ひらがな電卓 Calc-H の数学ノート（第三版）

片山博文 MZ

2014 年 8 月 24 日

1　準備

定義 1. 数 $1, 2, 3, 4, \cdots$ を自然数といい，その全体を $\mathbb{N}$ で表す．すなわち，$\mathbb{N} = \{1, 2, 3, 4, \cdots\}$ とおく．

定義 2. 自然数に数 $0, -1, -2, -3, \cdots$ を合わせたものを整数といい，その全体を $\mathbb{Z}$ で表す．すなわち，$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ とおく．

定義 3. x が集合 X に属することを $x \in X$ と表す．

定義 4. 要素を持たない集合，すなわち空集合を $\emptyset$ で表す．

定義 5. 任意の命題 P, Q に対して，P ならば Q が成り立つ，ということを

$$P \Longrightarrow Q$$

と表す．さらに P ならば Q が成り立ち，かつ，Q ならば P が成り立つとき，すなわち

$$P \Longrightarrow Q \quad \text{かつ} \quad Q \Longrightarrow P$$

であるとき，P と Q は同値であるといい，

$$P \Longleftrightarrow Q$$

と表す．

定義 6. 任意の述語 $\mathrm{P}(x)$ と任意の z に対して，

$$z \in \{x \mid \mathrm{P}(x)\} \quad \Longleftrightarrow \quad \mathrm{P}(z). \tag{1}$$

定理 1. 任意の述語 $\mathrm{P}(x), \mathrm{Q}(x)$ に対して，

$$\{x \mid \mathrm{P}(x)\} \cap \{x \mid \mathrm{Q}(x)\} = \{x \mid \mathrm{P}(x) \ \text{かつ} \ \mathrm{Q}(x)\}. \tag{2}$$

証明. $X = \{x \mid \mathrm{P}(x)\}$，$Y = \{x \mid \mathrm{Q}(x)\}$，$Z = \{x \mid \mathrm{P}(x) \ \text{かつ} \ \mathrm{Q}(x)\}$ とおく．$x \in X$ ならば，定義より $\mathrm{P}(x)$ である．また，$y \in Y$ ならば，定義より $\mathrm{Q}(y)$ である．$z \in X \cap Y$，すなわち $z \in X$ かつ $z \in Y$ ならば，$\mathrm{P}(z)$ かつ $\mathrm{Q}(z)$ であるから，$z \in Z$ である．逆に $z \in Z$ であれば，$\mathrm{P}(z)$ かつ $\mathrm{Q}(z)$ であり，$\mathrm{P}(z)$ かつ $\mathrm{Q}(z)$ ならば，$z \in X$ かつ $z \in Y$ であり，$z \in X \cap Y$ であると言える．すなわち任意の z について

$$z \in X \cap Y \quad \Longleftrightarrow \quad z \in Z \tag{3}$$

が成り立つ．よって $X \cap Y = Z$ である．$\square$

定義 7. 任意の整数 x, y のうち最大のものを $\max(x, y)$ と表す．また，任意の整数 x, y のうち最小のものを $\min(x, y)$ と表す．すなわち，

$$\max(x,y)=\begin{cases}x & (x \geqq y \text{ のとき}),\\ y & (x < y \text{ のとき}),\end{cases}\qquad \min(x,y)=\begin{cases}y & (x \geqq y \text{ のとき}),\\ x & (x < y \text{ のとき}).\end{cases} \tag{4}$$

定理 2. 任意の整数 x, y に対して $\max(x, y) + \min(x, y) = x + y$ である．

証明. $x \geqq y$ のときと，$x < y$ のときで場合分けして確かめられる． □

定理 3. 任意の整数 x, y に対して $\max(x - \min(x, y),\, y - \min(x, y)) = \max(x, y) - \min(x, y)$ である．

証明. $x \geqq y$ のときと，$x < y$ のときで場合分けして確かめられる． □

定義 8. 任意の集合 X に対して，X の最大値が存在するならば，その最大値を $\max(X)$ と表す．

定義 9. 任意の集合 X に対して，X の最小値が存在するならば，その最小値を $\min(X)$ と表す．

定義 10. 任意の自然数 x, y に対して，$x \neq 0$ かつ $y \neq 0$ のとき，それらの共通の正の倍数のうちで最小のものを**最小公倍数**といい，$\mathrm{lcm}(x, y)$ で表す．

定義 11. 任意の自然数 x, y に対して，$x \neq 0$ または $y \neq 0$ のとき，それらの共通の約数のうちで最大のものを**最大公約数**といい，$\gcd(x, y)$ で表す．

