素数べき と完全数

飯高 茂

平成 29 年 7 月 31 日

目 次

1　素数べき

2 を公比とし初項 1 の等比数列 $1, 2, 2^2 = 4, 2^3 = 8, \cdots$ は数学において基本的で大切な数列である.

3 を公比とする等比数列 $1, 3, 3^2 = 9, 3^3 = 27, \cdots$ も同様に大切である.

さて, 自然数 a の約数の和を $\sigma(a)$ で表すことは現在ほぼ確定した記号であるが, これを a の関数と見てユークリッド関数と言いたい.

たとえば, $a = p^3(p : \text{素数})$ ならその約数は $1, p, p^2, p^3$. この和 $1 + p + p^2 + p^3$ が $\sigma(a)$ である.

$S = 1 + p + p^2 + p^3$ とおくと, $pS = p + p^2 + p^3 + p^4$. $pS - S$ を作るとうまく消し合って $pS - S = p^4 - 1$. $p > 1$ なので $S = \dfrac{p^4 - 1}{p - 1}$.

一般には $a = p^e$ のとき $\sigma(p^e) = \dfrac{p^{e+1} - 1}{p - 1}$ が示される.

2 個以上の素因子を持つときは次のように考えるとよい.

$a = p^2q^2$ の約数は $1, p, p^2, q, pq, p^2q, q^2, pq^2, p^2q^2$. これらの和は

$$\begin{aligned}(1 + p + p^2) + (1 + p + p^2)q + (1 + p + p^2)q^2 &= (1 + p + p^2)(1 + q + q^2) \\ &= \sigma(p^2)\sigma(q^2).\end{aligned}$$

同じように考えると, $a = p^eq^f$ の約数は素因子分解の一意性より $p^rq^s, (r \leq e, s \leq f)$ と書ける. したがって

$$\sigma(a) = \sigma(p^e)\sigma(q^f). \tag{1}$$

a, b は互いに素とする. ab の約数 d は a の約数 δ と b の約数 D を用いて $d = \delta D$ と一意的に書ける. これを用いると

$$\sigma(ab) = \sigma(a)\sigma(b)$$

が成り立つことを証明できる. この性質を $\sigma(a)$ は乗法性を持つ, と言う.

素因数分解の一意性によって乗法性が成り立つことが証明される. 素因数分解がわかれば $\sigma(a)$ は直ちに計算できる.

1.1　$\sigma(a)$ の表

$\sigma(a)$ に親しむため a とその素因数分解 , $\sigma(a)$ を横に並べ $\sigma(a)$ の順にしたがって 並べてみた.

表 1: $\sigma(a)$ の順

a	素因数分解	$\sigma(a)$	a	素因数分解	$\sigma(a)$
2	$[2]$	3	33	$[3,11]$	48
3	$[3]$	4	35	$[5,7]$	48
5	$[5]$	6	47	$[47]$	48
4	$[2^2]$	7	34	$[2,17]$	54
7	$[7]$	8	53	$[53]$	54
6	$[2,3]$	12	28	$[2^2,7]$	56
11	$[11]$	12	39	$[3,13]$	56
9	$[3^2]$	13	49	$[7^2]$	57
13	$[13]$	14	24	$[2^3,3]$	60
8	$[2^3]$	15	38	$[2,19]$	60
10	$[2,5]$	18	59	$[59]$	60
17	$[17]$	18	61	$[61]$	62
19	$[19]$	20	32	$[2^5]$	63
14	$[2,7]$	24	67	$[67]$	68
15	$[3,5]$	24	30	$[2,3,5]$	72
23	$[23]$	24	46	$[2,23]$	72
12	$[2^2,3]$	28	51	$[3,17]$	72
29	$[29]$	30	55	$[5,11]$	72
16	$[2^4]$	31	71	$[71]$	72
25	$[5^2]$	31	73	$[73]$	74
21	$[3,7]$	32	45	$[3^2,5]$	78
31	$[31]$	32	57	$[3,19]$	80
22	$[2,11]$	36	79	$[79]$	80
37	$[37]$	38	44	$[2^2,11]$	84
18	$[2,3^2]$	39	65	$[5,13]$	84
27	$[3^3]$	40	83	$[83]$	84
20	$[2^2,5]$	42	40	$[2^3,5]$	90
26	$[2,13]$	42	58	$[2,29]$	90
41	$[41]$	42	89	$[89]$	90
43	$[43]$	44	36	$[2^2,3^2]$	91

