

書泉グランデでの講義
高校生も十分わかる新しい数論研究
New Series, 第 1 期 資料 1
2015 年 10 月 9 日

飯高 茂

平成 28 年 1 月 22 日

*New series をはじめるにあたって

書泉グランデでの講義

「高校生も十分わかる新しい数論研究」 ニューシリーズ 2015 年 10 月 9,23 日
11 月 13,27 日 (計 4 回) 時間 6:30-8:30

場所 神田 書泉グランデ 7 階

「高校生も十分わかる新しい数論研究」という題のもとで一般市民向けの数学研究中心の連続講座を行うとにし実際 2014 年に 4 回 2015 年 2,3 月に 4 回 6,7 月に 4 回 の講義をした。

高校生も十分わかる, という題で始めたが始めは高校生の参加は無かった。しかし小学 1 年生の参加があり、熱心に休み無く参加してくれた。また高校生も参加するようになった。

講義内容は古典的な完全数を底を一般の素数にして一般化をし究極の完全数と呼びこれを研究することを中心にした。これらに対しフェルマ, オイラー, ラグランジュの理論を一般化し、また Wieferich 素数の理論も一般化された。

これらは新しい研究内容なので参加者に過度の負担を与えることもあった。今回からはニューシリーズとしてリニューアルして始めることにした。今までの講義内容を既知とした取り扱いをせず、詳しい説明をつけて新しい参加者にも十分理解できるよう配慮することにした。

内容: フェルマー数を一般化しフェルマー弱完全数の概念を導入しこれについての研究から始める。

飯高 茂 2015 年 10 月

1 オイラー関数の歴史

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 $\varphi(n)$ を用いたことはない. この記号は 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

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

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

たとえば $n = 6, p = 2$ のとき $\Sigma_n(2) = 2\{1, 2, 3\} = \{2, 4, 6\}$.

2.1 オイラー関数

$W_n = \Sigma_n - \cup_{j=1}^s \Sigma_n(p_j)$ 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.

Σ_n の集合 T についてその元の個数を $|T|$ で示すと $|\Sigma_n(p_j)| = \frac{n}{p_j}, |\Sigma_n(p_j p_k)| =$

$\frac{n}{p_j p_k}, \dots$ が成り立つ.

2.2 包含関係の公式

一般に集合 Σ_n の部分集合 A_1, A_2, \dots, A_s について

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

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

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

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, Σ_n の部分集合 T についてその元の和を $|T|_1$ で示すと

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

2項展開を用いて $0 = (1-1)^s = 1 - s + s(s-1)/2 - s(s-1)(s-2)/6 + \cdots$ に注意すると

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

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

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

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

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

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

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

2.6 n の根基

n の根基 $\text{rad}(n) = p_1 p_2 \cdots p_s$ を用いると、

$$\frac{B}{\text{rad}(n)} = (-1)^s A = \frac{\varphi(n)}{n} \text{ が成り立つ.}$$

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

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

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

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。

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

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

$$|\Sigma_n|_3 = \frac{n^2(n^2 + 2n + 1)}{4} \text{ が成り立ち } |\Sigma_n(p_j)|_3 = \frac{n^2}{4}(2n + \frac{n^2}{p_j} + p_j).$$

$$\begin{aligned} \psi^{(3)}(n) &= |\Sigma_n - \cup_{j=1}^s \Sigma_n(p_j)|_3 \\ &= |\Sigma_n|_3 - |\cup_{j=1}^s \Sigma_n(p_j)|_3 \\ &= \frac{n^2}{4}(n^2 A + B). \\ &= \frac{n\varphi(n)}{4}(n^2 + (-1)^s \text{rad}(n)). \end{aligned}$$

よって

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

2.8 4乗和

次に4乗和を考える. $a < n$ かつ n と互いに素な a の4乗和を $\psi^{(4)}(n)$ と書く. 一般に集合 T についてその元の4乗和を $|T|_4$ で示すと

$$|\Sigma_n|_4 = \frac{n}{30}(15n^3 + 6n^4 + 10n^2 - 1), |\Sigma_n(p_j)|_4 = \frac{n}{30}(15n^2 + \frac{6n^4}{p_j} + 10n^2 p_j - p_j^3)$$

さらに $\Gamma_3(n) = (1 - p_1^3)(1 - p_2^3) \cdots (1 - p_s^3)$ を用いると

$$\begin{aligned} \psi^{(4)}(n) &= |\Sigma_n - \cup_{j=1}^s \Sigma_n(p_j)|_4 \\ &= |\Sigma_n|_4 - |\cup_{j=1}^s \Sigma_n(p_j)|_4 \\ &= \frac{n}{30}(6n^4 A + 10n^2 B - \Gamma_3(n)) \\ &= \frac{n}{30}(6n^3 \varphi(n) + 10n(-1)^s \text{rad}(n)\varphi(n) - \Gamma_3(n)). \end{aligned}$$

