第9章　位数

9.1　フェルマーの定理とオイラーの定理

本章の目的は，整数のベキ乗数 a^n の法 m におけるふるまいを考察することである． 素数を法とする次の定理が基本的である．

定理 9.1 (フェルマーの定理) p を素数とし，a を p と互いに素な整数とすると，

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．

証明 $a > 0$ のときに証明すればよい（どして？）． さらに，$a^p \equiv a \pmod{p}$ が任意の $a \in \boldsymbol{N}$ について成り立つことを確かめればよい（これまたどして？）． まず，$a = 1$ のときは明らかである． 次に，a のとき成り立つと仮定すれば

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

によって $a+1$ のときも成り立つことがわかるから，数学的帰納法によって示された． □

証明からわかるように，p が素数ならば，すべての整数 a に対して $a^p \equiv a \pmod{p}$ であり，とくに $a \not\equiv 0 \pmod{p}$ の場合がフェルマーの定理となっている．

次に，法 m が必ずしも素数ではないとき，フェルマーの定理で述べていることはそのままの形では一般に成り立たないことに注意する． たとえば，$5^{6-1} \equiv 5 \not\equiv 1 \pmod{6}$，$2^{9-1} \equiv 4 \not\equiv 1 \pmod{9}$ 等． フェルマーの定理を，法 m が合成数である場合にも適用できるように一般化するには，$a^N \equiv 1 \pmod{m}$ となるベキ指数 N を探さなければならない．一般の合成数を考える前に，まず素数ベキの場合を考えよう．

補題 9.2 p を素数とし，a を p と互いに素な整数とすると，任意の自然数 n に対して

$$a^{(p-1)p^{n-1}} \equiv 1 \pmod{p^n}$$

が成り立つ．

証明 n に関する数学的帰納法を用いる． $n = 1$ のときは上で示したフェルマーの定理に他ならない． n のとき成り立つと仮定すると $a^{(p-1)p^{n-1}} = 1 + p^n k$ $(k \in \boldsymbol{Z})$ と書ける．

これを p 乗すれば，$n+1 \leq 2n, 3n, \cdots$ に注意して

$$a^{(p-1)p^n} = (1+p^n k)^p = 1 + p \cdot p^n k + \sum_{j=2}^{p} {}_pC_j p^{jn} k^j \equiv 1 \pmod{p^{n+1}}.$$

これは $n+1$ のときに成り立つことを示している．　□

補題 6.12 によれば，$\varphi(p^n) = (p-1)p^{n-1}$ であり，よって上で示した補題 9.2 の合同式は $a^{\varphi(p^n)} \equiv 1 \pmod{p^n}$ と書き換えることができる．これをふまえて，フェルマーの定理の拡張版として次に提示するオイラーの定理が得られる．

定理 9.3 (オイラーの定理) 自然数 m と互いに素な任意の整数 a に対して

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

が成り立つ．

証明　m を素因数分解して $m = p_1^{n_1} \cdots p_r^{n_r}$ (ただし，p_j たちは相異なる素数で $n_j > 0$) とする．各 j について，p_j は a を割らないから，補題 9.2 より $a^{\varphi(p_j^{n_j})} \equiv 1 \pmod{p_j^{n_j}}$ を得る．一方，補題 6.11 より，$\varphi(m)$ は $\varphi(p_j^{n_j})$ の倍数だから，$a^{\varphi(m)} \equiv 1 \pmod{p_j^{n_j}}$ がすべての $j = 1, \cdots, r$ について成り立つことになり，これから直ちに定理が導かれる．□

証明を検討すると，$\varphi(p_j^{n_j})$ $(1 \leq j \leq r)$ の公倍数 M をとれば，$a^M \equiv 1 \pmod{m}$ が成り立つことがわかる．したがって，オイラーの定理は次のように少しだけ精密化される．

系 9.4 (オイラーの定理の精密化) 自然数 m の素因数分解を $m = p_1^{n_1} \cdots p_r^{n_r}$，ただし p_j たちは相異なる素数で $n_j > 0$ とし，M を $\varphi(p_j^{n_j})$ $(1 \leq j \leq r)$ の最小公倍数とする．このとき，m と互いに素な任意の整数 a に対して

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

が成り立つ．

例 9.5 $m = 63 = 3^2 \cdot 7$ の場合，$\varphi(m) = (9-3) \cdot (7-1) = 36$ なので，$\gcd(a, 3 \cdot 7) = 1$ をみたす任意の整数 a に対して，オイラーの定理から $a^{36} \equiv 1 \pmod{63}$．一方，系 9.4 を適用すれば，より強い合同式 $a^6 \equiv 1 \pmod{63}$ が得られる．

