1　中国剰余定理

定理 1.1.　正の整数 m, n の最大公約数を d，最小公倍数を l とすれば，整数 a, b について

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n} \tag{1}$$

が解を持つための必要十分条件は

$$a \equiv b \pmod{d}$$

である．解は l を法としてただ一つである．

証明.　(1) が解 x を持つとき，$d = (m, n)$ であるから，特に $x \equiv a \,(\mathrm{mod}\, d)$, $x \equiv b \,(\mathrm{mod}\, d)$，よって $a \equiv b \,(\mathrm{mod}\, d)$ である．

次に，$a \equiv b \,(\mathrm{mod}\, d)$ が成り立っているとき，(1) が解を持つことを示す．一番目の合同式を満たす x は，ある整数 t によって

$$x = a + mt \tag{2}$$

と書ける．このような x が二番目の合同式の解になるのは

$$a + mt \equiv b \pmod{n}$$

すなわち

$$mt \equiv b - a \pmod{n} \tag{3}$$

のときである．仮定によって $(m, n) = d$, $a \equiv b \,(\mathrm{mod}\, d)$ であるから

$$\frac{m}{d} t \equiv \frac{b-a}{d} \quad \left(\mathrm{mod}\ \frac{n}{d}\right)$$

よって (3) の解 t は，ある整数 t_0, s によって

$$t = t_0 + \frac{n}{d} s$$

と表すことができる．これを (2) に代入すれば

$$x = a + mt_0 + ls$$

ここで $dl = mn$ を用いた．この x は (1) の解である．また明らかに x と l を法として合同な整数はすべて (1) の解である．したがって

$$x \equiv a + mt_0 \pmod{l}$$

を満たす整数 x はすべて (1) の解である．

最後に一意性を示す．x, x' を (1) の解とすると，$x - x'$ は m, n で割れるから，それらの最小公倍数 l でも割り切れる．すなわち $x \equiv x' \,(\mathrm{mod}\, l)$ である．　□

補題 1.2.　整数 a, b の最小公倍数を $\{,\}$ によって表すことにする．整数 a, b, c について

$$(\{a, b\}, c) = \{(a, c), (b, c)\}$$

が成り立つ．

証明. $a=p_1^{a_1}\cdots p_r^{a_r}$, $b=p_1^{b_1}\cdots p_r^{b_r}$, $c=p_1^{c_1}\cdots p_r^{c_r}$ と素因数分解する．上の等式を証明することは，各 i について

$$\min\{\max\{a_i,\, b_i\},\, c_i\} = \max\{\min\{a_i,\, c_i\},\, \min\{b_i,\, c_i\}\} \tag{4}$$

を示すことに帰着される．

i を一つ固定する．$c_i \geq a_i$, $c_i \geq b_i$ ならば，左辺も右辺も $\max\{a_i,\, b_i\}$ になる．よって (4) が成り立つ．$a_i > c_i$ ならば

