オイラー関数の歴史と現在

飯高 茂

平成27年11月12日

1 オイラー関数の歴史

L.E.Dickson 著の The history of Theory of Numbers I,1919/20(Chelsea Publishing Company 版 1992) の第1章を参考にしてオイラー関数の歴史について書いて簡単にふれる.

オイラー関数は Leonhard Euler によって 1763 年に導入された. 導入の動機はフェルマーの小定理を非素数の場合に拡張することであった.

ただし, 記号 $\varphi(n)$ は Gauss の Disquisitiones Arithmeticae で初めて使われ広まった.

$\varphi(n)$ は Euler's phi function と呼ばれる.

1879 年に J. J. Sylvester が totient という言い方を導入しそのため, Euler's totient function と呼ばれることもある.

n の cototient は $n-\varphi(n)$ で定義され, これは 1 以上で,1 になるのは n が素数の場合だけである.

2 高次オイラー関数

2015 年に都内の私立高校 2 年生の三谷樹さんがはじめて高次オイラー関数の公式を見出した. 次のその紹介を行う.

自然数 n を素因数分解して

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

とおく.

集合 $S_n = \{1, 2, \cdots, n\}$ について n の素因子 p に対して p の倍数になる S_n の元の集合を $S_n(p)$ で表す.

$S_n(p) = pS_{\frac{n}{p}}$ と書くことができる.

たとえば

$n = 6, p = 2$ のとき $S_3 = \{1, 2, 3\}, S_6(2) = 2 * S_3 = 2\{1, 2, 3\} = \{2, 4.6\}$.

$n = 6, p = 3$ のとき $S_2 = \{1, 2\}, S(_6 3) = 3 * S_2 = 3\{1, 2\} = \{3, 6\}$.

2.1 オイラー関数

$W_n = S_n - \cup_{j=1}^{s} S_n(p_j)$ は $a < n$ かつ a, n:互いに素な a の集合である.
その個数を $\varphi(n)$ と書く. これがオイラー関数である.
S_n の部分集合 T についてその元の個数を $|T|$ で示すと $|S_n(p_j)| = \frac{n}{p_j}, |S_n(p_j p_k)| = \frac{n}{p_j p_k}, \cdots$ が成り立つ.

2.2 包含関係の公式

一般に集合 S の部分集合 $A_1, A_2, \cdots, A_s$ について

$$|\cup_{j=1}^{s} A_j| = \sum_{j=1}^{s} |A_j| - \sum_{j<k}^{s} |A_j \cap A_k| + \cdots$$

証明は s についての数学的帰納法でできる.

2.3 オイラー関数の表示式

$$\begin{aligned}
\varphi(n) &= |W_n| \\
&= |S_n - \cup_{j=1}^{s} S_n(p_j)| \\
&= |S_n| - |\cup_{j=1}^{s} S_n(p_j)| \\
&= n - \sum_{j=1}^{s} |S_n(p_j)| + \sum_{j<k}^{s} |S_n(p_j p_k)| - \cdots \\
&= n - (n/p_1 + n/p_2 + \cdots + n/p_s) + n/(p_1 p_2) + \cdots + n/(p_{s-1} p_s) - \cdots \\
&= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_s).
\end{aligned}$$

と書ける.
そこで $A = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_s)$ とおくと

$$\varphi(n) = nA.$$

2.4 和の場合

$a < n$ かつ n と互いに素な a の和を $\psi(n)$ と書き, S_n の部分集合 T についてその元の和を $|T|_1$ で示すと

$$|S_n|_1 = \frac{n(n+1)}{2}, |S_n(p)|_1 = p\frac{n/p(n/p+1)}{2} = \frac{n^2}{2p} + \frac{n}{2} = \frac{n}{2}(\frac{n}{p} + 1).$$

$0 = (1-1)^s = 1 - s + s(s-1)/2 - s(s-1)(s-2)/6 + \cdots$ に注意すると

$$\begin{aligned}\psi(n) &= |S_n - \cup_{j=1}^{s} S_n(p_j)|_1 \\ &= |S_n|_1 - |\cup_{j=1}^{s} S_n(p_j)|_1 \\ &= \frac{n(n+1)}{2} - \sum_{j=1}^{s} |S_n(p_j)|_1 + \sum_{j<k}^{s} |S_n(p_j p_k)|_1 - \cdots \\ &= \frac{n}{2}(n+1-n\sum_{j=1}^{s}\frac{1}{p_j} - s + n\sum_{j,k}\frac{1}{p_j p_j} + \frac{s(s-1)}{2} - \cdots) \\ &= \frac{n}{2}(nA) \\ &= \frac{n\varphi(n)}{2}.\end{aligned}$$

$$\psi(n) = \frac{n\varphi(n)}{2}.$$

これは Wikipedia の英語版に出ている公式である.

