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 2期　資料2
2015 年10月23日

飯高 茂

平成 27 年 10 月 22 日

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

$S(p) = pS(\frac{n}{p})$ と書くことができる.

たとえば　$n = 6, p = 2$ のとき $S(2) = 2\{1, 2, 3\} = \{2, 4.6\}$.

1.1　オイラー関数

$W_n = S - \cup_{j=1}^{s} S(p_j)$ 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 の集合 T についてその元の個数を $|T|$ で示すと $|S(p_j)| = \frac{n}{p_j}, |S(p_j p_k)| = \frac{n}{p_j p_k}, \cdots$ が成り立つ.

1.2　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.

1.3 オイラー関数の表示式

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

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

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

1.4 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 の部分集合 T についてその元の和を $|T|_1$ で示すと

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

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

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

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

これは Wikipedia の英語版に出ている公式である.

1.5 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

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

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

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

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

1.6 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.

1.7　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
$|S|_3=\frac{n^2(n^2+2n+1)}{4}$ が成り立ち $|S(p_j)|_3=\frac{n^2}{4}(2n+\frac{n^2}{p_j}+p_j)$.

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

よって

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

1.8　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

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

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

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

かくて次の結果に至る.

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

1.9　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

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

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

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.

1.10　m 乗和 の公式

集合 $S = \{1, 2, \cdots, n\}$ について, S の集合 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.

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

2　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.

$\dfrac{t}{e^t - 1}$ 指数型母関数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.

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

($B_1 = \frac{1}{2}$ とする場合もあり, この場合は 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.

2.1 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 $\zeta(2n) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}(Euler)$ など

4.

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

$n = 1$ 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.

2.2 $B_{2k+1} = 0$ 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

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

$F(t)$ が偶関数になるので $c_{2k+1} = 0$.

3　べき乗和 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 $S_m(n) = |S|_m = \sum_{k=1}^{n} k^m$ 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

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

3.1　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 $\frac{1}{1-e^{-z}}=-\sum_{j=1}^{\infty}B_j\frac{(-z)^{j-1}}{j!}$ 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:

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

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

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

これを用いて $G(z,n)$ を求める.

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

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

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

4 $\psi^{(m)}(n)$ の公式

n の素因子 $p=p_j$ について

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

に注意すると,

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

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

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

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

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

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

$m=5$ 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

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

$$\psi^{(5)}(n)=\frac{n^2}{12}(2\varphi(n)n^3+(-1)^s5\varphi(n)\mathrm{rad}(n)n-\Gamma(3,n)).$$

$m=6$ 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

$$\psi^{(6)}(n)=\frac{n}{7}(An^6+a_2Bn^4+a_4\Gamma(3,n)n^2+a_6\Gamma(5,n)).$$

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

5 $\psi(n)$ 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.

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.

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 (perfect numbers) 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.

この形の素数 $Q = 2^{e+1} - 1$ 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.

7　弱完全数

表 1: $P = 2$: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

* 非完全数

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 2: $P = 2$

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.

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

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

8 弱弱完全数の周期

一般に P を奇素数とし, $p = e+1$ が奇数のとき, $Q_p = \frac{P^p-1}{\overline{P}}$ に関して $a_p = P^eQ_p$ を P を**底とする弱弱完全数** (ww-perfect number) という.

$Q_p = \frac{P^p-1}{\overline{P}}$ 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

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

これより

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

これより

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

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.

8.1 完全数の Q, a の下 2 桁

完全数の場合は興味がある.

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.

表 3: $P = 2$; 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

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.

8.2 完全数の知られざる周期性

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

表 4: $P = 2$ のときの弱弱完全数の周期 その 1

p : 奇数	$Q = 2^p - 1$ の下 3 桁	弱弱完全数 a の下 3 桁
p	Q	a
3	7	28
5	31	496
7	127	128
9	511	816
11	47	128
13	191	336
15	767	528
17	71	56
19	287	328
21	151	976
23	607	528
25	431	96
27	727	128
29	911	416
31	647	128
33	591	936
35	367	528
37	471	656
39	887	328
41	551	576
43	207	528
45	831	696
47	327	128
49	311	16
51	247	128
53	991	536
55	967	528
57	871	256
59	487	328