$$c_i < a_i \leq \max\{a_i,\, b_i\}$$

より左辺は c_i である．一方

$$\min\{a_i,\, c_i\} = c_i, \qquad \min\{b_i,\, c_i\} \leq c_i$$

であるから右辺も c_i である．よって (4) が成り立つ．$b_i > c_i$ のときも同様である． □

定理 1.3. $m_1,\, \ldots,\, m_r$ を正の整数とする．このとき整数 $a_1,\, \ldots,\, a_r$ について

$$x \equiv a_k \pmod{m_k}, \qquad k = 1,\, 2,\, \ldots,\, r \tag{5}$$

に解があるための必要十分条件は

$$a_i \equiv a_j \pmod{(m_i,\, m_j)}, \qquad i,\, j = 1,\, 2,\, \ldots,\, r$$

である．解は $m_1,\, \ldots,\, m_r$ の最小公倍数を法としてただ一つである．

証明. 条件の必要性は明らかだから，条件が成り立っていると仮定して (5) が解を持つことを示す．定理 1.1 により，二つの合同式

$$x \equiv a_1 \pmod{m_1}, \qquad x \equiv a_2 \pmod{m_2}$$

の解を

$$x \equiv b \pmod{\{m_1,\, m_2\}}$$

のような形の合同式で表すことができる．これと第三の合同式とを組み合わせたとき

$$x \equiv b \pmod{\{m_1,\, m_2\}}, \qquad x \equiv a_3 \pmod{m_3} \tag{6}$$

が $\{m_1,\, m_2,\, m_3\}$ を法としてただ一つの解を持つことを示す．

仮定によって $b \equiv a_1 \pmod{m_1}$．ゆえに $b - a_3 \equiv a_1 - a_3 \pmod{m_1}$．したがって

$$b - a_3 \equiv a_1 - a_3 \equiv 0 \pmod{(m_1,\, m_3)}$$

すなわち $b - a_3$ は $(m_1,\, m_3)$ で割り切れる．同様にして $(m_2,\, m_3)$ でも割り切れることもわかる．したがって $\{(m_1,\, m_3),\, (m_2,\, m_3)\}$ で割り切れる．ところが補題 1.2 により

$$(\{m_1,\, m_2\},\, m_3) = \{(m_1,\, m_3),\, (m_2,\, m_3)\}$$

だから $b - a_3$ は $(\{m_1,\, m_2\},\, m_3)$ で割り切れる．したがって定理 1.1 により (6) は $\{m_1,\, m_2,\, m_3\}$ を法としてただ一つの解を持つ．

同様にして，r についての帰納法によって定理を証明することができる． □

系 1.4 (中国剰余定理). $m_1, \ldots, m_r$ を 2 つずつ互いに素な正の整数とする．このとき，任意の整数 $a_1, \ldots, a_r$ について

$$x \equiv a_k \pmod{m_k}, \qquad k = 1, 2, \ldots, r \tag{7}$$

を満たす x は $M = m_1 \cdots m_r$ を法としてただ一つ存在する．

証明. 定理 1.3 において，各 i, j について $(m_i, m_j) = 1$ となる場合である．ここでは Gauss による別証明を与える．

$$M = m_1 M_1 = m_2 M_2 = \cdots = m_r M_r \tag{8}$$

とおくと，$k = 1, 2, \ldots, r$ に対して

$$M_k t_k \equiv 1 \pmod{m_k} \tag{9}$$

となる整数 t_k が存在する．このとき

$$x = a_1 M_1 t_1 + a_2 M_2 t_2 + \cdots + a_r M_r t_r \tag{10}$$

が (7) の解である．実際，(9) によって，(10) の右辺の第一項は

$$a_1 M_1 t_1 \equiv a_1 \pmod{m_1}$$

である．第二項以下については，(8) によって $M_2, \ldots, M_r$ が m_1 で割り切れるから

$$a_2 M_2 t_2 \equiv \cdots \equiv a_r M_r t_r \equiv 0 \pmod{m_1}$$

よって

$$x \equiv a_1 \pmod{m_1}$$

$m_2, m_3, \ldots, m_r$ に関しても同様に議論すれば

$$x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_r \pmod{m_r}$$

がいえる．したがって (10) は (7) の解である．また明らかに (10) と M を法として合同な整数もまた (7) の解である．

x, x' を (7) の解とすると

$$x \equiv x' \pmod{m_k}, \qquad k = 1, 2, \ldots, r$$

であるから，$x - x'$ は $m_1, \ldots, m_r$ で割りきれる．したがって，それらの最小公倍数 M でも割り切れる．すなわち $x \equiv x' \pmod{M}$ である． □

2 単位元を持つ可換環への一般化

以下，R を単位元を持つ可換環とする．

定理 2.1. $\mathfrak{a}, \mathfrak{b}$ を R のイデアル，a, b を R の元とする．このとき，連立方程式

$$x \equiv a \pmod{\mathfrak{a}}, \qquad x \equiv b \pmod{\mathfrak{b}} \tag{11}$$

が R で解を持つための必要十分条件は

$$a \equiv b \pmod{\mathfrak{a}+\mathfrak{b}} \tag{12}$$

が成り立つことである．もし (11) に解があれば，それは $\mathfrak{a}\cap\mathfrak{b}$ を法として一意的である．

証明. (11) の解 x が存在するとき，(12) が成り立つことは明らかである．
(12) が成り立っているとすると

$$a-b=c+c' \qquad (\exists c\in\mathfrak{a},\ \exists c'\in\mathfrak{b})$$

そこで

$$x=a-c=b+c'$$

とおけば，x は (11) の解になる．
また，x, x' が共に (11) の解ならば $x-x'\in\mathfrak{a}\cap\mathfrak{b}$ である． □

