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3
2015 年11月13日

飯高 茂

平成 28 年 1 月 20 日

1　オイラー関数のギャップ値

オイラー関数のギャップ値の例を集めた.
$n = 2 * p, 2 * p + 1$: 合成数なら n はギャップ値である.
この他のギャップ値の十分条件を探そう

表 1: オイラー関数のギャップ値

14	[2,7]
26	[2,13]
34	[2,17]
39	[3,13]
50	[2,5^2]
62	[2,31]
68	[2^2,17]
76	[2^2,19]
86	[2,43]
90	[2,3^2,5]
98	[2,7^2]
114	[2,3,19]
118	[2,59]
124	[2^2,31]
134	[2,67]
142	[2,71]
146	[2,73]
154	[2,7,11]
158	[2,79]
170	[2,5,17]
174	[2,3,29]
182	[2,7,13]
188	[2^2,47]
194	[2,97]
202	[2,101]
206	[2,103]

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 $S_n = \{1, 2, \cdots, n\}$ 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

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

2.6 n の根基

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

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

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

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

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

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 $|S_n(p_j)|_3 = \frac{n^2}{4}(2n + \frac{n^2}{p_j} + p_j)$.

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

よって

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

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. 一般に部分集合 T についてその元の 4 乗和を $|T|_4$ で示すと

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

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

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

かくて次の結果に至る.

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

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. 部分集合 T についてその元の 5 乗和を $|T|_5$ で示すと

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

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

こうして次の結果が出る.

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

$n = 3$ として検算しよう.

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

一方 $2n^3\varphi(n) + 5n(-1)^s\mathrm{rad}(n)\varphi(n) - \Gamma_3(n) = 2 * 3^3 * 2 - 15 * 3 * 2 + 26 = 108 + 26 - 90 = 44.$ 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. ここではベルヌーイ数が出てくる.

2.10 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.

$\dfrac{t}{e^t - 1}$ 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 $B_k = 0$.

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

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

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

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,$c_{2k+1} = B_{2k+1}/(2k+1)! = 0$

3.3 m 乗和 の公式

集合 $S = \{1, 2, \cdots, n\}$ とおく. S 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.

4 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.

$\dfrac{t}{e^t - 1}$ 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 $B_k = 0$.

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

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

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.

4.1 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.

4.2 $B_{2k+1} = 0$ 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 $c_{2k+1} = 0$.

5 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

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

5.1 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 $j=m+1-q\le m$ により $m\ge j$.

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.

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

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

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

6 $\psi^{(m)}(n)$ 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

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

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

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

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

$m = 5$ 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

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

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

7　$\psi(n)$ 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

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

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.

$F(n) = \psi(n)$ のとき　$n = p^e$　ならば $\psi(n) = \frac{1}{2}p^{2e-1}\overline{p}$　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.

8　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 (perfect numbers) という. 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.

2 のべきから 1 引いた $Q = 2^{e+1} - 1$ が素数になるとき $a = 2^e Q$ は完全数でありとくにこの形の数をユークリッドの完全数という.

これを確認しよう.

$$\sigma(a) = \sigma(2^e)\sigma(Q) = (2^{e+1} - 1)(Q + 1) = 2a - Q + 2^{e+1} - 1 = 2a$$

素数 $Q = 2^{e+1} - 1$ をメルセンヌの素数という.

一般に $2^{e+1} - 1$ が素数になるとき $e + 1$ は素数になることが証明できる.

$Q = 2^{e+1} - 1$ が素数になるという条件をはずして, $e + 1$ が素数になるという条件のみをつけるとき $a = 2^e Q$ を弱い完全数 (weakly perfect numbers) ということにする.

9 弱完全数

表 2: $P = 2$:弱完全数

p	$Q = 2^p - 1$	素因数分解	a:弱完全数
2	(3)	3	6
3	(7)	7	28
5	(31)	31	496
7	(127)	127	8128
11*	(2047)	23*89	2096128
13	(8191)	8191	33550336
17	(131071)	131071	8589869056
19	(524287)	524287	137438691328
23*	(8388607)	47*178481	35184367894528
29*	(536870911)	233*1103*2089	144115187807420416
31	(2147483647)	2147483647	2305843008139952128

(* は非完全数を示す.)

