

## 9 1次合同式, 連立1次合同式(中国の剰余定理), Euler 関数

第9.1.1節では, 念のために有限集合の写像に関する重要な性質(命題9.1)の証明を書く. 第9.1.2節では, 参考のために1次合同式の一般的解法(定理9.2)を解説する.

### 9.1 解説編

#### 9.1.1 有限集合の写像

講義プリントの第7.2節で使われた, 有限集合の写像に関する重要な性質(命題9.1)の証明を, 念のために書く.

命題9.1. 有限集合  $A, B$  の元の個数が共に  $n$  個で,  $f: A \rightarrow B$  を  $A$  から  $B$  への写像とする. このとき次の3つの条件は互いに同値である.

- (1)  $f$  は単射.      (2)  $f$  は全射.      (3)  $f$  は全単射.

[証明]  $f$  が全単射とは  $f$  が単射かつ全射であることだから, 条件(1)と条件(2)の同値性を示せばよい.  $A$  のすべての元を列挙して  $a_1, a_2, \dots, a_n$  と書く:  $A = \{a_1, a_2, \dots, a_n\}$ . ここで  $a_1, a_2, \dots, a_n$  のうちどの2つの元も相異なるとする. そのとき  $f$  の像  $f(A)$  は,

$$f(A) := \{f(a_1), f(a_2), \dots, f(a_n)\} \subset B \cdots (*)$$

となる.

(1)  $\Rightarrow$  (2).  $f$  は単射であると仮定する. 定義により,  $f(a_1), f(a_2), \dots, f(a_n)$  のうちどの2つの元も相異なるから, 像  $f(A)$  の元の個数は全部で  $n$  個ある. 一方  $B$  の元の個数も  $n$  個だから, (\*) の両辺の集合は一致して  $f(A) = B$  となる. このように  $f$  は全射である.

(2)  $\Rightarrow$  (1).  $f$  は全射であると仮定する. そのとき  $b \in B$  とすると,  $b = f(a)$  をみたく  $A$  の元  $a$  が存在する. したがって  $a = a_k$  をみたく番号  $k, 1 \leq k \leq n$  がある. よって,  $b = f(a) = f(a_k) \in f(A)$ . ゆえに,  $B \subset f(A)$ . (\*) により逆の包含関係があるから,  $B = f(A)$  となる.  $B$  の元の個数は  $n$  個だから,  $f(A)$  の元の個数も  $n$  個になる. つまり,  $f(a_1), f(a_2), \dots, f(a_n)$  のうちどの2つの元も相異なる. これは  $A$  の相異なる2元  $a_i \neq a_j$  は,  $f$  により  $B$  の相異なる2元  $f(a_i) \neq f(a_j)$  に写ることを意味する. ゆえに  $f$  は単射である.  $\square$

$A, B$  が無限集合のとき, 命題9.1と同様なことが成り立つ場合があることを「線形代数II」で学んでいる.  $A, B$  が共に  $n$ 次元ベクトル空間で,  $f: A \rightarrow B$  が  $A$  から  $B$  への線形写像の場合である. それは「線形写像の次元定理」からわかる.

#### 9.1.2 1次合同式の一般的解法, 連立1次合同式(中国の剰余定理)

参考のために1次合同式の一般的解法を解説する. 一般に次が成立する.

定理9.2.  $m$  を自然数,  $a, b$  を整数で  $a \not\equiv 0 \pmod{m}$  となるものとする<sup>1</sup>. 1次合同式

$$ax \equiv b \pmod{m} \cdots (*)$$

が整数解をもつための必要十分条件は  $\gcd(a, m) \mid b$  であり, このとき, 1次合同式(\*)は  $\pmod{m}$  で  $\gcd(a, m)$  個の解をもつ. そのすべての解は(\*)の解の1つを  $x_0$  とするとき,

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d} \cdots (**)$$

<sup>1</sup> $a \not\equiv 0 \pmod{m}$  だから, 剰余環  $\mathbb{Z}/m\mathbb{Z}$  において  $\bar{a} \neq \bar{0}$ . 1次合同式を解くとは, 1次方程式「 $\bar{a}\bar{x} = \bar{b}, \bar{a} \neq \bar{0}$ 」を解くことに他ならない.

