第6章　剰余類

6.1　合同式いろいろ

[I]　足し算，引き算，掛け算については，法 m によって合同な数は “同じ数” と思って計算してよい，というのが合同式の計算法である（割り算については注意が必要であった）．また，すべての整数は m を法 として 0 以上 m 未満の整数と合同だから，合同式の計算は m 未満の整数の演算に帰着できる．これにより，大きな整数に関する計算も，合同式として扱えば簡単になる場合がある．

例 6.1 2011^{201212} を 7 で割った余りはいくつか？

直接 2011^{201212} を計算するのは現実には不可能である．そこで，まず $2011 \equiv 2 \pmod 7$ より 2^{201212} の計算に帰着させる．次に $2^3 = 8 \equiv 1 \pmod 7$ のべき 3 に注目する．$201212 \equiv 2 \pmod 3$ だから $201212 = 3k + 2$ $(k \in \boldsymbol{Z})$ と書け，よって

$$2011^{201212} \equiv 2^{3k+2} = (2^3)^k \cdot 2^2 \equiv 1^k \cdot 4 = 4 \pmod 7.$$

したがって余りは 4 である．

[II]　上の計算で，$201212 \equiv 2 \pmod 3$ については実際には割り算をしなくても良い方法がある．すなわち，各桁の数を足して $3, 6, 9$ になったら 0 とみなす方法である．

$$201212 \longrightarrow 2 + 0 + \underbrace{1 + 2}_{0 \text{ とみなす}} + \underbrace{1 + 2} \longrightarrow 2 \qquad \text{より} \quad 201212 \equiv 2 \pmod 3.$$

これを確かめるために，まず類似の方法で 9 で割り切れるかどうか判定できることを見てみよう．自然数 a に対して各桁を加えて得られる自然数を $S(a)$ とする．たとえば，$S(201212) = 8$，$S(65228) = 23$ である．このとき次が成り立つ．

命題 6.2 任意の自然数 a に対して，$a \equiv S(a) \pmod 9$.

証明　a を 10 進展開して $a = \sum_{k=0}^{N} a_k 10^k$ $(0 \le a_k \le 9)$ とすると，$10 \equiv 1 \pmod 9$ より，

$$a = \sum_{k=0}^{N} a_k 10^k \equiv \sum_{k=0}^{N} a_k = S(a) \pmod 9$$

を得る．　□

そこで，S の計算を少し変えて，a の各桁を加える過程で 9 になったら 0 とみなすことにし，一桁の数になるまでこれを繰り返して，その結果を $T(a)$ で表せば，上の命題から

$$a \equiv T(a) \pmod 9,$$

となる． すなわち，$T(a) = 0$ ならば a は 9 で割り切れることがわかる． さらに $10 \equiv 1 \pmod 3$ より，以上の議論は 3 の倍数の判定にも使え，それがはじめに述べた方法である．

また，T の計算によって古代から知られている**九去法**という検算法が説明できる． すなわち，自然数の足し算 $a + b = c$ を検算したいとき，a, b の各桁をすべて加え 9 が現われたら 0 とみなすことを繰り返し，c についても同様にして，両辺とも一桁の数にする． 得られた数が異なれば元の計算は間違いだと推論できる． この検算法の原理は，ＩＴ技術において**誤り検出符号**として現在広く使われている．

[III]　平方数が合同式でどのようにふるまうか調べてみる． まず，最も簡単なケースとして 4 を法とする場合を考える． a が偶数ならば明らかに $a^2 \equiv 0 \pmod 4$ であり，奇数ならば $a \equiv 1, 3 \equiv \pm 1 \pmod 4$ より $a^2 \equiv 1 \pmod 4$ である． さらに強く，次が成り立つ．

命題 6.3 整数 a に対して，

$$a \equiv \begin{cases} 0 \pmod 4 & (a：\text{偶数}), \\ 1 \pmod 8 & (a：\text{奇数}). \end{cases}$$

証明　a が奇数ならば $a \equiv \pm 1 \pmod 4$ をみたすから $a = 4k \pm 1$ と書ける． よって

$$a^2 = 16k^2 \pm 8k + 1 \equiv 1 \pmod 8$$

となる． □

これを用いて，たとえばピタゴラス方程式の整数解について以下のようなことが示せる．

例 6.4 整数 a, b, c が $a^2 + b^2 = c^2$ をみたすならば，$ab \equiv 0 \pmod 4$.