この表を観察すると $Q \equiv 1$ または 7 $\mod 10$; $a \equiv 6$ または 8 $\mod 10$ をやはり満たしていることがわかる.

詳しく述べると

- $p \equiv 1 \mod 4$ なら $Q \equiv 1 \mod 10$, $a \equiv 6 \mod 10$.
- $p \equiv 3 \mod 4$ なら $Q \equiv 7 \mod 10$, $a \equiv 8 \mod 10$.

一般に P を奇素数とし, $p = e + 1$ が素数のとき, $Q = \frac{P^p - 1}{P}$ に関して $a = p^e Q$ を P を**底とする弱完全数**という.

$N_p = \frac{P^p - 1}{P}$ と書くことも多い.

条件をさらに弱めて, p を奇数にしても次からわかるように 末尾 1 桁が 6 または 8, はやはり成立している.

表 3: $P = 2$

p	$Q = 2^p - 1$	素因数分解	a: 弱弱完全数
2	3	3	6
3	7	7	28
5	31	31	496
7	127	127	8128
9	511	7*73	130816
11	2047	23*89	2096128
13	8191	8191	33550336
15	32767	7*31*151	536854528
17	131071	131071	8589869056
19	524287	524287	137438691328
21	2097151	$7^2 * 127 * 337$	2199022206976
23	8388607	47*178481	35184367894528
25	33554431	31*601*1801	562949936644096
27	134217727	7*73*262657	9007199187632128
29	536870911	233*1103*2089	144115187807420416
31	2147483647	2147483647	2305843008139952128

p を奇数とだけ仮定している場合,$Q = 2^p - 1$ とおき $a = 2^e Q$ を弱々しいが完全な数, さらに簡潔に弱弱完全数と呼ぶ.

10　P を底とする弱弱完全数

一般に P を奇素数とし, p が奇数のとき, $Q = \frac{P^p-1}{\overline{P}}$ に関して $a = p^e Q$ を P を底とする弱弱完全数という.

$N_p = \frac{P^p-1}{\overline{P}}$ と書くことも多い.

10.1　$P = 3$ のとき 弱弱完全数の表

表 4: $P = 3$

$2\varepsilon - 1$	$Q = (3^{2\varepsilon-1} - 1)/2$	素因数分解	a: 弱弱完全数
3	(13)	13	117
5	(121)	11^2	9801
7	(1093)	1093	796797
9	(9841)	13*757	64566801
11	(88573)	23*3851	5230147077
13	(797161)	79716	423644039001
15	(7174453)	$11^2 * 13 * 4561$	34315186290957
17	(64570081)	1871*34511	2779530261754401
19	(581130733)	1597*363889	225141952751788437
21	(5230176601)	13*1093*368089	18236498186842001001
23	(47071589413)	47*1001523179	1477156353259726319517

Q の末尾 1 桁は 1,3 が繰り返される.

a の末尾 1 桁は 7,1 が繰り返される.

11　弱弱完全数の周期

$p = 2\varepsilon - 1$ を奇数とする. $Q_p = \frac{P^p-1}{\overline{P}}$ を変形する

$$\begin{aligned}\overline{P}Q_{p+2} &= P^2P^p - 1 \\ &= P^2(\overline{P}Q_p + 1) - 1 \\ &= P^2\overline{P}Q_p + P^2 - 1.\end{aligned}$$

これより

$$Q_{p+2} = P^2 Q_p + P + 1.$$

ゆえに

$$\begin{aligned} a_{p+2} &= P^{p+1} Q_{p+2} \\ &= P^{p+1}(P^2 Q_p + P + 1) \\ &= P^4 a_p + P^{p+1}(P+1) \\ &= P^4 a_p + P(P+1)(\overline{P} Q_p + 1). \end{aligned}$$

したがって

$$a_{p+2} = P^4 a_p + P(P^2 - 1) Q_p + P(P+1).$$

数列 (p : 奇数のみ) $\{Q_p\}, \{a_p\}$ は連立漸化式で定まるがこれを 10,100,1000 を法としてエクセルで計算すると容易にそれぞれの下 1 桁,2 桁,3 桁が求められる.