2.5 平方和

平方和について考える. $a < n$ かつ n と互いに素な a の平方和を $\psi^{(2)}(n)$ と書く. 一般に部分集合 T についてその元の平方和を $|T|_2$ で示すと

$$|S_n|_2 = \frac{n(n+1)(2n+1)}{6} = \frac{n}{6}(3n+2n^2+1), |S_n(p_j)|_2 = \frac{n}{6}(3n + \frac{2n^2}{p_j} + p_j)$$

$$\begin{aligned}\psi^{(2)}(n) &= |S_n - \cup_{j=1}^{s} S_n(p_j)|_2 \\ &= |S_n|_2 - |\cup_{j=1}^{s} S_n(p_j)|_2 \\ &= \frac{n(n+1)(2n+1)}{6} - \sum_{j=1}^{s} |S_n(p_j)|_2 + \sum_{j<k}^{s} |S_n(p_j p_k)|_2 + \cdots \\ &= \frac{n}{6}(3n+2n^2+1-(3ns+2n^2\sum_{j=1}^{s}\frac{1}{p_j} + \sum_{j=1}^{s} p_j) \\ &+ (3n\frac{s(s-1)}{2} + 2n^2\sum_{j,k}\frac{1}{p_j p_k} + \sum_{j,k} p_j p_k)\cdots) \\ &= \frac{n}{6}(2n^2+1-(2n^2\sum_{j=1}^{s}\frac{1}{p_j} + \sum_{j=1}^{s} p_j) + (2n^2\sum_{j,k}\frac{1}{p_j p_k} + \sum_{j,k} p_j p_k)\cdots) \\ &= \frac{n}{6}(2n^2 A + B).\end{aligned}$$

ここで $B=(1-p_1)(1-p_2)\cdots(1-p_s)$ とおいた. よって

$$\psi^{(2)}(n)=\frac{n}{6}(2n^2A+B).$$

2.6 n の根基

n の根基 $\mathrm{rad}(n)=p_1p_2\cdots p_s$ を用いると,
$\frac{B}{\mathrm{rad}(n)}=(-1)^sA=\frac{\varphi(n)}{n}$ が成り立つ.

$$\frac{B}{\mathrm{rad}(n)}=(1/p_1-1)(1/p_2-1)\cdots(1/p_s-1)=(-1)^sA.$$

$$nB=\mathrm{rad}(n)(-1)^snA=\mathrm{rad}(n)(-1)^s\varphi(n).$$

$$\psi^{(2)}(n)=\frac{1}{6}(2n^2\varphi(n)+nB)=\frac{\varphi(n)}{6}(2n^2+(-1)^s\mathrm{rad}(n)).$$

abc 予想の定式化で登場した n の根基がここにも出てきた.

$$\psi^{(2)}(n)=\frac{\varphi(n)}{6}(2n^2+(-1)^s\mathrm{rad}(n))$$

これは広尾学園の高校生三谷樹さんがはじめて見出した公式で簡明な美しい式である. 私はとても感心した.

2.7 立方和

三谷さんは立方和についても公式を与えた.
$a<n$ かつ n と互いに素な a の立方和を $\psi^{(3)}(n)$ と書く.
T についてその元の立方和を $|T|_3$ で示すと
$|S_n|_3=\frac{n^2(n^2+2n+1)}{4}$ が成り立ち $|S_n(p_j)|_3=\frac{n^2}{4}(2n+\frac{n^2}{p_j}+p_j)$.

$$\begin{aligned}
\psi^{(3)}(n)&=|S_n-\cup_{j=1}^{s}S_n(p_j)|_3\\
&=|S_n|_3-|\cup_{j=1}^{s}S_n(p_j)|_3\\
&=\frac{n^2}{4}(n^2+2n+1-\sum_{j=1}^{s}(\frac{n^2}{p_j}+2n+p_j)-\sum_{j,L}^{s}(\frac{n^2}{p_jp_L}+2n+p_jp_L))\cdots\\
&=\frac{n^2}{4}(n^2A+B).\\
&=\frac{n\varphi(n)}{4}(n^2+(-1)^s\mathrm{rad}(n)).
\end{aligned}$$

よって

$$\psi^{(3)}(n) = \frac{n\varphi(n)}{4}(n^2 + (-1)^s \mathrm{rad}(n)).$$

このようにしてやり方がわかると順調に次数をあげていくらでも調べることができる. それでは, m 乗和についてはどうなるか. ここでベルヌーイ数が出てくる.