定義 12. 任意の自然数 n と任意の整数 a, b に対して，差 $b - a$ が n の倍数であるとき，a と b は，n を法として互いに合同であるといい，$a \equiv b \pmod n$ と表し，このような $\equiv$ を含む式を**合同式**という．

定理 4. 任意の自然数 $m_1,\, m_2$ について $m_1 m_2 = \mathrm{lcm}(m_1,\, m_2) \cdot \gcd(m_1,\, m_2)$ である．

証明. $M = \mathrm{lcm}(m_1, m_2)$ かつ $N = \gcd(m_1, m_2)$ とおく．m_1, m_2, M, N を素因数 $p_1,\, p_2,\, \cdots,\, p_r$ により素因数分解すると，

$$m_1 = \prod_{i=1}^{r} p_i^{e_i}, \qquad m_2 = \prod_{i=1}^{r} p_i^{f_i}, \tag{5}$$

$$M = \prod_{i=1}^{r} p_i^{\max(e_i,\, f_i)}, \qquad N = \prod_{i=1}^{r} p_i^{\min(e_i,\, f_i)} \tag{6}$$

と表せる．すると，$\max(e_i, f_i) + \min(e_i, f_i) = e_i + f_i$ であるから

$$MN = \prod_{i=1}^{r} p_i^{\max(e_i,\, f_i)} \prod_{i=1}^{r} p_i^{\min(e_i,\, f_i)} = \prod_{i=1}^{r} p_i^{\max(e_i,\, f_i) + \min(e_i,\, f_i)} = \prod_{i=1}^{r} p_i^{e_i + f_i} \tag{7}$$

となるが，これは

$$m_1 m_2 = \prod_{i=1}^{r} p_i^{e_i} \prod_{i=1}^{r} p_i^{f_i} = \prod_{i=1}^{r} p_i^{e_i + f_i} \tag{8}$$

と等しい． □

定理 5. 任意の自然数 x, y について $d = \gcd(x, y)$ とおけば，$\gcd(x/d,\, y/d) = 1$ である．

証明. x/d と y/d に 1 以外の公約数は存在しない． □

定理 6 (**除法の定理**). 任意の整数 a と任意の自然数 b に対して

$$a = qb + r \quad \text{かつ} \quad 0 \leqq r < b \tag{9}$$

を満たす整数 q, r の組がただ一つ存在する．

証明．「$a = qb + r$ かつ $0 \leqq r < b$ を満たす整数 q, r の組が存在する」という述語を $\mathrm{P}(a,\, b,\, q,\, r)$ で表すことにする．$0 \leqq a < b$ とすると，$\mathrm{P}(a,\, b,\, 0,\, a)$ が満たされる．

$a \geqq b$ とする．数学的帰納法のために任意の $0 \leqq a' < a$ なる任意の整数 a' について，$\mathrm{P}(a',\, b,\, h,\, k)$ を満たす整数 h, k が存在すると仮定する．$0 \leqq a - b < a$ であるから，仮定より，$\mathrm{P}(a-b,\, b,\, q',\, r')$ を満たす整数 q', r' が存在する．よって $a - b = q'b + r'$，これより $a = (q'+1)b + r'$ となるので，$\mathrm{P}(a,\, b,\, q'+1,\, r')$ である．よって，数学的帰納法により，$a \geqq b$ のとき，$\mathrm{P}(a,\, b,\, q,\, r)$ を満たす整数 q, r が存在する．

$a < 0$ とする．$\mathrm{P}(-a,\, b,\, q_0,\, r_0)$ を満たす整数 $q_0,\, r_0$ が存在する．よって $-a = q_0 b + r_0$ かつ $0 \leqq r_0 < b$ である．ここで，$a = (-q_0)b + (-r_0) = -(q_0+1)b + (b - r_0)$ であり，$0 \leqq b - r_0 < b$ であるから，$a < 0$ のとき，$\mathrm{P}(a,\, b,\, -(q_0+1),\, b - r_0)$ を満たす $q = -(q_0+1)$，$r = b - r_0$ が存在する．

次に q, r の組の一意性を証明するために，ある整数 $q_1,\, r_1,\, q_2,\, r_2$ に対して $q_1 > q_2$ かつ $\mathrm{P}(a,\, b,\, q_1,\, r_1)$ かつ $\mathrm{P}(a,\, b,\, q_2,\, r_2)$ と仮定すると，

$$(q_2 - q_1)b = -(r_2 - r_1) \tag{10}$$

となるが，$(q_2 - q_1)$ は自然数であるから，

$$(q_2 - q_1)b \geqq b \tag{11}$$

である．一方，仮定より，$0 \leqq r_1 < b$ かつ $0 \leqq r_2 < b$ であるから，

$$|r_2 - r_1| < b \tag{12}$$

となる．式 (10),(11),(12) は矛盾する．よって $q_1 = q_2$ でなければならない．また，これと式 (10) より，$r_1 = r_2$ となる．これで q, r の組の一意性が証明された．