かくて次の結果に至る.

$$\psi^{(4)}(n) = \frac{n}{30}(6n^3\varphi(n) + 10n(-1)^s \text{rad}(n)\varphi(n) - \Gamma_3(n))$$

2.9 5乗和

次に5乗和を考える. $a < n$ かつ n と互いに素な a の5乗和を $\psi^{(5)}(n)$ と書く. 集合 T についてその元の5乗和を $|T|_5$ で示すと

$$|\Sigma_n|_5 = \frac{n^2}{12}(2n^4 + 6n^3 + 5n^2 - 1), |\Sigma_n(p_j)|_5 = \frac{n^2}{12}\left(6n^3 + \frac{2n^4}{p_j} + 5n^2p_j - p_j^3\right)$$

$$\begin{aligned} \psi^{(5)}(n) &= |\Sigma_n - \cup_{j=1}^s \Sigma_n(p_j)|_5 \\ &= |\Sigma_n|_5 - |\cup_{j=1}^s \Sigma_n(p_j)|_5 \\ &= \frac{n^2}{12}(2n^4 A + 5n^2 B - \Gamma_3(n)) \\ &= \frac{n^2}{12}(2n^3\varphi(n) + 5n(-1)^s \text{rad}(n)\varphi(n) - \Gamma_3(n)). \end{aligned}$$

こうして次の結果が出る.

$$\psi^{(5)}(n) = \frac{n^2}{12}(2n^3\varphi(n) + 5n(-1)^s \text{rad}(n)\varphi(n) - \Gamma_3(n))$$

$n = 3$ として検算しよう.

$$\psi^{(5)}(3) = 1 + 2^5 = 33.$$

一方 $2n^3\varphi(n) + 5n(-1)^s \text{rad}(n)\varphi(n) - \Gamma_3(n) = 2 * 3^3 * 2 - 15 * 3 * 2 + 26 = 108 + 26 - 90 = 44$. そして, $44 * 9/12 = 33$.

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だけ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. ここではベルヌーイ数が出てくる.

2.10 m 乗和の公式

集合 $\Sigma_n = \{1, 2, \dots, n\}$ について, Σ_n の集合 T についてその元の m 乗和を $|T|_m$ で示す.

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

とおく.

$S_m(n)$ の公式はベルヌーイ数 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.

$\frac{t}{e^t - 1}$ のテーラー展開の係数としてベルヌーイ数 B_k が定義される.

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

これは指数型母関数の応用である.

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.

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

$k > 1$, 奇数なら $B_k = 0$.

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

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

偶数項の分子の性質がとりわけ興味深い. $k = 12$ のときの分子 691 は素数. 分子に素数の多いことは注目に値する.

3.1 B_k の諸性質

漸化式

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

ベルヌーイ多項式

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

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

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

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

$n = 1$ とすると $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{6}{\pi^2}$ (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.
 $a_k = (-1)^k \binom{m+1}{k} B_k$ を使うと

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

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

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

$F(t)$ が偶関数になるので $a_{2k+1} = 0$.

$$a_0 = 1, a_1 = \frac{m+1}{2}, a_2 = \frac{m(m+1)}{12}, a_3 = 0, a_4 = -\frac{(m+1)m(m-1)(m-2)}{24 \times 30},$$

4 べき乗和の公式

m 乗和 $S_m(n) = |\Sigma_n|_m = \sum_{k=1}^n k^m$ は n について $m+1$ 次式であり $a_k = (-1)^k \binom{m+1}{k} B_k$ を使うと次の公式が成り立つ.

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

はじめの数項は次のようになる.

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

$m=3$ 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 べき乗和公式の証明

以下英語版 Wikipedia を参考にその証明を与える.
 $\{B_j\}$ 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

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

和の順序を入れ替えて

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

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

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

ここで $m = q + j - 1$ とおくと $j = m + 1 - q \leq m$ により $m \geq j$.

