第9章　フェルマー・オイラーの定理

9.1　フェルマーの定理

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　定理5.9 より a は法 p に関して可逆なので，任意の $n \in \boldsymbol{Z}$ に対して $n^p \equiv n \pmod{p}$ が成り立つことを確かめればよい． さらに $n > 0$ すなわち自然数 n に対して示せば十分である． そこで，n に関する数学的帰納法を用いる． まず，$n = 1$ のときは明らかである． 次に，n のとき成り立つと仮定すれば，$1 \leq j \leq p-1$ のとき ${}_pC_j \equiv 0 \pmod{p}$ より

$$(n+1)^p = n^p + \sum_{j=1}^{p-1} {}_pC_j n^j + 1 \equiv n^p + 1 \equiv n + 1 \pmod{p}$$

によって $n+1$ のときも成り立つ． □

系 9.2 p を素数とすると，すべての整数 a に対して $a^p \equiv a \pmod{p}$ が成り立つ．

上で見た通り，ここでは先にこの系を示すことによって上記定理を証明しているのだが，フェルマーの定理自体は他の証明もあり得るので，一応，系としておこう． 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．

例 9.3 フェルマーの定理を用いると累乗の計算が簡単になることがある． たとえば，5^{6789} は素数 59 を法として以下のように計算できる． フェルマーの定理より $5^{58} \equiv 1 \pmod{59}$ が成り立つことに着目して，6789 の 58 による割り算 $6789 = 117 \cdot 58 + 3$ を用いれば，

$$5^{6789} = (5^{58})^{117} \cdot 5^3 \equiv 5^3 = 125 \equiv 7 \pmod{59}$$

となる．

9.2　オイラーの定理

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られ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，

$$5^{6-1} \equiv 5 \not\equiv 1 \pmod 6, \qquad 2^{9-1} \equiv 4 \not\equiv 1 \pmod 9 \qquad \text{etc...}$$

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，$a^N \equiv 1 \pmod m$ をみたすベキ指数 N を，m に関連付けて探さなければならない．その際，$a^N = a \cdot a^{N-1} \equiv 1 \pmod m$ より，a は m を法として可逆，したがって定理 5.9 から，a, m は互いに素でなければならないことに注意する．

一般の合成数を考える前に，まず m が素数ベキの場合を考えよう．

補題 9.4 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そのものである．n のとき成り立つと仮定すると

$$a^{(p-1)p^{n-1}} = 1 + p^n k \quad (k \in \boldsymbol{Z})$$

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 8.8 によれば，$\varphi(p^n) = (p-1)p^{n-1}$ であり，上で示した補題 9.4 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，フェルマーの定理は次の定理に拡張される．

定理 9.5 (オイラーの定理) 自然数 $m > 1$ 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．p_j は a を割らないから，補題 9.4 より $a^{\varphi(p_j^{n_j})} \equiv 1 \pmod{p_j^{n_j}}$ を得る．一方，補題 8.7 より $\varphi(m)$ は $\varphi(p_j^{n_j})$ の倍数だから，$a^{\varphi(m)} \equiv 1 \pmod{p_j^{n_j}}$ が各 j に対して成り立つことになり，これからただちに定理が導かれる．□

いま，自然数 $m>1$ 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，$\varphi(p_j^{n_j})$ たちの最小公倍数を $\psi(m)$ とする;

$$\psi(m)=\mathrm{lcm}(\varphi(p_1^{n_1}),\cdots,\varphi(p_r^{n_r})).$$

このとき，上記の証明から，オイラーの定理は次の系のように少しだけ精密化されることがわかる． なお，$\varphi(m)$ が $\varphi(p_j^{n_j})$ たちの公倍数であることから，とくに $\psi(m)|\varphi(m)$ が成り立っていることに注意しよう．

系 9.6 (オイラーの定理の精密化) 自然数 $m>1$ と互いに素な任意の整数 a に対して

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

が成り立つ．

例 9.7 $m=35=5\cdot 7$ の場合，$\varphi(m)=(5-1)\cdot(7-1)=4\cdot 6=24$ なので，35 と互いに素な任意の整数 a に対して，オイラーの定理から $a^{24}\equiv 1 \pmod{35}$． 一方，系 9.6 を適用すれば，$\psi(m)=\mathrm{lcm}(4,6)=12$ から，より強い合同式 $a^{12}\equiv 1 \pmod{35}$ が得られる．

9.3 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 9.6 や例 9.7 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 9.8 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 9.9 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．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)　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．
(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 $y \leq u$ であり，位数の定義から，y は α^x の位数である．　□

命題 9.10　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．　□

オイラーの定理およびその精密化におけるベキ指数 $\varphi(m),\ \psi(m)$ と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 $\lambda(m)$ とする;

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

命題 9.6 および 9.9 (1) より，$\lambda(m) | \psi(m)$ が成り立っている．したがって，次の定理は，オイラーの定理の精密化である系 9.6 をさらに精密にしたものとみなすことができる．

定理 9.11 (カーマイケルの定理)　自然数 $m > 1$ と互いに素な任意の整数 a に対して

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

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，$s | \lambda(m)$ 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 $s = p^e t,\ \lambda(m) = p^f u,\ p \nmid tu$ とするとき，$e \leq f$ を確かめればよい．いま，位数が $\lambda(m)$ となる $\beta \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ をひとつとる．命題 9.9 (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 9.10 より，$\alpha^t \beta^{p^f}$ の位数は $p^e u$ となる．よって，$\lambda(m)$ の最大性から $p^e u \leq \lambda(m) = p^f u$，したがって $e \leq f$ が導かれる．　□