したがって，任意の整数 a と任意の自然数 b に対して，$\mathrm{P}(a,\, b,\, q,\, r)$ を満たす q, r の組がただ一つ存在することが証明された． □

定理 7 (**ディオファントス方程式の解の存在条件**). r を任意の自然数とする．任意の r 個の整数 $a_1,\ a_2,\ \cdots,\ a_r$ に対して，$a_1,\ a_2,\ \cdots,\ a_r$ の最大公約数 d が存在すると仮定する．このとき，ディオファントス方程式：

$$a_1 x_1 + a_2 x_2 + \cdots + a_r x_r = k \tag{13}$$

を満たす整数解 $x_1,\, x_2,\, \cdots,\, x_r$ が存在するための必要十分条件は，整数 k が d で割り切れることである．

証明． 集合 J を

$$J = \{a_1 x_1 + a_2 x_2 + \cdots + a_r x_r \mid x_1,\, x_2,\, \cdots,\, x_r \in \mathbb{Z}\} \tag{14}$$

とおく．証明すべきは，

$$k \in J \quad \Longleftrightarrow \quad k \text{ は } d \text{ で割り切れる} \tag{15}$$

である．J の要素のうち，正のものを集めた集合を K とおくと，K は空ではない可算集合なので最小値 $\min(K) > 0$ が存在する．$d' = \min(K)$ とおく．ここで任意の u, v に対して J において

性質 i) $u, v \in J$ ならば $u + v \in J$ である，
性質 ii) $u \in J$ ならば任意の整数 z に対して $zu \in J$ である，

という性質 i), ii) が成り立つ．$d' \in K \subseteq J$ である．$0 < u$ を満たす任意の $u \in K$ について，除法の定理より $u = qd' + r$ かつ $0 \leqq r < d'$ を満たす整数 q, r が存在する．性質 ii) より，$(-q)d' \in J$ であり，性質 i) より，$r = u - qd' = u + (-q)d' \in J$ かつ $r < d'$ であるが，d' は K のうち最小であったから，$0 < r < d'$ ではない．よって $r = 0$ かつ $r \notin K$ である．よって任意の $u \in K$ について u が，$u = qd'$，すなわち d' の倍数であることが示された．

$u < 0$ と仮定すると，性質 ii) より，すなわち $u \in J$ かつ $u \notin K$ について，$-u \in K$ であるから，$-u$ は d' の倍数である．よって任意の $u \in J$ について u は d' の倍数である．

逆に u が d' の倍数でなければ，$u \notin J$ である．なぜなら，u が d' の倍数ではなく，かつ $u \in J$ ならば，u は d' の倍数であるから，u が d' の倍数ではないことに矛盾する．

$a_1, a_2, \cdots, a_r$ はすべて J の元であるから，すべて d' の倍数である．言い換えれば d' は $a_1, a_2, \cdots, a_r$ の公約数である．$d' \in J$ であるから，

$$d' = a_1h_1 + a_2h_2 + \cdots + a_rh_r \tag{16}$$

を満たす整数 $h_1, h_2, \cdots, h_r$ が存在する．e を $a_1, a_2, \cdots, a_r$ の正の公約数とする．$a_1h_1, a_2h_2, \cdots, a_rh_r$ がすべて e で割り切れるので，それらの和の d' も e で割り切れる．よって $e \leqq d'$ である．d' は考えられる e のうち，最大のものである．したがって，d' は，$a_1, a_2, \cdots, a_r$ の正の公約数の最大のもの，すなわち $a_1, a_2, \cdots, a_r$ の最大公約数 d である．□

2　本題

定理 8. 任意の自然数 m, n と任意の整数 a, x について，

$$x \equiv a \pmod{mn} \quad \Longrightarrow \quad x \equiv a \pmod{m} \quad \text{かつ} \quad x \equiv a \pmod{n}. \tag{17}$$

証明. $x \equiv a \pmod{mn}$ ならば，$a - x$ は，mn の倍数である．よって $a - x$ は，m の倍数であり，n の倍数である．したがって，$x \equiv a \pmod{m}$ かつ $x \equiv a \pmod{n}$ である．□

定理 9. 任意の自然数 m, n と任意の整数 a, b について，

$$a \equiv b \pmod{n} \quad \Longrightarrow \quad ma \equiv mb \pmod{mn}. \tag{18}$$

