第10章　位数と原始根

10.1　位数

フェルマー，オイラーの定理では，法 m で 1 と合同になるためのべき指数として $\varphi(m)$ が採用されているが，前章の定理 9.8 や例 9.9 で見たように，$\varphi(m)$ より小さいべきでも 1 と合同になる可能性がある．そのようなべきを特徴付けるために次の定義を導入する．

定義 10.1 m を 2 以上の自然数とする．m と素な整数 a に対して

$$a^k \equiv 1 \pmod{m}$$

をみたす最小の自然数 k を**法 m に関する a の位数**という．また，剰余類 $\alpha \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ に対して α に属する元の法 m に関する位数はすべて等しい．それを α の**位数**という．

つまり，整数 a の法 m に関する位数とは

$$\min\left\{ k \in \boldsymbol{N} \,\middle|\, a^k \equiv 1 \pmod{m} \right\} = \min\left\{ k \in \boldsymbol{N} \,\middle|\, \overline{a}^k = \overline{1} \right\}$$

であり，これを簡単に剰余類 $\overline{a}$ の位数というわけである．1 の位数はどんな法に関しても 1 である．なお，m と素でない整数 a の位数は定義されないことに注意しよう．

命題 10.2 m を 2 以上の自然数，a を m と互いに素な整数とし，法 m に関する a の位数を s とする．
(1) $a^r \equiv 1 \pmod{m}$ をみたす整数 r は s の倍数である．
(2) $s = xy$ $(x, y \in \boldsymbol{N})$ のとき，法 m に関する a^x の位数は y である．

証明　簡単のため $\alpha = \overline{a} = a + m\boldsymbol{Z}$ とおき，$\overline{1} = 1 + m\boldsymbol{Z}$ も 1 と略す．このとき，たとえば $\alpha^s = 1$ とかける．また α は既約剰余類なので，α^{-1} が定義されることに注意せよ．
(1) r を s で割り算して，$r = us + v$, $(0 \le v < s)$ とすると，$1 = \alpha^r = (\alpha^s)^u \alpha^v = \alpha^v$ だから，もし $v > 0$ とすると位数 s の最小性に矛盾する．よって $v = 0$ であり $r = us$ は s の倍数である．
(2) まず $(\alpha^x)^y = \alpha^{xy} = \alpha^s = 1$ が成り立つ．いま，自然数 u が $(\alpha^x)^u = 1$ をみたすならば，$\alpha^{xu} = 1$ だから，(1) より $s = xy$ は xu の約数．これより $y \le u$ であり，位数の定義から，y は α^x の位数である．　□

命題 10.3 m を 2 以上の自然数，a, b をそれぞれ m と互いに素な整数とする．法 m に関する a, b のそれぞれの位数 s, t が互いに素ならば，法 m に関する ab の位数は st である．

証明 前命題の証明と同様に，$\alpha = \overline{a},\ \beta = \overline{b} \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ とする．いま，$(\alpha\beta)^{st} = (\alpha^s)^t(\beta^t)^s = 1$ が成り立つので，$(\alpha\beta)^w = 1$ をみたす自然数 w が st の倍数であることを確かめればよい．まず，s, t は互いに素なので $sx + ty = 1$ をみたす整数 x, y がとれる．このとき，$\alpha^s = \beta^t = 1$ に注意すれば，$\alpha = \alpha^{sx+ty} = \alpha^{ty} = (\alpha\beta)^{ty}$．よって，$\alpha^w = (\alpha\beta)^{wty} = 1$ となるから，前命題 (1) より，w は s の倍数である．α, β の役割を入れ換えれば，w が t の倍数であることもわかる．s, t は互いに素なので，結局 w は st の倍数となる． □

命題 10.4 m を 2 以上の自然数，a を m と互いに素な整数とし，法 m に関する a の位数を s とする．このとき，$1,\ a,\ a^2,\ \ldots,\ a^{s-1}$ はどの 2 つも m を法として合同ではない．したがって，集合 $\left\{\overline{1},\ \overline{a},\ \overline{a}^2,\ \cdots,\ \overline{a}^{s-1}\right\}$ は，$(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ における s 個の元からなる部分集合である．