ここでは素因数分解 $2^2 \cdot 3^2$ を $[2^2,3^2]$ のようにリスト表記で表した.
上の表を観察して次のことがわかる.

1. $\sigma(a)$ に出てこない数として 9,10,11 などがあり,
2. $\sigma(a) = 12$ なる数 a として 6,11 があげられる.
3. $\sigma(a) = 90$ になる数 a として 24,38,59.

これらを数学的に証明してみよう.

1.2　ユークリッド関数 のグラフ

ユークリッド関数 $\sigma(a)$ のグラフを描いて見た. きわめて複雑な形をしている.

図 1: $\sigma(a)$

2014 年 11 月の書泉グランデ 7 階で行われた私の講義でこの図を示しながら,「チョイ見では多価関数に見えるが実際は (一価) 関数である」と説明した.

最前列にいた小学 1 年生が手をまっすぐあげて「先生, 多価関数て, 何ですか」と質問した. 彼は熱心に講義を聴いており, 少しでもわからないと質問する. 私は, とても感心した.

さてこの図を見てみよう.

$x = a, y = \sigma(a)$ とおく.

$a = p > 1$ が素数なら $\sigma(a) = a + 1$ なので $y = x + 1$: これが素数の直線.

$a = p > 1$ が素数でないなら $\sigma(a) \geq a + 2$ なので $y \geq x + 2$. 素数の直線の上側になる.

与えられた 自然数 m に対してこれと素な素数を p とすると, $a = mp$ について

$b = \sigma(a) = \sigma(m)\sigma(p) = \widetilde{m}\widetilde{p}$ となるので $p = \dfrac{a}{m}$ を用いて, $\widetilde{m} = m + 1$ という記法を使うと

$$b = \widetilde{m}(\frac{a}{m} + 1) = \frac{\widetilde{m}a}{m} + \widetilde{m}$$

したがって, 素数 m に対して $a = mp, b = \sigma(a)$ とおけば (a, b) は直線

$$y = \frac{\widetilde{m}a}{m} + \widetilde{m}$$

の上にある.

1. $m = 2$ に対して直線 $y = \dfrac{3a}{2} + 3$,
2. $m = 3$, に対して直線 $y = \dfrac{4a}{3} + 4$,
3. $m = 5$, に対して直線 $y = \dfrac{6a}{5} + 6$,$\cdots$ などが対応する.

1.3　等比数列の和

$a = 2^n p, (p > 2$:素数$)$ の約数は

$$1, 2, 2^2, \cdots, 2^n, p, 2p, 2^2 p, \cdots, 2^n p$$

であり, これらの和は等比数列の和の公式を使うと $2^{n+1} - 1 + (2^{n+1} - 1)p$ になる.

ここで $p = 2^{n+1} - 1$ を仮定してみる.

$$2^{n+1} - 1 + (2^{n+1} - 1)p = (2^{n+1} - 1)(p + 1) = 2^{n+1}p + 2^{n+1} - (p + 1) = 2^{n+1}p = 2a$$

よって, $\sigma(a) = 2a$ を満たす.

2　完全数と概完全数

$\sigma(a) = 2a$ を満たす自然数 a を古代ギリシャの数学者は完全数 (perfect numbers) と命名した. 完全数 という名前は魅力的であり, 名前の力のおかげで数学者はもちろん一般にも広く知れるようになった

$p = 2^{n+1} - 1$ が素数のとき $a = 2^n p$ をユークリッドの完全数という. これは完全数になっている.

