligned}$$

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

$$\begin{aligned}
3141 &= 1592 \cdot 1 + 1549 \\
1592 &= 1549 \cdot 1 + 43 \\
1549 &= 43 \cdot 36 + 1
\end{aligned}$$

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 $x = 37, y = -73.$

1.4

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

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

$\square$

1.5

证明.

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

即证

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

$\square$

1.6

(1)

$$2345 = 5 \cdot 7 \cdot 67$$

(2)

$$3456 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$$

1.7

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. □

1.8

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

(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)

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

□

1.9

(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

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

1.10

(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.

1.11

1.11.1 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

$$\begin{aligned} 0.05x+0.1y+0.25(30-x-y)=5 &\Leftrightarrow x+2y+5(30-x-y)=100 \\ &\Leftrightarrow 4x+3y=50 \end{aligned}$$

$(4,3)=1|50$，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

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

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

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

1.11.2 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

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

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

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 $\left[\dfrac{100-5\times 14}{2}\right]-(70-4\times 14)+1=2$

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

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

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

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

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

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

即共有 $2+3+5+6+6+3+1=26$ 种兑换方法.

1.12

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

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

$(1,4)=1|45$，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.

1.13

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

又 $6k \equiv 6(\text{mod}4)$，有

$$\begin{aligned} 6k+5 &\equiv 7(\text{mod}4) \\ &\equiv 3(\text{mod}4) \end{aligned}$$

1.14

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.

□

1.15

证明.

不妨设这两个连续的立方数为 k^3 与 $(k+1)^3$.

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

□

1.16

证明.

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

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

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

$$\begin{aligned}A \equiv& \sum_{i=0}^{i=n} a_i \cdot 10^i (\bmod 3)\\ \equiv& \sum_{i=0}^{i=n} a_i (\bmod 3)\\ \equiv& 0(\bmod 3)\end{aligned}$$

□

1.17

证明.

(1)

$$10 \equiv -1(\bmod 11) \ \Rightarrow\ 10^k \equiv (-1)^k (\bmod 11)$$

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

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

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.

□

1.18

(1)

$$\begin{aligned}2x \equiv& 1(\bmod 17)\\ \equiv& 18(\bmod 17)\end{aligned} \xrightarrow{(2,17)=1} x \equiv 9(\bmod 17)$$

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

$$x \equiv 2 + 6t(\bmod 18) \quad (0 \le t \le 2).$$

即

$$x \equiv 2, 8, 14(\bmod 18).$$

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

$$\begin{aligned}2x\equiv&3(\text{mod}9)\\\equiv&12(\text{mod}9)\end{aligned}\xrightarrow{(2,9)=1} x\equiv 6(\text{mod}9).$$

即原方程解为

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

(4)

$$\begin{aligned}3x\equiv&1(\text{mod}17)\\\equiv&18(\text{mod}17)\end{aligned}\xrightarrow{(3,17)=1} x\equiv 6(\text{mod}17).$$

1.19

(1) $(2,3)=1$，有解。本题中

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

由

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

从而

$$\begin{aligned}y=&3\cdot 1\cdot 1+2\cdot 1\cdot 2\\=&7\end{aligned}\quad\Rightarrow\ y\equiv 1(\text{mod}6).$$

(2) $(41,26)=1$，有解。原式等价于

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

本题中

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

由

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

从而

$$\left.\begin{aligned} y &= 26\cdot 31\cdot 30 + 41\cdot 7\cdot 7 \\ &= 26819 \end{aligned}\right. \Rightarrow \ y \equiv 605(\text{mod}1066).$$

(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

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

从而

$$\left.\begin{aligned} y &= 21\cdot 1\cdot 1 + 14\cdot 1\cdot 2 + 6\cdot 6\cdot 6 \\ &= 265. \end{aligned}\right. \Rightarrow \ y \equiv 13(\text{mod}42).$$

(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

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

从而

$$\left.\begin{aligned} y &= 77\cdot 3\cdot 3 + 55\cdot 3\cdot 6 + 35\cdot 3\cdot 6 \\ &= 2313. \end{aligned}\right. \Rightarrow \ y \equiv 3(\text{mod}385).$$

1.20

设

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

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

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

1.21

由题意有

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

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

$$n = 62.$$

1.22

(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)

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

1.23

(1) 小于 18 且与 18 互素的正整数有

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

(2)

$$\begin{aligned} 1 \cdot 5 &\equiv 5(\text{mod}18) & \qquad 5 \cdot 5 &\equiv 25(\text{mod}18) \\ & & &\equiv 7(\text{mod}18) \end{aligned}$$

$$\begin{aligned} 7 \cdot 5 &\equiv 35(\text{mod}18) & \qquad 11 \cdot 5 &\equiv 55(\text{mod}18) \\ &\equiv 17(\text{mod}18) & &\equiv 1(\text{mod}18) \end{aligned}$$

$$\begin{aligned} 13 \cdot 5 &\equiv 65(\text{mod}18) & \qquad 17 \cdot 5 &\equiv 85(\text{mod}18) \\ &\equiv 11(\text{mod}18) & &\equiv 13(\text{mod}18) \end{aligned}$$

仍为缩系，引理 2.1 成立.