9.2　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ベキ指数として $\varphi(m)$ が採用されているが，系 9.4 や例 9.5 でも見たように $\varphi(m)$ より小さいベキでも 1 と合同になる可能性がある．そのようなベキを特徴付けるために次の定義を導入する．

定義 9.6 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． $\alpha \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ 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 $\overline{a}$ の位数というわけである．

命題 9.7 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) $0 \leq i < j < s$ ならば $a^i \not\equiv a^j \pmod{m}$ である．

(2) $a^r \equiv 1 \pmod{m}$ をみたす整数 r は s の倍数である．

(3) $s = xy$ $(x, y \in \boldsymbol{N})$ 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． したがって，たとえば $\alpha^s = 1$ となる． また α は既約剰余類なので，α^{-1} が定義されることにも注意せよ．
(1) $\alpha^i = \alpha^j$ ならば $\alpha^{j-i} = 1$ となるが，$0 < j - i < s$ だから位数 s の最小性に反する．
(2) r を s で割り算して，$r = us + v$, $(0 \leq v < s)$ 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．
(3) 自然数 u が $(\alpha^x)^u = 1$ をみたすならば，$\alpha^{xu} = 1$ だから，(2) より $s = xy \mid xu$，よって $y \leq u$ であることからわかる． □

命題 9.8 m を 2 以上の自然数とする． m と互いに素な 2 つの整数 a, b に対して，法 m に関する位数をそれぞれ s, t とする． このとき，$\gcd(s, t) = 1$ 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，$\alpha = \overline{a}$, $\beta = \overline{b} \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ と略す． 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 (2) 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． □

オイラーの定理と命題 9.7 (2) から，$\overline{a} \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ の位数はいつも $\varphi(m)$ の約数であることがわかる． 同様の役割を持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 9.7 (2) より，$\mu(m) \mid \varphi(m)$ が成り立っている．

命題 9.9 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．とくに，$\overline{a}$ の位数は $\mu(m)$ の約数である．

証明　$t = \mu(m)$ と略し，位数が t となる $\overline{b} \in (\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ をひとつとる．また $\overline{a}$ の位数を s とする．$\mu(m)$ の定義より $s \leq t$ であるが，以下において $s \mid t$ を示す（これがいえれば証明完了（どして?））．そのためには，s の各素因子 p について $s = p^e s'$, $t = p^f t'$, $p \nmid s't'$ とするとき，$e \leq f$ を示せばよい．いま，命題 9.7 (3) より，m を法として $a^{s'}$ の位数が p^e で，b^{p^f} の位数が t' であるが，p^e と t' は互いに素なので，命題 9.8 より，$a^{s'}b^{p^f}$ の位数は $p^e t'$ となる．よって，$t = p^f t'$ の最大性から $e \leq f$ が導かれる．　□

9.3　原始根

定義 9.10 自然数 $m > 1$ に対して，法 m に関する位数が $\varphi(m)$ となる整数 g 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 9.7 (1) 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;

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

逆にこのような $g \in \boldsymbol{Z}$ は法 m に関する原始根である．例 9.5 で見たように，法 m に関する原始根は必ずしも存在しない．

定理 9.11 素数 p に対して，法 p に関する原始根が存在する．

定理の証明のために補題をひとつ用意する．証明は講義で紹介する．

補題 9.12 p を素数とする．最高次係数が 1 の整数係数 d 次多項式 $f(x)$ に対して，$f(x) \equiv 0 \pmod{p}$ の整数解は p を法として d 個以下である．すなわち，$f(x)$ の各係数を p を法とする剰余類で置き換えた多項式 $\overline{f}(x)$ について，集合

$$\left\{ \alpha \in \boldsymbol{Z}/p\boldsymbol{Z} \,\middle|\, \overline{f}(\alpha) = \overline{0} \right\}$$

の元の個数は d 以下である．

定理 9.11 の証明　命題 9.9 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，前補題より $\mu(p) \geq \varphi(p) = p - 1$ でなければならない．一方，$\mu(p) \leq \varphi(p)$ であったから，$\mu(p) = \varphi(p)$ が導かれ，このことは，位数が $\varphi(p)$ である元，すなわち原始根の存在を示している．　□

実は，2 でない任意の素数 p と任意の自然数 n に対して，法 p^n に関する原始根が存在する．その証明は少し面倒だが課題としておこう．