合同式の性質と剰余類環

1. 用語の定義

- $\mathcal{Z}$：整数の集合
- $\mathcal{N}$：自然数の集合
- 素数：1 より大きい自然数で 1 とその数自身以外の正の約数を持たないもの
- 合成数：1 より大きい自然数で素数でないもの
- $a|b$：$a \in \mathcal{Z}$ が $b \in \mathcal{Z}$ を割り切る
- (a, b)：a と b の最大公約数

$(a, b) = 1$ であるとき、a と b は互いに素であるという。

2. 合同関係の定義

定義 1 整数 a、b と自然数 m について、

$$m|(a - b) \tag{1}$$

が成りたつ時、

$$a \equiv b \bmod m \tag{2}$$

と表す。 □

式 (2) は、任意の $a \in \mathcal{Z}$ について $a \equiv a \bmod m$ が成り立つ (**反射律**) こと、$a \equiv b \bmod m$ ならば $b \equiv a \bmod m$ が成り立つ (**対称律**) こと、$a \equiv b \bmod m$ かつ $b \equiv c \bmod m$ ならば $a \equiv c \bmod m$ が成立する (**推移律**) ことを容易に確かめることができ、数学的な同値関係であることがわかる。以下では、特に誤解が生じなければ、式 (2) を通常の等号記号を用いて $a = b \bmod m$ と表記することもある。

なお、式 (2) のような式を**合同式**とよび、数 m のことを**法**という。

3. 合同式の性質

合同式に関して以下の定理が成り立つ。

定理 1

$$a \equiv a' \bmod m, \text{かつ } b \equiv b' \bmod m$$

であるとき、

$$\begin{aligned} a + b &\equiv a' + b' \bmod m, \\ a \cdot b &\equiv a' \cdot b' \bmod m \end{aligned}$$

が成り立つ。 □

(証明) 合同式の定義より、$a - a' = mr$、$b - b' = ms$ と表すことができるので $(a+b)-(a'+b') = m(r+s)$ であり証明できた。乗算についても同様。 *Q.E.D.*

定理 1 は、例えば、123×456 を 7 で割った余りを求めたい場合に、$123 \times 456 = 56088$ を計算した後に $56088 \equiv 4 \bmod 7$ を求めても、$123 \equiv 4 \bmod 7$ および、$456 \equiv 1 \bmod 7$ を先に求めておき、これらの結果を乗じて余り 4 を求めても同じ結果が得られることを表している。前者の方法で計算をすると、一般に、途中の計算結果が大きくなるために計算効率が悪くなってしまうため、後者の方法で計算をする方が望ましいことがわかる。

定理 2

$$ac \equiv bc \bmod m$$

であるとき、$(c, m) = 1$ ならば

$$a \equiv b \bmod m$$

である。 □

(証明) 合同式の定義より、$ac - bc = mt$ が成り立つ。この式は、$m|(a-b)c$ を意味しているが、条件より $(c, m) = 1$ であるので、$m|(a-b)$ がいえる。 *Q.E.D.*

この定理は、合同式の計算においては、法mと互いに素な数であれば両辺をその数で割ることができることを意味している。$(c,m)>1$であるような数cで両辺を割ると、一般に合同関係が成りたたなくなってしまうので注意が必要である。

4. 剰余類

自然数mを一つ決めると、前節の合同関係を用いて、整数$\mathcal{Z}$を以下のようなm個の集合$C_0, C_1, \ldots, C_{m-1}$に分類することができる。

$$C_i = \{x | x \equiv i \bmod m, x \in \mathcal{Z}\}$$

すなわち、集合C_iは、mを法としてiと合同な整数の集合である。明らかに、$\cup_i C_i = \mathcal{Z}$かつ、$C_i \cap C_j = \phi (i \neq j)$であることがわかる。$C_i (i = 0, 1, \ldots, m-1)$を$m$を法とする$\mathcal{Z}$の**剰余類**と呼び、剰余類からなる集合$\{C_0, C_1, \ldots, C_{m-1}\}$を$\mathcal{Z}_m$と表記することにする。

また、m個の剰余類の各々からその要素$a_i \in C_i$を一つづつ選んで得られる集合

$$\{a_0, a_1, \ldots, a_{m-1}\}$$

を**完全代表系**と呼ぶことにする。例えば、$m=3$であるとき、$\{0,1,2\}$や$\{-3,1,5\}$はいずれも完全代表系である。完全代表系について、以下の定理が成り立つ。

定理 3 $\{a_0, a_1, \ldots, a_{m-1}\}$を$m$を法とする完全代表系とする。このとき、$(a,m)=1$ならば、$\{a \cdot a_0, a \cdot a_1, \ldots, a \cdot a_{m-1}\}$も完全代表系である。□

*(*証明*)* ある$i \neq j$について、$a \cdot a_i \equiv a \cdot a_j \bmod m$であったと仮定する。すると、$(a,m)=1$であるのでこの両辺を$a$で割ることができて、

$$a_i \equiv a_j \bmod m$$

となる。これは、$\{a_0, a_1, \ldots, a_{m-1}\}$が完全代表系であることに矛盾する。よって定理が証明できた。 *Q.E.D.*

いま、$x \in C_i$と$y \in C_j$に対して$z = x + y$を考える。このとき、$z \in C_k$であったとすれば、kはiとjのみによって決定し、xとyの選び方にはよらないことをすぐに確かめることができる。そこで、C_iとC_jの加算を

$$C_i + C_j = C_k$$

と定めることにする。同様にして、剰余類同士の乗算も定めることができる。

例 1 $m=3$とすると、剰余類は、

$$\begin{aligned} C_0 &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ C_1 &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ C_2 &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}$$

