数学の研究を始めよう (6)
擬素数とエイリアン

飯高 茂

平成 25 年 6 月 19 日

1　約数の和関数 $\sigma(a)$

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 $a = 12$ なら約数は $1, 2, 3, 4, 6, 12$ になるので $\sigma(a) = 1 + 2 + 3 + 4 + 6 + 12 = 28$.

$a > 1$ のとき簡単にわかる性質を挙げると

$\langle 1 \rangle$ $a + 1 \leq \sigma(a)$,(1 と a が約数)

$\langle 2 \rangle$ a が素数なら $\sigma(a) = a + 1$,(1 と a のみが約数だから)

$\langle 3 \rangle$ $\sigma(a) = a + 1$ なら a は素数 ,

$\langle 4 \rangle$ a が素数でないなら $\sigma(a) \geq a + \sqrt{a} + 1$,

$\langle 5 \rangle$ a, b が互いに素なら $\sigma(ab) = \sigma(a)\sigma(b)$ (乗法性).

$\langle 6 \rangle$ a が素数の累乗 p^e なら $\sigma(a) = 1 + p + \cdots + p^e = \frac{p^{e+1}-1}{p-1}$.(等比級数の公式)

乗法性は大切であり, 高校数学の範囲で出来るからその証明を書いておく.

k を ab の約数とする. k と a の最大公約数を d とおけば $a = da', k = dk'$ と書けて a' と k' は互いに素になる.

k は ab の約数なので k' は $a'b$ の約数だが a' と k' は互いに素だから k' は b の約数になる.

このことは, 新しい学習指導要領に基づいて書かれた高校の数学 A で（証明なし）記述されていることである.

結局 $k = k'd$ と書かれ, d は a の約数,k' は b の約数なのであり, また逆に a の約数 α ,b の約数 β に対して積 $\alpha\beta$ は a, b が互いに素なので ab の約数である. これより

$$\sigma(ab) = \sum_{ab\text{ の約数}} k = \sum_{a\text{ の約数}} \alpha \sum_{b\text{ の約数}} \beta = \sigma(a)\sigma(b).$$

1.1　オイラー関数の性質

オイラー関数 $\varphi(a)$ も類似した性質を持つのでそれらを列挙してみよう.

$\langle 1 \rangle$ $a - 1 \geq \varphi(a)$,

$\langle 2\rangle$ a が素数なら $\varphi(a)=a-1$,

$\langle 3\rangle$ $\varphi(a)=a-1$ なら a は素数 ,

$\langle 4\rangle$ a が素数でないなら $a \geq \varphi(a)+\sqrt{a}$,

$\langle 5\rangle$ a, b が互いに素なら $\varphi(ab)=\varphi(a)\varphi(b)$ (乗法性).

2 σ による素数倍の特徴づけ

8 月号で完全数の定理に関して紹介したオイラーの証明においては $\sigma(a)=a+1$ なら a は素数になることがキーとなる事実であった.

ここでは a が素数 p の 2 倍, 3 倍, 4 倍 などになるとき $\sigma(a)$ と a の関係がどうなるか調べてみよう.

3 $a=2p$ の場合

$a=2p(2<p$ は素数$)$ と書ける条件を考えてみる. 乗法性によれば $\sigma(a)=\sigma(2p)=3(p+1)$ となる. これを 2 倍すると $2\sigma(a)=3(2p+2)=3a+6$ となり

$$2\sigma(a)=3a+6 \tag{1}$$

をえる.

次に, この逆を考える. すなわち 2 より大きい自然数 a が式 (1) を満たすとしよう. このような a の様子をみるためパソコン君に依頼して次の表を作ってもらった.