11.1 完全数の Q, a の下２桁

完全数の場合は興味がある.

表 5: $P = 2$; 下 2 桁

p	Q	a
3	7	28
5	31	96
7	27	28
9	11	16
11	47	28
13	91	36
15	67	28
17	71	56
19	87	28
21	51	76
23	7	28

これより完全数の下 2 桁は, 16,28,56,76,96 のどれかである. 計 5 個.

メルセンヌ数の下 2 桁は, 7, 11, 27, 31, 47,51,67,71,87,91 のどれかである. 計 10 個.

Wikipedia によると完全数の下 2 桁は研究されているそうなので，これらの結果は既知であろう.

$P = 2$ のとき, すなわち完全数の場合に Q, a の下 3 桁を調べたのでその結果完全数の知られざる周期性が明らかにされた.

11.2 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. このことはオイラーによりはじめて証明された. 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.

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

$(2^{e+1} - 1)\sigma(L) = 2^{e+1} L$ 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 $\sigma(L) = L + 1$ は L が素数 p になる必要十分条件になることである.

11.3 $2p$ 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

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

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

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

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

整理すると

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

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.

11.4 $a = P^{\varepsilon}p$ 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.

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

となる. 分母を払ってから,P^{ε} を乗ずると

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

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

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

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.

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

となる. 分母を払ってから,P^{ε} を乗ずると

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

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

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

が基本方程式である.

11.5　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 $a \equiv 0 \bmod P$ 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.
$\sigma(a) = \frac{P^{e+1}-1}{P}\sigma(L)$ により
基本式

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

をえる.

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

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

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

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

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

$e = \varepsilon$ なら

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

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

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

を P^e で式を除して

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

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

これは L と P が互いに素であることに矛盾.

12　$a = 6p$ の特徴づけ

素因子が 1 個の場合には方程式の問題の完全に解決ができた. 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. しかしその証明は難しい.「奇数完全数は存在するか?」 という 2000 年来の数学世界の懸案より難しそうである.

ところでこの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 $a = 6 * 2^2, 6 * 3^2$ 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 6: $\sigma(a) = 2a + 12$ 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いずれも $a = 2^e p, (p = 2^{e+1} - 13$: 素数$)$ の形をしている. そこでその形になるエイリアン解を探す

表 7: $q = 2^{e+1} - 13$: 素数

e	$q = 2^e - 13$
12	8179
16	131059
56	144115188075855859
104	40564819207303340847894502572019
136	174224571863520493293247799005065324265459

エイリアン解は末尾が 9. また指数 e は 4 の倍数であるらしいことがわかる. 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.

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.

$q = 2^{e+1} - 13$ が素数になる e はコンピュータで探しても数はごく少ない. それにもかかわらず無数にあるにあるに違いない.

この予想はだれも証明してくれそうも無い. 実に恐ろしい予想である.

表 8: $q = 2^{e+1} - 13; e = 4k$

e	$q = 2^{e+1} - 13; e = 4$	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

12.1 e が 4 の倍数

$q = 2^{e+1} - 13$ が素数になるとき, $e \equiv 0 \mod 4$ または $e = 3$. このとき $q = 3, a = 2^3 * 3$.

Proof (金子氏による)

1) $e = 4k + 1$ のとき. $2^4 = 16 \equiv 1 \mod 3$ によって

$$q = 2^{4k+2} - 13 \equiv 4 - 13 = 9 \equiv 0 \mod 3$$

$q = 2^{e+1} - 13$ が素数なので $q = 3$. $2^{e+1} - 13 = 3$ によれば $e = 3$ となり矛盾.

2) $e = 4k + 2$ のとき. $2^4 = 16 \equiv 1 \mod 5$ によって

$$q = 2^{4k+3} - 13 \equiv 8 - 13 = -5 \equiv 0 \mod 5.$$

q が素数なので $q = 5$. $2^{e+1} - 13 = 5$ によれば $2^e = 9$ となり矛盾.