証明. 仮定より $b - a$ は n で割り切れる．よって $m \cdot (b - a)$ は mn で割り切れる．したがって $m \cdot (b - a) \equiv 0 \pmod{mn}$ であり，$ma \equiv mb \pmod{mn}$ である．□

定義 13. 任意の自然数 m と整数 a に対して，m を法として a と合同な整数の全体を a の剰余類といい，$\mathrm{R}(a, m)$ と表す．すなわち

$$\mathrm{R}(a, m) = \{b \mid a \equiv b \pmod{m}\} = \{mx + a \mid x \in \mathbb{Z}\} = m\mathbb{Z} + a. \tag{19}$$

定理 10. 任意の自然数 m と任意の整数 r, a に対して，

$$r \in \mathrm{R}(a, m) \quad \Longleftrightarrow \quad r \equiv a \pmod{m}. \tag{20}$$

証明. 定義より明らか. □

定理 11. 任意の自然数 $m_1,\, m_2$ と任意の整数 $y_1,\, y_2$ に対して,

$$y_1 \equiv y_2 \pmod{\mathrm{lcm}(m_1,\, m_2)} \iff \begin{cases} y_1 \equiv y_2 & \pmod{m_1}, \\ y_1 \equiv y_2 & \pmod{m_2}. \end{cases} \tag{21}$$

証明. 左辺を仮定する．$y_2 - y_1$ は $\mathrm{lcm}(m_1,\, m_2)$ の倍数である．すると最小公倍数の定義より，$y_2 - y_1$ は m_1 の倍数であり，m_2 の倍数である．よって $y_1 \equiv y_2 \pmod{m_1}$ かつ $y_1 \equiv y_2 \pmod{m_2}$ である．したがって左辺を仮定して右辺を証明できた．

逆に，右辺を仮定する．$y_1 \equiv y_2 \pmod{m_1}$ ならば，$y_2 - y_1$ は m_1 の倍数である．$y_1 \equiv y_2 \pmod{m_2}$ ならば，$y_2 - y_1$ は m_2 の倍数である．$y_2 - y_1$ は m_1 の倍数であり，m_2 の倍数であるから，最小公倍数の定義より，$y_2 - y_1$ は $\mathrm{lcm}(m_1,\, m_2)$ の倍数である．よって $y_1 \equiv y_2 \pmod{\mathrm{lcm}(m_1,\, m_2)}$ であるから，右辺を仮定して左辺を証明できた． □

定理 12. 任意の自然数 m と任意の整数 x, y に対して次の式が成り立つ.

$$x \equiv y \pmod{m} \iff \mathrm{R}(x, m) = \mathrm{R}(y, m). \tag{22}$$

証明. $x \equiv y \pmod{m}$ ならば

$$\mathrm{R}(x, m) = \{z \mid x \equiv z \pmod{m}\} = \{z \mid y \equiv z \pmod{m}\} = \mathrm{R}(y, m) \tag{23}$$

が得られる．逆に $\mathrm{R}(x, m) = \mathrm{R}(y, m)$ を仮定すると，任意の z に対して

$$z \in \mathrm{R}(x, m) \iff z \in \mathrm{R}(y, m) \tag{24}$$

であるから,

$$x \equiv z \pmod{m} \iff y \equiv z \pmod{m} \tag{25}$$

であり，矛盾を避けると $x \equiv y \pmod{m}$ が得られる. □

定理 13 (中国剰余定理). r を自然数とし，$m_1,\, m_2,\, \cdots,\, m_r$ を互いに素な自然数とすると，任意の整数 $a_1,\, a_2,\, \cdots,\, a_r$ に対して，連立合同式

$$\begin{cases} x \equiv a_1 & \pmod{m_1}, \\ x \equiv a_2 & \pmod{m_2}, \\ \quad\vdots & \\ x \equiv a_r & \pmod{m_r} \end{cases} \tag{26}$$

は，整数解 x を持つ．また，$M = m_1 m_2 \cdots m_r$ とすると，解は M を法として一意的に存在する.