一方 $A = 2^e$ なら $\sigma(A) = 2A - 1$ を満たす.

この場合, 完全数になるには 1 だけ足らない. 少し惜しいゆえ概完全数 (almost perfect number) と呼ぶ. $a = 2^e$ は概完全数になるが, 概完全数, すなわち

$\sigma(a) = 2a - 1$ を満たす自然数 a はに限るか?

が問題になった. この問題は未解決である.

2.1 完全数の数表

表 2: 完全数の場合,$q = 2^{n+1} - 1$ は素数

$e \bmod 4$	e	$e+1$	$2^e * q$	a	$a \bmod 10$
1	1	2	$2 * 3$	6	6
2	2	3	$2^2 * 7$	28	8
0	4	5	$2^4 * 31$	496	6
2	6	7	$2^6 * 127$	8128	8
0	12	13	$2^{12} * 8191$	33550336	6
0	16	17	$2^{16} * 131071$	8589869056	6
2	18	19	$2^{18} * 524287$	137438691328	8
2	30	31	A	B	8
0	60	61	C	D	6
0	88	89	E	F	6

ここで, $A = 2^{30} * 2147483647$
$B = 2305843008139952128$(Euler による)
$C = 2^{60} * 2305843009213693951$
$D = 2658455991569831744654692615953842176$
$E = 2^{88} * 618970019642690137449562111$
$F = 191561942608236107294793378084303638130997321548169216$
などと続く.

a の末尾の数は 6 か 8. 言い換えると $a \equiv 6$ または $8 \mod 10$. これは完全数の持つ周知の性質のひとつ.

数表を観察すると次の結果がわかる. ただし, ここで $e > 1$ の場合しか扱わない.
$e = 1$ は例外の場合として考える.
$e \equiv 0 \mod 4$ なら $q \equiv 1 \mod 10$. $a \equiv 6 \mod 10$.
$e \equiv 2 \mod 4$ なら $q \equiv 7 \mod 10$. $a \equiv 8 \mod 10$.

Proof. (金子元さんの援助による)

$2^4 = 16 \equiv 1 \mod 5$ を以下用いる.

1). $e = 4k$. $q = 2^{e+1} - 1 = 2^{4k+1} - 1 \equiv 1 \mod 5$ によって $q = 1 + 5L$. q は奇数なので L は偶数. $q \equiv 1 \mod 10$.

$a = 2^e q \equiv q \equiv 1 \mod 5$; $a = 1+5L$. a は偶数なので $L = 2m+1$. $a = 1+5(2m+1) \equiv 6 \mod 10$.

2). $e = 4k + 1$. $c = 2^{2k+1}$ とおくとき

$q = 2^{e+1} - 1 = 2^{4k+2} - 1 = c^2 - 1 = (c-1)(c+1)$ は素数なので $c - 1 = 1$. ゆえに $c = 2; q = 3, k = 0, e = 1$. $a = 2 * q = 6$. これは例外的な場合.

3). $e = 4k + 2$. $q = 2^{e+1} - 1 = 2^{4k+3} - 1 \equiv 2 \mod 5$ によって $q = 2 + 5L$. L は奇数になり, $q \equiv 7 \mod 10$.

$a = 2^e q \equiv -q \equiv 3 \mod 5$; $a = 3+5L$. a は偶数なので $L = 2m+1$. $a = 3+5(2m+1) \equiv 8 \mod 10$.

4). $e = 4k + 3$. $q = 2^{e+1} - 1 = 2^{4k+4} - 1 \equiv 0 \mod 5$ によって $q = 5$. しかし $q = 2^{e+1} - 1 = 5$ は矛盾する.