となる<sup>2</sup>. ここで  $d := \gcd(a, m)$  とおく.

[証明] 始めに前半の主張 (解の存在判定) を示す. 合同式 (\*) が整数解  $x$  をもつと仮定する. そのとき  $m \mid (ax - b)$  だから,  $ax - b = my$  をみたす整数  $y$  がある.  $a \not\equiv 0 \pmod{m}$  により, とくに  $a \neq 0$  だから  $d > 0$  であり,  $a/d, m/d$  は整数である. よって,

$$d \left( \frac{a}{d}x - \frac{m}{d}y \right) = b$$

の左辺の第 2 項は整数である. ゆえに,  $d \mid b$ . 逆に  $d \mid b$  を仮定する. そのとき講義プリントの定理 3.2 により,  $ax_0 + my_0 = b$  をみたす整数  $x_0, y_0$  が存在する. ( $x_0, y_0$  は Euclid の互除法により求まる.) よって,  $ax_0 - b = m(-y_0)$ .  $-y_0$  は整数だから,  $ax_0 \equiv b \pmod{m}$  となる. このように合同式 (\*) は整数解  $x_0$  をもつ.

次に,  $d \mid b$  を仮定して合同式 (\*) の  $\pmod{m}$  での解をすべて求める. いま証明したことから, 合同式 (\*) は解  $x_0$  をもつ. 合同式 (\*) の別の整数解を  $y$  とする. そのとき

$$ay \equiv b \equiv ax_0 \pmod{m}$$

だから,  $m \mid a(y - x_0)$  となる. よって,  $\frac{m}{d} \mid \frac{a}{d}(y - x_0)$ . 問題 3.4 により  $\gcd(m/d, a/d) = 1$  だから, 問題 3.3 により  $\frac{m}{d} \mid (y - x_0)$  を得る. ゆえに,  $y \equiv x_0 \pmod{\frac{m}{d}}$ . このように (\*) の整数解は  $\pmod{\frac{m}{d}}$  で唯 1 つに定まる.  $0 \leq k \leq d - 1$  とする.

$$a \left( x_0 + k \frac{m}{d} \right) = ax_0 + k \frac{a}{d}m \equiv ax_0 \equiv b \pmod{m}$$

だから, 整数  $x_0 + k \frac{m}{d}$  は合同式 (\*) の解であることがわかる.  $d$  個の整数 (\*\*) が合同式 (\*) のすべての解の候補になる. (\*\*) の中に  $\pmod{m}$  で合同となる 2 つの整数があったとする. すなわち,  $x_0 + \ell \frac{m}{d} \equiv x_0 + k \frac{m}{d} \pmod{m}$  となる番号  $k, \ell$ , ( $0 \leq k < \ell \leq d - 1$ ) があったとする. そのとき,  $\ell \frac{m}{d} \equiv k \frac{m}{d} \pmod{m}$ . よって,  $\ell \frac{m}{d} - k \frac{m}{d} = mz$  をみたす整数  $z$  がある. この両辺を  $m/d$  で割ると,  $\ell - k = dz$ . したがって,  $d \mid (\ell - k)$ . 一方  $0 < \ell - k \leq d - 1$  だから,  $\ell - k$  は  $d$  の倍数でない. これは矛盾である. ゆえに  $d$  個の整数 (\*\*) のうちのどの 2 つも  $\pmod{m}$  で不合同となり, 1 次合同式 (\*) は  $\pmod{m}$  で  $d$  個の解をもつことがわかる.  $\square$

注意 9.1. いくつか注意をする.