表 1: $2\sigma(a)=3a+6$ を満たす a

a	素因数分解	$\sigma(a)$
6	[2,3]	12
8^*	[2,2,2]	15
10	[2,5]	18
14	[2,7]	24
22	[2,11]	36
26	[2,13]	42
34	[2,17]	54
38	[2,19]	60
46	[2,23]	72
58	[2,29]	90
62	[2,31]	96

$*$ のついている 2 番目の $a=8$ を唯一の例外として

$$a=6=2\cdot 3, 10=2\cdot 5, 14=2\cdot 7, \cdots$$

となり, $a=2p$ となることが推察できる. $a=8$ という例外的な場合がでてきたことに注目しよう.
以上のことを念頭において, 式 (1) を満たす a に関して次のような計算を行う.

$$2(\sigma(a)-3)=3a$$

と変形すると, 2 と 3 は互いに素なので $\sigma(a)-3$ は 3 の倍数になる. すなわち 整数 k により $\sigma(a)-3=3k$ と書ける. これより $a=2k$ になるので

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

ここで場合を分ける.

1. k が奇数のとき.
$\sigma(2k)=\sigma(2)\sigma(k)=3\sigma(k)$ なので, $2(\sigma(a)-3)=3a$ によれば $\sigma(k)=k+1$. よって k は素数 p になり $a=2p$ となる.

2. k が偶数のとき.
$k=2^eL(L$ は奇数, $e>0)$ と表す.
すると, 2^{e+1} と L は互いに素なので, $\sigma(2^{e+1}L)=\sigma(2^{e+2}-1)\sigma(L)$ となる. よって

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

$\sigma(2k)=3k+3$ に $k=2^eL$ を代入することで

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

ここで, $L=1$ のとき $\sigma(1)=1$ により

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

$2^{e+2}-1=4\times 2^e-1=3\times 2^e+3$ となり, $2^e=2^2$. よって $e=2$ になり. $k=4, a=8$ となる.
実際, $a=8$ なら $\sigma(a)=15$ なので式 (1) を満たす.

$L>1$ のとき, 矛盾を導く. 実際 $\sigma(L)\geq L+1$ によって

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

L の係数を揃えて

$$0<(2^{e+2}-1-3\cdot 2^e)L=(2^e-1)L\leq 3-(2^{e+2}-1)=4(1-2^e)<0.$$

これは矛盾である.

次のように定理としてまとめておこう.

定理 1 自然数 a が $2\sigma(a)=3a+6$ を満たす条件は $a=2p$ とかけることである. ここで $p=4$ または 奇素数.

はじめは $a = 2p(p$ **は 奇素数)** という形の定理を期待したが, $a = 8 = 2 \cdot 4$ が例外として出てきた. 4 があたかも素数のような顔をして出てきたところが面白い. こういう 4 を**擬素数**とここでは呼ぶ.

次に $a = 3p$ などの場合を試みるべきである. 読者は, ここでノートを広げ鉛筆を用いて計算しいろいろやってみると良い. 私自身もそれを行い実に楽しく面白かった.

4 $a = 4p$ の場合

$a = 3p$ の場合は読者にまかせて $a = 4p(2 < p$ は素数) と書けるときを調べよう.

$\sigma(a) = \sigma(4p) = 7(p+1)$ になるので, 4 倍すると $4\sigma(a) = 4\sigma(4p) = 7(4p+4) = 7a+28$ になる. そこで

$$4\sigma(a) = 7a + 28 \tag{2}$$

をえる.

次に, 2 より大きい自然数 a が式 (2) を満たすとしよう. パソコン君は次の表を作ってくれた.

表 2: $4\sigma(a) = 7a + 28$

a	素因数分解	$\sigma(a)$
12	[2,2,3]	28
20	[2,2,5]	42
28	[2,2,7]	56
32*	[2,2,2,2,2]	63
44	[2,2,11]	84
52	[2,2,13]	98
68	[2,2,17]	126
76	[2,2,19]	140
92	[2,2,23]	168
116	[2,2,29]	210
124	[2,2,31]	224
148	[2,2,37]	266
164	[2,2,41]	294
172	[2,2,43]	308

4 番目の a は 32 である. さて $a = 32$ なら $\sigma(a) = 63$. $4\sigma(a) = 252$. かつ $28 + 7a = 28 + 7 \cdot 32 = 252$. したがってこの場合も 式 (2) を満たす. これ以外なら 奇素数 p によって $a = 4p$ と書けている. したがって 8 は擬素数であると考えてよい.