2.8 m 乗和 の公式

集合 $S_n = \{1, 2, \cdots, n\}$ とおく. S_n の部分集合 T についてその元の m 乗和を $|T|_m$ で示す.

$$S_m(n) = |S|_m = \sum_{k=1}^{n} k^m = 1 + 2^m + \cdots + n^m$$

とおく. $S_m(n)$ の式はベルヌーイ数 B_k を用いると表すことができる.

3 ベルヌーイ数 B_k

一般に数列 $\{c_n\}$ について $f(x) = \sum_{j=0}^{\infty} c_j x^j$ を母関数,$h(x) = \sum_{j=0}^{\infty} \frac{c_j}{j!} x^j$ を指数型母関数という.

$\frac{t}{e^t - 1}$ を指数型母関数とするときの展開係数としてベルヌーイ数 B_k が定義される. すなわち

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

以後も指数型母関数がいろいろ使われる.

ベルヌーイ数 B_k を一般に明示的に与えることは困難だが簡単な場合は次のようになる.

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42}, B_7 = 0.$$

($B_1 = \frac{1}{2}$ とする場合もあり, この場合 m 乗和 の公式は微妙に違う)

$k > 1$, 奇数なら $B_k = 0$.

$$B_8 = \frac{-1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, B_{14} = \frac{7}{6},$$

$$B_{16} = -\frac{3617}{510}, B_{18} = \frac{43867}{798}, B_{20} = -\frac{174611}{330}.$$

3.1 B_k の諸性質

1. 漸化式

$$B_k = -\sum_{q=0}^{k-1} \binom{k}{q} \frac{B_q}{(k-q+1)}$$

2. ベルヌーイ多項式

$$\frac{te^{xt}}{e^t-1} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}.$$

3.

$$\zeta(2n) = (-1)^{n+1} B_{2n} \frac{(2\pi)^{2n}}{2\times(2n)!}.$$

これより $\zeta(2) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}$(Euler) など

4.

$$\zeta(-n) = \frac{-B_{n+1}}{n+1}, n > 0$$

$n = 2k$ なら $B_{n+1} = 0$. よって $\zeta(-2k) = 0 : -2k$ をゼータ関数の自明な零点という.
$n = 1$ とすると $\sum_{k=1}^{\infty} = -\frac{1}{12}$ (Euler) これは最近物理で人気のある式.

3.2 $B_{2k+1} = 0$ の証明

$\frac{t}{e^t-1} = 1 - \frac{t}{2} + F(t)$ により　　$F(t)$ を定義する.
$c_k = B_k/k!$ を使うと

$$F(t) = \sum_{k=2}^{\infty} c_k t^k.$$

これが偶関数になることを以下で確認する.

$$F(t) = \frac{t}{e^t-1} - 1 + \frac{t}{2} = \frac{2+t+(t-2)e^t}{2(e^t-1)}$$

により

$$F(-t) = \frac{2-t-(t+2)e^{-t}}{2(e^{-t}-1)} = \frac{(2-t)e^t-(t+2)}{2(1-e^t)}.$$

$X = e^t - 1$ とおけば $X + 1 = e^t$ によって,

$$\frac{(2-t)e^t-(t+2)}{2(1-e^t)} = \frac{(2-t)(X+1)-(t+2)}{-2X} = \frac{t}{2} - 1 + \frac{t}{X} = F(t).$$

$F(-t) = F(t)$ になり $F(t)$ が偶関数になる. よって $c_{2k+1} = 0$. したがって,$c_{2k+1} = B_{2k+1}/(2k+1)! = 0$

4 べき和 の公式

$a_{k,m} = (-1)^k \binom{m+1}{k} B_k$ を定める.
たとえば

$$a_{0,m} = 1, a_{1,m} = \frac{m+1}{2}, a_{2,m} = \frac{m(m+1)}{12}, a_{3,m} = 0, a_{4,m} = -\frac{(m+1)m(m-1)(m-2)}{24 \times 30},$$

m 乗和 $S_m(n) = |S_n|_m = \sum_{k=1}^{n} k^m$ は n について $m+1$ 次式であり次の公式が成り立つ.

$$S_m(n) = \frac{n}{m+1} \sum_{k=0}^{m} a_{k,m} n^{m-k}.$$

はじめの数項は次のようになる.

