離散数学演習 10　解答例

1. $a \equiv b \pmod{p}$ だから, ある整数 k が存在して, $a - b = kp$. また, $d \mid p$ だから, ある整数 k' が存在して, $p = k'd$. ゆえに, $a - b = kk'd$. kk' は整数だから, $a \equiv b \pmod{d}$.

2. $2 \mid n$ であるとき. 整数 q が存在して, $n = q \cdot 2$. ゆえに, $n^2 = 4q^2 \equiv 0 \pmod{4}$.
一方, $2 \mid n$ でないとき. 除法定理から, 整数 q, r が存在して, $n = q \cdot 2 + r$ $(0 \leq |r| < 2)$. このとき, $r = \pm 1$ だから, $n = q \cdot 2 \pm 1$. ゆえに, $n^2 = 4q^2 \pm 4q + 1 \equiv 1 \pmod{4}$.

3. (1) $3x \equiv 13 \equiv 30 \pmod{17}$
$\gcd(3, 17) = 1$ だから, $x \equiv 10 \pmod{17}$

   (2) $7x \equiv 1 \pmod{13}$
一方, $13x \equiv 13 \pmod{13}$
ゆえに, $6x \equiv 12 \pmod{13}$
$\gcd(6, 13) = 1$ だから, $x \equiv 2 \pmod{13}$

   (3) $6x \equiv 22 \pmod{40}$
$\gcd(6, 22, 40) = 2$ だから, $3x \equiv 11 \pmod{20}$
ゆえに, $3x \equiv -9 \pmod{20}$
$\gcd(3, 20) = 1$ だから, $x \equiv -3 \equiv 17 \pmod{20}$

4. $\mathrm{lcm}(3, 5, 7) = 105$ である.
$x \equiv 2 \pmod{3}$ から, $35x \equiv 70 \pmod{105}$.
$x \equiv 3 \pmod{5}$ から, $21x \equiv 63 \pmod{105}$.
$x \equiv 4 \pmod{7}$ から, $15x \equiv 60 \pmod{105}$.
ゆえに, $21x + 15x - 35x \equiv 63 + 60 - 70 \pmod{105}$. すなわち, $x \equiv 53 \pmod{105}$.

（別解）次の連立 1 次不定方程式の一般解を求めればよい.

$$\begin{cases} x - 2 &= 3y \quad (1) \\ x - 3 &= 5z \quad (2) \\ x - 4 &= 7u \quad (3) \end{cases}$$

(1), (2) から, $3y + 2 = 5z + 3$. すなわち, $3y - 5z = 1$.
このとき, $3y - 5z = 3(y - 2z) + z = 3p + z$ $(p = y - 2z)$ だから, $3p + z = 1$. すなわち, $z = 1 - 3p$.
一方, (2), (3) から, $5z + 3 = 7u + 4$. すなわち, $5z - 7u = 1$.
これに $z = 1 - 3p$ を代入すると, $5(1 - 3p) - 7u = 5 - 15p - 7u = 1$. すなわち, $15p + 7u = 4$.
$15p + 7u = 7(u + 2p) + p = 7q + p$ $(q = u + 2p)$ だから, $7q + p = 4$.
このとき, $p = 4 - 7q$.
また, $u = q - 2p = q - 2(4 - 7q) = 15q - 8$.
ゆえに, $x = 7u + 4 = 7(15q - 8) + 4 = 105q - 52$.
したがって, $x \equiv -52 \equiv 53 \pmod{105}$.

（別解）
$M_1 = p_2p_3 = 5 \cdot 7 = 35$, $M_2 = p_1p_3 = 3 \cdot 7 = 21$, $M_3 = p_1p_2 = 3 \cdot 5 = 15$.
不定方程式 $35u_1 + 21u_2 + 15u_3 = 1$ を解く.

$$\begin{aligned} 35u_1 + 21u_2 + 15u_3 &= 15(2u_1 + u_2 + u_3) + 5u_1 + 6u_2 \\ &= 15p + 5u_1 + 6u_2 && (p = 2u_1 + u_2 + u_3) \\ &= 5(3p + u_1 + u_2) + u_2 \\ &= 5q + u_2 && (q = 3p + u_1 + u_2) \end{aligned}$$

ゆえに, $5q + u_2 = 1$ だから, $u_2 = 1 - 5q$.
$u_1 = q - 3p - u_2 = q - 3p - (1 - 5q) = 6q - 3p - 1$.
したがって, $u_3 = p - 2u_1 - u_2 = p - 2(6q - 3p - 1) - (1 - 5q) = 7p - 7q + 1$.
$p = q = 0$ とおくと, 特殊解は $u_1 = -1, u_2 = 1, u_3 = 1$.
連立方程式の一般解は,

$$\begin{aligned} x &\equiv M_1u_1x_1 + M_2u_2x_2 + M_3u_3x_3 \pmod{M} \\ &\equiv 35 \cdot (-1) \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 4 \pmod{105} \\ &\equiv -70 + 63 + 60 \pmod{105} \\ &\equiv 53 \pmod{105} \end{aligned}$$

5. $3x^2 - x - 2 \equiv 0 \pmod{7}$ だから, $(3x + 2)(x - 1) \equiv 0 \pmod{7}$.
7 は素数だから, $3x + 2 \equiv 0 \pmod{7}$ または $x - 1 \equiv 0 \pmod{7}$.