偶数完全数の末尾の 1 桁は 6, または 8 になるという結果は完全数の中でもやさしいが美しい性質である. q の末尾の 1 桁は 1 (最初だけ 3), または 7 になるという性質は完全数の歴史では取り上げられていなかった.

2.2 完全数の歴史

完全数の歴史について書いて簡単にふれる.

L.E.Dickson 著: Theory of Numbers I,1919/20(Chelsea Publishing Company 版 1992) の第 1 章を参考にした.

- ユークリッドは原論 IX,prop.36 において $p = 1 + 2 + 2^2 + \cdots + 2^n$ が素数なら $a = 2^n p$ は完全数になることを示した.
- AD 100 年の頃 Nichomchus はすべての数 を
  過剰数 ($\sigma(a) - a > a$), 不足数 ($\sigma(a) - a < a$), 完全数 ($\sigma(a) - a = a$) に分類した.
- 完全数は 6,28,496,8128, などであり, これらの末尾の数が 6 または 8 であることに注目が集まった.
  (6,8 は交互にきて、さらに桁が上がる度に 1 つずつあることを観察したがこれらは正しくなかったことが後にわかった).
- 1456 年の文書に 5 番目の完全数 33550336 が記載された.
- Luca Paciuolo (1494 年 ?) は $1 + 2 + 2^2 + \cdots + 2^n$ が素数になることは実行して初めてわかることだが無限にあるだろう, と述べた.
- Cardano (1501–1576) は完全数はユークリッドが与えた方法ですべて構成されるだろう, と述べた.
- Tartaglia (1506–1559) $1 + 2 + 4, 1 + 2 + 4 + 8, 1 + 2 + 4 + 8 + 16, \cdots$ は交互に素数か合成数になる, と述べた.
- F.Maurolucus (1494– 1575) は完全数は三角数になることを注意した.

  実際, $q = 2^{e+1} - 1$ とおくと $q + 1 = 2 * 2^e$ によって

$$1 + 2 + 3 + \cdots + q = \frac{q(q+1)}{2} = 2^e q = a$$

- R.Descartes(1596-1650) は 1638 年の Mersenne(1588-1648) への手紙で偶数完全数はユークリッドが与えた形になることを証明できたと思う, と書いた. また, 奇数完全数は ps^2 の形になると主張した.
- P.Fermat (1607– 1665) は 1640 年の Mersenne への手紙で n が合成数なら $2^n - 1$ も合成数. n が素数なら $2^n - 2$ は $2n$ で割れることを示した.
- L.Euler(1707–1783) は 1752 年の Goldbacher への手紙で 7 個の完全数は $2^{p-1}(2^p - 1), p = 2, 3, 5, 7, 13, 17, 19$ であるが $p = 31$ のときは分からない, と述べた. 後に は Bernoulli への手紙で $p = 31$ のときは完全数であることを確認した, と述べた. さらに 没後, 出された論文で 偶数完全数は $2^{p-1}(2^p - 1)$; $(2^p - 1 :$ 素数) と表せることの証明を与えた.(次項で証明する)

カルダノ (Cardano) とタルタリア (Tartaglia) は一般の 3 次方程式の解法で争った間柄という事情があり当時のイタリア数学界の巨匠. 完全数に関してはタルタリアの方は正しくない. これは容易に確認できる. カルダノの言明は正しく後にオイラーが証明する.

このように偶数の完全数はオイラーによってその形が決められた. しかし, 偶数完全数は無限にあるか, あるいは奇数の完全数は存在するかなどは依然として未解決の大難問である.

2.3 オイラーによる偶数の完全数定理の証明

a を偶数完全数 ($\sigma(a) = 2a$ を, $a = 2^e L(e > 0, L$: 奇数) の形に書く.

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

となるので $N = 2^{e+1} - 1$ とおけば $N\sigma(L) = (N + 1)L$ となり

$$N(\sigma(L) - L) = L.$$

$d = \sigma(L) - L$ とおくとき $Nd = L$. したがって d は L の約数である. つぎの 3 つの場合がある.

