

オイラー関数

赤間

平成19年11月2日

定義 1 (最大公約数) 二つの整数 n, m の最大公約数 $\gcd(n, m)$ とは、

1. $\gcd(n, m) \geq 0$;
2. n と m は $\gcd(n, m)$ の整数倍 ; かつ、
3. n と m が g の整数倍ならば、 $\gcd(n, m)$ は g の整数倍。

たとえば $\gcd(0, x) = x$ である。

定義 2 正整数 n に対して、 n 以下の正整数で n との最大公約数が 1 であるものの個数を $\varphi(n)$ で表す。 φ はオイラー関数と呼ばれる。 $\varphi(1) = 1$ である。

問題 1 以下を証明せよ。

1. 正整数 N に関して $\sum_{d|N} \varphi(d) = N$.
2. 正整数 N_1 と N_2 が互いに素ならば $\varphi(N_1 N_2) = \varphi(N_1) \varphi(N_2)$.

命題 1 n の素因数分解が $n = p_1^{e_1} \cdots p_k^{e_k}$ (p_1, \dots, p_k は異なる素数、 $e_1 \geq 1, \dots, p_k \geq 1$) のとき、

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \leq n - 1.$$

証明はいくつかあるが、ここでは包除原理を用いたものを紹介する

命題 2 (包除原理) 有限集合 A の濃度を $\#A$ で表す。 A_1, \dots, A_k は互いに異なる有限集合とする。 それら和集合の濃度 $\#\left(\bigcup_{i=1}^k A_i\right)$ は

$$\begin{aligned} & \sum_{i=1}^k \#A_i - \sum_{i_1 \neq i_2} \#(A_{i_1} \cap A_{i_2}) + \sum_{\substack{i_1, i_2, i_3 \\ \text{は互いに異なる}}} \#(A_{i_1} \cap A_{i_2} \cap A_{i_3}) + \cdots \\ & - (-1)^m \sum_{\substack{i_1, i_2, \dots, i_m \\ \text{は互いに異なる}}} \#(A_{i_1} \cap \cdots \cap A_{i_m}) \cdots - (-1)^k \#(A_1 \cap \cdots \cap A_k). \end{aligned}$$

ここで A_j を n 以下の p_j の正の倍数全体とすると, それら和集合の濃度 $\#(\bigcup_{i=1}^k A_i)$ は n と素でない n 以下の正整数の個数であり, $n - \varphi(n)$ となる.

一方, $\#A_j = n/p_j$ であり, 上の式の右辺における $\#(A_{i_1} \cap A_{i_2})$ は n 以下の $p_{i_1}p_{i_2}$ の正の倍数の個数 $n/(p_{i_1}p_{i_2})$ となる. 従って上の式は

$$\begin{aligned} n - \varphi(n) &= n \left(\sum_i 1/p_i - \sum_{i_1 \neq i_2} 1/(p_{i_1}p_{i_2}) + \cdots \right. \\ &\quad \left. - (-1)^m \sum_{\substack{i_1, i_2, \dots, i_m \\ \text{は互いに異なる}}} 1/(p_{i_1}p_{i_2} \cdots p_{i_m}) - (-1)^k 1/(p_1 p_2 \cdots p_k) \right) \\ &= n \{ (1 - 1/p_1) \cdots (1 - 1/p_1) - 1 \}. \end{aligned}$$

ゆえに

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \leq n - 1.$$