•  $\gcd(a, m) = 1$  のとき,  $\gcd(a, m) = 1 \mid b$  だから, 定理 9.2 により 1 次合同式 (\*) は  $\pmod{m}$  でいつも 1 個の解をもつ.

•  $a$  が  $\pmod{m}$  で可逆とは, 定義により合同式  $ax \equiv 1 \pmod{m}$  が解をもつことである. 定理 9.2 により, これは  $\gcd(a, m) \mid 1$ , つまり  $\gcd(a, m) = 1$  のときに限り起こる.  $\square$

いくつか具体例を述べる.

問題 A. 1 次合同式  $4x \equiv 2 \pmod{5} \cdots (*)$  を解け.

[解答例]  $4 = 2^2$  で, 5 は素数だから,  $\gcd(4, 5) = 2^0 \cdot 5^0 = 1$  (講義プリントの定理 4.4(2)(問題 4.4(2))). よって, 合同式 (\*) は 1 個の整数解をもつ (定理 9.2). 法が小さいので代入して解を求める. 整数  $x$  について,  $x \equiv 0, 1, 2, 3, 4 \pmod{5}$  なので, それぞれを (\*) の左辺に代入してみると,  $4 \cdot 0 = 0$ ,  $4 \cdot 1 = 4 \pmod{5}$ ,  $4 \cdot 2 = 8 \equiv 3 \pmod{5}$ ,  $4 \cdot 3 = 12 \equiv 2 \pmod{5}$ ,  $4 \cdot 4 = 16 \equiv 1 \pmod{5}$  より, 求める解は  $x \equiv 3 \pmod{5}$ .  $\square$

<sup>2</sup>このような解の記述は,  $m$  次方程式  $z^m = \alpha$  を極形式により解いたときの偏角の記述にも現れる.

問題 B. 1 次合同式  $201x \equiv 2 \pmod{2839} \cdots (*)$  を解け.

[解答例] 定理 9.2 と法に関する逆元を使う.

$$2839 = 201 \cdot 14 + 25 \quad (9.1)$$

$$201 = 25 \cdot 8 + 1 \quad (9.2)$$

$$25 = 1 \cdot 25 + 0$$

により,  $\gcd(201, 2839) = 1$ . よって, 合同式  $(*)$  は 1 個の整数解をもつ (定理 9.2).

$$\begin{aligned} 1 &= 201 - 25 \cdot 8 \quad (\because (9.2)) \\ &= 201 - (2839 - 201 \cdot 14) \cdot 8 \quad (\because (9.1)) \\ &= 201 \cdot (1 + 112) - 2839 \cdot 8 = 201 \cdot 113 - 2839 \cdot 8 \end{aligned}$$

だから,  $201 \cdot 113 - 1 = 2839 \cdot 8$ . よって,  $201 \cdot 113 \equiv 1 \pmod{2839}$ . 113 は  $\pmod{2839}$  に関する 201 の逆元である. したがって合同式  $(*)$  の解として,

$$x = 1x \equiv 113 \cdot 201x \equiv 113 \cdot 2 = 226 \pmod{2839}$$

を得る. □

問題 C. 1 次合同式  $129x \equiv 21 \pmod{1566} \cdots (*)$  を解け.

[解答例]

$$1566 = 129 \cdot 12 + 18 \quad (9.3)$$

$$129 = 18 \cdot 7 + 3 \quad (9.4)$$

$$18 = 3 \cdot 6 + 0$$

により,  $\gcd(129, 1566) = 3$ .  $21 = 3 \cdot 7$  だから, 合同式  $(*)$  は 3 個の整数解をもつ (定理 9.2).

$$\begin{aligned} 3 &= 129 - 18 \cdot 7 \quad (\because (9.4)) \\ &= 129 - (1566 - 129 \cdot 12) \cdot 7 \quad (\because (9.3)) \\ &= 129 \cdot (1 + 84) - 1566 \cdot 7 = 129 \cdot 85 - 1566 \cdot 7 \end{aligned}$$