ゆえに, $3x \equiv -2 \pmod 7$ $(*)$ または $x \equiv 1 \pmod 7$.
$(*)$ から, $6x \equiv -4 \pmod 7$ $(**)$.
ここで, $7x \equiv 0 \pmod 7$ $(***)$.
$(***) - (**)$ から, $x \equiv 4 \pmod 7$.
ゆえに, $x \equiv 4 \pmod 7$ または $x \equiv 1 \pmod 7$.
（別解）
法は 7 であるから, 解は $x = 0, 1, \cdots, 6$ のうちにある.
そこで, 与えられた合同方程式の左辺に $x = 0, 1, \cdots, 6$ をそれぞれ代入すると,
$x = 1$ のとき, $3 \cdot x^2 - x = 3 \cdot 1^2 - 1 = 2 \equiv 2 \pmod 7$.
$x = 4$ のとき, $3 \cdot x^2 - x = 3 \cdot 4^2 - 4 = 44 \equiv 2 \pmod 7$.
ゆえに, これらは与えられた合同方程式の解である. したがって, $x \equiv 1 \pmod 7$ または $x \equiv 4 \pmod 7$.

6. (1) (a) $a \equiv b \pmod p$ とする.
$x \in [a]_p$ とすると, $x \equiv a \pmod p$. $a \equiv b \pmod p$ だから, $x \equiv b \pmod p$. ゆえに, $x \in [b]_p$. したがって, $[a]_p \subseteq [b]_p$.
同様に, $[b]_p \subseteq [a]_p$.
ゆえに, $[a]_p = [b]_p$.
一方, $[a]_p = [b]_p$ とする. 明らかに, $a \in [a]_p$ だから, $a \in [b]_p$. ゆえに, $a \equiv b \pmod p$.

(b) $a \not\equiv b \pmod p$ とする.
ここで, $[a]_p \cap [b]_p \neq \phi$ と仮定すると, $x \in [a]_p \cap [b]_p$ が存在する. ゆえに, $x \equiv a \pmod p$ かつ $x \equiv b \pmod p$ だから, $a \equiv b \pmod p$. これは矛盾.
したがって, $[a]_p \cap [b]_p = \phi$.
一方, $[a]_p \cap [b]_p = \phi$ とする.
ここで, $a \equiv b \pmod p$ と仮定すると, $a \in [b]_p$. また, 明らかに, $a \in [a]_p$. ゆえに, $a \in [a]_p \cap [b]_p$ だから, $[a]_p \cap [b]_p \neq \phi$. これは矛盾.
したがって, $a \not\equiv b \pmod p$.

(2) (a) 任意の $n \in \mathbf{Z}$ に対して, $q, r \in \mathbf{Z}$ が存在して, $n = qp + r$ $(0 \leq r < p)$ である. このとき, $n \equiv r \pmod p$. ゆえに, 任意の $[n]_p \in \mathbf{Z}/\equiv_p$ に対して, $r + 1 \in \mathbf{N}_p$ を考えると, $f(r+1) = [r]_p = [n]_p$. したがって, f は全射である.
$n_1, n_2 \in \mathbf{N}_p$ $(n_1 \neq n_2)$ に対して, $f(n_1) = f(n_2)$ とする. このとき, $[n_1 - 1]_p = [n_2 - 1]_p$. ゆえに, $n_1 - 1 \equiv n_2 - 1 \pmod p$ だから, $n_1 \equiv n_2 \pmod p$. ところが, $1 \leq n_1, n_2 \leq p$, $n_1 \neq n_2$ だから, $n_1 = n_2$. したがって, f は単射である.
以上から, f は全単射である.

(b) (a) から f は全単射だから, $\mathbf{Z}/\equiv_p = \{f(1), f(2), \cdots, f(p)\} = \{[0]_p, [1]_p, \cdots, [p-1]_p\}$.