$$S_m(n) = \frac{n}{m+1}(n^m + \frac{m+1}{2} n^{m-1} + \frac{m(m+1)}{12} n^{m-2} - \frac{(m+1)m(m-1)(m-2)}{24 \times 30} n^{m-4} + \cdots$$

$m = 3$ のとき検算

$$S_3(n) = \frac{n}{4}(n^3 + 2n^2 + n) = \frac{n^2}{4}(n+1)^2.$$

4.1 べき和公式の証明

以下英語版 Wikipedia を参考に証明を与える.
$\{B_j\}$ について その指数型母関数は簡単になる.

$$\frac{z}{e^z - 1} = \sum_{j=0}^{\infty} B_j \frac{z^j}{j!}$$

これより

$$\frac{1}{e^z - 1} = \sum_{j=0}^{\infty} B_j \frac{z^{j-1}}{j!}$$

m 乗和 $S_m(n)$ について その指数型母関数を $G(z,n)$ とおくとき

$$G(z,n) = \sum_{m=0}^{\infty} S_m(n) \frac{z^m}{m!} = \sum_{m=0}^{\infty} \sum_{k=1}^{n} k^m \frac{z^m}{m!}$$

和の順序を入れ替えて

$$G(z,n) = \sum_{k=1}^{n} \sum_{m=0}^{\infty} \frac{(kz)^m}{m!} = \sum_{k=1}^{n} e^{kz}.$$

$W = e^z$ とおくと

$$\sum_{k=1}^{n} e^{kz} = \sum_{k=1}^{n} W^k = \sum_{k=0}^{n} W^k - 1 = \frac{W^{n+1}-1}{W-1} - 1 = W \times \frac{W^n - 1}{W-1}$$

これより

$$G(z,n) = W \times \frac{W^n-1}{W-1} = \frac{e^{nz}-1}{1-e^{-z}} = (e^{nz}-1) \times \frac{1}{1-e^{-z}}.$$

$e^{nz}-1 = \sum_{q=1}^{\infty} \frac{1}{q!}(nz)^q$ と $\frac{1}{1-e^{-z}} = -\sum_{j=0}^{\infty} B_j \frac{(-z)^{j-1}}{j!}$ と
を代入すると

$$\begin{aligned} G(z,n) &= -\sum_{j=0}^{\infty} B_j \frac{(-z)^{j-1}}{j!} \sum_{q=1}^{\infty} \frac{1}{q!}(nz)^q \\ &= \sum_{j=0}^{\infty} B_j (-1)^j \sum_{q=1}^{\infty} \frac{z^{q+j-1} n^q}{j!q!}. \end{aligned}$$

ここで $m = q+j-1$ とおくとき $j = m+1-q \leq m$ により $m \geq j$.
q を m で置き換えて式を整理する:

$$\frac{B_j(-1)^j z^{q+j-1} n^q}{j!q!} = \frac{B_j(-1)^j z^m n^{m+1-j}}{j!(m+1-j)!}$$

$\binom{m+1}{j} = \frac{m!(m+1)}{(m+1-j)!j!}$ に注意すると

$$\frac{B_j(-1)^j z^m n^{m+1-j}}{j!(m+1-j)!} = B_j(-1)^j z^m n^{m+1-j} \binom{m+1}{j} \frac{1}{m!(m+1)}.$$

これを用いて $G(z,n)$ を求める.

$$\begin{aligned} G(z,n) &= \sum_{m=0}^{\infty} \Big(\sum_{j=0}^{m} B_j (-1)^j n^{m+1-j} \binom{m+1}{j} \Big) \frac{z^m}{m!(m+1)} \\ &= \sum_{m=0}^{\infty} \Big(\frac{n}{m+1} \sum_{j=0}^{m} B_j (-1)^j n^{m-j} \binom{m+1}{j} \Big) \frac{z^m}{m!} \\ &= \sum_{m=0}^{\infty} \frac{n}{m+1} \sum_{j=0}^{m} a_{j,m} n^{m-j} \frac{z^m}{m!} \end{aligned}$$

よって $G(z,n) = \sum_{m=0}^{\infty} S_m(n) \frac{z^m}{m!}$ により

$$S_m(n) = \frac{n}{m+1} \sum_{j=0}^{m} a_{j,m} n^{m-j}.$$

5 $\psi^{(m)}(n)$ の公式

n の素因子 $p=p_j$ について

$$|pS_n(\frac{n}{p})|_m = p^m \frac{n/p}{m+1}\sum_{k=0}^{m} a_{k,m}(n/p)^{m-k} = \frac{n}{m+1}\sum_{k=0}^{m} a_{k,m}n^{m-k}p^{k-1}$$

