オイラーの定理

nが正の整数でaをnと互いに素な正の整数としたとき,
$a^{\phi(n)} \equiv 1 \pmod{n}$
が成立する。

ここで、$\phi(n)$は、オイラーのϕ関数
この定理はフェルマーの小定理の一般化であり、この定理をさらに一般化したものがカーマイケルの定理である。

応用1

7^{2009}の下2桁を求めたい場合、
$\phi(100) = 40$　(下2桁なので100を選択)

オイラーの定理から、$7^{40} \equiv 1 \pmod{100}$

よって、
$7^{2009} = 7^9 \times (7^{40})^{50} \equiv 7^9 \equiv 7 \pmod{100}$
$7^9 = 40353607$

ゆえに下2桁は07

証明

nと互いに素なn以下の正の整数の集合を
$A = \{b_1, b_2, \ldots, b_{\phi(n)}\}$ とする。

この要素のそれぞれにaを乗じた集合
$B = \{ab_1, ab_2, \ldots, ab_{\phi(n)}\}$ を考えれば、
aとnは互いに素だから、集合A,Bは法をnとしたときに一致し、その積も法nにおいて等しい。

すなわちAの要素の積をPとすれば、
$P \equiv a^{\phi(n)}P \pmod{n}$

nとPは互いに素だから、
$a^{\phi(n)} \equiv 1 \pmod{n}$　　q.e.d

応用2

公開鍵暗号、オイラーのϕ関数が使われる。

素数 p、q を選択し、その積 n を求める。
ϕ(n)未満の正の整数でϕ(n) と互いに素な数を1つ決め、e と書く。
公開鍵は{e、n}となる。
この公開鍵を用いて平文 Mを暗号化する。

暗号化：$M^e \equiv C \pmod{n}$
平文を数と見なし、e乗してnで割った剰余を使って暗号文とする。
暗号文の長さは n 以下となる。

復号化には、nを法とした eの逆数を用いる。
n を法としたeの逆数をdとすると、

復号化： $C^d \equiv M \pmod{n}$
暗号文をd乗し、nで割った余りを計算すると元の文字列が求まる。
この dを秘密鍵とする。