(1) $d = 1$. $N = L.d = 1 = \sigma(L) - L$ により L は素数 p であり, $p = L = N = 2^{e+1} - 1$. $p = 2^{e+1} - 1$ は素数で $a = 2^e p$. これはユークリッドの与えた完全数の形となっている.

(2) $d = L$. $N = 1 = 2^{e+1} - 1$ になるので $e = 0$. a が奇数になり仮定に反す.

(3) $1 < d < L$. d は $1, L$ 以外の約数なので $\sigma(L) \geq 1+L+d$. よって $d = \sigma(L)-L \geq 1+d$. これは矛盾.

2.4 素数の判定法

オイラーの証明では $\sigma(a) - a = 1$ なら a は素数ということが有効に使われている.

$\sigma(a) = a + 1$ と書き換えればこれは a の約数は $1, a$ だけということだから定義によって, a は素数.

したがってこのことはごく当たり前のことなのだ.

私は高校生への研究課題として $a = 2p, (p > 2$ 素数の 2 倍) になることを $\sigma(a)$ で判定したらどうなるか. という問題をを出してみた. しかし高校生に質問されたら適切に答える必要があると反省し事前に自分でいろいろ考えてみた.

$a = 2p, (p > 2$: 素数) のとき

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

すると $2\sigma(a) = 3a + 6$ になる. この逆問題は次のように解けた.

$2\sigma(a) = 3a + 6$ を満たすとき, $a = 2p$ の他に 8 もある.

$a = 2p$ の特徴づけは,8 を例外としてうまくできた.

しかし, $a = 6p$, $28p$ など完全数が係数につく場合の特徴づけは極端に難しい. 証明ができそうもないである.

これに関連した問題は高校生でも解けそうな場合がある. しかし解けそうもない数多くの問題がでてきたので, 好都合であった.

2.5 3 点セット

Wikipedia で調べたところ $\sigma(a) - 2a = 1$ を満たす自然数は pseudo perfect number (疑似完全数) と呼ばれることがある. これは果たして存在するかどうかが問われている.

$\sigma(a) - 2a = -1, 0, 1$ を満たす自然数 a を求める問題 (3 点セット) はどれも未解決である. 完全数の問題は 2300 年かかっても解けない難問だが, その前後の問題 (3 点セット) も解けていない.

これらの問題は解けないで残されている点に価値がある, ということである.

1995 年にフェルマーの大定理の証明が確認されて,350 年におよぶ数論の難問が解けた. これによって目標を失った人は数知れない. しかし 3 点セット問題などは手つかずに残されている未解決問題である.

2.6 素数べきの約数の和

$\sigma(2^e) = 2^{e+1} - 1$ が素数になるとき, $e + 1$ も素数である. 次の表では $e + 1$ が素数になる場合に限り ,$\sigma(2^e)$ の素因数分解をしている.

素数になる $\sigma(2^e)$ は 7,31,127,8191,131071,524287,$\cdots$ などであり意外に多い. これらをメルセンヌ素数という.

$e + 1$ が素数となる場合 $\sigma(2^e)$ を単にメルセンヌ数という.

図 2: メルセンヌ（Marin Mersenne, 1588– 1648）

1588 年は豊臣秀吉の刀狩 の年で日本史では重要.

