第7章　中国の剰余定理

7.1　中国の剰余定理

この章の主目的は次の定理を証明することである．

定理 7.1 (中国の剰余定理) $m_1, m_2, \cdots, m_r$ をどの２つも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

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \cdots\cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

は整数解 x をもつ．さらに，$M = m_1 \cdots m_r$ とすると，解は M を法として一意的である．すなわち，$x, x' \in \boldsymbol{Z}$ がともに解ならば $x \equiv x' \pmod{M}$ が成り立つ．

最後の部分，一意性は次のようにして確かめられる．$x, x' \in \boldsymbol{Z}$ がどちらも上の合同式をみたすならば，$x - x'$ は $m_1, m_2, \cdots, m_r$ すべての倍数である．一方，仮定より m_i 達はどの２つも互いに素だから，これらの最小公倍数は M であり，$x \equiv x' \pmod{M}$ が確かめられた．

以下において，解が存在することの証明を３通り与える．

第１証明　$r = 1$ のときは明らかなので $r \geq 2$ としよう．まず，第１の合同式から解は $a_1 + m_1 y$ の形をしている．これが第２の式をみたしているので

$$a_1 + m_1 y \equiv a_2 \pmod{m_2} \quad \text{すなわち} \quad m_1 y \equiv a_2 - a_1 \pmod{m_2}$$

であるが，m_1, m_2 は互いに素なので，定理 5.9 より，法 m_2 に関する m_1 の逆元 b がとれ，それを用いて $y \equiv b(a_2 - a_1) \pmod{m_2}$ と書ける．m_1 を掛けて $m_1 y \equiv m_1 b(a_2 - a_1) \pmod{m_1 m_2}$，したがって，第１，第２の合同式はひとつの合同式

$$x \equiv a_1 + m_1 b(a_2 - a_1) \pmod{m_1 m_2}$$

に置き換えることができ，$r = 2$ ならばこれが解を与えることになる．$r \geq 3$ のときも，この操作を繰り返すことで最終的にひとつの合同式に帰着され，それが解となる（正確には数学的帰納法による）．　□

第 2 証明　まず，$n_1, \cdots, n_r \in \boldsymbol{Z}$ を次式で定める;

$$n_i m_i = m_1 \cdots m_r \quad (i = 1, \cdots r).$$

すなわち n_i は $m_1, \cdots, m_r$ から m_i を除いたものの積であり，仮定より m_i, n_i は互いに素である．このとき，$n_1, \cdots, n_r$ の最大公約数は 1 である．実際，そうでないとすると，$n_1 \equiv \cdots \equiv n_r \equiv 0 \pmod{p}$ をみたす素数 p が存在する．とくに $m_2 \cdots m_r = n_1 \equiv 0 \pmod{p}$ より，$m_j \equiv 0 \pmod{p}$ をみたす $2 \leq j \leq r$ がとれるが，これは m_j, n_j が互いに素であることに矛盾する．よって $\gcd(n_1, \cdots, n_r) = 1$ が示され，定理 3.4 より

$$n_1 t_1 + \cdots + n_r t_r = 1$$

をみたす $t_1, \cdots, t_r \in \boldsymbol{Z}$ が存在する．このとき，n_i の定め方から，$1 \leq i, j \leq r$ に対して

$$n_i t_i \equiv \begin{cases} 1 & (i = j) \\ 0 & (i \neq j) \end{cases} \pmod{m_j}$$

であることがすぐにわかり，したがって $x = a_1 n_1 t_1 + \cdots + a_r n_r t_r$ が解を与える．　□

上記 2 つの証明は，実際に解を求める計算法も与えている．数学的帰納法による第 1 証明は，合同式を 2 つずつ順々に解いていく方法，第 2 証明はすべての合同式を同時に扱い，解を一気に構成する方法である．第 3 証明は次の節で与えることとし，ここではひとつの例題に対し，第 1 および第 2 証明にそった解法をそれぞれ例示する．