定理 2.2. $n\geq 3$ とし，$\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ を R のイデアル，$a_1, \ldots, a_n$ を R の元とし

$$\left(\bigcap_{i=1}^{m-1}\mathfrak{a}_i\right)+\mathfrak{a}_m=\bigcap_{i=1}^{m-1}(\mathfrak{a}_i+\mathfrak{a}_m), \qquad (3\leq m\leq n) \tag{13}$$

が成り立っていると仮定する．このとき，連立方程式

$$x \equiv a_i \pmod{\mathfrak{a}_i} \qquad (i=1, \ldots, n) \tag{14}$$

が解を持つための必要十分条件は

$$a_i \equiv a_j \pmod{\mathfrak{a}_i+\mathfrak{a}_j} \qquad (1\leq i\leq n,\ 1\leq j\leq n) \tag{15}$$

が成り立つことである．
もし (14) に解があれば，それは $\mathfrak{a}\cap\mathfrak{b}$ を法として一意的である．

証明. (14) の解 x が存在するとき，(15) が成り立つことは明らかである．
(15) が成り立っているとする．定理 2.1 により，二つの合同式

$$x \equiv a_1 \pmod{\mathfrak{a}_1}, \qquad x \equiv a_2 \pmod{\mathfrak{a}_2}$$

の解を

$$x \equiv b \pmod{\mathfrak{a}_1\cap\mathfrak{a}_2}$$

のような形の合同式で表すことができる．これと第三の合同式とを組み合わせたとき

$$x \equiv b \pmod{\mathfrak{a}_1\cap\mathfrak{a}_2}, \qquad x \equiv a_3 \pmod{\mathfrak{a}_3} \tag{16}$$

が $\mathfrak{a}_1\cap\mathfrak{a}_2\cap\mathfrak{a}_3$ を法としてただ一つの解を持つことを示す．
仮定によって $b\equiv a_1 \pmod{\mathfrak{a}_1}$．ゆえに $b-a_3\equiv a_1-a_3 \pmod{\mathfrak{a}_1}$．したがって

$$b-a_3\equiv a_1-a_3\equiv 0 \pmod{\mathfrak{a}_1+\mathfrak{a}_3}$$

すなわち $b-a_3 \in \mathfrak{a}_1+\mathfrak{a}_3$．同様にして $b-a_3 \in \mathfrak{a}_2+\mathfrak{a}_3$ もわかる．したがって

$$b-a_3 \in (\mathfrak{a}_1+\mathfrak{a}_3)\cap(\mathfrak{a}_2+\mathfrak{a}_3)$$

仮定により，この条件は

$$b-a_3 \in (\mathfrak{a}_1\cap\mathfrak{a}_2)+\mathfrak{a}_3$$

と同値である．したがって定理 2.1 により (16) は $\mathfrak{a}_1\cap\mathfrak{a}_2\cap\mathfrak{a}_3$ を法としてただ一つの解を持つ．

同様にして，n についての帰納法によって定理を証明することができる． □

注意 2.3. 条件 (13) は $R=\mathbb{Z}$ のとき常に成り立つ (補題 1.2)．けれども一般には成り立たない．例えば $R=\mathbb{Q}[X, Y]$ とし，R のイデアルとして

$$\mathfrak{a}=(X), \qquad \mathfrak{b}=(Y), \qquad \mathfrak{c}=(X+Y)$$

をとると

$$\begin{aligned}
&\mathfrak{a}\cap\mathfrak{b}=(XY),\\
&\mathfrak{a}+\mathfrak{c}=\mathfrak{b}+\mathfrak{c}=(X,Y),\\
&(\mathfrak{a}\cap\mathfrak{b})+\mathfrak{c}=(X+Y,\, XY),\\
&(\mathfrak{a}+\mathfrak{c})\cap(\mathfrak{b}+\mathfrak{c})=(X,\, Y)
\end{aligned}$$