に注意すると,

$$|pS(\frac{n}{p})|_m = \frac{n}{m+1}\sum_{k=0}^{m} a_{k,m}n^{m-k}p^{k-1}$$

これを展開すると $a_{3,m}=0$ によって

$$\frac{n}{m+1}(\frac{n^m}{p} + a_{1,m}n^{m-1} + pa_{2,m}n^{m-2} + p^3a_{4,m}n^{m-4}) + \cdots$$

n の素因子 $p=p_j, q=p_L$ について

$$|pqS_n(\frac{n}{pq})|_m = \frac{n}{m+1}\sum_{k=0}^{m} a_{k,m}n^{m-k}p^{k-1}q^{k-1}$$

$n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ について $\Gamma(r,n)=\prod_{j=1}^{s}(1-p_j^r)$ とおく.
強いて言えば, $\Gamma(-1,n)=\prod_{j=1}^{s}(1-1/p_j)=A$,$\Gamma(1,n)=B$.

$$\begin{aligned}
\psi^{(m)}(n) &= |S_n - \cup_{j=1}^{s} S_n(p_j)|_m \\
&= |S_n|_m - |\cup_{j=1}^{s} S_n(p_j)|_m \\
&= S_m(n) - \sum_{j=1}^{s}|S_n(p_j)|_m + \sum_{j<L}^{s}|S_n(p_jp_L)|_m + \cdots \\
&= \frac{n}{m+1}(\sum_{k=0}^{m} a_{k,m}n^{m-k} - \sum_{j=1}^{s}(\sum_{k=0}^{m} a_{k,m}n^{m-k}p_j^{k-1}) + \sum_{j<L}^{s}\sum_{k=0}^{m} a_{k,m}n^{m-k}p_j^{k-1}p_L^{k-1} + \cdots \\
&= \frac{n}{m+1}(An^m + a_{2,m}Bn^{m-2} + a_{4,m}\Gamma(3,n)n^{m-4} + a_{6,m}\Gamma(5,n)n^{m-6} + \cdots)
\end{aligned}$$

以上により,m 乗和についての高次オイラー関数の公式をえる (S.Iitaka).

$$\psi^{(m)}(n) = \frac{n}{m+1}(An^m + a_2Bn^{m-2} + a_{4,m}\Gamma(3,n)n^{m-4} + a_{6,m}\Gamma(5,n)n^{m-6} + \cdots).$$

ここで $A=(1-1/p_1)(1-1/p_2)\cdots(1-1/p_s)$, $B=(1-p_1)(1-p_2)\cdots(1-p_s)$ とおいた.

$m=5$ として検算
$a_{2,m}=\frac{m(m+1)}{12}=\frac{5}{2}, a_{4,m}=-\frac{m(m+1)(m-1)(m-2)}{30}=-\frac{1}{2}$ により

$$\psi^{(5)}(n) = \frac{n^2}{12}(2\varphi(n)n^3 + 5Bn^2 - \Gamma(3,n)).$$

$$\psi^{(5)}(n) = \frac{n^2}{12}(2\varphi(n)n^3 + (-1)^s 5\varphi(n)\mathrm{rad}(n)n - \Gamma(3,n)).$$

$m = 6$ とすると新しい公式をえる.
$a_{2,m} = \frac{m(m+1)}{12} = \frac{7}{2}, a_{4,m} = \frac{m(m+1)(m-1)(m-2)}{4!}B_4 = -\frac{7}{6}$,
$a_{6,m} = \frac{m(m+1)(m-1)(m-2)(m-3)(m-4)}{6!}B_4 = \frac{1}{6}$ により

$$\psi^{(6)}(n) = \frac{n}{7}(An^6 + a_{2,m}Bn^4 + a_{4,m}\Gamma(3,n)n^2 + a_{6,m}\Gamma(5,n)).$$

$$\psi^{(6)}(n) = \frac{n}{7}(\varphi(n)n^5 + (-1)^s\frac{7}{2}\varphi(n)\mathrm{rad}(n)n^3 - \frac{7}{6}\Gamma(3,n)n^2 + \frac{1}{6}\Gamma(5,n)).$$

6 完全数

a を自然数とするときその約数の和を $\sigma(a)$ と書く.