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

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

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

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

$$S_m(n) = \frac{n}{m+1} \sum_{j=1}^m a_j n^{m-j}$$

5 $\psi^{(m)}(n)$ の公式

n の素因子 $p = p_j$ について

$$\left| p \Sigma_n \left(\frac{n}{p} \right) \right|_m = \frac{n}{m+1} \sum_{k=0}^m a_k n^{m-k} p^{k-1}$$

これを展開すると $a_3 = 0$ によって

$$\frac{n}{m+1} \left(\frac{n^m}{p} + a_1 n^{m-1} + p a_2 n^{m-2} + p^3 a_4 n^{m-4} \right) + \dots$$

n の素因子 $p = p_j, q = p_L$ について

$$\left| pq \Sigma_n \left(\frac{n}{pq} \right) \right|_m = \frac{n}{m+1} \sum_{k=0}^m a_k n^{m-k} p^{k-1} q^{k-1}$$

$n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ について $\Gamma(r, n) = \prod_{j=1}^s (1 - p_j^r)$ とおく.

強いて言えば, $\Gamma(-1, n) = \prod_{j=1}^s (1 - 1/p_j) = A, \Gamma(1, n) = B.$

$a < n$ かつ n と互いに素な a の m 乗和を $\psi^{(m)}(n)$ と書く. これを総称して高次オイラー関数という.

$$\begin{aligned}
\psi^{(m)}(n) &= |\Sigma_n - \cup_{j=1}^s \Sigma_n(p_j)|_m \\
&= |\Sigma_n|_m - |\cup_{j=1}^s \Sigma_n(p_j)|_m \\
&= S_m(n) - \sum_{j=1}^s |\Sigma_n(p_j)|_m + \sum_{j < L}^s |\Sigma_n(p_j p_L)|_m + \dots \\
&= \frac{n}{m+1} \left(\sum_{k=0}^m a_k n^{m-k} - \sum_{j=1}^s \left(\sum_{k=0}^m a_k n^{m-k} p_j^{k-1} \right) - \sum_{j < L}^s \sum_{k=0}^m a_k n^{m-k} p_j^{k-1} p_L^{k-1} + \dots \right) \\
&= \frac{n}{m+1} (An^m + a_2 Bn^{m-2} + a_4 \Gamma(3, n)n^{m-4} + a_6 \Gamma(5, n)n^{m-6} + \dots)
\end{aligned}$$

$$\psi^{(m)}(n) = \frac{n}{m+1} (An^m + a_2 Bn^{m-2} + a_4 \Gamma(3, n)n^{m-4} + a_6 \Gamma(5, n)n^{m-6} + \dots).$$

$m = 5$ として検算

$$a_2 = \frac{m(m+1)}{12} = \frac{5}{2}, a_4 = -\frac{m(m+1)(m-1)(m-2)}{30} = -\frac{1}{2} \text{ により}$$

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

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

$m = 6$ とすると新しい公式をえる.

$$a_2 = \frac{m(m+1)}{12} = \frac{5}{2}, a_4 = -\frac{m(m+1)(m-1)(m-2)}{30} = -\frac{1}{2} \text{ により}$$

6 $\psi(n)$ の乗法性の問題

n, m が互いに素なら

$$\varphi(nm) = \varphi(n)\varphi(m)$$

が成立しこれを $\varphi(n)$ の乗法性という.

乗法性は $\psi(n)$ などでは成り立たない.

一般に関数 $F(n)$ が乗法性を持たないとする. 自然数 n の素因数分解

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

を利用して

$$\tilde{F}(n) = F(p_1^{e_1})F(p_2^{e_2}) \cdots F(p_s^{e_s})$$

とおくとこれは乗法性を持つ.

$$F(n) = \psi(n) \text{ のとき } n = p^e \text{ ならば } \psi(n) = \frac{1}{2}p^{2e-1}\bar{p} \text{ なので, 結局}$$

$$\tilde{F}(n) = \frac{n\varphi(n)}{2^s}$$

ここで, s は n の相異なる素因子の個数を示す.

$\tilde{F}(n)$ は単に n 倍なのでこれで割って新しい関数 $\tilde{\varphi}(n) = \frac{\varphi(n)}{2^s}$ を導入しこれをオイラー関数の陪関数 (associated function) という.

ごく簡単な場合の値を計算してみよう:

$$\tilde{\varphi}(2) = \frac{1}{2}, \tilde{\varphi}(3) = 1, \tilde{\varphi}(4) = 1, \tilde{\varphi}(5) = 2, \tilde{\varphi}(6) = \frac{1}{2}$$

陪関数の値は分母が2べきの有理数になる.

7 完全数

a を自然数とするときその約数¹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.

$a = 2^e q (q = 2^{e+1} - 1 : \text{素数})$ 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.

7.1 オイラーによる証明

偶数の完全数はユークリッドの完全数に限ることはオイラーがはじめて証明した. 没後に公表された彼の証明をリライトすると次のとおり.