表 5: 弱弱完全数の周期 その 2

p : 奇数	2^p-1 の下 3 桁	弱弱完全数の下 3 桁
p	Q	a
61	951	176
63	807	528
65	231	296
67	927	128
69	711	616
71	847	128
73	391	136
75	567	528
77	271	856
79	87	328
81	351	776
83	407	528
85	631	896
87	527	128
89	111	216
91	447	128
93	791	736
95	167	528
97	671	456
99	687	328
101	751	376
103	7	528
105	31	496

$p=5, Q=31, a=496$ から始まり周期の表 2 の最後 $p=105, Q=31, a=496$ で 1 つの周期が完結する.

周期の長さは $(105-5)/2=50$ である.

$P = 2$ のときの弱弱完全数 a の下 3 桁の表は次の通り.

完全数が 100 個ほど求められた時代が来たらそのとき下 3 桁を調べると次の 25 個ある候補の中にあるだろう.

表 6: a の下 3 桁

16	176	376	576	776
28	216	416	616	816
56	256	456	656	856
96	296	496	696	896
136	336	536	736	936

25 個ある.

オイラーの時代の完全数の数表と比べてみよう.

表 7: 完全数の場合

e	$e+1$	$2^e * q$	a	$a \bmod 1000$
1	2	$2 * 3$	6	6
2	3	$2^2 * 7$	28	28
4	5	$2^4 * 31$	496	496
6	7	$2^6 * 127$	8128	128
12	13	$2^{12} * 8191$	33550336	336
16	17	$2^{16} * 131071$	8589869056	056
18	19	$2^{18} * 524287$	137438691328	328
30	31	$2^{30} * 2147483647$	2305843008139952128	128

8.3 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.

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.

8.4 $2p$ 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 $a=2^eL(L:\text{奇数})$ と書けるのでこれを代入する.

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

ゆえに

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

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.

8.5 $a = P^{\varepsilon}p$ 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.

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

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.

8.6　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.
$\sigma(a) = \frac{P^{e+1}-1}{\overline{P}}\sigma(L)$ 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.

8.7 $a = 6p$ 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. 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 8: $\sigma(a) = 2a + 12$ 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 $a = 2^e p, (p = 2^{e+1} - 13$: 素数$)$ の形をしている. そこでその形に拘ってエイリアン解を探す

表 9: $q = 2^{e+1} - 13$

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

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

8.8 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.

8.9　弱エイリアン

$Q = 2^{e+1} - 13$ が素数になるとき $a = 2^e Q$ はエイリアンとまでは言えない. 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 11: 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.

8.10　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 12: 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 13: 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 14: 弱エイリアンの表 , 下 3 桁, その 1

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

8.11 $s(a)=2$ 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.

8.12 $a = 28p$ の特徴づけ

第 2 の完全数 28 が係数の場合を計算する.

表 15: $m = 28$: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 16: $m = 28$:$2 < a < 1,500,000$,* 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 17: $s(a) = 2; a = 2^e q$;: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 18: $s(a) = 3, a = 2^e q_1 * q_2$;:エイリアン解

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

8.13 $a = 496p$ の特徴づけ

第 3 の完全数 496

表 19: $m = 496$::$2 < a < 1,500,000$,* 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	$2^5 * 71 * 443$

8.14 $a = 8128p$ の特徴づけ

第 4 の完全数 8128

表 20: $m = 8128$: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	$2^5 * 47 * 827$

9 $a = mp$ の特徴づけ

表 21: $a = mp$

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 22: $a = mp$

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 23: $a = mp$

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	$2^3 * 5^3$

表 24: $2\varphi(a) - a = 1$,

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

表 25: $2\varphi(a) - a = 1$,

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

表 26: $2\varphi(a) - a = 3$,

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 27: $2\varphi(a) - a = 5$,

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

表 28: $2\varphi(a) - a = 7$,

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

表 29: $2\varphi(a) - a = -3$,

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

表 30: $2\varphi(a) - a = -5$,

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

表 31: $2\varphi(a) - a = -6$,

a	素因数分解
18	$2 * 3^2$

表 32: $2\varphi(a) - a = -9$,

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

表 33: $2\varphi(a) - a = -10$,

a	素因数分解
50	$2 * 5^2$