である．ところが

$$X\in(X,\, Y), \qquad X\notin(X+Y,\, XY)$$

より $(X,\, Y)\neq(X+Y,\, XY)$．よって今の場合 (11) は成り立たない．

補題 2.4. $\mathfrak{a}_1,\, \ldots,\, \mathfrak{a}_n,\, \mathfrak{b}$ を R のイデアルとする．このとき

$$\mathfrak{a}_i+\mathfrak{b}=R \qquad (i=1,\, \ldots,\, n)$$

ならば

$$\mathfrak{a}_1\cdots\mathfrak{a}_n+\mathfrak{b}=\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n+\mathfrak{b}=R$$

が成り立つ．

証明. 仮定から，各番号 i について

$$1=a_i+b_i \qquad (\exists a_i\in\mathfrak{a}_i,\, \exists b_i\in\mathfrak{b})$$

このとき

$$a_1\cdots a_n=(1-b_1)\cdots(1-b_n)=1+b \qquad (\exists b\in\mathfrak{b})$$

ゆえに

$$1=a_1\cdots a_n-b\in\mathfrak{a}_1\cdots\mathfrak{a}_n+\mathfrak{b}$$

このことは $\mathfrak{a}_1\cdots\mathfrak{a}_n+\mathfrak{b}=R$ と同値である．

また，一般に

$$\mathfrak{a}_1\cdots\mathfrak{a}_n\subseteq\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n$$

であるから，$\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n+\mathfrak{b}=R$ となる． □

補題 2.5.　$\mathfrak{a}_1, \dots, \mathfrak{a}_n$ を R のイデアルとし

$$i \neq j \Longrightarrow \mathfrak{a}_i + \mathfrak{a}_j = R$$

が成り立っていると仮定する．このとき

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$$

が成り立つ．

証明．　n に関する数学的帰納法で証明する．

$n = 2$ のとき．$\mathfrak{a}_1 + \mathfrak{a}_2 = R$ より

$$\mathfrak{a}_1 \cap \mathfrak{a}_2 = (\mathfrak{a}_1 \cap \mathfrak{a}_2)(\mathfrak{a}_1 + \mathfrak{a}_2) \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$$

したがって $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$ である．

$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}$ と仮定する．補題 2.4 より

$$\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} + \mathfrak{a}_n = R$$

よって $n = 2$ の場合により

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$$

となる．　□

注意 2.6.　補題 2.5 は $i \neq j \Longrightarrow \mathfrak{a}_i + \mathfrak{a}_j = R$ なる条件を除くと必ずしも成り立たない．

例えば，$R = \mathbb{Z}, \mathfrak{a} = 2\mathbb{Z}, \mathfrak{b} = 4\mathbb{Z}$ とすると

$$\mathfrak{a}\mathfrak{b} = 8\mathbb{Z}, \qquad \mathfrak{a} \cap \mathfrak{b} = 4\mathbb{Z}$$

ゆえに $\mathfrak{a}\mathfrak{b} \subsetneq \mathfrak{a} \cap \mathfrak{b}$.

定理 2.7 (中国剰余定理の一般化).　$\mathfrak{a}_1, \dots, \mathfrak{a}_n$ を R のイデアル，$a_1, \dots, a_n$ を R の元とし

$$i \neq j \Longrightarrow \mathfrak{a}_i + \mathfrak{a}_j = R \tag{17}$$

が成り立っていると仮定する．このとき，連立方程式

$$x \equiv a_i \pmod{\mathfrak{a}_i} \qquad (i = 1, \dots, n) \tag{18}$$

は必ず解を持つ．

もし (18) に解があれば，それは $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ を法として一意的である．

証明．　条件 (17) が成り立つならば，定理 2.2 における条件 (15) が成り立つ．また，補題 2.4 により，定理 2.2 における条件 (13) が成り立つこともいえる．よって連立方程式 (18) は解を持ち，それは $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ を法として一意的である．ところが補題 2.5 より $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ である．　□