$\sigma(a) = 2a$ を満たす数を 完全数といい, 6,28,496,8128 などがあり古代の数学者ユークリッドによって考えられた.

これらを素因数分解すると $6 = 2*(2^2-1), 28 = 2^2*(2^3-1), 496 = 2^4*(2^5-1), 8128 = 2^6*(2^7-1)$ などとなる.

$a = 2^e q(q = 2^{e+1} - 1$: 素数) と書かれる数は完全数になることはユークリッドによって知られていた. そこでこれらをユークリッドの完全数という.

7 究極の完全数の探究

P を素数とし $\sigma(P^e)$ が素数 q のとき $a = P^e q$ を底が P の **究極の完全数**と呼ぼう.

このとき $q = \frac{P^{e+1}-1}{P}$ となる. 言葉ができると諒解しやすくまた研究したくなるという効果がある.

究極の完全数を整数 m だけ平行移動しよう.

$q = \frac{P^{e+1}-1}{P} + m$ は素数として $a = P^e q$ を m だけ平行移動した底が P の完全数と呼ぶ.

平行移動も許した究極の完全数の満たす方程式を求めよう.

$q = \frac{P^{e+1}-1}{P} + m$ であって

$$\overline{P}\sigma(a) = \overline{P}\sigma(P^e q) = (P^{e+1} - 1)(q+1)$$

になり, $q + 1 = \frac{P^{e+1}+P-2}{P} + m$ を用いて次のように式変形する.

$$\begin{aligned}\sigma(a) &= \frac{P^{e+1}-1}{\overline{P}}(q+1)\\ &= (q-m)(q+1)\\ &= q(q+1)-m(q+1)\\ &= \frac{q}{\overline{P}}(P^{e+1}+P-2)+mq-m(q+1)\\ &= \frac{Pa+q(P-2)}{\overline{P}}-m.\end{aligned}$$

これより $q=\mathrm{Maxp}(a)$ を用いて

$$\overline{P}\sigma(a)-Pa=(P-2)\mathrm{Maxp}(a)-m(P-1). \tag{1}$$

これを m 平行移動した究極の完全数の基本方程式という.
例えば $P=2$ なら

$$\sigma(a)=2a-m.$$

$P=2$ に限って不愉快な $\mathrm{Maxp}(a)$ が消えた.
$P=3$ なら

$$2\sigma(a)=3a+\mathrm{Maxp}(a)-2m.$$

m 平行移動した究極の完全数の基本方程式を解くことは究極の課題である. この解決は一般的にはできるはずがない.

8 φ 完全数

究極の完全数の定義を参考にユークリッド関数の代わりにオイラー関数を使って究極の完全数に類似した概念を定義しよう.

素数 $P, e\geq 2$ に対して $\varphi(P^e)$ は合成数なので完全数の定義をそのままは使えない.

そこで, 1 を加えて $\varphi(P^e)+1$ が素数 q になるとき $a=P^eq$ をもって P を底とする φ **完全数**と定義する.

φ 完全数は次の方程式を持つ:

$$P\varphi(a)=\overline{P}a-P\overline{\mathrm{Maxp}(a)}.$$

これはとくに微小解 $(a=Pq, P>q: q:$ 素数$)$ をもち, 微小解は φ **完全数**ではない.

$P=2$ の場合は微小解がない. この場合 φ 完全数の方程式を満たす解は φ 完全数に限ることが示される.

$P\geq 3$ の場合は φ 完全数の方程式を満たす解は微小解または φ 完全数に限ることが示される.

9 P を底とする φ 完全数の例

$P=2$ なら $q=2^{e-1}+1$ が素数の場合なので, これらはフェルマー素数である.

9.1 2 を底とするとき

表 1: 2 を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	12	2^2*3	4
3	40	2^3*5	16
5	544	2^5*17	256
9	131584	2^9*257	65536
17	8590065664	$2^{17}*65537$	4294967296

$e>4$ なら $q\equiv 7; a\equiv 4$; $\varphi(a)\equiv 6 \bmod 10$ が成り立つ.

5 つのフェルマー素数に応じて 5 つの φ 完全数ができた. これらはフェルマー φ 完全数 と呼ぶこともできる. 後で本物の φ 完全数がでてくる.

9.2 3 を底とするとき

$$q=2*3^{e-1}+1, a=3^e q.$$

表 2: 3 を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	63	3^2*7	36
3	513	3^3*19	324
5	39609	3^5*163	26244
6	355023	3^6*487	236196
7	3190833	3^7*1459	2125764
10	2324581983	$3^{10}*39367$	1549681956
17	11118121262251209	$3^{17}*86093443$	7412080755407364
18	100063090585419903	$3^{18}*258280327$	66708726798666276

- $e\equiv 2 \bmod 4$ のとき $q\equiv 7, a\equiv 3 \bmod 10$.