¹1, a も約数

a を偶数の完全数とし, $a = 2^e L (L : \text{奇数})$ の形に書く.

$$\sigma(a) = \sigma(2^e)\sigma(L) = (2^{e+1} - 1)\sigma(L), 2 \times a = 2^e L = 2^{e+1}L$$

となるので

$$(2^{e+1} - 1)\sigma(L) = 2^{e+1}L \text{ により}$$

$$\frac{2^{e+1} - 1}{2^{e+1}} = \frac{L}{\sigma(L)}.$$

左辺は既約分数だから $L = c(2^{e+1} - 1), \sigma(L) = 2^{e+1}c$ を満たす自然数 c がある.

- 1). $c = L$ なら $2^{e+1} - 1 = 1$ になり $e = 0$. a は奇数となり仮定に反する.
- 2). $c = 1$ なら $\sigma(L) = L + 1$ になるので L は素数.
- 3). $c > 1$ なら c は $1, L$ 以外の L の約数である. $\sigma(L) \geq 1 + L + c$ を満たすから

$$2^{e+1}c = \sigma(L) \geq 1 + L + c = 1 + c(2^{e+1} - 1) + c = 1 + 2^{e+1}c$$

となって矛盾.

証明のキーは 2). で使われた $\sigma(L) = L + 1$ は L が素数 となる必要十分条件になることである.

7.2 $2p$ の特徴づけ

$a = 2p, p \neq 2$ のとき関数 $\sigma(a)$ の乗法性を用いて

$$\sigma(a) = \sigma(2p) = \sigma(2)\sigma(p) = 3(p + 1) = 3\left(\frac{a}{2} + 1\right)$$

となるので整理すると

$$2\sigma(a) = 3(a + 2).$$

$a = 2p$ のときにあった p がうまく消えている.

そこでこの逆問題を考える. すなわちこの式を a についての方程式と考えこれを満たす解 a をすべて求めよう.

方程式の解 a としては $2p$ がある. これらに限るか? という問題を考える.

式から a は偶数になることがわかる. これは大きなアドバンテージである.

それゆえ $a = 2^e L (L : \text{奇数})$ と書けるのでこれを代入する.

$$2\sigma(a) = 2(2^{e+1} - 1)\sigma(L) = 3(a + 2) = 3(2^e L) + 6.$$

ゆえに

$$2(2^{e+1} - 1)\sigma(L) = 3(2^e L) + 6.$$

2で除して

$$(2^{e+1} - 1)\sigma(L) = 3(2^{e-1}L) + 3.$$

$L = 1$ のとき.

$$2^{e+1} - 1 = 3 \cdot 2^{e-1} + 3.$$

よって $2^{e-1} = 3 + 1 = 4$. ゆえに $e = 3; a = 8$.

$L > 1$ のとき. $\sigma(L) \geq L + 1$ を用いて

$$3(2^{e-1}L) + 3 = (2^{e+1} - 1)\sigma(L) \geq (2^{e+1} - 1)(L + 1).$$

右辺は

$$(2^{e+1} - 1)(L + 1) = (4 \cdot 2^{e-1} - 1)L + 4 \cdot 2^{e-1} - 1.$$

これより

$$3(2^{e-1}L) + 3 \geq (4 \cdot 2^{e-1} - 1)L + 4 \cdot 2^{e-1} - 1.$$

ゆえに

$$-4(2^{e-1} - 1) \geq (2^{e-1} - 1)L.$$

$e = 1$ とすると $0 = 0$ となって上の式は成り立つ. そこで前の式に戻り,

$$(4 - 1)\sigma(L) = 3L + 3.$$

3で割ったら $\sigma(L) = L + 1$. よって L は素数 p . ゆえに $a = 2p$.

$e > 1$ とすると $2^{e-1} - 1 > 0$ なのでこれで割ると $-4 \geq L$ となり大なる矛盾.

以上によって, 方程式の解は $a = 2p$ (通常解という) のほかに $a = 8$ があることがわかった.

通常解 $2p$ 以外の解 $8 = 2 \times 4$ の形を見ると, 4 が「ボクも素数に入れて」と叫んでいるようである. そこで 4 を擬素数とみて $a = 2 \times 4$ を擬素数解という.

できしてみると証明はやさしいがオイラーの証明と似ているところがカワイイ.