表 3: $\sigma(2^e) = 2^{e+1} - 1$:メルセンヌ数,($e+1$:素数)

$2^e = A$	$\sigma(A)$	素因数分解
$2 = 2$	3	[3]
$2^2 = 4$	7	[7]
$2^4 = 16$	31	[31]
$2^6 = 64$	127	[127]
$2^{10} = 1024$	2047	$[23, 89]$
$2^{12} = 4096$	8191	[8191]
$2^{16} = 65536$	131071	[131071]
$2^{18} = 262144$	524287	[524287]
$2^{22} = 4194304$	8388607	$[47, 178481]$
$2^{30} = 1073741824$	2147483647	[2147483647]

たとえば $[23, 89]$ は 2047 の素因数分解 $23 \cdot 89$ をリストで表記したものである.
$\sigma(2^e)$ が素数のとき $2^e\sigma(2^e)$ は完全数になる. 例えば

$$2 * 3 = 6, 4 * 7 = 28, 16 * 31 = 496, 64 * 127 = 8128, \cdots$$

となり, これらは古代人が発見した 4 つの完全数である.

実際, $A = 2^e$ に対して $\sigma(A)$ が素数 q のとき $a = Aq$ とおく. $q = \sigma(2^e) = 2^{e+1} - 1$ より $q + 1 = 2^{e+1} = 2A$ なので

$$\sigma(a) = \sigma(A)\sigma(q) = q(q+1) = 2Aq = 2a.$$

したがって a は完全数になる.

完全数の定義には約数の和が必要である.

素因数分解の一意性と約数の和の公式の証明には, 等比数列の和の公式が不可欠である. これらはユークリッドに代表される古代ギリシャの数学者が見いだしたものである.

日本の高校生なら誰でも知っている等比数列の和の公式は 2300 年も前に発見され完全数の理論に使われた. 日本がようやく弥生式の稲作を始めたころ (BC300 年頃) 等比数列の和の公式 (ユークリッド BC300) はすでにできていた. 本当にすごいことだ.

しかし, 完全数 a は $\sigma(2^e)$ が素数 q になる 2^e を用いて $a = 2^e q$ と必ず書けるか ?

という問いは依然として解けていない.

ここでは完全数 a に対しその素因子の個数 (それを $s(a)$ と書く) が 2 の場合に限って解くことにする.

3　$s(a)=2$ のときの完全数の証明

ここでは $s(a)=2$ のときだけ扱う.

a を素因数分解し $a=p^eq^f(p<q:$ 素数$)$ とする. $X=p^e, Y=q^f$ とおくと $a=XY$ となる. すると $\overline{p}=p-1, \overline{q}=q-1$ を使うと

$$\sigma(a)=\frac{(pX-1)(qY-1)}{\overline{pq}}$$

であり,$A=pX-1, B=qY-1, \rho'=\overline{pq}$ とおけば

$$\frac{AB}{\rho'}=2XY.$$

書き直して

$$AB=2\rho' XY.$$

$AB-2\rho' XY$ の XY の係数を R とおくとき $R=pq-2\rho'$ となり

$$RXY=pX+qY-1.$$

この式を**基本等式**という.

$R=pq-2\rho'=2-(p-2)(q-2)$ であり基本等式から $R>0$ なので $p=2$ かつ $R=2$. したがって $2XY=2X+qY-1$. よって $(2X-q)Y=2X-1$ が成り立ち, $Y\geq q$ によって,

$$\begin{aligned}0=2XY-(2X+qY-1)&=(2X-q)Y-(2X-1)\\&\geq(2X-q)q-(2X-1)\\&=2X(q-1)-(q^2-1)\\&=\overline{q}(2X-q-1).\end{aligned}$$

$\overline{q}$ を払うと,

$$q+1\geq 2X.$$

一方, $(2X-q)Y=2X-1>0$ によれば $2X-q\geq 1$. すなわち $2X\geq q+1$. よって $2X=q+1$ により $q=2^{e+1}-1, a=XY=2^eq$. したがって,a はユークリッドの完全数.

4　完全数の平行移動

完全数を m だけ平行移動するとは次の意味である.

パラメータ m に対して $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した (狭義の) 完全数という. 結果として m は偶数になる.

