数学の研究を始めよう(7)
完全数の平行移動

飯高 茂

平成 25 年 6 月 13 日

1 完全数

自然数 a の約数の和を $\sigma(a)$ と表し, 約数の和関数と呼ぶ. たとえば $a = 6$ なら約数は $1, 2, 3, 6$ なのでこれらを足すと $1 + 2 + 3 + 6 = 12$ となり元の数 6 の 2 倍になる. 自然数 a の約数の和を $\sigma(a)$ と書くとき $\sigma(a) = 1 + 2 + 3 + 6 = 12 = 2a$.

そこで,$\sigma(a) = 2a$ を満たす a を完全数という. これは古くからある概念で, ユークリッドの数学原論に載っている. $\sigma(a) - 2a = 0$ を満たすとき a は完全数になる.

2 $\sigma(a) - 2a$ の平行移動

$\sigma(a) - 2a$ の値によって a の性質がわかるときがある. とりあえず, パソコン君に作ってもらった次の表を見てみよう.

表 1: $\sigma(a) - 2a = -2, -1, 0$ の値

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
3	[3]	4	-2
10	[2,5]	18	-2
136	[2,2,2,17]	270	-2
2	[2]	3	-1
4	[2,2]	7	-1
8	[2,2,2]	15	-1
16	[2,2,2,2]	31	-1
32	[2,2,2,2,2]	63	-1
64	[2,2,2,2,2,2]	127	-1
128	[2,2,2,2,2,2,2]	255	-1
256	[2,2,2,2,2,2,2,2]	511	-1
512	[2,2,2,2,2,2,2,2,2]	1023	-1
1024	[2,2,2,2,2,2,2,2,2,2]	2047	-1
6	[2,3]	12	0
28	[2,2,7]	56	0
496	[2,2,2,2,31]	992	0

3 $\sigma(a) - 2a = -2$ の場合

ここでは 3 個の a の値しかないが, a の最大素因数は $3, 5, 17$ でこれらはフェルマー素数である.

3.1 フェルマー数

$f_n = 2^{2^n}, F_n = f_n + 1$ とおき数列を $\{f_n\}$ と $\{F_n\}$ を考える. ただし $n = 0$ から始める.
定義により,

$$f_n{}^2 = (2^{2^n})^2 = 2^{2^{n+1}} = f_{n+1}.$$

ゆえに

$$f_n{}^2 = f_{n+1}.$$

F_n を**フェルマー数**という.

$n = 0, 1, 2, 3, 4$ のときのフェルマー数 F_n はみな素数である. そのとき **フェルマー素数**という.

$F_5 = 4294967297$ はオイラーにより素因数分解された:

$$4294967297 = 641 \times 6700417$$

実は皮肉なことに $n \geq 5$ のとき素数になるフェルマー数 (すなわち, フェルマー素数) は未だに 1 つも発見されていない.

$a = \dfrac{f_n F_n}{2}$ とおくと $\sigma(a) = \sigma(f_n/2)\sigma(F_n) = (f_n - 1)(F_n + 1)$ および $2a = f_n F_n$ により

$$\sigma(a) - 2a = -1 + f_n - F_n = -2.$$

表 2: フェルマー数

n	f_n	F_n
0	2	3
1	4	5
2	16	17
3	256	257
4	65536	65537

研究課題

$\sigma(a) - 2a = -2$ なら上の形に書けるか?

4 $\sigma(a) - 2a = -1$ の場合

$a = 2^e$ なら $\sigma(a) = 2^{e+1} - 1 = 2a - 1$. よって $\sigma(a) - 2a = -1$ になることはすぐわかる.

この逆は成り立つだろうか ?.

$\sigma(a) = 2a - 1$ によって $\sigma(a)$ は奇数である. そこで一般的な次の結果に注目しよう.

命題 1 $\sigma(n)$ が奇数ならば $n = 2^e \times L^2$ と書ける. ここで L は奇数.