証明. まず，整数解が 2 個以上あったと仮定して，それらを $x_1,\, x_2$ とおく．すると

$$\begin{cases} x_1 \equiv a_1 & \pmod{m_1}, \\ x_1 \equiv a_2 & \pmod{m_2}, \\ \quad\vdots & \\ x_1 \equiv a_r & \pmod{m_r} \end{cases} \quad \text{かつ} \quad \begin{cases} x_2 \equiv a_1 & \pmod{m_1}, \\ x_2 \equiv a_2 & \pmod{m_2}, \\ \quad\vdots & \\ x_2 \equiv a_r & \pmod{m_r} \end{cases} \tag{27}$$

となるが，$x_1 \equiv a_i \equiv x_2 \pmod{m_i}$ より，$x_1 \equiv x_2 \pmod{m_i}$ でなければならない．ここで定理 11 より

$$
\begin{aligned}
x_1 &\equiv x_2 \pmod{\mathrm{lcm}(m_1,\, m_2)}, && (28)\\
x_1 &\equiv x_2 \pmod{\mathrm{lcm}(m_2,\, m_3)}, && (29)\\
&\vdots\\
x_1 &\equiv x_2 \pmod{\mathrm{lcm}(m_{r-1},\, m_r)} && (30)
\end{aligned}
$$

であるから，定理 11 と $\mathrm{lcm}(m_i,\, m_j,\, m_k) = \mathrm{lcm}(\mathrm{lcm}(m_i,\, m_j),\, m_k)$ より

$$
\begin{aligned}
x_1 &\equiv x_2 \pmod{\mathrm{lcm}(m_1,\, m_2,\, m_3)}, && (31)\\
&\vdots\\
x_1 &\equiv x_2 \pmod{\mathrm{lcm}(m_{r-2},\, m_{r-1},\, m_r)}. && (32)
\end{aligned}
$$

このように定理 11 を繰り返し適用することで，

$$x_1 \equiv x_2 \pmod{\mathrm{lcm}(m_1,\, m_2,\, \cdots,\, m_r)} \tag{33}$$

が得られる．ここで $m_1,\, m_2,\, \cdots,\, m_r$ は互いに素であるから，$M = \mathrm{lcm}(m_1,\, m_2,\, \cdots,\, m_r)$ である．よって，

$$x_1 \equiv x_2 \pmod{M} \tag{34}$$

であり，整数解が存在すれば M を法として一意的に存在すると言える．

さて，$1 \leqq i \leqq r$ に対して，$n_i = M/m_i$ とおく．

$$
\begin{aligned}
\gcd(n_i,\, n_j) &= \frac{M}{m_i\, m_j} && (i \neq j), && (35)\\
\gcd(n_i,\, n_j,\, n_k) &= \frac{M}{m_i\, m_j\, m_k} && (i, j, k \text{ は互いに異なる}), && (36)\\
\vdots \quad &\vdots \quad \vdots && && (37)\\
\gcd(n_1,\, n_2,\, \cdots,\, n_r) &= \frac{M}{m_1\, m_2\, \cdots\, m_r} = 1 && (1, 2, \cdots, r \text{ は互いに異なる}). && (38)
\end{aligned}
$$

であるから，$n_1,\, n_2,\, \cdots,\, n_r$ の最大公約数は 1 である．したがって，定理 7 より，整数 $t_1,\, t_2,\, \cdots,\, t_r$ が存在して，

$$n_1 t_1 + n_2 t_2 + \cdots + n_r t_r = 1 \tag{39}$$

を満たす．$i \neq j$ ならば，n_i は m_j の倍数である．よって，

$$n_i t_i \equiv 0 \pmod{m_j} \quad (i \neq j \text{ のとき}). \tag{40}$$

これと式 (39) より，

$$n_i t_i \equiv 1 \pmod{m_j} \quad (i = j \text{ のとき}) \tag{41}$$

である．まとめると，

$$n_i t_i \equiv \begin{cases} 1 & \pmod{m_j} \quad (i = j \text{ のとき}) \\ 0 & \pmod{m_j} \quad (i \neq j \text{ のとき}) \end{cases} \tag{42}$$

である．ここで

$$z = a_1 n_1 t_1 + a_2 n_2 t_2 + \cdots + a_r n_r t_r \tag{43}$$

とおくと，

$$\begin{cases} z \equiv a_1 \pmod{m_1}, \\ z \equiv a_2 \pmod{m_2}, \\ \quad\vdots \\ z \equiv a_r \pmod{m_r} \end{cases} \tag{44}$$

となるので，z は式 (26) の解となる． □

定理 14．任意の自然数 m_1, m_2 と任意の整数 a_1, a_2 に対して，$N = \gcd(m_1,\, m_2)$ とおく．このとき，

$$z \in \mathrm{R}(a_1, m_1) \cap \mathrm{R}(a_2, m_2) \iff z \equiv a_1 \equiv a_2 \pmod{N}. \tag{45}$$