さて自然数 a は $4\sigma(a) = 28 + 7a$ を満たすと仮定する.

このとき $4(\sigma(a) - 7) = 7a$ により整数 k を用いて $a = 4k, \sigma(a) - 7 = 7k$ と書ける.

故に, k が奇数なら $\sigma(4k) = 7\sigma(k) = 7(k+1)$ により, $\sigma(k) = k+1$. ゆえに k は素数 p. したがって $a = 4p$ となる.

k が偶数なら $k=2^eL(e>0, L$ は奇数$)$ とおく.

- $\sigma(4k)=\sigma(2^{e+2}L)=(2^{e+3}-1)\sigma(L)$,
- $7(k+1)=7(2^eL+1)=(2^3-1)(2^eL+1)=2^3-1+(2^{e+3}-2^e)L$.

したがって式 (2) によって,

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

$L=1$ ならば

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

よって $2^e=2^3; e=3$. したがって $a=4k=2^5=32$.

$L>1$ ならば $\sigma(L)\geq 1+L$ なので

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

これより L のかかる項を左辺にまとめると

$$0>(1-2^e)L\geq(2^{e+3}-1)-2^3+1=2^{e+3}-2^3>0.$$

かくて矛盾した.

5　$a=q^\varepsilon p$ の場合

さて $a=mp$ において $m=2,3,4,5$ の場合をカバーする定理を考えて見よう.
a が素数 $q(\neq p)$ の累乗 q^ε 倍になっているとする. 便宜上 $A=q^\varepsilon$ とおけば $a=Ap$. よって

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

これより $C=\frac{q^{\varepsilon+1}-1}{q-1}$ とおけば $\sigma(A)=C$ となり, これに A を掛けると

$$A\sigma(a)=AC(p+1)=C(a+A).$$

$C=1+q+\cdots+q^\varepsilon$ と $A=q^\varepsilon$ は互いに素なので
$\sigma(a)=Ck, a+A=Ak$ と整数 k で書ける. これより $a=A(k-1)$ になり

$$\sigma(a)=\sigma(A(k-1))=Ck.$$

1. $k-1$ と q が互いに素のとき.
乗法性により $\sigma(A(k-1))=\sigma(A)\sigma(k-1)$. さらに $\sigma(A)=C$ なので

$$Ck=\sigma(a)=\sigma(A(k-1))=\sigma(A)\sigma(k-1)=C\sigma(k-1).$$

これより $\sigma(k-1)=k$. よって $k-1$ は素数なのでこれを p とおけば $a=A(k-1)=Ap$.

2. $k-1$ と q が互いに素でないとき.

$k-1=q^eL(e>0, L$ と q は互いに素) と書ける. 等比数列の和の公式により

$$Ck=\sigma(a)=\sigma(A(k-1))=\sigma(Aq^eL)=\sigma(q^{e+\varepsilon}L)=\frac{q^{e+\varepsilon+1}-1}{q-1}\sigma(L).$$

かくて

$$Ck=C(1+q^eL)=\frac{q^{e+\varepsilon+1}-1}{q-1}\sigma(L). \tag{4}$$

$C=\frac{q^{\varepsilon+1}-1}{q-1}$ を思い出すと

$$(1+q^eL)(q^{\varepsilon+1}-1)=(q^{e+\varepsilon+1}-1)\sigma(L). \tag{5}$$

1. $L=1$ のとき.

$(1+q^e)(q^{\varepsilon+1}-1)=q^{e+\varepsilon+1}-1$ により, $q^{\varepsilon+1}=q^e$. よって $e=\varepsilon+1$. すなわち, $a=A(k-1)=q^{\varepsilon}q^e=q^{2\varepsilon+1}$. したがって $q^{\varepsilon+1}$ を擬素数とみることができる.

2. $L>1$ のとき.