- $e \equiv 1 \bmod 4$ のとき $q \equiv 3, a \equiv 9 \bmod 10$.
- $e \equiv 3 \bmod 4$ のとき $q \equiv 9, a \equiv 3 \bmod 10$.

10 φ 完全数の平行移動

m だけ平行移動した φ 完全数の定義は次の通り.

$\varphi(P^e)+1+m$ が素数 q になるとき $a = P^e q$ を (P を底とする) m だけ平行移動した φ 完全数の定義とする.

特にこれを満たす a を (φ, m) 完全数とも言う.

10.1 $[P = 2, m = 2]$

表 3: $P = 2, m = 2$

$e \bmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	20	$2^2 * 5$	8
3	3	56	$2^3 * 7$	24
0	4	176	$2^4 * 11$	80
1	5	608	$2^5 * 19$	288
3	7	8576	$2^7 * 67$	4224
0	8	33536	$2^8 * 131$	16640
1	13	33579008	$2^{13} * 4099$	16785408
0	16	2147680256	$2^{16} * 32771$	1073807360
1	17	8590327808	$2^{17} * 65539$	−−
3	19	137440526336	$2^{19} * 262147$	−−
1	29	144115189686468608	$2^{29} * 268435459$	−−

$q = 2^{e-1} + 3$ が素数の場合である.

$e > 2$ のとき a の末尾 1 桁が 6,8 になっている.

11 φ 完全数の平行移動の方程式

$q=\varphi(P^e)+1+m$ が素数になるとき $a=P^eq$ とすると,

$$\begin{aligned}\varphi(a)=\varphi(P^eq)&=P^{e-1}\overline{P}\overline{q}\\&=P^e\overline{P}(q-1)/P\\&=P^eq\overline{P}/P-P^{e-1}\overline{P}\\&=\overline{P}a/P-(q-1-m).\end{aligned}$$

かくして $\mathrm{Maxp}(a)=q$ に注意し

$$\varphi(a)=\frac{\overline{P}}{P}a-\overline{\mathrm{Maxp}(a)}+m. \tag{2}$$

が得られた. 分母を払った次の式もよく使われる.

$$P\varphi(a)=\overline{P}a-P\overline{\mathrm{Maxp}(a)}+Pm. \tag{3}$$

が得られた.

これが m だけ平行移動した φ 完全数の方程式 $(*)$ である.

φ 完全数の方程式 $(*)$ で定義された数は必ずしも φ 完全数になるわけではない.

φ 完全数においては $q=\varphi(p^e)+1+m$ が素数になると仮定されているので $1+m$ は p で割れない.

φ 完全数の方程式 $(*)$ 自身を扱うとき $1+m$ は p で割れない, などのことにこだわらない. 実際に $m=p-1$ の場合が重要な結果を与えるのである.

11.1 微小解

$m=0$ のとき $p=Maxp(a)$ とおくと $a=Pq(P>q)$ は

$$\varphi(a)=\frac{\overline{P}a}{P}-\overline{\mathrm{Maxp}(a)}$$

の解になることは一般的に証明できる.

実際, $\varphi(a)=\overline{P}\overline{q}$, $\mathrm{Maxp}(a)=P$ によって

$$\frac{\overline{P}a}{P}-\overline{\mathrm{Maxp}(a)}=\overline{P}q-\overline{P}=\overline{P}\overline{q}=\varphi(a).$$

よって $\varphi(a)=\frac{\overline{P}a}{P}-\overline{\mathrm{Maxp}(a)}$.

$m=0$ のときの解 $a=Pq(P>q)$ を微小解という. 微小解は φ 完全数の方程式 $(*)$ に特有の解である.

12 定理と証明

次の補題に注目する.

補題 1 $a > 1$ が素数でないとき

$$a - \varphi(a) \geq Maxp(a)$$

Proof. $a = P^e, (e > 1)$ のとき $\mathrm{Maxp}(a) = P$ なので
$a - \varphi(a) - P = P^{e-1} - P \geq 0$ となり正しい.