4.1　$m = 2$

2 だけ平行移動した場合を見てみよう. $q = 2^{e+1} + 1$ が素数になるので $e + 1$ は 2 のべき, すなわち $e + 1 = 2^r$ と書くことができる. 一般に $F_r = 2^{2^r} + 1$ をフェルマ数といい, これが素数になるならフェルマ素数という. フェルマはフェルマ数はすべて素数になると死に至るまで予想していた.

表 4: $q = 2^{e+1} + 1$ が素数

e	$e+1$	$e \bmod 4$	$2^e * q$	a
0	1	0	3	3
1	2	1	$2 * 5$	10
3	4	3	$2^3 * 17$	136
7	8	3	$2^7 * 257$	32896
15	16	3	$2^{15} * 65537$	2147516416

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ らはフェルマ素数である.

F_5 は合成数であることを 641 が因数であることを示したのはオイラーである. このほかにフェルマ素数があるかどうかは未解決の難問. (私は無数のフェルマ素数があると想像している)

$e \geq 3$ のとき $q \equiv 7, a \equiv 6 \mod 10$.

とくに a の末尾の数は 6.

Proof. $e + 1 = 2^r$ により $r \geq 2$ なら $e + 1 = 4N$ と書けるので

$q = 2^{e+1} + 1 \equiv 2 \bmod 5$. 一方, q は奇数なので $2^e \equiv 3 \times 2^{e+1}$ なので $q \equiv 7 \mod 10$.

$a = 2^e * q \equiv 3 * q \equiv 6 \bmod 5$, a は偶数なので $a \equiv 6 \mod 10$.

4.2 $m = 4$

この場合 $q = 2^{e+1} + 3$ は素数.

表 5:

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
0	0	5	5	5
1	5	$2^5 * 67$	2144	4
2	6	$2^6 * 131$	8384	4
3	11	$2^{11} * 4099$	8394752	2
2	14	$2^{14} * 32771$	536920064	4
3	15	$2^{15} * 65539$	2147581952	2
1	17	$2^{17} * 262147$	34360131584	4
3	27	A	B	2
1	29	C	D	4
2	54	E	F	4
2	66	G	H	4

$A = 2^{27} * 268435459, B = 36028797421617152$
$C = 2^{29} * 1073741827, D = 576460753914036224$
$E = 2^{54} * 36028797018963971, F = 576460753914036224$
$G = 2^{66} * 147573952589676412931$
$H = 649037107316853507609507569598464$

表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 7, a \equiv 4 \mod 10$.
- $e \equiv 2 \bmod 4$ なら $q \equiv 1, a \equiv 4 \mod 10$.
- $e \equiv 3 \bmod 4$ なら $q \equiv 4, a \equiv 2 \mod 10$.

Proof.

$e = 4k + 1$ のとき, $2^4 \equiv 1 \bmod 5$ を以下で用いる.
$q \equiv 4 + 3 \equiv 7 \bmod 5$, $q \equiv 7 \mod 10$.
$a = 2^e q \equiv 2 * 7 = 14 \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 2$ のとき,
$q \equiv -2 + 3 \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.
$a = 2^e q \equiv 4 * q \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 3$ のとき,
$q \equiv 1 + 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.
$a = 2^e q \equiv 3 * 4 = 12 \equiv 2 \bmod 5$, $a \equiv 2 \mod 10$.

4.3 $m = -2$

$q = 2^{e+1} - 3$ が素数になるがこの場合 $2^e q$ は指数 e の擬素数 $\mathbf{p}_e$ と呼ばれる. 完全数と比べると素数になる場合が多い.