例 7.2 次の連立合同式を解け.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

解 1　まず第 1 の合同式から，解は $2 + 3k$ の形をしている．これが第 2 の式をみたすから $2 + 3k \equiv 3 \pmod{5}$，これを解いて $k \equiv 2 \pmod{5}$ したがって $3k \equiv 6 \pmod{15}$ となるから，第 1，第 2 の合同式はひとつの合同式 $x = 2 + 3k \equiv 8 \pmod{15}$ に帰着する．次に，この解は $8 + 15l$ の形をしているから，第 3 の合同式に当てはめ，$8 + 15l \equiv 2 \pmod{7}$ を解いて $l \equiv 1 \pmod{7}$，したがって 15 を掛けて $15l \equiv 15 \pmod{105}$．これから，解 $x = 8 + 15l \equiv 23 \pmod{105}$ を得る.

解 2　まず，$35t_1 + 21t_2 + 15t_3 = 1$ の形の式を見つけたい．そのために $5 \cdot (-1) + 3 \cdot 2 = 1$ と $7 \cdot (-2) + 15 = 1$ に注目して，

$$1 = 7 \cdot (-2) + 15 = 7 \cdot (-2) \cdot (5 \cdot (-1) + 3 \cdot 2) + 15 = 35 \cdot 2 + 21 \cdot (-4) + 15 \cdot 1,$$

すなわち $(t_1, t_2, t_3) = (2, -4, 1)$ が求まる．これを用いて，解

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot (-4) + 2 \cdot 15 \cdot 1 = -82$$

を得る．$-82 \equiv 23 \pmod{105}$ より，**解 1** と同じ解が得られたことに注意せよ.

この例は 3〜5 世紀頃書かれた中国の算術書【孫子算經】に載っていて，上にあげた**解 2** と同趣旨の解法も与えられている． **解 2** は各合同式を同等に扱い（つまり対称性があり）理論的にも優れていると思われるが，途中の計算の意味がとらえにくいのが欠点である．**解 1** の方が計算しやすいと私は思うが，皆さんはどうかな？

7.2 第 3 証明

定理 7.1 の第 1 および第 2 証明は，証明自体が解の計算法を与えていたが，以下に述べる第 3 証明からは直接に解を求める方法を見出すことができない． しかし，理論上はきわめて重要であり，その内容は今後の講義でもたびたび扱われるはずである． 証明の根拠となるのは，有限集合 A, B の元の個数が同じとき，A から B への写像は，**単射**ならば**全射**でもあるという事実である．

第 3 証明

$r = 2$ の場合を示せば，数学的帰納法によって一般の場合も示せるので，互いに素な $m, n \in \boldsymbol{N}$ と任意の $a, b \in \boldsymbol{Z}$ に対して

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

の整数解の存在を証明することにする． いま，$u \equiv v \pmod{mn}$ ならば，$u \equiv v \pmod{m}$ かつ $u \equiv v \pmod{n}$ なので，二つの写像

$$\begin{aligned} \boldsymbol{Z}/mn\boldsymbol{Z} &\longrightarrow \boldsymbol{Z}/m\boldsymbol{Z}, \qquad u + mn\boldsymbol{Z} \mapsto u + m\boldsymbol{Z}, \\ \boldsymbol{Z}/mn\boldsymbol{Z} &\longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}, \qquad u + mn\boldsymbol{Z} \mapsto u + n\boldsymbol{Z} \end{aligned}$$

を定めることができる． これらをあわせて剰余集合の直積への写像

$$F \ : \ \boldsymbol{Z}/mn\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z}), \qquad u + mn\boldsymbol{Z} \mapsto (u + m\boldsymbol{Z}, u + n\boldsymbol{Z})$$

