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，整数のべき乗数 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）．

9.2　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，$5^{6-1} \equiv 5 \not\equiv 1 \pmod{6}$, $2^{9-1} \equiv 4 \not\equiv 1 \pmod{9}$, など． 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ために，まず m が素数のべきの場合を考えよう．

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，$a^{(p-1)p^{n-1}}=1+p^nk$　$(k\in \boldsymbol{Z})$ と書ける．これを p 乗すれば，$n+1\leq 2n<3n<\cdots$ に注意して

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

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 9.2 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，フェルマーの定理は次の定理に拡張される．

定理 9.3 (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 9.2 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．□

フェルマーの定理やオイラ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^{120} 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，120 の 58 による割り算 $120=2\cdot 58+4$ を用いれば，$5^{120}=(5^{58})^2\cdot 5^4\equiv 5^4=625\equiv 35 \pmod{59}$ となる．

この計算を一般化して次の命題を得る．

命題 9.4 整数 a が自然数 $m>1$ と互いに素であるとする．

(1)　整数 k,l に対して，$k\equiv l \pmod{\varphi(m)}$ ならば $a^k\equiv a^l \pmod{m}$.

(2)　整数 n を $\varphi(m)$ で割った余りを r とすれば，$a^n\equiv a^r \pmod{m}$.

証明　(1)　$k\equiv l \pmod{\varphi(m)}$ ならば $k=l+c\varphi(m)$ をみたす整数 c がとれるが，オイラーの定理より $a^{\varphi(m)}\equiv 1 \pmod{m}$ だから，$a^k=a^l(a^{\varphi(m)})^c\equiv a^l \pmod{m}$ が成り立つ．(2) は (1) より直ちに得られる．□

例 9.5 大きなべきをもつ整数 17^{3129} を 168 で割った余りを求めたい．まず 17 と 168 が互いに素であることから，命題 9.4 が適用できることに注意する．$168=2^3\cdot 3\cdot 7$ と素因数分解され，$\varphi(246)=(8-4)(3-1)(7-1)=48$ と計算でき，$3129\equiv 9 \pmod{48}$ だから，$17^{3129}\equiv 17^9 \pmod{168}$．よって，

$$17^9=17\cdot((17^2)^2)^2=17\cdot(121^2)^2\equiv 17\cdot 25^2\equiv 17\cdot 121\equiv 41 \pmod{168}$$

と計算され余り 41 を得る．

例 9.6 前の例は，中国の剰余定理を援用することにより，少し簡単に計算できる． 実際，$\varphi(8)=4,\ \varphi(3)=2,\ \varphi(7)=6$ に着目し，$3129\equiv 1 \pmod 4$ と $3129\equiv 3 \pmod 6$ から，$x=17^{3129}$ がみたすべき $8,3,7$ を法とする合同式

$$x\equiv 1 \pmod 8,\quad x\equiv (-1)^{3129}=-1 \pmod 3,\quad x\equiv 17^3\equiv 3^3\equiv -1 \pmod 7$$

が，168 を法とする合同式よりずっと簡単に得られる． この連立合同式は中国の剰余定理から 168 を法として一意的に解をもち，実際に $x\equiv 41 \pmod{168}$ が求まる．

9.3 ちょっとだけ精密化

オイラーの定理の証明において，$\varphi(p_1^{n_1}),\dots,\varphi(p_r^{n_r})$ 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．

以下，もうちょっとだけ改良できることを示そう． まず，次の補題が成り立つ．

補題 9.7 任意の奇数 a と自然数 $n\geq 3$ に対して，

$$a^{2^{n-2}}\equiv 1 \pmod{2^n}$$

が成り立つ．

証明 $n=3$ のとき，$a=1+2k$ $(k\in \boldsymbol{Z})$ と表しておけば $k(k+1)$ は偶数だから，$a^2=1+4k+4k^2=1+4k(k+1)\equiv 1 \pmod 8$ より成り立つ． あとは補題 9.2 と同様にすればよい． □

$\varphi(2^n)=2^{n-1}$ なので，この補題はオイラーの定理にはビミョーに含まれていないことに注意する． いま，$\lambda(2)=1,\ \lambda(4)=2$ とし，$n\geq 3$ のとき $\lambda(2^n)=2^{n-2}$ として，さらに奇素数 p のべきに対しては $\lambda(p^n)=\varphi(p^n)=p^n-p^{n-1}$ $(n\geq 1)$ とする． このとき，オイラーの定理と補題 9.7 から，任意の素数 p と自然数 n に対して，

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

が，p と互いに素なすべての整数 a について成り立つ． そこで，自然数上の関数 λ を，$m=p_1^{n_1}\cdots p_r^{n_r}$ (ただし p_j は相異なる素数で $n_j\geq 1$) に対して，

$$\lambda(m)=\mathrm{lcm}(\lambda(p_1^{n_1}),\dots,\varphi(p_r^{n_r}))$$

と定義すると，$\lambda(m)|\psi(m)|\lambda(m)$ であって，オイラーの定理の精密化として次が得られる．

定理 9.8 (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.

例 9.9 $m = 168 = 8 \cdot 3 \cdot 7$ の場合，$\varphi(m) = 48$ より，168 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 $a^{48} \equiv 1 \pmod{168}$ を得る． 一方，$\psi(m) = \mathrm{lcm}(4, 2, 6) = 12$ なので，$a^{12} \equiv 1 \pmod{168}$ とできる． さらに，カーマイケルの定理を適用すれば，$\lambda(m) = \mathrm{lcm}(2, 2, 6) = 6$ と計算でき，より強い合同式 $a^6 \equiv 1 \pmod{168}$ が得られる． これを使って例 9.5 の計算を簡単化することが可能である． 実際，$3129 \equiv 3 \pmod{6}$ より $17^{3129} \equiv 17^3 \equiv 41 \pmod{168}$ が得られる．

9.4 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 9.10 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コーディング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.