

第9章 フェルマーの定理と位数

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 $f_a : (\mathbf{Z}/p\mathbf{Z})^\times \rightarrow (\mathbf{Z}/p\mathbf{Z})^\times$ を $f_a(x) = ax$ 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、

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

が成り立つが、 $(p-1)!$ は p を法として可逆だから、定理の合同式を得る。□

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 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、 $a^N \equiv 1 \pmod{m}$ をみたすべき指数 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 が素数べきの場合を考えよう。

補題 9.3 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, $a^{(p-1)p^{n-1}} = 1 + p^n k$ ($k \in \mathbf{Z}$) と書ける. これを p 乗すれば, $n+1 \leq 2n < 3n < \dots$ に注意して

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

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 8.5 (または補題 8.6) によれば, $\varphi(p^n) = (p-1)p^{n-1}$ だから, 補題 9.3 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 9.4 (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 9.3 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. □

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.

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. 証明は, $n=3$ のとき直接計算すれば確かめられ, あとは補題 9.3 と同様にできる. $\varphi(2^n) = 2^{n-1}$ なので, オイラーの定理にはピミヨーに含まれていないことに注意する.

補題 9.5 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.

そこで, $m = p_1^{n_1} \cdots p_r^{n_r}$ (ただし, $p_1 < \cdots < p_r$ は素数で $n_j > 0$) のとき,

$$\lambda(m) = \begin{cases} \text{lcm}(\varphi(p_1^{n_1}), \dots, \varphi(p_r^{n_r})) & (8 \nmid m \text{ のとき}), \\ \text{lcm}(2^{n_1-2}, \varphi(p_2^{n_2}), \dots, \varphi(p_r^{n_r})) & (8 \mid m \text{ のとき}) \end{cases}$$

とする. このようにして定まる自然数上の関数 λ をカーマイケル関数という. このとき, $\lambda(m) \mid \psi(m) \mid \varphi(m)$ 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 9.6 (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 9.7 $m = 168 = 8 \cdot 3 \cdot 7$ の場合, $\varphi(m) = (8-4) \cdot (3-1) \cdot (7-1) = 4 \cdot 2 \cdot 6 = 48$ 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, $\psi(m) = \text{lcm}(4, 2, 6) = 12$ より, $a^{12} \equiv 1 \pmod{168}$ とできる. さらに, カーマイケルの定理を適用すれば, $\lambda(m) = \text{lcm}(2, 2, 6) = 6$ と計算できるから, より強い合同式 $a^6 \equiv 1 \pmod{168}$ 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べき指数として $\varphi(m)$ 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 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. また, 剰余類 $\alpha \in (\mathbf{Z}/m\mathbf{Z})^\times$ 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

$$\min \{ k \in \mathbf{N} \mid a^k \equiv 1 \pmod{m} \} = \min \{ k \in \mathbf{N} \mid \bar{a}^k = \bar{1} \}$$

であり, これを簡単に剰余類 \bar{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せよ.

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

(2) $s = xy$ ($x, y \in \mathbf{N}$) ならば, 法 m に関する a^x の位数は y である.

証明 簡単のため $\alpha = \bar{a} = a + m\mathbf{Z}$ とおき, $\bar{1} = 1 + m\mathbf{Z}$ 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) 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. よって, t を α^x の位数とすると $t \leq y$. 一方, $\alpha^{xt} = 1$ だから, (1) より $s = xy$ は xt の約数であり $y \leq t$. ゆえに $y = t$. \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, $\alpha = \bar{a}, \beta = \bar{b} \in (\mathbf{Z}/m\mathbf{Z})^\times$ 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, 前命題 (1) 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, $\alpha^w = (\alpha\beta)^{wt} = 1$ となるから, 前命題 (1) 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

いま, 自然数 $m > 1$ に対して $(\mathbf{Z}/m\mathbf{Z})^\times$ の元の最大位数を $\mu(m)$ とする;

$$\mu(m) = \max \left\{ \alpha \text{ の位数} \mid \alpha \in (\mathbf{Z}/m\mathbf{Z})^\times \right\}.$$

カーマイケルの定理および命題 9.9(1) より, $\mu(m)|\lambda(m)$ 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カーマイケルの定理を, さらに精密にしたもののように見える….

定理 9.11 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 $\alpha = \bar{a} \in (\mathbf{Z}/m\mathbf{Z})^\times$ 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 $\beta \in (\mathbf{Z}/m\mathbf{Z})^\times$ 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, $\mu(m)$ 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. \square

じつは, $\mu(m)$ は $\lambda(m)$ と等しい. したがって, 上に書いた定理 9.11 の証明は, 結果として, カーマイケルの定理 (定理 9.6) の別証明を与えているに過ぎない. なお, $\lambda(m) = \mu(m)$ の証明は, 群論的な知識を本質的に使うので, ここでは紹介しない. もう少し大人になってからの楽しみといたしましょう.