定理 2.8.　$\mathfrak{a}_1$, ..., $\mathfrak{a}_n$ を R のイデアル，$\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ とし

$$i \neq j \Longrightarrow \mathfrak{a}_i + \mathfrak{a}_j = R$$

が成り立っていると仮定する．このとき，写像

$$R/\mathfrak{a} \longrightarrow R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n, \qquad x + \mathfrak{a} \longmapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$$

は環の同型写像である．

証明.　環の準同型写像

$$f : R \longrightarrow R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n, \qquad x \longmapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$$

を考える．定理 2.7 において，解が存在することは f が全射であることを意味し，解が $\mathfrak{a}$ を法として一意的であることは $\mathrm{Ker}\ f = \mathfrak{a}$ を意味する．ゆえに準同型定理により求める同型写像が得られる． □

補題 2.9.　$\mathfrak{a}$ を R のイデアルとし，$(R/\mathfrak{a})^\times$ を $R/\mathfrak{a}$ の単元全体からなる乗法群とする．このとき

$$(R/\mathfrak{a})^\times = \{a + \mathfrak{a} \in R/\mathfrak{a} \mid (a, \mathfrak{a}) = R\}$$

が成り立つ．

証明.　R の元 a について

$$\begin{aligned} a + \mathfrak{a} \in (R/\mathfrak{a})^\times &\Longleftrightarrow ax + \mathfrak{a} = 1 + \mathfrak{a}\ (\exists x \in R) \\ &\Longleftrightarrow ax - 1 \in \mathfrak{a}\ (\exists x \in R) \\ &\Longleftrightarrow ax + y = 1\ (\exists x \in R,\ \exists y \in \mathfrak{a}) \\ &\Longleftrightarrow 1 \in (a) + \mathfrak{a} \\ &\Longleftrightarrow (a, \mathfrak{a}) = R \end{aligned}$$

である． □

定理 2.10.　$\mathfrak{a}_1$, ..., $\mathfrak{a}_n$ を R のイデアル，$\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ とし

$$i \neq j \Longrightarrow \mathfrak{a}_i + \mathfrak{a}_j = R$$

が成り立っていると仮定する．このとき，写像

$$(R/\mathfrak{a})^\times \longrightarrow (R/\mathfrak{a}_1)^\times \times \cdots \times (R/\mathfrak{a}_n)^\times, \qquad x + \mathfrak{a} \longmapsto (x + \mathfrak{a}_1,\ \ldots,\ x + \mathfrak{a}_n)$$

は乗法群の同型写像である．

証明.　R の元 a について

$$(a,\ \mathfrak{a}) = R \Longrightarrow (a,\ \mathfrak{a}_1) = \cdots = (a,\ \mathfrak{a}_n) = R$$

であるから，写像 f は well-defined である (補題 2.9).

　f が群の準同型写像であることは明らかである．

f の単射性は次のことから分かる：

$$\begin{aligned} f(a+\mathfrak{a}) = (1+\mathfrak{a}_1,\,\ldots,\,1+\mathfrak{a}_n) &\Longrightarrow a \equiv 1 \pmod{\mathfrak{a}_i}\ (i=1,\,\ldots,\,n) \\ &\Longrightarrow a \equiv 1 \pmod{\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n} \\ &\Longrightarrow a \equiv 1 \pmod{\mathfrak{a}} \qquad (\because \text{補題 } 2.5) \end{aligned}$$

$(a_1+\mathfrak{a}_1,\,\ldots,\,a_n+\mathfrak{a}_n)$ を $(R/\mathfrak{a}_1)^\times \times \cdots \times (R/\mathfrak{a}_n)^\times$ の元とする．定理 2.2 より，R の元 x で

$$x \equiv a_i \pmod{\mathfrak{a}_i}\ (i=1,\,\ldots,\,n)$$

を満たすものが存在する．$(a,\,\mathfrak{a}_1) = \cdots = (a,\,\mathfrak{a}_n) = R$ であるから，$(x,\,\mathfrak{a}) = R$ でなければならない．よって補題 2.9 より $x+\mathfrak{a} \in (R/\mathfrak{a})^\times$．しかも

$$f(x+\mathfrak{a}) = (a_1+\mathfrak{a}_1,\,\ldots,\,a_n+\mathfrak{a}_n)$$

が成り立つ．したがって f は全射である． □