証明． 次の式が成り立つ．

$$z \in \mathrm{R}(a_1, m_1) \cap \mathrm{R}(a_2, m_2) \text{ となる } z \text{ が存在する} \tag{46}$$
$$\iff m_1x_1 + a_1 = m_2x_1 + a_2 \text{ を満たす整数 } x_1,\, x_2 \text{ が存在する} \tag{47}$$
$$\iff m_2x_1 - m_1x_1 = a_1 - a_2 \text{ を満たす整数 } x_1,\, x_2 \text{ が存在する} \tag{48}$$
$$\iff a_1 - a_2 \text{ は } N \text{ の倍数} \iff a_1 - a_2 \equiv 0 \pmod{N} \tag{49}$$
$$\iff a_1 \equiv a_2 \pmod{N}. \tag{50}$$

さらに，$z = m_1x_1 + a_1 = m_2x_2 + a_2$ となる整数 $x_1,\, x_2$ が存在すれば，m_1 が N の倍数であり，m_2 が N の倍数であるから，$z \equiv a_1 \pmod{N}$ かつ $z \equiv a_2 \pmod{N}$ となる．逆に，$z \equiv a_1 \pmod{N}$ かつ $z \equiv a_2 \pmod{N}$ となれば，$z = m_1x_1 + a_1 = m_2x_2 + a_2$ となる整数 $x_1,\, x_2$ が存在して，$z \in \mathrm{R}(a_1, m_1) \cap \mathrm{R}(a_2, m_2)$ となる．よって正しい． □

定理 15．任意の自然数 m_1, m_2 に対して，$M = \mathrm{lcm}(m_1,\, m_2)$，$N = \gcd(m_1,\, m_2)$ とおく．すると，

$$\mathrm{lcm}(m_1/N,\, m_2/N) = M/N. \tag{51}$$

証明． $m_1,\, m_2,\, M,\, N$ を素因数 $p_1,\, p_2,\, \cdots,\, p_r$ で素因数分解すると，式 (5),(6) のようになる．ここで

$$m_1/N = \prod_{i=1}^{r} p_i^{e_i - \min(e_i,\, f_i)}, \qquad m_2/N = \prod_{i=1}^{r} p_i^{f_i - \min(e_i,\, f_i)} \tag{52}$$

となり，

$$\mathrm{lcm}(m_1/N,\, m_2/N) = \prod_{i=1}^{r} p_i^{\max(e_i - \min(e_i,\, f_i),\, f_i - \min(e_i,\, f_i))} \tag{53}$$
$$= \prod_{i=1}^{r} p_i^{\max(e_i,\, f_i) - \min(e_i,\, f_i)} \tag{54}$$
$$= \frac{\prod_{i=1}^{r} p_i^{\max(e_i,\, f_i)}}{\prod_{i=1}^{r} p_i^{\min(e_i,\, f_i)}} = M/N \tag{55}$$

である． □

定理 16．任意の自然数 a, b に対して整数 x が a の倍数であり，x が b の倍数であれば，x は $\mathrm{lcm}(a, b)$ の倍数である．

証明. 最小公倍数の定義より明らか. □

定理 17. 任意の自然数 m_1, m_2 に対して，$N = \gcd(m_1, m_2)$ とおく．このとき，m_1 は $\mathrm{lcm}(m_1/N, N)$ の倍数である.

証明. m_1 が m_1/N の倍数であり，かつ m_1 が N の倍数であるから，定理 16 より正しい. □

定理 18 (**片山 QZ の定理**). 任意の自然数 m_1, m_2 と任意の整数 a_1, a_2 に対して，$M = \mathrm{lcm}(m_1, m_2)$, $N = \gcd(m_1, m_2)$ とおく．このとき，

$$a_1 \equiv a_2 \pmod N \tag{56}$$

ならば

$$\begin{cases} y \equiv a_1 \pmod{m_1} \\ y \equiv a_2 \pmod{m_2} \end{cases} \tag{57}$$

を満たす y が M を法として一意的に存在し，y は a_1, m_1, a_2, m_2 より計算可能である.

証明. 任意の自然数 $m_1,\ m_2$ と任意の整数 $y,\ a_1,\ a_2$ に対して，式 (57) が満たされることを，述語 $\mathrm{Q}(y, a_1, m_1, a_2, m_2)$ で表すことにする.