が定義できる． F が単射であることを示そう． そのために，$F(u+mn\boldsymbol{Z}) = F(v+mn\boldsymbol{Z})$ とすると，$u + m\boldsymbol{Z} = v + m\boldsymbol{Z}$ かつ $u + n\boldsymbol{Z} = v + n\boldsymbol{Z}$． よって $u - v$ は m の倍数でもあり n の倍数でもある． ここで m, n は互いに素だから $u - v$ は mn の倍数，すなわち $u + mn\boldsymbol{Z} = v + mn\boldsymbol{Z}$ を得る． これで F が単射であることが示された． ところで，$\boldsymbol{Z}/mn\boldsymbol{Z}$ の元の個数は mn であり，これは直積集合 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ の元の個数と等しい． したがって F は全射でもある． すなわち，任意の $a, b \in \boldsymbol{Z}$ に対して $F(x + mn\boldsymbol{Z}) = (a + m\boldsymbol{Z}, b + n\boldsymbol{Z})$ をみたす $x \in \boldsymbol{Z}$ が存在するが，これを書き換えると

$$x + m\boldsymbol{Z} = a + m\boldsymbol{Z} \quad \text{かつ} \quad x + n\boldsymbol{Z} = b + n\boldsymbol{Z}.$$

これらの等式は，x がはじめの合同式の解であることを示している． □

この証明によって，m, n が互いに素ならば，自然な全単射

$$\boldsymbol{Z}/mn\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$$

が存在することがわかる． さらに，一般に $m_1, \cdots, m_r$ のどの 2 つも互いに素ならば，$M = m_1 \cdots m_r$ として，自然な全単射

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m_1\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/m_r\boldsymbol{Z})$$

が存在する． ここで “自然な” とは，対応が $\overline{a} \mapsto (\overline{a}, \cdots, \overline{a})$ によって与えられることを意味する． ただし，それぞれの $\overline{a}$ は，法 M および法 m_1，$\cdots$，法 m_r に関する剰余類を考えるのである． さらに重要なことは，この全単射が “演算を保存する” ことだが，それを説明するためには剰余類の間の和や積を定義しなければならない． 次回を乞ご期待！

7.3　ひとつの応用例

中国の剰余定理には様々な応用がある． ここでは，高次合同式への応用のひとつとして 2 次合同式

$$(1) \qquad x^2 + 998x + 241 \equiv 0 \pmod{7560}.$$

の整数解を考えよう． 素朴に考えれば，x に $0, 1, 2, \cdots, 7559$ を順に代入して行けばいつか解に到達する可能性があるが，これでは効率が悪いので別の方法を試みる． 法 7560 の素因数分解 $7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$ に注目すれば，(1) が次の 4 つの合同式に帰着されることは簡単な計算からわかる．

$$(2) \qquad \begin{cases} x^2 - 2x + 1 \equiv 0 \pmod{8} \\ x^2 - \ x - 2 \equiv 0 \pmod{27} \\ x^2 - 2x + 1 \equiv 0 \pmod{5} \\ x^2 - 3x + 3 \equiv 0 \pmod{7} \end{cases}$$

これらそれぞれについて（x に値を順に代入して）解を見つけるのはそれほど大変ではない． 実際，それぞれ以下のような解が見つかる．

$$(3) \qquad x \equiv 1 \pmod{8}, \quad x \equiv -1 \pmod{27}, \quad x \equiv 1 \pmod{5}, \quad x \equiv -1 \pmod{7}$$

中国の剰余定理を適用してこれらを連立させれば，$x \equiv 3401 \pmod{7560}$ が得られるが，これがもとの 2 次合同式 (1) の解になっている． 解の導出と確認は演習としよう．

さて，以上の方法で (1) のひとつの解が求まったが，(2) の解は (3) 以外にもあることに注意しよう． たとえば 8 を法とする合同式には $x \equiv 5 \pmod{8}$ という解もありこれ以外にはない． 7 を法とする解もあとひとつだけ見つかる． 法 5 については他にはないが，法 27 に関しては全部で 6 個の解をもつ． よって，(1) は 7560 を法として $2 \cdot 6 \cdot 1 \cdot 2 = 24$ 個の解をもつことがわかる． これらをすべて求めるのは無謀だからやめた方がいいってば！