3) $e = 4k + 3$ のとき. $2^4 = 16 \equiv 1 \mod 3$ によって

$$q = 2^{4k+4} - 13 \equiv 1 - 13 = -12 \equiv 0 \mod 3.$$

q が素数なので $q = 3$. $2^{e+1} - 13 = 3$ によれば $e = 3$ となる. $a = 2^3 * 3$ なのでこれは擬素数になる.

12.2 弱エイリアン

e が 4 の倍数のとき $Q = 2^{e+1} - 13$ が素数になるとはいえない. そこでこのとき $a = 2^e Q$ はエイリアンとは言えない. そこで弱虫のエイリアン, 略して弱エイリアンと言う.

$Q_k = 2^{4k+1} - 13, a_k = 2^{4k} Q_k$ とおく.

表 9: 弱エイリアンの表

k	Q_k	a_k
1	19	304
2	499	127744
3	8179	33501184
4	131059	8589082624
5	2097139	2199009624064
6	33554419	562949735317504
7	536870899	144115184586194944
8	8589934579	36893488091584528384

a_k の末尾 1 桁は 4, Q_k の末尾 1 桁は 9. これはすごい,4 と 9 という昔の人が嫌った数がでてきた.

12.3 弱エイリアンの下 2 桁

$Q_k = 2^{4k+1} - 13, a_k = 2^{4k} Q_k$ に関して

$$Q_{k+1} = 2^{4k+4+1} - 13 = 16 * 2^{4k+1} - 13 = 16 * (Q_k + 13) - 13 = 16 * Q_k + 15 * 13$$

なので数列 Q_k, a_k についての連立漸化式とみてかつこれを $\mathrm{mod} 10, 100, 1000$ とみてエクセルでプログラムを作る.

表 10: 弱エイリアンの表 , 下 2 桁

k	Q_k	a_k	2^{4k}
1	19	4	16
2	99	44	56
3	79	84	96
4	59	24	36
5	39	64	76
6	19	4	16

表 11: 弱エイリアンの表 , 下 3 桁, その 1

k	Q_k	a_k	2^{4k}
1	19	304	16
2	499	744	256
3	179	184	96
4	59	624	536
5	139	64	576
6	419	504	216
7	899	944	456
8	579	384	296
9	459	824	736
10	539	264	776
11	819	704	416
12	299	144	656
13	979	584	496
14	859	24	936
15	939	464	976
16	219	904	616
17	699	344	856
18	379	784	696
19	259	224	136
20	339	664	176
21	619	104	816
22	99	544	56
23	779	984	896
24	659	424	336

表 12: 弱エイリアンの表 , 下 3 桁, その 2

k	Q_k	a_k	2^{4k}
25	739	864	376
26	19	304	16
27	499	744	256
28	179	184	96
29	59	624	536
30	139	64	576
31	419	504	216
32	899	944	456
33	579	384	296
34	459	824	736
35	539	264	776
36	819	704	416
37	299	144	656
38	979	584	496
39	859	24	936
40	939	464	976
41	219	904	616
42	699	344	856
43	379	784	696
44	259	224	136
45	339	664	176
46	619	104	816
47	99	544	56
48	779	984	896
49	659	424	336
50	739	864	376
51	19	304	16

13　$s(a)=2$ 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.

$a=p^eq^f(p<q)$ 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 $\rho'=\overline{pq}; \overline{p}=p-1, \overline{q}=q-1$ とおいた.

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

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

$2q-2\overline{q}=2$ なので次の基本式をえる:

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

$Y(2X-q)=12\overline{q}+2X-1>0$ 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) $Y\geq q^2$.

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

$q^2(2X-q)=2Xq^2-q^3$ を移項して

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

ここで $\tilde{q}=q+1$ とおいた. さらに $q^3-1=\overline{q}(q^2+q+1)$ 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) $q = 3$.

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

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

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

$X = 4$ 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.

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

しかし $2X > q = 11$ に反する.

ii) $Y = q$.

$q(2X-q) = 12\overline{q}+2X-1$ によって,$2X = 12+q+1$. これより $q = 2^{e+1}-13$. $e = 3$ にとき $q = 3$. 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.