整数 y_1, y_2 に対して，$\mathrm{Q}(y_1, a_1, m_1, a_2, m_2)$ かつ $\mathrm{Q}(y_2, a_1, m_1, a_2, m_2)$ ならば，$y_1 \equiv y_2 \equiv a_1 \pmod{m_1}$ かつ $y_1 \equiv y_2 \equiv a_2 \pmod{m_2}$ でなければならない．よって定理 11 より，$y_1 \equiv y_2 \pmod M$ となる．したがって，式 (57) を満たす整数解が存在するならば，M を法としてただ一つである.

m_1, m_2 が互いに素ならば，$N = 1$ であり，$a_1 \equiv a_2 \pmod N$ である．このとき，$M = m_1 m_2$ となり，中国剰余定理より，$\mathrm{Q}(y, a_1, m_1, a_2, m_2)$ であり，y は a_1, m_1, a_2, m_2 より計算可能である.

m_1, m_2 が互いに素ではないと仮定する．このとき，$N > 1$ である．$n_1 = m_1/N$, $n_2 = m_2/N$ とおく．n_1 と n_2 は，自然数であり，互いに素であるから，$\mathrm{lcm}(n_1, n_2) = n_1 n_2$ であり，中国剰余定理より，$\mathrm{Q}(y', a_1, n_1, a_2, n_2)$ を満たす整数解 y' が

$$n_1 n_2 = (m_1/N)(m_2/N) = m_1 m_2/N^2 = MN/N^2 = M/N \tag{58}$$

を法としてただ一つ存在し，y' は a_1, m_1, a_2, m_2 より計算可能である．よって

$$\begin{cases} y' \equiv a_1 \pmod{n_1} \\ y' \equiv a_2 \pmod{n_2} \end{cases} \tag{59}$$

である．y' は，M/N を法として一意的に存在するから，除法の定理を用いると，ある整数 h, k により，

$$y' = (M/N)h + k \qquad (0 \leqq k < h) \tag{60}$$

と書ける．h, k は a_1, m_1, a_2, m_2 より計算可能である．M/N が $n_1 = m_1/N$ の倍数であり，$n_2 = m_2/N$ の倍数であるから，

$$\begin{cases} y' \equiv k \equiv a_1 \pmod{n_1} \\ y' \equiv k \equiv a_2 \pmod{n_2} \end{cases} \tag{61}$$

である．ここで

$$y = Mh + k \tag{62}$$

とおくと，y は $a_1,\, m_1,\, a_2,\, m_2$ より計算可能であり，M は $m_1,\, m_2$ の倍数であるから，

$$\begin{cases} y \equiv k \equiv a_1 & \pmod{m_1} \\ y \equiv k \equiv a_2 & \pmod{m_2} \end{cases} \tag{63}$$

となるので，$\mathrm{Q}(y,\, a_1,\, m_1,\, a_2,\, m_2)$ である．

y が存在するためには，定理 14 より，$a_1 \equiv a_2 \pmod{N}$ でなければならない．よって，一般に $a_1 \equiv a_2 \pmod{N}$ のとき，式 (57) を満たす y が常に存在し，y は $a_1,\, m_1,\, a_2,\, m_2$ より計算可能である． □

3 結論

任意の自然数 m_1, m_2 と任意の整数 a_1, a_2 に対して，$M = \mathrm{lcm}(m_1,\, m_2)$，$N = \gcd(m_1,\, m_2)$ とおく．このとき，$a_1 \not\equiv a_2 \pmod{N}$ ならば，定理 14 より $\mathrm{R}(a_1,\, m_1) \cap \mathrm{R}(a_2,\, m_2) = \emptyset$ である．$a_1 \equiv a_2 \pmod{N}$ のときは，定理 18 より $\mathrm{R}(a_1,\, m_1) \cap \mathrm{R}(a_2,\, m_2) = \mathrm{R}(y,\, M)$ を満たす y が存在し，$a_1,\, m_1,\, a_2,\, m_2$ より計算可能である．まとめると，

$$\mathrm{R}(a_1,\, m_1) \cap \mathrm{R}(a_2,\, m_2) = \begin{cases} \emptyset & (a_1 \not\equiv a_2 \pmod{N} \text{ のとき}), \\ \mathrm{R}(y,\, M) & (a_1 \equiv a_2 \pmod{N} \text{ のとき}), \end{cases} \tag{64}$$

である．ここに定理 18 より y は $a_1,\, m_1,\, a_2,\, m_2$ から計算可能である．

このことを確かめるために，実行環境 Intel Core i5, CPU 2.5GHz と日本語版 64 ビット Windows 7 で図 1, 図 2, 図 3 のような C++ のテストプログラム katatest.cpp を作り，C++ コンパイラ g++（tdm64-2）4.8.1 でコンパイルして，2 から 100 までの法についてテストが成功した．実行に要した時間は約 3 分 50 秒．

参考文献

[1]『解析入門 1』松坂 和夫（まつざか・かずお），1997 年，株式会社岩波書店

[2]『工科系のための初等整数論入門』楫　元（かじ・はじめ），2000 年，株式会社培風館

[3]『プログラムの背景』http://www2.cc.niigata-u.ac.jp/~takeuchi/tbasic/BackGround/

[4]『中国剰余定理』藤田 博司，2013 年，
http://tenasaku.com/academia/notes/chinese-remainder.pdf