矛盾を導こう. $\sigma(L)\geq L+1$ が成り立つので 式 (5) から

$$(1+q^eL)(q^{\varepsilon+1}-1)=(q^{e+\varepsilon+1}-1)\sigma(L)\geq(q^{e+\varepsilon+1}-1)(L+1).$$

これより

$$(1+q^eL)(q^{\varepsilon+1}-1)=q^e(q^{\varepsilon+1}-1)L+q^{\varepsilon+1}-1\geq(q^{e+\varepsilon+1}-1)L+q^{e+\varepsilon+1}-1.$$

したがって

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

よって

$$0>(1-q^e)L\geq q^{\varepsilon+1}(q^e-1)>0.$$

これは矛盾.

定理としてまとめておこう.

定理 2 素数 q の累乗 q^{ε} について $A=q^{\varepsilon}$ および $C=\frac{q^{\varepsilon+1}-1}{q-1}$ とおく. 自然数 a が

$$A\sigma(a)=C(a+A).$$

を満たす条件は $a=Ap$ とかけることである. ここで p は 擬素数 $q^{\varepsilon+1}$ または q と異なる素数.

ここで扱われる A は小さい方から 2,3,4,5,7,8,9 であり 6 が除かれる. その次に除外されるのは 10 である.

5.1 擬素数

q の累乗 q^ε に関して, 数値が小さい場合について具体的に擬素数を書いてみよう.

表 3: 擬素数の表

係数 q^ε	擬素数 $q^{\varepsilon+1}$	$a = q^{2\varepsilon+1}$
2	4	$8 = 2^3$
3	9	$27 = 3^3$
4	8	$32 = 2^5$
5	25	$125 = 5^3$
7	49	$343 = 7^3$
8	16	$128 = 2^7$
9	27	$125 = 3^5$

6 $a = 6p$ の場合

$a = 6p$ の場合は $p \geq 5$ を満たす素数 p に関して

$$\sigma(a) = \sigma(6p) = \sigma(6)\sigma(p) = 12(p+1) = 2a + 12$$

により $\sigma(a) = 2a + 12$ をえる. この形の式では整除性の議論が全く使えない. すなわち前と同様に考えようとしてもどうにもならない. 手も足もでないのである.

6 は 完全数である. 一般に m が完全数なら $\sigma(m) = 2m$ をみたす. したがって p を m と互いに素な素数とすると

$$\sigma(a) = \sigma(mp) = \sigma(m)\sigma(p) = 2m(p+1) = 2a + 2m.$$

このときも整除性を用いた議論をすることはできない. 完全数は扱いが難しいのである.

パソコン君に作ってもらった表をみると, a が素数の 6 倍にならない場合がいくつも出てきた.

$a = 24$ (4 を擬素数とみよう), $a = 120$ (9 を擬素数とみよう) の他に $304 = 2^4 \cdot 19$ が出てきた. これは驚いた. これまでの擬素数とは明らかに違う異質性がある. 本当にエイリアンが出たと思った.

6.1 大きな制約下で

そこでエイリアンを敬遠して $\sigma(a) = 2a + 12$ を満たす自然数 a を 6 の倍数という制約下で決定してみよう.

1. a を偶数と仮定.

$a = 2^e k, (e > 0, k:$ 奇数) とおく.

$$\sigma(a) = \sigma(2^e) \cdot \sigma(k) = (2^{e+1} - 1)\sigma(k).$$

表 4: $\sigma(a) = 2a + 12$ の場合

a	素因数分解	$\sigma(a)$
24^*	[2,2,2,3]	60
30	[2,3,5]	72
42	[2,3,7]	96
54^*	[2,3,3,3]	120
66	[2,3,11]	144
78	[2,3,13]	168
102	[2,3,17]	216
114	[2,3,19]	240
138	[2,3,23]	288
174	[2,3,29]	360
186	[2,3,31]	384
222	[2,3,37]	456
246	[2,3,41]	504
258	[2,3,43]	528
282	[2,3,47]	576
304^*	[2,2,2,2,19]	620
318	[2,3,53]	648
354	[2,3,59]	720
366	[2,3,61]	744

$2a + 12 = 2^{e+1}k + 12$ によって

$$(2^{e+1} - 1)\sigma(k) = 2^{e+1}k + 12 \tag{6}$$

をえる.