7. (1)
$X_1 = \{1\}$
$X_2 = \{1\}$
$X_3 = \{1, 2\}$
$X_4 = \{1, 3\}$
$X_5 = \{1, 2, 3, 4\}$
$X_6 = \{1, 5\}$
$X_7 = \{1, 2, 3, 4, 5, 6\}$
$X_8 = \{1, 3, 5, 7\}$
$X_9 = \{1, 2, 4, 5, 7, 8\}$
$X_{10} = \{1, 3, 7, 9\}$

(2)
$\varphi(1) = |X_1| = 1$
$\varphi(2) = |X_2| = 1$
$\varphi(3) = |X_3| = 2$
$\varphi(4) = |X_4| = 2$
$\varphi(5) = |X_5| = 4$
$\varphi(6) = |X_6| = 2$
$\varphi(7) = |X_7| = 6$
$\varphi(8) = |X_8| = 4$
$\varphi(9) = |X_9| = 6$
$\varphi(10) = |X_{10}| = 4$

8. (1) (a) 自然数 n $(1 \leq n \leq p^2)$ に対して, $p \mid n$ であるとすると, $n \in \{1 \cdot p, 2 \cdot p, \cdots, p \cdot p\}$. すなわち, $p \mid n$ となる n は p 個である. ゆえに, $\varphi(p^2) = p^2 - p$.

(b) 自然数 n $(1 \leq n \leq p^e)$ に対して, $p \mid n$ であるとすると, $n \in \{1 \cdot p, 2 \cdot p, \cdots, p^{e-1} \cdot p\}$. すなわち, $p \mid n$ となる n は p^{e-1} 個である. ゆえに, $\varphi(p^e) = p^e - p^{e-1}$.

(c) $\gcd(p_1, p_2, \cdots, p_r) = 1$ だから, $\gcd(p_1^{e_1}, p_2^{e_2}, \cdots, p_r^{e_r}) = 1$. $\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r})$.
(b) から, $\varphi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i - 1} = p_i^{e_i}\left(1 - \dfrac{1}{p_i}\right)$.

$$\begin{aligned} \text{ゆえに,} \quad \varphi(n) &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_1^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{e_r}\left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

(2) $24 = 2^3 \cdot 3$ だから，$\varphi(24) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8.$

9. (1) $\gcd(p,m) = 1$ かつ $\gcd(p,n) = 1$ とする．
$\gcd(p,m) = 1$ だから，整数 x, y が存在して，$px + my = 1$.
また，$\gcd(p,n) = 1$ だから，整数 u, v が存在して，$pu + nv = 1$.
ゆえに，$(px+my)(pu+nv) = p \cdot (pxu + xnv + myu) + mn \cdot yv = 1$.
$\gcd(p, mn)$ は p, mn の約数だから，$p \cdot (pxu + xnv + myu) + mn \cdot yv$ の約数である．ゆえに，$\gcd(p, mn)$ は 1 の約数でもあるから，$\gcd(p, mn) = 1$.
一方，$\gcd(p, mn) = 1$ とする．
$\gcd(p, m)$ は p, m の公約数だから，p, mn の公約数でもある．$\gcd(p, mn) = 1$ だから，p, mn の公約数は 1 または -1．ゆえに，p, m の公約数も 1 または -1 であり，$\gcd(p, m) = 1$.
同様に，$\gcd(p, n) = 1$.

(2) $x \equiv b_1 \pmod{m}$ だから，ある整数 q_1 が存在して，$x = q_1 \cdot m + b_1$.
$\gcd(q_1 \cdot m + b_1, m) = \gcd(m, b_1)$ だから，$\gcd(x, m) = \gcd(m, b_1)$.
同様に，$\gcd(x, n) = \gcd(n, b_2)$.
ゆえに，(1) より，$\gcd(m, b_1) = 1$ かつ $\gcd(n, b_2) = 1$ であるとき，かつそのときに限り，$\gcd(mn, x) = 1$.

10. (1) $(a+b)^p = \sum_{k=0}^{p} {}_pC_k a^p b^{p-k} = a^p + {}_pC_1 a^{p-1}b + {}_pC_1 a^{p-1}b + {}_pC_2 a^{p-2}b^2 + \cdots + {}_pC_{p-1} ab^{p-1} + b^p.$
ここで，${}_pC_k = \frac{p!}{k!(p-k)!}$ は整数であり，$k \neq 0, p$ のとき，${}_pC_k$ は p で割り切れる．ゆえに，${}_pC_1 \equiv 0 \pmod{p}$, ${}_pC_2 \equiv 0 \pmod{p}$, $\cdots$, ${}_pC_{p-1} \equiv 0 \pmod{p}$.
すなわち，$(a+b)^p \equiv a^p + 0 + 0 + \cdots + 0 + b^p = a^p + b^p \pmod{p}$.