[5]『Yahoo!知恵袋』http://chiebukuro.yahoo.co.jp

[6]『ウィキペディア (Wikipedia)』http://ja.wikipedia.org

[7]『2ちゃんねる』http://2ch.net

図 1　C++ のテストプログラム katatest.cpp（次のページへ続く）

```
// katatest.cpp --- 片山QZの定理をテストする.
// Copyright (C) 2014 Katayama Hirofumi MZ <katayama.hirofumi.mz@gmail.com>.
#include <cstdio>
#include <cassert>
using namespace std;

// 法の最大値.
```

図 2　C++ のテストプログラム katatest.cpp（続き，次のページに続く）

```
#define MAX 100

// エラー処理．
void error(int num, int a1, int m1, int a2, int m2, int M, int N)
{
    printf("ERROR #%d at (a1:%d, m1:%d, a2:%d, m2:%d, M:%d, N:%d)\n",
           num, a1, m1, a2, m2, M, N);
}

// ユークリッド互除法で最大公約数を求める．
int mygcd(int x, int y)
{
    assert(x != 0 || y != 0);
    if (x < 0) x = -x;
    if (y < 0) y = -y;
    if (y == 0) return x;
    for (;;)
    {
        int z = x % y;
        if (z == 0) break;
        x = y;
        y = z;
    }
    return y;
}

// 最小公倍数を求める．
int mylcm(int x, int y)
{
    assert(x != 0 || y != 0);
    return x * y / mygcd(x, y);
}

// 拡張ユークリッド互除法．
// a>0, b>0に対して，ax + by = dとなるx, yとd = gcd(a, b)を求める．
// dは戻り値．
int gcdx(int& x, int& y, int a, int b)
{
    assert(a > 0 || b > 0);
    int r0 = a, r1 = b, x0 = 1, x1 = 0, y0 = 0, y1 = 1;
    while (r1 > 0)
    {
        int q1 = r0 / r1;
        int r2 = r0 % r1;
        int x2 = x0 - q1 * x1;
        int y2 = y0 - q1 * y1;
        r0 = r1; r1 = r2; x0 = x1; x1 = x2; y0 = y1; y1 = y2;
    }
    x = x0; y = y0;
    return r0;
}

// 中国剰余定理の解を求める．
int chrem(int a1, int m1, int a2, int m2)
{
    assert(m1 > 0 && m2 > 0);
    int x, y;
    int d = gcdx(x, y, m1, m2);
    assert(d == 1);
    return a1 + (a2 - a1) * x * m1;
}

// 片山QZの定理のyと，最小公倍数Mと，最大公約数Nを求める．
// yが存在すれば1を，存在しなければ0を返す．
int katayama(int& y, int& M, int& N, int a1, int m1, int a2, int m2)
{
    N = mygcd(m1, m2); M = m1 * m2 / N;
    //printf("a1:%d, m1:%d, a2:%d, m2:%d, M:%d, N:%d\n",
    //       a1, m1, a2, m2, M, N);

    if ((a2 - a1) % N != 0) return 0;
    if (N != 1)
    {
        m1 /= N; m2 /= N;
```

図 3　C++ のテストプログラム katatest.cpp（続き）

```
    }
    y = chrem(a1, m1, a2, m2);
    while (y < 0) y += M;
    y %= M;
    return 1;
}

// 主処理.
int main(void)
{
    for (int m1 = 1; m1 <= MAX; ++m1)
    {
        for (int m2 = 1; m2 <= MAX; ++m2)
        {
            for (int a1 = 0; a1 < m1; ++a1)
            {
                for (int a2 = 0; a2 < m2; ++a2)
                {
                    int y, M, N;
                    int f = katayama(y, M, N, a1, m1, a2, m2);
                    if (!f && (a2 - a1) % N == 0)
                    {
                        error(1, a1, m1, a2, m2, M, N);
                        return 1;
                    }
                    if (!f)
                        continue;
                    f = 0;
                    for (int k = 0; k < M; ++k)
                    {
                        if (a1 % m1 == k % m1 && a2 % m2 == k % m2)
                        {
                            if (k == y % M)
                            {
                                if (f)
                                {
                                    error(2, a1, m1, a2, m2, M, N);
                                    return 2;
                                }
                                f = 1;
                            }
                        }
                    }
                    if (!f)
                    {
                        printf("y:%d\n", y);
                        error(3, a1, m1, a2, m2, M, N);
                        return 3;
                    }
                }
            }
        }
    }
    printf("success\n");
    return 0;
}
```