7.3 $a = P^\varepsilon p$ の特徴づけ

素数 P の累乗 P^ε をとる. $p \neq P$ を満たす素数 p をとり $a = P^\varepsilon p$ とおく.

$$\sigma(a) = \sigma(P^\varepsilon p) = \sigma(P^\varepsilon)\sigma(p) = \frac{P^{\varepsilon+1} - 1}{\bar{P}}(p + 1)$$

となる (ここで $\bar{P} = P - 1$ とおいた). 分母を払ってから, P^ε を乗ずると

$$\begin{aligned}\bar{P}P^\varepsilon\sigma(a) &= (P^{\varepsilon+1} - 1)(a + P^\varepsilon) \\ &= a(P^{\varepsilon+1} - 1) + \delta.\end{aligned}$$

ここで $\delta = P^\varepsilon(P^{\varepsilon+1} - 1)$ とおく. すなわち

$$\bar{P}P^\varepsilon\sigma(a) = a(P^{\varepsilon+1} - 1) + \delta$$

が基本方程式である.

この解は擬素数解 $a = P^{2\varepsilon+1}$ と通常解 $a = P^\varepsilon p$ ($p \neq P$ となる素数) となることが証明できる.

係数 m として, 素数 P の累乗 P^ε をとる. $p \neq P$ を満たす素数 p をとり $a = P^\varepsilon p$ とおく.

$$\sigma(a) = \sigma(P^\varepsilon p) = \sigma(P^\varepsilon)\sigma(p) = \frac{P^{\varepsilon+1} - 1}{\bar{P}}(p + 1)$$

となる. 分母を払ってから, P^ε を乗ずると

$$\begin{aligned}\bar{P}P^\varepsilon\sigma(a) &= (P^{\varepsilon+1} - 1)(a + P^\varepsilon) \\ &= a(P^{\varepsilon+1} - 1) + \delta.\end{aligned}$$

ここで $\delta = P^\varepsilon(P^{\varepsilon+1} - 1)$ とおいた. すなわち

$$\bar{P}P^\varepsilon\sigma(a) = a(P^{\varepsilon+1} - 1) + \delta$$

が基本方程式である.

7.4 方程式を解く

この逆, すなわちこれを満たす解 a を決定しよう.

P を法として考えると $a \equiv 0 \pmod{P}$ がただちにわかる.

$a = P^e L$ とかける. ここで L は P の倍数ではない.

$$\sigma(a) = \frac{P^{e+1} - 1}{P} \sigma(L) \text{ により}$$

基本式

$$P^\varepsilon(P^{e+1} - 1)\sigma(L) = P^e(P^{e+1} - 1)L + \delta$$

をえる.

$L = 1$ のとき

$P^\varepsilon(P^{e+1} - 1) = P^e(P^{e+1} - 1) + \delta$ になり, 整理すると $P^e = P^{2\varepsilon+1}$
これより $e = 2\varepsilon + 1$. すなわち, $a = P^{2\varepsilon+1}$ となり擬素数解になる.

$L > 1$ のとき $\sigma(L) \geq L + 1$ を満たすので

$$P^\varepsilon(P^{e+1} - 1)L + \delta \geq P^\varepsilon(P^{e+1} - 1)(L + 1).$$

これを整理すると

$$L(P^\varepsilon - P^e) \geq \delta_1 - \delta.$$

ここで $\delta_1 = P^\varepsilon(P^{e+1} - 1)$ とおいた.

$\delta_1 - \delta = P^\varepsilon(P^{e+1} - P^{e+1})$ により

$$L(P^\varepsilon - P^e) \geq P^\varepsilon(P^{e+1} - P^{e+1}).$$

$e > \varepsilon$ なら左辺: $L(P^\varepsilon - P^e) < 0$. しかし右辺 $P^\varepsilon(P^{e+1} - P^{e+1}) > 0$ なので
あっさり矛盾.

$e = \varepsilon$ なら

$$P^\varepsilon(P^{e+1} - 1)\sigma(L) = P^e(P^{e+1} - 1)L + \delta$$

において 左辺: $P^\varepsilon(P^{e+1} - 1)\sigma(L) = \delta\sigma(L)$ 右辺 $P^e(P^{e+1} - 1)L + \delta = \delta L + \delta$.

よって $\delta\sigma(L) = \delta L + \delta$. δ を払うと $\sigma(L) = L + 1$. すなわち L は素数. したがって $p = L$ とおけば $a = P^\varepsilon p$ となりこれを通常解という.

$e < \varepsilon$ なら基本式

$$P^\varepsilon(P^{e+1} - 1)\sigma(L) = P^e(P^{e+1} - 1)L + \delta$$

を P^e で式を除して

$$P^{\varepsilon-e}(P^{e+1} - 1)\sigma(L) = (P^{e+1} - 1)L + \delta P^{-e}.$$

$\delta P^{-e} = P^{\varepsilon-e}(P^{e+1} - 1)$ は P の倍数なのでこれらを P を法としてみれば $L \equiv 0 \pmod{P}$.

これは L と P が互いに素であることに矛盾.