証明. 一般に q を奇素数とするとき $q \equiv 1 \mod 2$ なので

$$\sigma(q^f) = 1 + q + q^2 + \cdots + q^f \equiv 1 + f \mod 2.$$

n を次の形に素因数分解する.

$$n = 2^e {q_1}^{f_1} \cdots {q_s}^{f_s}.$$

これより

$$\sigma(n) = \sigma(2^e)\sigma({q_1}^{f_1}) \cdots \sigma({q_s}^{f_s}) \equiv (1 + f_1) \cdots (1 + f_s) \mod 2.$$

$\sigma(n)q \equiv 1 \mod$ により $f_j q \equiv 1 \mod$. よって各 f_i は偶数である. $f_i = 2\varepsilon_i$ と書けて, $L = {q_1}^{\varepsilon_1} \cdots {q_s}^{\varepsilon_s}$ とおけば $n = 2^e L^2$.

そこで, $a = 2^e \times L^2$ と書けるから $\sigma(a) = \sigma(2^e)\sigma(L^2) = (2^{e+1} - 1)\sigma(L^2)$.

一方 $2a - 1 = 2^{e+1} \times L^2 - 1$ なので $\sigma(a) = 2a - 1$ によって

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

これより

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

これより先が進まない.

5　$\sigma(a) - 2a = 0$ の場合

a が完全数の場合．これは深く研究されているのでここで考えるには及ばない．

$\sigma(a) - 2a = 1$ の場合は解がないらしいのだがそれを証明できるかどうか不明である．

6 $\sigma(a) - 2a = 2, 4, 8$ の場合

表 3: $\sigma(a) - 2a = 2, 4, 8$ の場合

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
20	[2,2,5]	42	2
104	[2,2,2,13]	210	2
464	[2,2,2,2,29]	930	2
650	[2,5,5,13]	1302	2
1952	[2,2,2,2,2,61]	3906	2
18	[2,3,3]	39	3
12	[2,2,3]	28	4
70	[2,5,7]	144	4
88	[2,2,2,11]	180	4
1888	[2,2,2,2,2,59]	3780	4
196	[2,2,7,7]	399	7
56	[2,2,2,7]	120	8
368	[2,2,2,2,23]	744	8
836	[2,2,11,19]	1680	8
40	[2,2,2,5]	90	10
1696	[2,2,2,2,2,53]	3402	10

6.1　$\sigma(a) - 2a = 2$ の場合

$a < 2000$ の中では,

$\langle 1 \rangle$ $a = 20 = 2^2 \times 5 \times$,

$\langle 2 \rangle$ $a = 104 = 2^3 \times 13$,

$\langle 3 \rangle$ $a = 464 = 2^4 \times 29$,

$\langle 4 \rangle$ $a = 650 = 2 \times 5^2 \times 13$,

$\langle 5 \rangle$ $a = 1952 = 2^6 \times 61$

のみが解である. $2^e p, (p:$ 素数) の形の解が目立つのでこれに限って解を探索しよう.

ややー般にして $a = 2^e p$ が $\sigma(a) - 2a = w$ を満たす場合

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

なので $p = 2^{e+1} - w - 1$ を満たす.
$w = 0$ なら完全数の場合の素数だから, それに似ている点でこれらはカワイイ素数である. パソコン君に依頼すると $a = 2^5 \times 61$ を超える解を 5 個打ち出してくれてた.
$p = 2^{e+1} - 3$ を満たす解の表.

$\langle 1 \rangle$ $a = 2^8 \times 509$,

$\langle 2 \rangle$ $a = 2^9 \times 1021$,

$\langle 3 \rangle$ $a = 2^{11} \times 4093$,

$\langle 4 \rangle$ $a = 2^{13} \times 16381$,

$\langle 5 \rangle$ $a = 2^{19} \times 1048573$.

$\sigma(a) - 2a = 2$ の場合の解は無限にあることはほぼ確かだがそれを証明することはできそうも無い.