14　第 2 の完全数 28 の場合

表 13: $Q = 2^{e+1} - 57$ が素数, $a = 2^e Q$

(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)	$2^2 * 7 * 61$

通常解は表示しない場合:

表 14: $m = 28$: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	$2^9 * 967$

エイリアン解に限る場合:

表 15: $s(a) = 2; a = 2^e q;$:エイリアン解

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

エイリアン解をもっと求める:

表 16: $e > 9; q = 2^{e+1} - 57$:素数

e	$q = 2^{e+1} - 57$:素数
15	65479
18	524231
21	4194247
27	268435399
42	8796093022151
45	70368744177607
55	72057594037927879
57	288230376151711687
61	4611686018427387847
66	147573952589676412871
73	1888946593147858085472 7
81	4835703278458516698824647
139	a
159	b

$$a = 139379657490816394634598239204052259412 3719$$

$$b = 146150163733090291820368483271628301965593 2542919$$

弱虫エイリアンの下２桁表示

表 17:

k	e	Q	e	R	e	S
1	5	7	6	71	7	199
2	9	67	10	91	11	51
3	13	27	14	11	15	59
4	17	87	18	31	19	91
5	21	47	22	51	23	19
6	25	7	26	71	27	31

$$e = 4k + 1, Q_k = 2^{4k+2} - 57, a = 2^{4k+1}Q_k,$$
$$e = 4k + 2, R_k = 2^{4k+3} - 57, a_k = 2^{4k+2}Q_k,$$
$$e = 4k + 3, S_k = 2^{4k+4} - 57, a_k = S_k = 2^{4k+3}Q_k.$$

表 18: 弱虫エイリアンの下 3 桁表示

k	e	Q	e	R	e	S
1	5	7	6	71	7	199
2	9	967	10	991	11	651
3	13	327	14	711	15	459
4	17	87	18	231	19	691
5	21	247	22	551	23	619
6	25	807	26	671	27	331
7	29	767	30	591	31	179
8	33	127	34	311	35	571
9	37	887	38	831	39	139
10	41	47	42	151	43	411
11	45	607	46	271	47	499
12	49	567	50	191	51	851
13	53	927	54	911	55	259
14	57	687	58	431	59	891
15	61	847	62	751	63	419
16	65	407	66	871	67	531
17	69	367	70	791	71	979
18	73	727	74	511	75	771

表 19:

k	e	Q	e	R	e	S
19	77	487	78	31	79	939
20	81	647	82	351	83	611
21	85	207	86	471	87	299
22	89	167	90	391	91	51
23	93	527	94	111	95	59
24	97	287	98	631	99	91
25	101	447	102	951	103	219
26	105	7	106	71	107	731
27	109	967	110	991	111	779
28	113	327	114	711	115	971
29	117	87	118	231	119	739
30	121	247	122	551	123	811
31	125	807	126	671	127	99
32	129	767	130	591	131	251
33	133	127	134	311	135	859

表 20:

k	e	Q	e	R	e	S
34	137	887	138	831	139	291
35	141	47	142	151	143	19
36	145	607	146	271	147	931
37	149	567	150	191	151	579
38	153	927	154	911	155	171
39	157	687	158	431	159	539
40	161	847	162	751	163	11
41	165	407	166	871	167	899
42	169	367	170	791	171	451
43	173	727	174	511	175	659
44	177	487	178	31	179	491
45	181	647	182	351	183	819
46	185	207	186	471	187	131
47	189	167	190	391	191	379
48	193	527	194	111	195	371
49	197	287	198	631	199	339
50	201	447	202	951	203	211
51	205	7	206	71	207	699
52	209	967	210	991	211	651

表 21: $s(a) = 3, a = 2^e q_1 * q_2$;:エイリアン解

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

14.1 $a = 496p$ の特徴づけ

第 3 の完全数 496

表 22: $m = 496::2 < a < 1,500,000,$* 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	$2^5 * 71 * 443$

14.2 $a = 8128p$ の特徴づけ

第 4 の完全数 8128

表 23: $m = 8128$: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	$2^5 * 47 * 827$

15 $a = mp$ の特徴づけ

表 24: $a = mp$

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

表 25: $a = mp$

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 26: $a = mp$

a	素因数分解
m = 32	
2048	$2^1 1$
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	$2^3 * 5^3$