7.5 $a = 6p$ の特徴づけ

素因子が 1 個の場合には方程式の解の完全解決ができた. 次に簡単な素因子が 2 個, とくに $a = 6p$ の場合を考える. $p \neq 2, 3$ と仮定する. 6 はいわゆる完全数である.

$\sigma(a) = \sigma(6)\sigma(p) = 12(p+1) = 2a + 12$ により $\sigma(a) = 2a + 12$ ができる.

そこで方程式 $\sigma(a) = 2a + 12$ の解をすべて求めたい.

この式を使うだけでは a が偶数とは言えない. 奇数完全数は存在するか? という 2000 年来の懸案より難しそうである.

解をコンピュータで探索すると

通常解 $a = 6p$ ($p \neq 2, 3$: 素数) と擬素数解 $a = 6 * 2^2, 6 * 3^3$ の他にわけのわからない解が出てきた. このような解をエイリアン解と呼ぶ.

表 1: $\sigma(a) = 2a + 12$ のエイリアン解

a	素因数分解
304	$2^4 * 19$
127744	$2^8 * 499$

エイリアン解は 2 個しか出てこなかったが $2^e p$, ($p = 2^{e+1} - 13$: 素数) の形をしている. そこでその形に拘ってエイリアン解を探す

表 2: $q = 2^{e+1} - 13$

e	$q = 2^e - 13$
12	8179
16	131059
56	144115188075855859

エイリアン解は末尾が 9. また指数 e 4 の倍数である.

これらはユークリッド完全数を -12 だけ平行移動した形をしている.

エイリアン解は完全数の場合のように、無数にあるに違いない。完全数は無限にあるという予想は、完全なるものが無数にあるという意味で美しい。数学のコンテキストにおいてこれらのエイリアン解は無数にあるという予想は実に恐ろしい。

表 3: $q = 2^{e+1} - 13; e = 4m$

e	$q = 2^{e+1} - 13; e = 4m$ 素因数分解
4	(19)=19
8	(499)=499
12	(8179)=8179
16	(131059)=131059
20	(2097139)=11*190649
24	(33554419)=197*170327
28	(536870899)=23*23342213
32	(8589934579)=1237*1549*4483
36	(137438953459)=5507*24957137
40	(2199023255539)=11*19*10521642371
44	(35184372088819)=59*596345289641
48	(562949953421299)=229*919*17729*150881
52	(9007199254740979)=149*60451001709671
56	(144115188075855859)=144115188075855859

7.6 $s(a) = 2$ のときの証明

$\sigma(a) = 2a + 12$ の解 a をすべて求めたいがこれは難しい. 2300 年かかっても解けない完全数の問題よりさらに難しい. ここでは, $s(a) = 2$ すなわち 解 a が 2 個の素因子 p, q を持つ場合に証明を行う.

$a = p^e q^f (p < q)$ となる解を求める. $X = p^e, Y = q^f$ とおけば

$$a = XY, \sigma(a) = \frac{(pX - 1)(qY - 1)}{\rho'}$$

と書ける. ここで $\rho' = \bar{p}\bar{q}; \bar{p} = p - 1, \bar{q} = q - 1$ とおいた.

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\rho'}, 2a + 12 = 2XY + 12 \text{ を用いて}$$

$$(pX - 1)(qY - 1) = 2\rho'(XY + 6).$$

さてここからは $p = 2$ を仮定する.

$A = 2X - 1, B = qY - 1$ とおくことにより

$$AB = 2\rho'(XY + 6), AB = 2qXY - (2X + qY) + 1.$$

$2q - 2\bar{q} = 2$ なので次の基本式をえる:

$$2XY = 12\bar{q} + 2X + qY - 1.$$

$Y(2X - q) = 12\bar{q} + 2X - 1 > 0$ によれば $2X \geq q + 1$.

$Y = q^f \geq q$ により次の場合わけを行う.

1) $Y \geq q^2$.

$$12\bar{q} + 2X - 1 = Y(2X - q) \geq q^2(2X - q).$$

$q^2(2X - q) = 2Xq^2 - q^3$ を移項して

$$12\bar{q} + q^3 - 1 \geq 2X(q^2 - 1) = 2X\bar{q}\tilde{q}.$$

ここで $\tilde{q} = q + 1$ とおいた. さらに $q^3 - 1 = \bar{q}(q^2 + q + 1)$ によって, 上の不等式から

$$q^2 + q + 1 + 12 \geq 2X\tilde{q}.$$

$q^2 + q + 1 + 12 \geq 2X\tilde{q} \geq (q + 1)\tilde{q} = q^2 + 2q + 1$ によって

$12 \geq q$. q は奇素数なので $q = 11, 7, 5, 3$.