6.2　$\sigma(a) - 2a = 4$ の場合

$\sigma(a) - 2a = 4$ の場合の解をパソコン君に書き出してもらった.

表 4:

a	素因数分解	$\sigma(a)$
12	[2,2,3]	28
70	[2,5,7]	144
88	[2,2,2,11]	180
1888	[2,2,2,2,2,59]	3780
4030	[2,5,13,31]	8064
5830	[2,5,11,53]	11664
32128	[2,2,2,2,2,2,2,251]	64260

$2^e p, (p:$ 素数) の形が目立つのでこれに限って解を探索したらさらに 4 個の解が出てきた.

$\langle 1\rangle$ $a = 2^9 \times 1019$,

$\langle 2\rangle$ $a = 2^{11} \times 4091$,

$\langle 3\rangle$ $a = 2^{17} \times 262139$,

$\langle 4\rangle$ $a = 2^{19} \times 1048571$.

6.3 $\sigma(a) - 2a = 8$ の場合

$\sigma(a) - 2a = 8$ の場合の解をパソコン君に書き出してもらった.

表 5: $\sigma(a) - 2a = 8$ の場合

a	素因数分解	$\sigma(a)$
56	[2,2,2,7]	120
368	[2,2,2,2,23]	744
836	[2,2,11,19]	1680
11096	[2,2,2,19,73]	22200
17816	[2,2,2,17,131]	35640
45356	[2,2,17,23,29]	90720
77744	[2,2,2,2,43,113]	155496
91388	[2,2,11,31,67]	182784

$2^e p$ 型の解の割合が減ってきたのに注意したい.

7 $\sigma(a) - 2a = 12$ の場合

これらは $a = 6p$ が通常解であり, 8 月号で調べた. 実際 $a = 24, 54$ を除くと,$a = 6p$ の形になり $24 = 6 \times 4, 54 = 6 \times 9$ なので $4 = 2^2, 9 = 3^2$ が擬素数である. エイリアン探索のため $a = 2^e p$ の型の解を探した. その結果 3 匹が見つかった.

表 6: $\sigma(a) - 2a = 12$ の値

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
24	[2,2,2,3]	60	12
30	[2,3,5]	72	12
42	[2,3,7]	96	12
54	[2,3,3,3]	120	12
66	[2,3,11]	144	12
78	[2,3,13]	168	12
102	[2,3,17]	216	12
114	[2,3,19]	240	12
138	[2,3,23]	288	12

$\langle 1 \rangle$ $2^8 \times 499$,

$\langle 2 \rangle$ $2^{12} \times 8179$,

$\langle 3 \rangle$ $2^{16} \times 131059$.

8　$\sigma(a) - 2a = 14, 16$ の場合

表 7: 12

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
272	[2,2,2,2,17]	558	14
550	[2,5,5,11]	1116	16
748	[2,2,11,17]	1512	16
1504	[2,2,2,2,2,47]	3024	16

以上の表から次のことがわかった.

- $\sigma(a) - 2a = 14$ になるときは $a = 272$ になっている.
- $\sigma(a) - 2a = 16$ になるときは $a = 550, 748, 1504$ になっている.

さて, $\sigma(a) - 2a = 14$ は単独解だろうか. エイリアン探索のため $a = 2^e p, (e < 35)$ の型の解を探した. その結果 6 匹が見つかった.

$\langle 1 \rangle$ $2^4 \times 17$,

$\langle 2 \rangle$ $2^6 \times 113$,

$\langle 3 \rangle$ $2^7 \times 241$,

$\langle 4 \rangle$ $2^9 \times 1009$,

$\langle 5 \rangle$ $2^{13} \times 16369$,

$\langle 6 \rangle$ $2^{15} \times 65521$,

$\langle 7 \rangle$ $2^{22} \times 8388593$.