となる。そして、

$$C_1 + C_2 = C_0$$

や、

$$C_2 \times C_2 = C_1$$

等を確認することができる。 □

剰余類同士の演算を考えるとき、表記を簡単にするために、C_iを単にiと表記する。この表記を用いれば、例えば、$\mathcal{Z}_3 = \{0,1,2\}$となる。

例 2 $\mathcal{Z}_5 = \{0,1,2,3,4\}$について、その要素間の加算および乗算の演算表は以下のようになる。

$\mathcal{Z}_5$の加算

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathcal{Z}_5$の乗算

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

□

5. 剰余類環

前節で述べた $\mathcal{Z}_m$ の演算について、整数 $\mathcal{Z}$ の演算と同様に以下で述べる性質が成り立っていることを確かめることができる。

性質 G1(閉性) 任意の 2 元 $a, b \in \mathcal{Z}_m$ に対して、$a+b \in \mathcal{Z}_m$ である。

性質 G2(結合則) 任意の元 $a, b, c \in \mathcal{Z}_m$ に対して、$a+(b+c)=(a+b)+c$ が成立する。

性質 G3(単位元) 任意の元 $a \in \mathcal{Z}_m$ に対して、$a+e=e+a=a$ となる単位元 (零元)$e \in \mathcal{Z}_m$ が存在する。

性質 G4(逆元) 任意の元 $a \in \mathcal{Z}_m$ に対して、$a+b=b+a=e$ となる逆元 $b \in \mathcal{Z}_m$ が存在する。

一般に、ある集合 $\mathcal{G}$ の要素間に演算 $+$ が定義され、性質 G1〜G4 を満たすとき、この集合 $\mathcal{G}$ を**群 (Group)** と呼ぶ。集合 $\mathcal{Z}_m$ は演算 $+$ に関して群になっている。例えば、$\mathcal{Z}_5$ の場合、単位元は 0 であり、元 1 の逆元は 4 であることがわかる。

なお、性質 G1〜G4 に加えて、交換則 (任意の 2 元 $a, b \in \mathcal{G}$ に対して、$a+b=b+a$ である) が成り立つ場合は、**可換群**と呼ばれる。明らかに、$\mathcal{Z}_m$ は演算 $+$ に関して可換群である。

群では 1 種類の演算 $(+)$ しか考えていないが、2 種類の演算 $(+, \times)$ を考慮すると、$\mathcal{Z}_m$ は以下のような性質を有していることがわかる。

性質 R1 $\mathcal{Z}_m$ は、演算 $+$ に対して可換群である。

性質 R2(閉性) 任意の 2 元 $a, b \in \mathcal{Z}_m$ に対して、$a \times b \in \mathcal{Z}_m$ である。

性質 R3(結合則) 任意の元 $a, b, c \in \mathcal{Z}_m$ に対して、$a \times (b \times c) = (a \times b) \times c$ が成立する。

性質 R4(分配則) 任意の元 $a, b, c \in \mathcal{Z}_m$ に対して、$a \times (b+c) = a \times b + a \times c$ および $(b+c) \times a = b \times a + c \times a$ が成立する。

一般に、ある集合 $\mathcal{R}$ の要素間に演算 $+$ と $\times$ が定義され、性質 R1〜R4 を満たすとき、この集合 $\mathcal{R}$ を**環 (Ring)** と呼ぶ。集合 $\mathcal{Z}_m$ は演算 $+$ と $\times$ に関して環になっており、この環を剰余類環と呼ぶ。$\mathcal{Z}_m$ が環であることを明示するため、$\mathcal{R}_m$ と表記することもある。

なお、性質 R1〜R4 に加えて、演算 $\times$ に関して交換則 (任意の 2 元 $a, b \in \mathcal{R}$ に対して、$a \times b = b \times a$ である) が成り立つ場合は、**可換環**と呼ばれる。$\mathcal{Z}_m$ は可換環である。

ある集合 $\mathcal{F}$ が以下の性質 F1〜F3 を有する時、$\mathcal{F}$ は**体 (Field)** と呼ばれる。

性質 F1 $\mathcal{F}$ は、可換環である。

性質 F2 任意の元 $a \in \mathcal{F}$ に対して、$a \times u = u \times a = a$ となる単位元 $u \in \mathcal{F}$ が存在する。

性質 F3 零元でない任意の元 $a \in \mathcal{F}$ に対して、$a \times b = b \times a = u$ となる元 $b \in \mathcal{F}$ が存在する。

集合 $\mathcal{Z}_m$ は、m が素数の場合にのみ体となる。例えば、$\mathcal{Z}_5$ は体である。素数 p に対して、$\mathcal{Z}_p$ が体であることを明示するため、$\mathcal{F}_p$ と表記することもある。

6. 既約剰余類

定義 2 $\mathcal{Z}_m = \{0, 1, \ldots, m-1\}$ について

$$\tilde{\mathcal{Z}}_m = \{i | (i, m) = 1, i \in \mathcal{Z}_m\}$$

により定義される集合 $\tilde{\mathcal{Z}}_m$ の要素を**既約剰余類**と呼ぶ。 □

例 3 $m = 10$ であるとき、既約剰余類 $\tilde{\mathcal{Z}}_m$ は、

$$\tilde{\mathcal{Z}}_m = \{1, 3, 7, 9\}$$

であり、$m = 7$ のときは、

$$\tilde{\mathcal{Z}}_m = \{1, 2, 3, 4, 5, 6\}$$

である。