$q^2 + q + 1 + 12 \geq 2X\tilde{q}$ によって

$$X \leq \frac{q^2 + q + 1 + 12}{2\tilde{q}}.$$

(i) $q = 3$.

$$X \leq \frac{q^2 + q + 1 + 12}{2\tilde{q}} = \frac{25}{8} < 3.5 \text{ により } X = 2.$$

$2XY = 12\bar{q} + 2X + qY - 1$ に代入すると $4Y = 12 * 2 + 2 * 2 + 3Y - 1 = 27 - 3Y$ を得るので

$Y = 27, Y = 3^f$ により $f = 3, a = 2 * 3^3$. これは擬素数解.

(ii) $5 \leq q \leq 11$

$q = 5$ のとき $X \leq \frac{q^2 + q + 1 + 12}{2\tilde{q}} = \frac{43}{12} < 4$. よって $X = 2$. さらに $2X \geq q + 1$ を思い出せば $4 = 2X \geq q + 1 = 6$. 矛盾

$q = 7$ のとき $X \leq \frac{q^2 + q + 1 + 12}{2\tilde{q}} = \frac{69}{16} < 5$. よって $X = 2, 4$. さらに基本式に戻り

$$Y(2X - q) = 12\bar{q} + 2X - 1$$

$X = 4$ なら $Y = 12 * 6 + 2 * X - 1 = 79$. $Y = 7^f$ に反する.

$X = 2$ なら $4 = 2X > q = 7$. 矛盾.

$$q = 11 \text{ のとき } x \leq \frac{q^2 + q + 1 + 12}{2\tilde{q}} = \frac{121}{24} + 1 < 5.2. \text{ よって } X = 2, 4.$$

しかし $2X > q = 11$ に反する.

ii) $Y = q$.

$q(2X - q) = 12\bar{q} + 2X - 1$ によって, $2X = 12 + q + 1$. これより $q = 2^{e+1} - 13$. $e = 3$ とき $q = 3$. ゆえに $a = 2 * 3^3$. これは擬素数解.

$q = 2^{e+1} - 13$ が素数になる場合を探す.

7.7 $a = 28p$ の特徴づけ

第2の完全数 28 が係数の場合を計算する.

表 4: $m = 28$:素数

(a)	素因数分解
(84)	$2^2 * 3 * 7$
(140)	$2^2 * 5 * 7$
(224)	$2^5 * 7 *$
(308)	$2^2 * 7 * 11$
(364)	$2^2 * 7 * 13$
(476)	$2^2 * 7 * 17$
(532)	$2^2 * 7 * 19$
(644)	$2^2 * 7 * 23$
(812)	$2^2 * 7 * 29$
(868)	$2^2 * 7 * 31$
(1036)	$2^2 * 7 * 37$
(1148)	$2^2 * 7 * 41$
(1204)	$2^2 * 7 * 43$
(1316)	$2^2 * 7 * 47$
(1372)	$2^2 * 7^3 *$
(1484)	$2^2 * 7 * 53$
(1652)	$2^2 * 7 * 59$
(1708)	$2^2 * 7 * 61$

表 5: $m = 28: 2 < a < 1,500,000, *$ 擬素数解

(a)	素因数分解
224	$2^5 * 7 *$
1372	$2^2 * 7^3 *$
4544	$2^6 * 71$
9272	$2^3 * 19 * 61$
14552	$2^3 * 17 * 107$
25472	$2^7 * 199$
74992	$2^4 * 43 * 109$
495104	$2^9 * 967$

表 6: $s(a) = 2; a = 2^e q;$:エイリアン解

(a)	素因数分解
4544	$2^6 * 71$
25472	$2^7 * 199$
495104	$2^9 * 967$

表 7: $s(a) = 3, a = 2^e q_1 * q_2;$:エイリアン解

(a)	素因数分解
9272	$2^3 * 19 * 61$
14552	$2^3 * 17 * 107$
74992	$2^4 * 43 * 109$

7.8 $a = 496p$ の特徴づけ

第 3 の完全数 496

表 8: $m = 496::2 < a < 1,500,000,*$ 擬素数解

(a)	素因数分解
2892	$2^2 * 3 * 241$
6104	$2^3 * 7 * 109$
15872	$2^9 * 31 *$
170612	$2^2 * 13 * 17 * 193$
458144	$2^5 * 103 * 139$
476656	$2^4 * 31^3 *$
857312	$2^5 * 73 * 367$
1006496	$2^5 * 71 * 443$