表 6: $q = 2^{e+1} - 3$ が素数

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
2	2	$2^2 * 5$	20	0
3	3	$2^3 * 13$	104	4
0	4	$2^4 * 29$	464	4
1	5	$2^5 * 61$	1952	2
0	8	$2^8 * 509$	130304	4
1	9	$2^9 * 1021$	522752	2
3	11	$2^{11} * 4093$	8382464	4
1	13	$2^{13} * 16381$	134193152	2
3	19	A	B	4
1	21	C	D	2
3	23	E	F	4
0	28	G	H	4
1	93	I	J	2

$A = 2^{19} * 1048573, B = 549754241024$
$C = 2^{21} * 4194301, D = 8796086730752$
$E = 2^{23} * 16777213, F = 140737463189504$
$G = 2^{28} * 536870909, H = 144115187270549504$
$I = 2^{93} * 19807040628566084398385987581$
$J = 1961594292308337738698684194455290145603494810419220971 52$
表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 1, a \equiv 2 \mod 10$.
- $e \equiv 0 \bmod 4$ なら $q \equiv 9, a \equiv 4 \mod 10$.
- $e \equiv 3 \bmod 4$ なら $q \equiv 3, a \equiv 4 \mod 10$.

Proof.
$e = 4k + 1$ のとき,
$q \equiv 4 - 3 \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.
$a = 2^e q \equiv 2 * 1 = 2 \bmod 5$, $a \equiv 2 \mod 10$.

$e = 4k$ のとき,
$q \equiv 2 - 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.

$a = 2^e q \equiv 9 \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 3$ のとき,
$q \equiv 1 - 3 \equiv 3 \bmod 5$, $q \equiv 3 \mod 10$.
$a = 2^e q \equiv 9 \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 2$ のとき,
$q \equiv 3 - 3 \equiv 0 \bmod 5$. したがって $q = 5$. $q = 2^{e+1} - 3 = 5$; $e = 2$. $a = 2^e q = 4 * 5 = 20$.

5　m だけ平行移動した完全数の定義式

パラメータ m に対して $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した (狭義の) 完全数ということはすでに紹介したとおりである. 次にこれの満たす方程式を求めよう.

$N = 2^{e+1} - 1$ とおく. $q = N + m$ は素数であることに注意.

$$\sigma(a) = \sigma(2^e q) = (2^{e+1} - 1)(q + 1) = Nq + N, N + m = q$$

に注意して次の式変形を行う.

$Nq = 2^{e+1}q - q = 2a - q$, が成り立ちさらに

$$\begin{aligned}
\sigma(a) &= \sigma(2^e q) \\
&= N(q + 1) \\
&= Nq + N \\
&= 2a - q + N \\
&= 2a - q + q - m \\
&= 2a - m.
\end{aligned}$$

かくして $\sigma(a) = 2a - m$ がえられた.

方程式 $\sigma(a) = 2a - m$ の解 a を平行移動 m の広義の完全数という.

広義の平行移動 m の広義の完全数, すなわち方程式 $\sigma(a) = 2a - m$ の解は, $q = 2^{e+1} - 1 + m$ が素数となる e によって $a = 2^e q$, となるか (したがって $s(a) = 2$ を満たす), という問題を考えよう.

一般的に言って m が少し大きいと反例が出やすい.

$m = 0, 2$ では反例が見つからない, 次に $m = 4$ の場合を扱う.

5.1 $\sigma(a) = 2a - 4$ の場合

$a = 4$ とき $\sigma(a) = 2a - 4$ を満たす解をパソコンで順次計算たところ次の表ができた.

表 7: $\sigma(a) = 2a - 4$

a	素因数分解	$\sigma(a)$
5	$[5]$	6
14	$[2, 7]$	24
44	$[2^2, 11]$	84
110	$[2, 5, 11]$	216
152	$[2^3, 19]$	300
884	$[2^2, 13, 17]$	1764
2144	$[2^5, 67]$	4284
8384	$[2^6, 131]$	16764
18632	$[2^3, 17, 137]$	37260

$a = 110, a = 884, a = 18632$ は解だが $s(a) = 3$.

$s(a) = 3$ の解は他に 2 個あるが $2^e rq, (e < q$: 素数) の形をしている. これらは第 2 正規形の解と呼ばれる.