さて, $\sigma(a) - 2a = 16$ のエイリアン探索のため $a = 2^e p, (e < 37)$ の型の解を探した. その結果 3 匹が見つかった.
$\sigma(a) - 2a = 16$ の場合は $a = 2^e p$ の型の解を探したところなんと 9 匹が見つかった.

$\langle 1 \rangle$ $2^5 \times 47$,

$\langle 2 \rangle$ $2^7 \times 239$,

$\langle 3 \rangle$ $2^{11} \times 4079$,

$\langle 4 \rangle$ $2^{15} \times 65519$,

$\langle 5 \rangle$ $2^{17} \times 262127$,

$\langle 6 \rangle$ $2^{19} \times 1048559$,

$\langle 7 \rangle$ $2^{21} \times 4194287$,

$\langle 8\rangle$ $2^{23}\times 16777199$,

$\langle 9\rangle$ $2^{31}\times 4294967279$,

$\langle 10\rangle$ $2^{35}\times 68719476719$.

9　第2の完全数28

$a=28p$ とすると，

$$\sigma(a)=\sigma(28)\sigma(p)=56p+56$$

なので，

$$\sigma(a)=2a+56 \tag{2}$$

を満たす a の決定をしたい．$a=28p$ の形にかける場合が基本である．p が素数でかつ $2,7$ と異なる場合がもっとも当たり前の場合であるが，素数の数は無限なので沢山ある．この場合を**通常解**という．

$a=28p$ の形にかけても p が素数でない場合が**擬素数**の場合である．これ以外の解は**エイリアン**と呼ばれる．

とりあえず，通常解の場合以外のものをパソコン君に求めてもらおう．

表 8: $\sigma(a)=2a+56$ の非通常解

a	素因数分解	$\sigma(a)$
224	[2,2,2,2,2,7]	504
1372	[2,2,7,7,7]	2800
4544	[2,2,2,2,2,2,71]	9144
9272	[2,2,2,19,61]	18600
14552	[2,2,2,17,107]	29160

$2^e\times p$ 型のエイリアンを探すと $2^6\times 71$ 以外にたくさん出てきた．

$$2^7\times 199, 2^9\times 967, 2^{15}\times 65479.$$

9.1　擬素数解

エイリアンの決定問題は難しいのであきらめて擬素数解 a を探そう．すなわち $a=28k=2^2\times 7$ とかけて k が素数でない場合を探すのである．

$a=2^e7^fk, e\geq 2, f\geq 1$ と仮定する．

$$\sigma(a)=\sigma(2^e7^fk)=(2^{e+1}-1)(\frac{7^{f+1}-1}{6})\sigma(k)$$

なので，$X=2^e\geq 4, Y=7^f\geq 7$ とおけば

- $\sigma(a)=(2X-1)(\frac{7Y-1}{6})\sigma(k)$,

- $2a+56=2XYk+56$

によって

$$(2X-1)(7Y-1)\sigma(k)=6(2XYk+56). \tag{3}$$

$k=1$ のとき $(2X-1)(7Y-1)=6(2XY+56)$ を変形して

$$Y-1=\frac{342}{2X-7}.$$

これより, (1) $X=4, Y=343=7^3$,(2) $2X-7=3\times 19, Y-1=6; X=32=2^5, Y=7$. となる擬素数解が 2 つ得られた.

$k\geq 2$ のとき.

$$6(2XYk+56)=(2X-1)(7Y-1)\sigma(k)\geq (2X-1)(7Y-1)(k+1).$$

これより $k\geq 3$ によって

$$\begin{aligned}6\times 56 &\geq (2XY-7Y-2X+1)k+14XY-7Y-2X+1\\ &\geq 3(2XY-7Y-2X+1)+14XY-7Y-2X+1\\ &=20XY-28Y-8X+4.\end{aligned}$$

ゆえに

$$6\times 14\geq 5XY-7Y-2X+1.$$

$X\geq 4, Y\geq 7$ より

$$6\times 14\geq 5XY-7Y-2X+1=(5Y-2)X-7Y+1\geq 13Y-7=83$$

によって $X=4, Y=7$. 式 (3) に代入すると

- $(2X-1)(7Y-1)=7\times 48=336$,
- $6(2XYk+56)=6\times 56(k+1)=336(k+1)$.

