オイラーの定理（整数）

フェルマーの小定理[1] の一般化であるオイラーの定理を証明する．

定義. n 以下の自然数 $1, \cdots, n$ のうち，n と互いに素であるものの個数を $\varphi(n)$ で表す．

例.
- 素数 p に対して，$\varphi(p) = p - 1$ である．
- 素数の冪 p^k に対して，$\varphi(p^k) = (p-1)p^{k-1}$ である．
- 一般に，$n = p_1^{r_1} \cdots p_m^{r_m}$ と素因数分解できる数 n に対して，

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

である．

定理 (Euler). n を正の整数とし，a を n と互いに素な整数とする．このとき，次が成り立つ．

$$a^{\varphi(n)} \equiv 1 \mod n$$

証明. n を正の整数とし，a を n と互いに素な整数とする．$1, \cdots, n$ のうち，n と互いに素であるもの全体の集合を

$$S := \{s_1, \cdots, s_{\varphi(n)}\}$$

とする．$i = 1, \cdots, \varphi(n)$ に対して，s_i と a は，どちらも n と互いに素なので，as_i も n と互いに素である．よって，as_i に対して，

$$t_i \equiv as_i \mod n, \quad 1 \le t_i \le n$$

を満たす整数 t_i をとると，t_i も n と互いに素である[2] ．これら t_i を用いて，集合 T を

$$T := \{t_1, \cdots, t_{\varphi(n)}\}$$

で定義すると，$T \subset S$ が成り立つ．$T = S$ を示す．そのためには，$s_i \neq s_j$ なら，$t_i \neq t_j$ であることを示せば良い．対偶を示す．$t_i = t_j$ を仮定すると，

$$as_i \equiv t_i = t_j \equiv as_j \mod n$$

が成り立つ．a を n は互いに素であったから，$s_i = s_j$ が従う．

以上から，集合 S, T は，添字の番号を付け替えた（順番を入れ替えた）だけで同じ集合であることがわかった．よって，全ての元の積を n を法として考えることにより，

$$\begin{aligned} s_1 \cdots s_{\varphi(n)} &= t_1 \cdots t_{\varphi(n)} \\ &\equiv as_1 \cdots as_{\varphi(n)} \\ &= a^{\varphi(n)} s_1 \cdots s_{\varphi(n)} \qquad \mod n \end{aligned}$$

が成り立つ．a と積 $s_1 \cdots s_{\varphi(n)}$ は，互いに素なので，上の合同式の両辺を $s_1 \cdots s_{\varphi(n)}$ で割ることができ，これから主張が従う． □

---

[1] p を素数，a を p と互いに素な整数とすると，$a^{p-1} \equiv 1 \mod p$ が成り立つ．

[2] ユークリッドの互除法：$A = Bq + r$ なら，A, B の最大公約数と，B, r の最大公約数は一致する．