(2) n に関する数学的帰納法を用いる．
（基底段階）
$n = 1$ のとき．明らか．
$n = 2$ のとき[1]．(1) から明らか．
（帰納段階）$n = k$ $(k \geq 2)$ のときに命題は成り立つと仮定する．
$n = k + 1$ のとき．

$$\begin{aligned}
(a_1 + a_2 + \cdots + a_n)^p &= (a_1 + a_2 + \cdots + a_{k+1})^p \\
&= ((a_1 + a_2 + \cdots + a_k) + a_{k+1})^p \\
&\equiv (a_1 + a_2 + \cdots + a_k)^p + a_{k+1}^p \pmod{p} && \text{((1) から)} \\
&\equiv (a_1^p + a_2^p + \cdots + a_k^p) + a_{k+1}^p \pmod{p} && \text{(帰納法の仮定)} \\
&= a_1^p + a_2^p + \cdots + a_k^p + a_{k+1}^p \\
&= a_1^p + a_2^p + \cdots + a_n^p
\end{aligned}$$

(3) （基底段階）$a = 1$ のとき．$a^p = 1^p = 1 \equiv 1 = a \pmod{p}$.
（帰納段階）$a = k$ のときに命題が成り立つと仮定する．
$a = k + 1$ のとき，(1) から，$a^p = (k+1)^p \equiv k^p + 1^p = k^p + 1 \pmod{p}$.
帰納法の仮定から，$k^p + 1 \equiv k + 1 = a \pmod{p}$．ゆえに，$a^p \equiv a \pmod{p}$.

(4) $b = -a$ とおくと，b は自然数だから，(3) から，$b^p \equiv b \pmod{p}$．ゆえに，$(-a)^p \equiv -a \pmod{p}$.
すなわち，$(-1)^p a^p \equiv (-1)a \pmod{p}$.
$p = 2$ のとき．$(-1)^p = (-1)^2 = 1$, $-1 \equiv 1 \pmod{2}$ だから，$a^p \equiv a \pmod{p}$.
p が奇素数のとき．$(-1)^p = -1$ だから，$-a^p \equiv -a \pmod{p}$．ゆえに，$a^p \equiv a \pmod{p}$.
以上から，$a^p \equiv a \pmod{p}$.

(5) a が自然数のとき，(3) から明らか．
a が負の整数のとき，(4) から明らか．
$a = 0$ のとき，$a^p = 0^p = 0 \equiv 0 = a \pmod{p}$.
以上から，a が整数のとき，$a^p \equiv a \pmod{p}$.

(6) (5) において，p は素数で，$a \not\equiv 0 \pmod{p}$ だから，明らか．

[1] 基底段階は $n = 1$ のときだけでなく，$n = 2$ のときも証明する必要があることに注意せよ．なぜならば，帰納段階の証明は，$n \geq 3$ のときにのみ正しいからである．すなわち，$n = 2$ のときに命題が成り立つことは，$n = 1$ のときに命題が成り立つことを仮定しても導かれない．

11. 17 は素数, $2 \not\equiv 0 \pmod{17}$ だから, Fermat の小定理により, $2^{16} \equiv 1 \pmod{17}$. $1000000 = 16 \cdot 62500$ だから, $2^{1000000} = (2^{16})^{62500} \equiv 1^{62500} \equiv 1 \pmod{17}$. ゆえに, 剰余は 1 である.

12. (1) $d \mid n$ とする. このとき, d は自然数だから, 自然数 q が存在して, $n = qd$. ゆえに, $a^n = a^{qd} = (a^d)^q$. $a^d \equiv 1 \pmod{p}$ だから, $a^n \equiv 1^q \pmod{p}$. したがって, $a^n \equiv 1 \pmod{p}$.
一方, $a^n \equiv 1 \pmod{p}$ とする. $d \mid n$ でないと仮定すると, 自然数 q, r が存在して, $n = qd + r$ $(0 < r < d)$. ゆえに, $a^n = a^{qd+r} = a^{qd}a^r = (a^d)^q a^r$. $a^d \equiv 1 \pmod{p}$ だから, $a^n \equiv 1^q a^r \pmod{p}$. ゆえに, $a^n \equiv a^r \pmod{p}$ だから, $a^r \equiv 1 \pmod{p}$. $r < d$ だから, $r = 0$. これは矛盾. ゆえに, $d|n$.

(2) Fermat の小定理から, $a^{p-1} \equiv 1 \pmod{p}$. (1) から, $d|p-1$, すなわち, d は $p-1$ の約数である.

(3) $a^i \equiv a^j \pmod{p}$ であるとき, かつそのときに限り, $a^{i-j} \equiv 1 \pmod{p}$. (1) から, このとき, かつそのときに限り, $d|i-j$. ゆえに, $a^i \equiv a^j \pmod{p}$ であるならば, かつそのときに限り, $i \equiv j \pmod{d}$.