実際，a, b どちらも偶数ならば，$ab \equiv 0 \pmod 4$ が成り立つことは明らかである． よって a, b のどちらかは奇数，たとえば a が奇数とする． このとき b も奇数とすると，

$$c^2 = a^2 + b^2 \equiv 1 + 1 = 2 \pmod 4$$

となって矛盾する． よって b は偶数，c は奇数であり，

$$b^2 = c^2 - a^2 \equiv 1 - 1 = 0 \pmod 8.$$

これより，b は 4 の倍数でなければならず（どして？），とくに $ab \equiv 0 \pmod 4$ を得る．

以上は 4 または 8 を法として考えたが，3 や 5 を法とするとき，平方数はどんな合同式をみたすか考えてみよ．

6.2 剰余類

前の節のはじめでも述べたように，合同式においては m を法として合同な数を “等しい” とみなして計算する． 法 m で合同な整数は，m で割った余りが等しい整数である．それらをひとまとめにした整数の集合を剰余類という． 正確な定義は以下のとおり．

定義 6.5 $m \in \boldsymbol{Z}$ とする． 次をみたす $\boldsymbol{Z}$ の空でない部分集合 $\mathcal{R}$ を**法 m に関する剰余類**という．

- $a, b \in \mathcal{R}$ ならば $a \equiv b \pmod{m}$.
- $a \in \mathcal{R}$ かつ $a \equiv c \pmod{m}$ とすると，$c \in \mathcal{R}$.

この定義は初学者には少しわかりにくいかもしれないが，実際には，以下の定理で示すように，次の定義で与えられる具体的な集合が剰余類に他ならない．

定義 6.6 整数 m および a に対して，$x \equiv a \pmod{m}$ をみたす整数 x 全体の集合を $a + m\boldsymbol{Z}$ で表す．

$$a + m\boldsymbol{Z} = \left\{ x \in \boldsymbol{Z} \,\middle|\, x \equiv a \pmod{m} \right\}.$$

$0 + m\boldsymbol{Z}$ は $m\boldsymbol{Z}$ のことである． 文脈から m がわかる場合には $\bar{a}$ と略記することが多い．

定理 6.7 整数 m に対して次が成り立つ．

(1) 整数 a に対して，集合 $a + m\boldsymbol{Z}$ は法 m に関する剰余類である．
(2) $\boldsymbol{Z}$ の部分集合 $\mathcal{R}$ が法 m に関する剰余類ならば，$\mathcal{R} = a + m\boldsymbol{Z}$ をみたす $a \in \boldsymbol{Z}$ が存在する．

証明 (1) $a+m\boldsymbol{Z}$ が定義 6.5 の二つの性質をみたすことを確かめよう．まず，$x, y \in a+m\boldsymbol{Z}$ とすると $x \equiv a \equiv y \pmod{m}$ が成り立つ． 次に，$x \in a + m\boldsymbol{Z}$ かつ $x \equiv z \pmod{m}$ ならば，$z \equiv x \equiv a \pmod{m}$ より $z \in a + m\boldsymbol{Z}$ を得る．
(2) $a \in \mathcal{R}$ を任意にとって固定する． このとき $\mathcal{R} = a + m\boldsymbol{Z}$ であることを以下で示す．まず，任意の $x \in \mathcal{R}$ に対して，定義 6.5 のはじめの性質より $x \equiv a \pmod{m}$ となるから，$x \in a+m\boldsymbol{Z}$，したがって $\mathcal{R} \subset a+m\boldsymbol{Z}$ が成り立つ． 逆を示すために，$x \in a+m\boldsymbol{Z}$ を任意にとれば，$a \equiv x \pmod{m}$ と定義 6.5 のあとの性質を使って $x \in \mathcal{R}$，よって $a+m\boldsymbol{Z} \subset \mathcal{R}$ が示された． □