だから,  $129 \cdot 85 - 3 = 1566 \cdot 7$ . この両辺に 7 をかけると,  $129 \cdot (85 \cdot 7) - 21 = 1566 \cdot 7^2$ . よって,  $129 \cdot (85 \cdot 7) \equiv 21 \pmod{1566}$ . それで  $85 \cdot 7$  は合同式  $(*)$  の 1 つの解となる. したがってすべての解は,

$$x \equiv 85 \cdot 7, \quad 85 \cdot 7 + \frac{1566}{3}, \quad 85 \cdot 7 + 2\frac{1566}{3} \pmod{1566}$$

である (定理 9.2). □

注意 9.2. 合同式の解を求める際, 適当な数を法とした逆元を利用すると効率的になることがある. 逆元は互除法で必ず求められるが, 法が小さい場合は  $1, 2, \dots$  と代入して調べていった方がよい. □

連立 1 次合同式に関する基本定理<sup>3</sup> は次である.

---

<sup>3</sup>定理 9.3 で  $d = \gcd(m_1, m_2) = 1$  としたものが, 講義プリントの定理 7.1(中国の剰余定理) の  $r = 2$  の場合である.

**定理 9.3.**  $m_1, m_2 \in \mathbb{N}$ ,  $a_1, a_2 \in \mathbb{Z}$  とする.  $d := \gcd(m_1, m_2)$ ,  $M := \text{lcm}(m_1, m_2)$  とおく. このとき次が成り立つ.

(1) 連立 1 次合同式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \cdots (*)$$

が整数解をもつための必要十分条件は,  $a_1 \equiv a_2 \pmod{d}$  となることである.

(2) もし合同式 (\*) が整数解をもつならば, 解は  $\text{mod } M$  で唯 1 つである.

**問題 D.** 連立合同式  $\begin{cases} x \equiv 9 \pmod{15} \\ x \equiv 17 \pmod{22} \end{cases} \cdots (*)$  を解け.

[解答例 1]  $15 = 3 \cdot 5$ ,  $22 = 2 \cdot 11$  により,

$$\gcd(15, 22) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 11^0 = 1$$

(講義プリントの定理 4.4(2)(問題 4.4(2))). よって,  $\text{lcm}(15, 22) = 15 \cdot 22$  (講義プリントの定理 4.4(3) (問題 4.4(3))). したがって, 連立合同式 (\*) には整数解が存在し, それは  $15 \cdot 22$  を法として唯 1 つである (定理 9.3). 第 1 の合同式から  $x = 9 + 15k$  ( $k \in \mathbb{Z}$ ) と表わすことができる. 第 2 の合同式から

$$9 + 15k = x \equiv 17 \pmod{22} \Leftrightarrow 15k \equiv 8 \pmod{22}$$

である.  $3 \cdot 15 = 45 \equiv 1 \pmod{22}$  ( $\because 45 = 22 \cdot 2 + 1$ ) だから, 右側の合同式の両辺に 3 をかけて

$$k \equiv 3 \cdot 15k \equiv 3 \cdot 8 = 24 \equiv 2 \pmod{22}$$

を得る. つまり,  $k = 2 + 22k'$  ( $k' \in \mathbb{Z}$ ) と表わすことができる. よって

$$x = 9 + 15k = 9 + 15(2 + 22k') = 39 + 15 \cdot 22k'$$

となり, 求める連立合同式の解は  $x \equiv 39 \pmod{15 \cdot 22}$  である.  $\square$

[解答例 2] (法が互いに素なときに有効な解法: Gauss の方法) [解答例 1] で見たように  $\gcd(15, 22) = 1$ ,  $\text{lcm}(15, 22) = 15 \cdot 22$  だから, 連立合同式 (\*) には  $15 \cdot 22$  を法として唯 1 つの整数解が存在する. 始めに  $15\alpha + 22\beta = 1$  をみたく  $\alpha, \beta$  として  $\alpha = 3, \beta = -2$  をとる. (Euclid の互除法によりわかる.) そこで

$$x = 9 \cdot \beta \cdot 22 + 17 \cdot \alpha \cdot 15 = -396 + 765 = 369$$

とおくと, 15 を法として

$$x = 9 \cdot (-2) \cdot 22 + 17 \cdot 3 \cdot 15 \equiv 9 \cdot (-2) \cdot 22 \equiv 9 \cdot 1 \equiv 9 \pmod{15},$$

