オイラー関数

定義 4.9 $n \in \mathbb{N}$ とする.

$\varphi(n) := |\{m \mid 1 \leq m \leq n,\ \gcd(m,n) = 1\}|$ とする.

例 (1) $\varphi(1) = 1$ である.

(2) pが素数なら $\varphi(p) = p-1$ である.

(3) $\varphi(6)$ を考えると. 6と素なのは.

1, 5 の2つなので $\varphi(6) = 2$

(4) $\varphi(15)$ を考えると 15と素なのは

1, 2, 4, 7, 8, 11, 13, 14 より $\varphi(15) = 8$.

(5) $\varphi(90)$ を求める. $90 = 2 \times 3^2 \times 5$ より

1から90の数の中で.

2の倍 : $\frac{90}{2}$ 2, 3の倍 : $\frac{90}{2\times 3}$

3の倍 : $\frac{90}{3}$ 3. 5の倍 : $\frac{90}{3\times 5}$

5の倍 : $\frac{90}{5}$ 5. 2の倍 : $\frac{90}{2\times 5}$

2, 3. 5の倍 : $\frac{90}{2\times 3\times 5}$ となる

$$\therefore \varphi(90) = 90 - \left(\frac{90}{2} + \frac{90}{3} + \frac{90}{5}\right) + \left(\frac{90}{2\times 3} + \frac{90}{3\times 5} + \frac{90}{2\times 5}\right) - \frac{90}{2\times 3\times 5}$$

$$= 90\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$ となる.

$$= 24$$

これを一般化すると、次が得られる

定理4.10　$n = p_1^{k_1} \cdots p_m^{k_m}$ のとき

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

∵ n以下の数 kが p_1と素になる確率は $1-\frac{1}{p_1}$ である。

ここで p_1と素になることと、p_2と素になることが独立であることを示す。

∵ kが p_2 と素になる条件の下で、p_1と素になる条件付確率を求めると、

p_2と素：$n - \frac{n}{p_2} = n\left(1-\frac{1}{p_2}\right)$

p_1, p_2と素：$n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 \times p_2} = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$.

∴求める条件付確率は $1-\frac{1}{p_1}$

∴ $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_m}\right)$ である。 //

次にフェルマーの小定理を示すが、その前に補題を1つ示す

補題4.11　pを素数、$a, b \in \mathbb{Z}$ とすると、

$(a+b)^p \equiv a^p + b^p \pmod{p}$ が成立

∵ まず $\frac{p!}{q!(p-q)!} \equiv 0 \quad (\text{mop } p) \quad (q<p)$ に注意

これより2項展開すれば

$(a+b)^p = \sum_{k=0}^{p} a^k \cdot b^{p-k} \cdot {}_pC_k \equiv a^p + b^p \pmod{p}$ となる //

定理4.12　pを素数，$a \in \mathbb{Z}$ とすると．

$a^p \equiv a \pmod p$ である．とくに aとpが素なら．

$a^{p-1} \equiv 1 \pmod p$ である

∵ まず $a \geq 0$ として．帰納法で示す．

$a = 0$ のときは明らか．さらに

$(a+1)^p \equiv a^p + 1^p = a^p + 1 \equiv a + 1$ となる．

補題　　帰納法の仮定．

$a < 0$ のとき．さらにpが奇数なら．

$(-a)^p \equiv -a \pmod p$ だが．

$-a^p \equiv -a$，$a^p \equiv a$ となる．

pが偶数なら．①$a \equiv 1$ or ②$a \equiv 0$ なので．

① $a^p \equiv 1^p = 1 \equiv a$．② $a^p \equiv 0 \equiv a$ となる．

//.

例．$3^{100} \pmod{13}$ を求めると．$3^{12} \equiv 1$ より

$3^{100} = 3^{12 \times 8 + 4} \equiv 3^4 = 81 \equiv 3$ となる．

定理4.13　$n \in \mathbb{N}$，$a \in \mathbb{Z}$ に対し．

$\gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$ が成り立つ．

∵ n以下で nと互いに素な整数の集合を

$A = \{b_1, b_2, \cdots, b_{\varphi(n)}\}$ とする．

ここで、次の集合を考える。

$B=\{ab_1, \cdots, ab_{\varphi(n)}\}$.

この集合の元は、nと素であり、nを法としたとき、Aと一致する。

<u>nと素であること。</u>

素因数分解を考えれば、aとb_1がnと素 $\Rightarrow$ ab_1とnが素となる。

<u>nを法としたとき、Aと一致すること</u>：

もし、$ab_i \equiv ab_j$ とすると、$b_i \equiv b_j$ となり矛盾。

$\therefore$ Bの元は nを法としたとき、全て異なる元になる。

一方、Aは nと互いに素な元を全て集めた集合であり

Bの元はnと素なので $A=B \pmod n$ である。

$\therefore$ $b_1 \cdot b_2 \cdots b_{\varphi(n)} \equiv ab_1 \cdots ab_{\varphi(n)} \pmod n$.

$$1 \equiv a^{\varphi(n)} \pmod n$$ となる。