証明 $a^i \equiv a^j \pmod{m}$ $(0 \leq i < j \leq s-1)$ と仮定すると，$a^{j-i} \equiv 1 \pmod{m}$ が得られ，位数 s の最小性に矛盾する． □

オイラーの定理およびカーマイケルの定理におけるべき指数 $\varphi(m),\ \lambda(m)$ と同様の役割をもつ数を，位数の概念を使って定義することができる．いま，自然数 $m > 1$ に対して $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ の元の最大位数を $\mu(m)$ とする;

$$\mu(m) = \max\left\{\, \alpha \text{ の位数} \,\middle|\, \alpha \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times \,\right\}.$$

命題 10.2 (1) より，$\mu(m)|\lambda(m)|\varphi(m)$ が成り立っている．

定理 10.5 自然数 $m > 1$ と互いに素な任意の整数 a に対して

$$a^{\mu(m)} \equiv 1 \pmod{m}$$

が成り立つ．

証明 $\alpha = \overline{a} \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ とおく．その位数を s とするとき，$s|\mu(m)$ を示せばよい．さらにそのためには，任意の素数 p について，$s = p^e t,\ \mu(m) = p^f u,\ p\nmid tu$ とするとき，$e \leq f$ を確かめればよい．いま，位数が $\mu(m)$ となる $\beta \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ をひとつとる．命題 10.2 (2) より，α^t の位数は p^e であり，β^{p^f} の位数は u である．ここで，p^e と u は互いに素なので，命題 10.3 より，$\alpha^t\beta^{p^f}$ の位数は $p^e u$ となる．よって，$\mu(m)$ の最大性から $p^e u \leq \mu(m) = p^f u$，したがって $e \leq f$ が導かれる． □

実は，$\mu(m)$ は $\lambda(m)$ と等しい．したがって，ここで述べた定理 10.5 の証明は，結果として，カーマイケルの定理（定理 9.8）の別証明を与えていることになる．なお，$\lambda(m) = \mu(m)$ の証明は，群論の知識を本質的に使うので，ここでは紹介しない．来年度「代数」で群論を勉強してからのお楽しみといたしましょう．

10.2　多項式に関する注意

多項式 $f(x)$ を一次式 $x-a$ で割ったときの余りは $f(a)$ であり，

$$f(x)=(x-a)g(x)+f(a)$$

をみたす $n-1$ 次多項式 $g(x)$ が存在する． とくに，$f(x)$ が $x-a$ で割り切れるための必要十分条件は $f(a)=0$ である． これらは，多項式に関する「剰余定理・因数定理」とよばれるものであるが，ここではさらに，$f(x)$ が整数係数で a が整数のとき，$g(x)$ として整数係数の多項式がとれることに注意する．

整数 m と整数係数の二つの多項式 $f_1(x), f_2(x)$ について，それぞれ同じ次数の係数が法 m に関して合同のとき，

$$f_1(x)\equiv f_2(x) \pmod{m}$$

と書くことにする． これは，$f_1(x)-f_2(x)$ を整理して得られる多項式の係数がすべて m の倍数であることを意味する． 次の命題は，上記「剰余定理・因数定理」の合同式バージョンともいえるものであり，証明は簡単なので演習としておこう． なお，最高次係数が 1 の多項式を**モニック**な多項式よぶことにする．