同様に  $x \equiv 17 \pmod{22}$  となる. よって求める解は  $x = 369 \equiv 39 \pmod{15 \cdot 22}$  である.  $\square$

**定義 9.3.** Euler 関数  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  を

$$\varphi(m) := \text{「} 1 \text{ 以上 } m \text{ 以下の自然数 } a \text{ で } \gcd(a, m) = 1 \text{ となるものの個数」}$$

により定義する.  $\mathbb{Z}/m\mathbb{Z}$  の既約剰余類とは,  $m$  と互いに素な整数  $a$  で代表される剰余類  $\bar{a}$  のことである. (法  $m$  に関する逆元をもつ剰余類のことでもある.) したがって

$$\varphi(m) = \text{「} \mathbb{Z}/m\mathbb{Z} \text{ の既約剰余類の個数」}$$

である. 既約剰余類全体の集合は法  $m$  に関する既約剰余類群と呼ばれ, 記号で  $(\mathbb{Z}/m\mathbb{Z})^\times$  と書く. それで,  $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ .  $\square$

## 9.2 問題編

問題 9.1. 法  $m$  に関する逆元を使って次の合同式を解け.

(1)  $4x \equiv 1 \pmod{15}$     (2)  $8x \equiv 3 \pmod{9}$

問題 9.2. 合同式の計算を使って次を示せ.

(1)  $5^{20} + 5^{21}$  は 6 で割り切れる.    (2)  $2^{100}$  の 1 の位は 6 である.

問題 9.3. 6 桁の自然数  $a$  が 7 で割り切れるならば,  $a$  の最下位の数を最上位に持っていった出来た数も 7 で割り切れることを示せ.

(ヒント:  $a$  の上 5 桁を  $x$ , 下 1 桁を  $y$  とすると,  $a = 10x + y$  と書ける. そのとき  $a$  の最下位の数を最上位に持っていった出来た数は,  $b = y \times 10^5 + x$  となる.  $10b \pmod{7}$  を考えよ.)

問題 9.4. (問題 7.1 の再提出と補足)  $m$  を自然数とし,  $a, b$  を整数とする.  $a$  で代表される剰余類を

$$\bar{a} = a + m\mathbb{Z} := \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

と表わす. 次のことを確かめよ.

(1)  $\bar{a} = \bar{b} \iff a \equiv b \pmod{m}$ .

(2)  $\bar{a} \cap \bar{b} = \emptyset \iff a \not\equiv b \pmod{m}$ .

(3)  $\bar{a} = \bar{b}$  かつ  $\gcd(a, m) = 1$  ならば,  $\gcd(b, m) = 1$  となる.  
(ヒント: 講義プリントの第 7 章 p.2, 上から 4~7 行目の議論を参照.)

(4)  $\gcd(a, m) = 1$  かつ  $\gcd(b, m) = 1$  ならば,  $\gcd(ab, m) = 1$  となる.  
(ヒント: 講義プリントの定理 4.4(2)(問題 4.4(2)) または講義プリントの第 7 章 p.2, 上から 4~7 行目の議論を参照.)

問題 9.5.  $r$  を 2 以上の自然数とし,  $m_1, \dots, m_r$  を  $r$  個の自然数,  $a$  を整数とする. 次を示せ.

(1)  $\gcd(m_1, m_2) = 1$ ,  $m_1 \mid a$  かつ  $m_2 \mid a$  ならば,  $(m_1 m_2) \mid a$  となる.  
(ヒント: 講義プリントの系 4.5(問題 4.4(4)), 解説編第 4.1.2 節または講義プリントの定理 4.4(1, 2)(問題 4.4(1, 2)) を参照.)