2. その上, k を 3 の倍数と仮定.
$k = 3^f L (f > 0, L$ は 3 で割れない奇数) とすると

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

以上によって, $X = 2^e, Y = 3^f$ とおけば式 (**??**) から

$$(2^{e+1} - 1)\sigma(k) = (2^{e+1} - 1)\frac{3^{f+1} - 1}{2}\sigma(L) = \frac{(2X - 1)(3Y - 1)}{2}\sigma(L),$$

かつ

$$2^{e+1}k + 12 = 2^{e+1}3^f L + 12 = 2XYL + 12.$$

ゆえに

$$(2X - 1)(3Y - 1)\sigma(L) = 4XYL + 24.$$

$L=1$ のとき

$$(2X-1)(3Y-1)-4XY=24.$$

これより

$$Y=\frac{2X+23}{2X-3}=1+\frac{26}{2X-3}.$$

よって, $2X-3=1,2,13,26$.

表 5: $L=1$ のとき

$2X-3$	1	2	13	26
X	2	$\frac{5}{2}$	8	$\frac{29}{2}$
e	1		3	
Y	27		3	
f	3		1	

ゆえに解は $X=2,8$. これより (1) $e=1,f=3;a=2\times 3^3$,(2) $e=3,f=1;a=2^3\times 3$.
これが 2 つの擬素数 54 と 24 を与える.

$L\geq 2$ のとき $\sigma(L)\geq L+1$ によって

$$4XYL+24=(2X-1)(3Y-1)\sigma(L)\geq (2X-1)(3Y-1)(L+1). \tag{7}$$

整理して

$$(2XY-3Y-2X+1)L+(2X-1)(3Y-1)\leq 24.$$

$L\geq 2$ によって

$$(2XY-3Y-2X+1)2+(2X-1)(3Y-1)\leq 24.$$

変形して

$$10XY-9Y-6X\leq 21.$$

$X=2^e\geq 2, Y=3^f\geq 3$ に注意して

$$21\geq 10XY-9Y-6X=(10X-9)Y-6X\geq (10X-9)3-6X=24X-27\geq 48-27=21.$$

ゆえに $X=2,Y=3$. 式 (7) によれば

$$4XYL+24=24(L+1)=(2X-1)(3Y-1)\sigma(L)=24\sigma(L).$$

したがって, $\sigma(L)=L+1$. だから L は素数 p. よって, $a=2\times 3\times p=6p$.

6.2 エイリアンを探せ

a が 2 と 3 の倍数の場合はわかったので,

A).a が 2 の倍数で 3 の倍数でない場合,

B).a が 2 の倍数でない場合

を考える. A) のときは $304 = 2^4 \times 19$ を参考にして $a = 2^e p($ p は奇素数$)$ の形に限定して解を探してみよう.

$\sigma(a) = \sigma(2^e)\sigma(p) = (2^{e+1} - 1)(p + 1)$ なので $\sigma(a) = 2a + 12$ に代入すれば直ちに $2^{e+1} - 13 = p$ を満たす. そこでパソコン君にこのような素数を探してもらう.

表 6: $2^{e+1} - 13 = p$ を満たす場合

e	p	$a = 2^e p$	
3	3	$2^3 \times 3$	擬素数
4	19	$2^4 \times 19$	エイリアン
8	499	$2^8 \times 499$	エイリアン
12	8179	$2^{12} \times 8179$	エイリアン
16	131059	$2^{16} \times 131059$	エイリアン

なんと, 多くのエイリアンが出てきた. 偶数の完全数の場合は $2^e - 1$ が素数 p になるような素数を探す. しかし 2500 年かかっても 48 個しか見つからなかった. たぶん 無限にあると思われる. これと同様に $a = 6p$ の場合も $2^e p$ に関係したエイリアンは無限にいると思われる.

研究課題 上の表でエイリアンについての e は 4 の倍数になるようだ. 本当だろうか考えよ.

B). この場合は起きないと思われるが何もわからない.

