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．素数を法とする場合から始めよう．

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　写像 $f_a : (\boldsymbol{Z}/p\boldsymbol{Z})^\times \to (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ を $f_a(\overline{x}) = \overline{ax}$ によって定義する． a が p を法として可逆であることに注意すれば，f_a が全単射であることが確認できる． したがって，

$$(p-1)! = \prod_{x=1}^{p-1} x \equiv \prod_{x=1}^{p-1} (ax) = a^{p-1} \cdot (p-1)! \pmod{p}.$$

ここで p は素数だから，$(p-1)!$ は p を法として可逆，よって定理の合同式を得る．□

この定理は「フェルマーの小定理」ともよばれる（「フェルマーの最終定理」と区別するため）．

例 9.2 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　フェルマーテスト

フェルマーの定理に現れる合同式は，p が素数であるための必要条件を与えているが，十分条件というわけではない． たとえば，$4^{14} \equiv 1 \pmod{15}$，$19^{48} \equiv 1 \pmod{49}$ であるが，15, 49 のどちらも素数ではない． しかし，多くの a について合同式が成り立てば十分条件にもなり得るかもしれない，と（ダメ元で）考えてみよう．

定義 9.3 n を 2 以上の自然数とする． 整数 a が $a^{n-1} \equiv 1 \pmod{n}$ をみたすとき，n を底 a に関する**確率的素数**という．

フェルマーの定理から，ひとつの底に関して確率的素数になっていなければ合成数である． たとえば，$2^{220} \equiv 16 \not\equiv 1 \pmod{221}$ だから 221 は素数ではない． 一方，十分多くの底に関して確率的素数であるならば，素数である可能性は高いと考えられる． 例として

$$2^{29338} \equiv 3^{29338} \equiv 5^{29338} \equiv 7^{29338} \equiv 11^{29338} \equiv 1 \pmod{29339},$$

（こいつら，どうやって計算すんだよ！ という疑問はごもっとも． 時間があれば講義で説明しましょう.）したがって，29339 は底 $2, 3, 5, 7, 11$ に関する確率的素数であり，実際に素数であることが確かめられる．このような素数判定法（別の言い方をすれば，合成数を排除するための方法）を**フェルマーテスト**という．

フェルマーテストはプログラムも簡単で計算も速く有用であるが，完全な素数判定法ではない． たとえば，$n = 29341$ は，底 $2, 3, 5, 7, 11$ に関する確率的素数であるにもかかわらず，$13|n$ より素数ではないことが確認できる． 2002 年にフェルマーテストを改良した **AKS 素数判定法**が発表され脚光を浴びたが，詳しくは別の機会に…ね．

9.3 オイラーの定理

法 m が素数ではないとき，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，$5^{6-1} \equiv 5 \not\equiv 1 \pmod{6}$, $2^{9-1} \equiv 4 \not\equiv 1 \pmod{9}$, 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． $n = 1$ のときはフェルマーの定理そのものであり，すでに示されている． 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． □

ここで，定理 8.6（または補題 8.7）によれば，$\varphi(p^n) = (p-1)p^{n-1}$ だから，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 8.8 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． □

この証明において，$\varphi(p_j^{n_j})$ たちの最小公倍数を $\psi(m)$ とすれば，

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

が成り立つこともわかる． 一方，$\varphi(m)$ は $\varphi(p_j^{n_j})$ たちの公倍数なので $\psi(m)|\varphi(m)$，したがって，この合同式はオイラーの定理の精密化を与えていることになる．

9.4 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，前節の最後でも見たように $\varphi(m)$ 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． 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． 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 9.7 m を 2 以上の自然数，a を m と互いに素な整数，s を法 m に関する a の位数とする． 自然数 r が

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

をみたすならば，位数 s は r の約数である． とくに $s|\varphi(m)$ が成り立つ．

証明 r を s で割り算して，$r = us + v$, $(0 \leq v < s)$ とすると，$1 \equiv a^r = (a^s)^u a^v \equiv a^v \pmod{m}$ 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． $\square$

例 9.8 $\varphi(100) = 40$ だからオイラーの定理より，$3^{40} \equiv 1 \pmod{100}$． したがって，命題 9.7 によれば，100 を法とする 3 の位数は 40 の約数 $1, 2, 4, 5, 8, 10, 20, 40$ のどれかである． 根気よく（そしてちょっと工夫して）計算すれば，$3^8 \not\equiv 1$, $3^{10} \not\equiv 1 \pmod{100}$ かつ $3^{20} \equiv 1 \pmod{100}$ が得られ，位数は 20 であることがわかる．

命題 9.9 m を 2 以上の自然数，a を m と互いに素な整数，s を法 m に関する a の位数とする．

(1) $s = uv$ $(u, v \in \boldsymbol{N})$ ならば，法 m に関する a^u の位数は v である．
(2) $t \in \boldsymbol{N}$ が s と互いに素ならば，法 m に関する a^t の位数も s 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． いま，a, m は互いに素なので α は可逆であり，α^{-1} が定義されることにも注意せよ．
(1) まず $(\alpha^u)^v = \alpha^{uv} = \alpha^s = 1$ が成り立つ． よって，w を α^u の位数とすると，命題 9.7 より $w|v$． 一方，$\alpha^{uw} = 1$ だから，再び命題 9.7 より $s = uv$ は uw の約数であり $v|w$． ゆえに $w = v$．
(2) まず $(\alpha^t)^s = (\alpha^s)^t = 1$ が成り立つ． よって，w を α^t の位数とすると，命題 9.7 より $w|s$． いま，s, t は互いに素だから，$sx + ty = 1$ $(x, y \in \boldsymbol{Z})$ と書けて，$\alpha = \alpha^{sx+ty} = (\alpha^s)^x(\alpha^t)^y = (\alpha^t)^y$． 一方，$\alpha^{tw} = 1$ だから $\alpha^w = (\alpha^t)^{yw} = 1$，したがって，再び命題 9.7 より $s|w$ となるから，$w = s$ を得る． $\square$

命題 9.10 m を 2 以上の自然数，a, b をともに 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． w を $\alpha\beta$ の位数とする． まず，$(\alpha\beta)^{st} = (\alpha^s)^t(\beta^t)^s = 1$ なので，命題 9.7 より $w|st$ が成り立つ． そこで，逆に $st|w$ 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 $x, y \in \boldsymbol{Z}$ 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，再び命題 9.7 より $s|w$ である． α, β の役割を入れ換えれば，$t|w$ 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． $\square$