(2)  $m_1, \dots, m_r$  のうちの 2 つも互いに素, かつすべての番号  $k$ ,  $1 \leq k \leq r$  について  $m_k \mid a$  が成り立つとする. このとき,  $(m_1 \cdots m_r) \mid a$ .

注意 9.4.  $r$  を 2 以上の自然数とし,  $m_1, \dots, m_r$  を  $r$  個の自然数,  $x, y$  を整数とする.  $m_1, \dots, m_r$  のうちの 2 つも互いに素であると仮定する. 問題 9.5 と問題 6.4(2) により,  $x \equiv y \pmod{m_1 \cdots m_r}$  が成り立つための必要十分条件は,

$$x \equiv y \pmod{m_k} \quad (1 \leq \forall k \leq r)$$

となる. □

問題 9.6. 17 で割ると 3 余り, 13 で割ると 7 余る 3 桁の整数で最大のものを求めよ.

問題 9.7. 次の連立 1 次合同式のすべての解を求めよ.

$$(1) \begin{cases} x \equiv 7 & \pmod{10} \\ x \equiv 10 & \pmod{21} \end{cases} \quad (2) \begin{cases} x \equiv 1 & \pmod{11} \\ x \equiv 2 & \pmod{13} \\ x \equiv 3 & \pmod{17} \end{cases}$$

問題 9.8. 次の連立 1 次合同式は解をもつかどうか答えよ.

$$\begin{cases} x \equiv 6 & \pmod{15} \\ x \equiv 10 & \pmod{21} \end{cases}$$

問題 9.9. 注意 9.4 と法の素因数分解を使って次の 2 次合同式を解け.

(1)  $x^2 - 3x + 10 \equiv 0 \pmod{20}$     (2)  $x^2 + 3x + 6 \equiv 0 \pmod{60}$

問題 9.10.  $\mathbb{Z}/6\mathbb{Z}$  中での和と積の演算表を完成せよ. (第 7.1 節を参照.)

問題 9.11. 1 の 6 乗根全体のなす集合を  $\mu_6$  とする. つまり,

$$\mu_6 := \{z \in \mathbb{C} \mid z^6 = 1\}$$

とする. 次の手順で  $\mu_6$  は  $\mathbb{Z}/6\mathbb{Z}$  の和と同じ演算をもつ集合であることを示せ<sup>4</sup>.

(1)  $\mu_6$  の元をすべて求めよ.

(2) 次を示せ.

(G1)  $1 \in \mu_6$ .    (G2)  $z, w \in \mu_6 \implies zw \in \mu_6$ .    (G3)  $z \in \mu_6 \implies z^{-1} \in \mu_6$ .

(3) 小問 (2) の性質 (G2) をもとに,  $\mu_6$  中での積の演算表を完成させよ.

(4) 全単射写像  $f: \mathbb{Z}/6\mathbb{Z} \rightarrow \mu_6$  であって任意の  $x, y \in \mathbb{Z}/6\mathbb{Z}$  に対して

$$f(x + y) = f(x)f(y)$$

となるものを求めよ.

問題 9.12. Euler 関数の値  $\varphi(84)$ ,  $\varphi(1715)$  を求めよ.

(ヒント: 講義プリントの定理 6.10 を使う.)

問題 9.13.  $m$  を自然数とする. 1 以下の正の既約分数で分母が  $m$  より大きくないものの個数は

$$\varphi(1) + \varphi(2) + \cdots + \varphi(m)$$

であることを示せ.

問題 9.14. Euler 関数の値  $\varphi(m)$  が奇数となる自然数  $m$  をすべて求めよ.

---

<sup>4</sup>同様のことが 1 の  $n$  乗根全体の集合  $\mu_n$  と  $n$  を法とする剰余類集合  $\mathbb{Z}/n\mathbb{Z}$  の間にも成立する.