$\sigma(k)=k+1$ となり k は素数となることがわかった.
$\sigma(k)=k+1$ が有効な素数判定法であることがよく分かったことであろう.

10 $a=10p$ の場合

$a=10p$ の場合は $p\neq 2,5$ を満たす素数 p に関して

$$\sigma(a)=\sigma(10p)=\sigma(10)\sigma(p)=18(p+1).$$

により $5\sigma(a)=9a+90$ をえる. この式を満たす a をパソコン君に依頼して表にしてもらう.
$a=40,250$ が例外でこのとき $4,25$ が擬素数である. これらを入れて p を 2,5 以外の素数と擬素数とすると $a=10p$ と書かれることが想定される. これを証明したいのである.

表 9: $5\sigma(a) = 9a + 90$ の場合

a	素因数分解	$\sigma(a)$
30	[2,3,5]	72
40^*	[2,2,2,5]	90
70	[2,5,7]	144
110	[2,5,11]	216
130	[2,5,13]	252
170	[2,5,17]	324
190	[2,5,19]	360
230	[2,5,23]	432
250^*	[2,5,5,5]	468
290	[2,5,29]	540
310	[2,5,31]	576
370	[2,5,37]	684
410	[2,5,41]	756
430	[2,5,43]	792
470	[2,5,47]	864
530	[2,5,53]	972
590	[2,5,59]	1080

10.1 未完の証明

自然数 a が $5\sigma(a) = 9a+90$ を満たすとする. $5(\sigma(a)-18) = 9a$ が成り立つので, 整数 k により

$$\sigma(a) - 18 = 9k, a = 5k$$

と書ける. これより

$$\sigma(5k) = 9k + 18. \tag{4}$$

1. 5 と k が互いに素な場合

$\sigma(5k) = \sigma(5)\sigma(k) = 6\sigma(k)$ なので式 (4) により $2\sigma(k) = 3k+6$ になり, 定理 1 が使えて $k = 2p$. ここで $p = 4$, または奇素数 $\neq 5$. したがって $a = 10p$. ここで $p = 4$ または奇素数 $\neq 5$.

2. k が 5 の倍数の場合

$k = 5^e L$ ($e > 0, 5$ と L が互いに素) と書けるから

$$\sigma(5k) = \sigma(5^{e+1}L) = \frac{5^{e+2}-1}{4}\sigma(L).$$

この式は $9k + 18 = 9(5^e L + 2)$ と等しいので

$$\frac{5^{e+2}-1}{4}\sigma(L) = 9(5^e L + 2).$$

分母を払うと

$$(5^{e+2}-1)\sigma(L) = 36 \times 5^e L + 72.$$

$2-1.$ $L=1$ の場合.
$5^{e+2}-1 = 36 \times 5^e + 72$, から $11 \times 5^2 = 73$ となりこれは不成立.

$2-2.$ L が素数の場合.
$(5^{e+2}-1)(L+1) = 36 \times 5^e L + 72$ を変形して

$$(5^{e+2}-1-36 \times 5^e)L = 73 - 25 \times 5^e.$$

さらに整理すると

$$5^e(11L-25) = -L-73 < 0.$$

故に $L=2$. このとき $3 \times 5^e = 75$. これから $5^e = 25$ をえて $e=2$. すなわち, $a = 5k = 2 \times 5^3$. これは 式 (4) を満たし 25 が擬素数になる.

$2-3.$ $L>2$ が素数でない場合.
この場合は矛盾が起きることを証明したいが今のところできない. エイリアンは出そうもないのだが, 確かなことは分からない.

研究課題 $a = 14p, a = 30p, a = 42p$ の場合を論じよ.