7.9 $a = 8128p$ の特徴づけ

第4の完全数 8128

表 9: $m = 8128:2 < a < 1,500,000$, * 擬素数解

a	素因数分解
48684	$2^2 * 3 * 4057$
112952	$2^3 * 7 * 2017$
353672	$2^3 * 11 * 4019$
396112	$2^4 * 19 * 1303$
1040384	$2^{13} * 127 *$
1243808	$2^5 * 47 * 827$

8 $a = mp$ の特徴づけ

表 10: $a = mp$

a	素因数分解
m= 5 125	5^3
m = 6 24 54 304	$2^3 * 3$ $2 * 3^3$ $2^4 * 19$
m = 7 343	7^3
m = 8 128	2^7
m = 9 243	3^5
m = 10 40 250	$2^3 * 5$ $2 * 5^3$
m = 11 1331	11^3
m = 12 96 108	$2^5 * 3$ $2^2 * 3^3$
m = 13 2197	13^3
m = 14 56 686	$2^3 * 7$ $2 * 7^3$
m = 15 135 375	$3^3 * 5$ $3 * 5^3$
m = 16 512	2^9
m = 17 4913	17^3
m = 18 72 486	$2^3 * 3^2$ $2 * 3^5$
m = 19 6859	19^3

表 11: $a = mp$

a	素因数分解
m = 20	
160	$2^5 * 5$
500	$2^2 * 5^3$
m = 21	
189	$3^3 * 7$
1029	$3 * 7^3$
m = 22	
88	$2^3 * 11$
2662	$2 * 11^3$
m = 23	
12167	23^3
m = 24	
216	$2^3 * 3^3$
384	$2^7 * 3$
m = 25	
3125	5^5
m = 26	
104	$2^3 * 13$
4394	$2 * 13^3$
m = 27	
2187	3^7
m = 28	
224	$2^5 * 7$
1372	$2^2 * 7^3$
4544	$2^6 * 71$
9272	$2^3 * 19 * 61$
14552	$2^3 * 17 * 107$
25472	$2^7 * 199$
m = 29	
24389	29^3
m = 30	
120	$2^3 * 3 * 5$
270	$2 * 3^3 * 5$
750	$2 * 3 * 5^3$
1520	$2^4 * 5 * 19$
m = 31	
29791	31^3

表 12: $a = mp$

a	素因数分解
m = 32	
2048	2^11
m	33
297	$3^3 * 11$
3993	$3 * 11^3$
m = 34	
136	$2^3 * 17$
9826	$2 * 17^3$
m = 35	
875	$5^3 * 7$
1715	$5 * 7^3$
m = 36	
288	$2^5 * 3^2$
972	$2^2 * 3^5$
m = 37	
m = 38	
152	$2^3 * 19$
13718	$2 * 19^3$
m = 39	
351	$3^3 * 13$
6591	$3 * 13^3$
m = 40	
640	$2^7 * 5$
1000	$2^3 * 5^3$

表 13: $2\varphi(a) - a = 1$,

a	素因数分解
3	3
15	$3 * 5$
255	$3 * 5 * 17$
65535	$3 * 5 * 17 * 257$

表 14: $2\varphi(a) - a = 1$,

a	素因数分解
3	3
15	$3 * 5$
255	$3 * 5 * 17$
65535	$3 * 5 * 17 * 257$

表 15: $2\varphi(a) - a = 3$,

a	素因数分解
$w = 2\varphi(a) - a = 3$	
5	5
9	3^2
21	$3 * 7$
45	$3^2 * 5$
285	$3 * 5 * 19$
765	$3^2 * 5 * 17$

表 16: $2\varphi(a) - a = 5$,

a	素因数分解
7	7
75	$3 * 5^2$
1275	$3 * 5^2 * 17$
327675	$3 * 5^2 * 17 * 257$

表 17: $2\varphi(a) - a = 7$,

a	素因数分解
33	$3 * 11$
345	$3 * 5 * 23$
67065	$3 * 5 * 17 * 263$

表 18: $2\varphi(a) - a = -3$,

a	素因数分解
195	$3 * 5 * 13$
5187	$3 * 7 * 13 * 19$

表 19: $2\varphi(a) - a = -5$,

a	素因数分解
165	$3 * 5 * 11$
64005	$3 * 5 * 17 * 251$

表 20: $2\varphi(a) - a = -6$,

a	素因数分解
18	$2 * 3^2$

表 21: $2\varphi(a) - a = -9$,

a	素因数分解
105	$3 * 5 * 7$
585	$3^2 * 5 * 13$
15561	$3^2 * 7 * 13 * 19$

表 22: $2\varphi(a) - a = -10$,

a	素因数分解
50	$2 * 5^2$