命題 10.6 m を 2 以上の自然数，$f(x)$ をモニックな整数係数 n 次多項式，a を整数とする． もし，$f(a)\equiv 0 \pmod{m}$ が成り立つならば，

$$f(x)\equiv (x-a)g(x) \pmod{m}$$

をみたすモニックな整数係数 $n-1$ 次多項式 $g(x)$ が存在する．

とくに，素数を法とする場合にこの命題を適用することで，次の定理を得る．

定理 10.7 p を素数とする． モニックな整数係数 n 次多項式 $f(x)$ に対して，合同式

$$f(x)\equiv 0 \pmod{p}$$

の整数解は p を法として n 個以下である．

証明　もし整数解がひとつもなければ証明すべきことは何もない． 整数解があるとしてそれを a とする． 以下，n に関する数学的帰納法を用いる． $n=1$ のときは，p を法として a のみが解であることはすぐにわかる． $n>1$ のときは，前命題より，モニックな整数係数 $n-1$ 次多項式 $g(x)$ がとれて

$$f(x)\equiv (x-a)g(x) \pmod{p}$$

と書ける． いま，整数 b も解だとすると

$$(b-a)g(b)\equiv f(b)\equiv 0 \pmod{p}$$

であるが，p は素数だから，$b \equiv a$ または $g(b) \equiv 0 \pmod{p}$． すなわち，p を法として a と合同でない整数解は $g(x) \equiv 0 \pmod{p}$ の解でなければならない． 一方，この合同式は，帰納法の仮定より p を法として $n-1$ 個以下の整数解しかもたないから，n 次の場合に定理の主張が得られたことになる． □

定理は,「$\boldsymbol{Z}/p\boldsymbol{Z}$ の元を係数とするモニックな n 次方程式 $F(x) = \overline{0}$ の $\boldsymbol{Z}/p\boldsymbol{Z}$ における解の個数は n 以下である」と言い換えることができる．

10.3 原始根

定義 10.8 自然数 $m > 1$ に対して，法 m に関する位数が $\varphi(m)$ である整数を法 m に関する**原始根**という．

g が法 m に関する原始根ならば, 命題10.4 より，$\varphi(m)$ 個の剰余類 $\overline{1}$, $\overline{g}$, $\overline{g}^2$, $\cdots$, $\overline{g}^{\varphi(m)-1}$ は互いに相異なり，したがってこれらが $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ のすべての元となる;

$$(\boldsymbol{Z}/m\boldsymbol{Z})^\times = \left\{ \overline{g}^j \,\middle|\, 0 \le j < \varphi(m) \right\} = \left\{ \overline{g}^j \,\middle|\, j \in \boldsymbol{Z} \right\}.$$

逆にこのような整数 g は法 m に関する原始根である．

位数は剰余類によって定まるから，法 m に関する原始根は $\{1, 2, \cdots, m-1\}$ から選ぶことができる． 小さい m について調べてみると，法 $m = 2, 3, 4, 5$ に関してはそれぞれ $1, 2, 3, 2$ が原始根としてとれ，とくに，法 $m = 5$ に関しては，2 の他に 3 も原始根になっている． しかし，一般に，法 m に関する原始根は必ずしも存在しない． たとえば，$m = 8$ のとき $3, 5, 7$ の位数はすべて 2 であり，$\varphi(8) = 4$ を位数とする元は $(\boldsymbol{Z}/8\boldsymbol{Z})^\times$ にはなく，したがって法 8 に関する原始根は存在しないことがわかる．

定理 10.9 素数 p に対して，法 p に関する原始根が存在する．

証明 定理10.5 より，すべての $\overline{a} \in (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ が $x^{\mu(p)} - \overline{1} = \overline{0}$ の解となるから，定理10.7 より $\mu(p) \ge \varphi(p)$ でなければならない． 一方，$\mu(p) | \varphi(p)$ であったから，$\mu(p) = \varphi(p)$ が導かれ，$\mu(p)$ の定義より $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ は位数 $\varphi(p)$ の元をもつ． □

小さな素数に対する最小自然数の原始根は次の表のようになる．

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
g	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2

表を眺めると，原始根に 2 が比較的多く現れることに気付く． そこで,「2 が原始根となる素数 p が無数に存在するのではないか」と期待される． これは**原始根に関するアルティン予想**とよばれる予想の一部であり，現在も完全には解決されていない．

奇素数 p のべき p^n $(n \ge 1)$ を法とする原始根も存在する． その証明は少し面倒なので，補遺に記すことにする．