$s(a) \geq 2$ なら $\mathrm{Maxp}(a) = P$ とすれば $a = \alpha P^e (e > 0, \mathrm{Maxp}(\alpha)) < P)$ と書けて

$$\begin{aligned} a - \varphi(a) &= \alpha P^e - \varphi(\alpha) P^{e-1} \overline{P} \\ &= P^{e-1}(\alpha P - \varphi(\alpha)\overline{P}) \\ &= P^{e-1}(\alpha P - \varphi(\alpha)P + \varphi(\alpha)) \\ &= P^{e-1}((\alpha - \varphi(\alpha))P + \varphi(\alpha)) \\ &> P^{e-1}(P + \varphi(\alpha)) \\ &> P^e \\ &\geq \mathrm{Maxp}(a). \end{aligned}$$

定理 1 $m \geq 0$ のとき

$$P\varphi(a) = \overline{P}a + Pm - P\overline{Maxp(a)}$$

を満たす解は

1. $m = 0$ のとき微小解 $a = Pq(P > q)$.
2. $m = P - 1$ のとの微小解 $a = P^e$.
3. $e > 1$ のとき a は $(\varphi, m)-$ 完全数
4. $e = 1$ のとき $a = Pq$, $q = P + m$ は素数.

Proof.
a は定義式より P の倍数なので $a = P^e L$ $(P, L$ は互いに素$)$ と書ける. よって次式を満たす:

$$P\varphi(a) = P^e \overline{P}\varphi(L), \overline{P}a = P^e \overline{P} L.$$

(i) $L = 1$ のとき $a = P^e$, $P\varphi(a) = P^e\overline{P} = \overline{P}a, \mathrm{Maxp}(a) = P$ なので

$$P\varphi(a) = P^e\overline{P}, \overline{P}a + Pm - P\overline{\mathrm{Maxp}(a)} = \overline{P}P^e + Pm - P\overline{P}$$

により $Pm - P\overline{P} = 0$. P で除して,$m = P - 1, a = P^e$.

(ii) $L \geq 2$ のとき $a = P^e L$.
$P\varphi(a) = P^e\overline{P}\varphi(L), \overline{P}a = P^e\overline{P}L$ なので

$$P\varphi(a) - \overline{P}a = P^e\overline{P}(L - \varphi(L)) = Pm - P\overline{\mathrm{Maxp}(a)}.$$

P で除して

$$\overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P}(L - \varphi(L)) + m.$$

(1) L が素数でないとき.
$L - \varphi(L) \geq \mathrm{Maxp}(L)$ を用いて

$$\overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P}(L - \varphi(L)) + m \geq P^{e-1}\overline{P}(\mathrm{Maxp}(L)).$$

(a) $P > \mathrm{Maxp}(L)$ の場合,$\mathrm{Maxp}(a) = P, \mathrm{Maxp}(L) \geq 2$.

$$\overline{P} = P - 1 = \overline{\mathrm{Maxp}(a)} \geq P^{e-1}\overline{P}(\mathrm{Maxp}(L)) \geq 2\overline{P}.$$

(b) $P < \mathrm{Maxp}(L)$ の場合,$\mathrm{Maxp}(a) = \mathrm{Maxp}(L) \geq 2$.

$$\overline{\mathrm{Maxp}(L)} = \overline{\mathrm{Maxp}(a)} \geq P^{e-1}\overline{P}(\mathrm{Maxp}(L)) \geq \mathrm{Maxp}(L).$$

かくて矛盾.
(2) L が素数 q のとき.

$$\overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P}(L - \varphi(L)) + m = P^{e-1}\overline{P}(q - \varphi(q)) + m \geq P^{e-1}\overline{P}.$$

$a = P^e q$ なので $\mathrm{Maxp}(a) = P$ または $\mathrm{Maxp}(a) = \mathrm{Maxp}(q) = q$.

(a) $\mathrm{Maxp}(a) = P$ とすると,

$$\overline{P} = \overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P} + m.$$

これより, $e = 1, m = 0, P > q$. $a = Pq$ は微小解.

(b) $\mathrm{Maxp}(a) = q$ とすると,

$$\overline{q} = \overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P} + m.$$

これより, $q = P^{e-1}\overline{P} + 1 + m$. $e > 1$ のとき a は $(\varphi, m)-$ 完全数.
$e = 1$ のとき $q = P + m, a = Pq$.

m 平行移動した究極の完全数の基本方程式を解くことはできるはずがない.

しかし,φ 完全数の場合 $m \geq 0$ のとき

$$P\varphi(a) = \overline{P}a + Pm - P\overline{\mathrm{Maxp}(a)}$$

を満たす解は完全に決定できた. これはひとつの奇跡であろう.