1.24

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

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

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

$$
\begin{aligned}
\phi(m)\phi(n) &= \phi\left(p^{M}\cdot\prod_{i=1}^{x} m_i^{k_i}\right)\cdot\phi\left(p^{N}\cdot\prod_{j=1}^{y} n_j^{l_j}\right)\\
&= \phi(p^M)\cdot\phi(p^N)\cdot\prod_{i=1}^{x}\phi(m_i^{k_i})\cdot\prod_{j=1}^{y}\phi(n_j^{l_j})\\
&= p^M\cdot(1-\frac{1}{p})\cdot p^N\cdot(1-\frac{1}{p})\cdot\prod_{i=1}^{x} m_i^{k_i}(1-\frac{1}{m_i})\cdot\prod_{j=1}^{y} n_j^{l_j}(1-\frac{1}{n_j})\\
&= mn\cdot(1-\frac{1}{p})^2\cdot\prod_{i=1}^{x}(1-\frac{1}{m_i})\cdot\prod_{j=1}^{y}(1-\frac{1}{n_j})
\end{aligned}
$$

即

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

1.25

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.

$\square$

1.26

1.27

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

1.28

(1) 求末位即求模 10 余数

$$\begin{aligned} 7^{355} &\equiv (7^4)^{88} \cdot 7^3 \pmod{10} \\ &\equiv (2400+1)^{88} \cdot (340+3) \pmod{10} \\ &\equiv 3 \pmod{10} \end{aligned}$$

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

$$\begin{aligned} 7^{355} &\equiv (7^4)^{88} \cdot 7^3 \pmod{100} \\ &\equiv (2400+1)^{88} \cdot (300+43) \pmod{100} \\ &\equiv 43 \pmod{100} \end{aligned}$$

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

1.29

证明.

(1)

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

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

$$\begin{aligned} a^p &\equiv \sum_{k=0}^{a-1}((k+1)^p - k^p) \pmod p \\ &\equiv \sum_{k=0}^{a-1} 1 \pmod p \\ &\equiv a \pmod p \end{aligned}$$

又 $(a^p, a) = a, (p, a) = 1$，故有

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

□

1.30

证明.

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

故

$$\begin{aligned} \sum_{i=1}^{p-1} i^{p-1} &\equiv \sum_{i=1}^{p-1} 1 \pmod p \\ &\equiv p-1 \pmod p \\ &\equiv -1 \pmod p. \end{aligned}$$

(2)

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

故

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

□

1.31

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

$$\begin{aligned}\sigma(42) &= \sigma(2\cdot 3\cdot 7)\\ &= \frac{2^2-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{7^2-1}{7-1}\\ &= 96.\end{aligned} \qquad \begin{aligned}\sigma(420) &= \sigma(2^2\cdot 3\cdot 5\cdot 7)\\ &= \frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}\cdot\frac{7^2-1}{7-1}\\ &= 1344.\end{aligned}$$

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

1.32

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

$$\lceil \log_2(10^4)\rceil = 13 \;\Rightarrow\; k_1+k_2+\cdots+k_x \le 13$$

$$n = 2^4\cdot 3^2\cdot 5\cdot 7 = 5040 \qquad 或 \qquad n = 2^4\cdot 5^2\cdot 3\cdot 7 = 8400$$

1.33

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

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

不妨取一个排列使得 $i + j = k + 1$.

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

$\square$

1.34

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

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

综上，即证

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

□

1.35

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

$$\begin{aligned} 2\cdot 4^k - 1 &\equiv 2\cdot 4 - 1 \pmod 9 \\ &\equiv 7 \pmod 9 \end{aligned} \quad\Rightarrow\quad \begin{aligned} 4^k\cdot(2\cdot 4^k - 1) &\equiv 4\cdot 7 \pmod 9 \\ &\equiv 1 \pmod 9 \end{aligned}$$

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

$$\begin{aligned} 2\cdot 4^k - 1 &\equiv 2\cdot 7 - 1 \pmod 9 \\ &\equiv 4 \pmod 9 \end{aligned} \quad\Rightarrow\quad \begin{aligned} 4^k\cdot(2\cdot 4^k - 1) &\equiv 7\cdot 4 \pmod 9 \\ &\equiv 1 \pmod 9 \end{aligned}$$

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

$$\begin{aligned} 2\cdot 4^k - 1 &\equiv 2\cdot 1 - 1 \pmod 9 \\ &\equiv 1 \pmod 9 \end{aligned} \quad\Rightarrow\quad \begin{aligned} 4^k\cdot(2\cdot 4^k - 1) &\equiv 1\cdot 1 \pmod 9 \\ &\equiv 1 \pmod 9 \end{aligned}$$

综上，即证

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

□

1.36

证明. □

1.37

1.38

1.39

1.40

1.41

1.42