完全数の場合で考えてみると, 偶数ならオイラーの方法で a の素因数分解の形が分かったが奇数の場合は難しく未だに決定的な結果がない. 我々の扱っている場合も著しい困難に向き合っているかもしれない. こういうときは無理に押さないで, 撤退することを考えてよい. しかし著者としては読者のチャレンジを待ちたい.

7 $a = 10p$ 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 4,25 とすると a は $10p$ 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 7: $5\sigma(a) = 9a + 90$ 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

7.1 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

$$\sigma(5k) = 9k + 18. \tag{8}$$

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 (8) 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 (8) 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.
ところである高校生がこの場合の研究を開始した. 期待しよう. うまく行けば, 研究経過も誌上で中継します.

研究課題 $a=14p, a=30p$ の場合を論じよ.

8 第 2 の完全数 28

28 は 2 番目の完全数なのでこの場合を調べよう. $a=28p$ とすると,

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

なので,

$$\sigma(a) = 2a + 56 \tag{9}$$

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.
$2^6\times 71$ 以外に $2^e\times p$ 型のエイリアンを探すと次の表にあるようにたくさん出てきた.

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

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

8.1 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 $a = 28k$ とかけて k が素数でない場合を探すのである．

$a = 2^e 7^f L, (e \geq 2, f \geq 1, L : 2{,}5$ でわれない) と仮定する．

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

なので, $X = 2^e \geq 4, Y = 7^f \geq 7$ とおけば

- $\sigma(a) = (2X-1)(\frac{7Y-1}{6})\sigma(L)$,
- $2a + 56 = 2XYL + 56$

によって

$$(2X-1)(7Y-1)\sigma(L) = 6(2XYL + 56). \tag{10}$$

1. $L = 1$ 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．

2. $L \geq 2$ のとき．

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

これより $L \geq 3$ によって

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

ゆえに

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

$X \geq 4, Y \geq 7$ より

$$84 = 6 \times 14 \geq 5XY - 7Y - 2X + 1 = (5Y-2)X - 7Y + 1 \geq 13Y - 7 = 84$$

によって $X = 4, Y = 7$. 式 (10) に代入すると

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

$\sigma(L) = L + 1$ となり L は素数 p となることがわかった. よって $a = XYp = 28p.$
$\sigma(L) = L + 1$ 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.

9　擬素数の条件

少し一般に論じてみよう.
$m = q_1q_2$ として q_1, q_2 は異なる素数とする.
$Q_1 = \sigma(q_1), Q_2 = \sigma(q_2)$, $Q^* = Q_qQ_2$ とおくと, q_1, q_2 と異なる素数 p に対して $a = mp$ に対して

$$\sigma(a) = \sigma(m)\sigma(p) = Q^*(p+1)$$

なので,

$$m\sigma(a) = Q^*(mp + m) = Q^*(a+m).$$

$a = m{q_1}^2$ が解になることを確認しよう. すなわち ${q_1}^2, {q_2}^2$ は擬素数であることを証明しよう.

$$\sigma(m{q_1}^2) = \sigma({q_1}^3q_2) = \frac{{q_1}^4 - 1}{q_1 - 1}(q_2 + 1) = \frac{{q_1}^4 - 1}{{q_1}^2 - 1}(q_1 + 1)(q_2 + 1) = ({q_1}^2 + 1)Q^*$$

と変形できるので

$$m\sigma(m{q_1}^2) = (m{q_1}^2 + m)Q^* = Q^*(a + m).$$

これは, $a = m{q_1}^2$ が解であることを示す.

研究課題 次の結果を示せ

定理 3 $m = {q_1}^{\varepsilon_1} \cdots {q_s}^{\varepsilon_s}$, ここで $q_1, \cdots, q_s$ は異なる素数とする.
このとき, ${q_1}^{\varepsilon_1+1}, \cdots, {q_s}^{\varepsilon_s+1}$ はすべて擬素数である.

しかしこれらで擬素数が尽きているかどうかは不明である.

研究課題 $m, \sigma(m)$ が互いに素なら 解は必ず擬素数解になることを示せ.