

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, \dots, 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, \dots, a_r に対して, 連立合同式

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

は整数解 x をもつ。さらに, $M = m_1 \cdots m_r$ とすると, 解は M を法として一意である。すなわち, $x, x' \in \mathbb{Z}$ 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。 $x, x' \in \mathbb{Z}$ がどちらも上の合同式をみたすならば, $x - x'$ は m_1, m_2, \dots, 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, $n_1, \dots, n_r \in \mathbb{Z}$ を次式で定める;

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

すなわち n_i は m_1, \dots, 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, \dots, n_r の最大公約数は 1 である. 実際, そうでないとする, $n_1 \equiv \dots \equiv n_r \equiv 0 \pmod{p}$ 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 $\gcd(n_1, \dots, n_r) = 1$ が示され, 定理 3.4 より

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

をみたす $t_1, \dots, t_r \in \mathbb{Z}$ が存在する. このとき, n_i の定義から, $1 \leq i, j \leq r$ に対して

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

であることがわかり, したがって $x = a_1 n_1 t_1 + \dots + a_r n_r t_r$ 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. これを解けば, $x \equiv 8 \pmod{15}$, すなわち解は $8 + 15l$ 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, $35t_1 + 21t_2 + 15t_3 = 1$ の形の式を見つけない. 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？

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、解を求める方法を直接には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、元の個数が等しい2つの有限集合 A, B に対して、 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 $m, n \in \mathbb{N}$ と任意の $a, b \in \mathbb{Z}$ 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 $u \equiv v \pmod{m}$ なので、法 mn の剰余環 $\mathbb{Z}/mn\mathbb{Z}$ から法 m の剰余環 $\mathbb{Z}/m\mathbb{Z}$ への写像

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad u + mn\mathbb{Z} \mapsto u + m\mathbb{Z}$$

を定めることができる。同様に、写像

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad u + mn\mathbb{Z} \mapsto u + n\mathbb{Z}$$

が定まり、これらをあわせて剰余環の直積への写像

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

が定義できる。 F が単射であることを示そう。そのために、 $F(u + mn\mathbb{Z}) = F(v + mn\mathbb{Z})$ とすると、

$$u + m\mathbb{Z} = v + m\mathbb{Z} \quad \text{かつ} \quad u + n\mathbb{Z} = v + n\mathbb{Z},$$

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

$$u + mn\mathbb{Z} = v + mn\mathbb{Z}$$

を得る。これで F が単射であることが示された。ところで、 $\mathbb{Z}/mn\mathbb{Z}$ の元の個数は mn であり、これは直積集合 $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ 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 $a, b \in \mathbb{Z}$ に対して $F(x + mn\mathbb{Z}) = (a + m\mathbb{Z}, b + n\mathbb{Z})$ をみたす $x \in \mathbb{Z}$ が存在し

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

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

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

が存在することがわかる．ここで，“自然な”とは，対応が $\bar{a} \mapsto (\bar{a}, \bar{a})$ によって与えられることを意味する．ただし，それぞれの \bar{a} は，法 mn および法 m ，法 n 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“和・積を保存する”ことだが，それについては後で詳しく述べる予定である．

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が，ここでは，2次合同式

$$(1) \quad x^2 + 227x + 354 \equiv 0 \pmod{504}.$$

の整数解を考えよう．素朴に考えれば， x に $0, 1, 2, \dots, 503$ 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 504 の素因数分解 $504 = 2^3 \cdot 3^2 \cdot 7$ 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．

$$(2) \quad \begin{cases} x^2 + 3x + 2 \equiv 0 \pmod{8} \\ x^2 + 2x + 3 \equiv 0 \pmod{9} \\ x^2 + 3x + 4 \equiv 0 \pmod{7} \end{cases}$$

これらそれぞれについ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．

$$(3) \quad x \equiv -1 \pmod{8}, \quad x \equiv 3 \pmod{9}, \quad x \equiv 2 \pmod{7}$$

中国の剰余定理を適用してこれらを連立させれば， $x \equiv 471 \pmod{504}$ が得られ，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)以外にもあり得ることに注意しよう．たとえば8を法とする合同式には $x \equiv -2 \pmod{8}$ という解もありこれ以外にはない．9を法とする解もあとひとつだけ $x \equiv 4 \pmod{9}$ が見つかるが，法7については他にはない．よって，(1)は504を法として $2 \cdot 2 \cdot 1 = 4$ 個の解をもつことがわかる．これらをすべて求めるのは，ちょっと面倒だけどやってみてごらん．