定義 6.8 整数 m に対して，法 m に関するすべての剰余類を元とする集合を**法 m に関する剰余集合**といい，$\boldsymbol{Z}/m\boldsymbol{Z}$ で表す． 上記定理から，

$$\boldsymbol{Z}/m\boldsymbol{Z} = \{\, a + m\boldsymbol{Z} \mid a \in \boldsymbol{Z} \,\}.$$

自然数 m に対して，法 m に関する剰余類は全部で m 個ある． 実際，すべての整数は m を法として $0, 1, 2, \cdots, m$ のどれかと合同で，さらにこれらは互いに合同でないから

$$\boldsymbol{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{m-1}, \qquad \overline{a} \cap \overline{b} = \phi \quad (0 \leq a < b \leq m).$$

したがって，

$$\boldsymbol{Z}/m\boldsymbol{Z} = \left\{ \overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1} \right\}$$

と書くこともできる． たとえば，$\boldsymbol{Z}/5\boldsymbol{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ であるが，これを

$$\boldsymbol{Z}/5\boldsymbol{Z} = \left\{ \overline{7810}, \overline{-29}, \overline{382}, \overline{38^{81}}, \overline{987-128} \right\}$$

と書いてもかまわない（どうしてか？ とくに $38^{81} \equiv 3 \pmod 5$ は？）． また，

$$a \equiv b \pmod m \iff a \in b + m\boldsymbol{Z} \iff b \in a + m\boldsymbol{Z} \iff a + m\boldsymbol{Z} = b + m\boldsymbol{Z}$$

が成り立つことに注意せよ（もう、いろんなとこで使っちゃってるけどね）．

定義 6.9 m を自然数とする． m と素な整数をもつ剰余類を**法 m に関する既約剰余類**という． 法 m に関する既約剰余類の個数を $\varphi(m)$ で表す． また，このようにして定まる自然数上の関数 φ を**オイラー関数**という．

すなわち，既約剰余類とは，$\gcd(a, m) = 1$ である $a \in \boldsymbol{Z}$ によって表される剰余類 $a + m\boldsymbol{Z}$ のことであり，$\varphi(m)$ は $0 \leq a < m$ なる整数 a のうち m と互いに素なものの個数である．小さい数に対するオイラー関数の値は次の表のようになる．

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

たとえば，$\varphi(10) = 4$ は $1, 3, 7, 9$ の 4 個が 10 と互いに素となることからわかる． しかし，このような方法で $\varphi(m)$ を求めるのは，大きい m に対しては効率が悪い． 次の定理を使えば，どんなに大きな m についてもその素因数分解さえわかればオイラー関数の計算が簡単にできる．

定理 6.10 自然数 m の素因数分解を $m = \prod_{j=1}^{r} p_j^{e_j}$ $(p_j$ は相異なり $e_j > 0)$ とすると，

$$\varphi(m) = \prod_{j=1}^{r} \left(p^{e_j} - p^{e_j - 1} \right) = m \prod_{j=1}^{r} \left(1 - \frac{1}{p_j} \right).$$

たとえば，

$$\varphi(2160) = \varphi(2^4 \cdot 3^3 \cdot 5) = (16 - 8)(27 - 9)(5 - 1) = 576$$

と計算される． この定理は，次の二つの補題から導かれる．

補題 6.11 互いに素な自然数 m, n に対して $\varphi(mn) = \varphi(m)\varphi(n)$.

補題 6.12 素数のべき p^e $(e > 0)$ に対して $\varphi(p^e) = p^e - p^{e-1}$.