数学の研究を始めよう (18) 2014/September
ユークリッド関数の陪関数

飯高 茂

平成 26 年 4 月 28 日

1　ユークリッド関数

自然数 a に対して a の約数の和を $\sigma(a)$ と書いてきた. これを約数の和関数と呼ぶのは美しくない. 関数 $\sigma(a)$ はユークリッドの数学原論で論ぜられた完全数の理論で最も大切な関数なので, これを**ユークリッド関数**とよぶことを提案したい.

1.1　$a = 6p$ 問題

ユークリッド関数導入の記念として, これについて $a = 6p$ 問題を部分的に解いてみよう.

ユークリッド関数は乗法性がある. この性質を紀元前 5 世紀のユークリッド達は知っていたのだそうだ. これはすごい.

一般に $a = mp$ とおく. ここで p は素数, m は p で割れない自然数.

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

を変形して

$$\frac{\sigma(a)}{\sigma(m)} = \frac{a}{m} + 1 \tag{1}$$

$m = 6$ とすると $\sigma(6) = 12$ なので

$$\sigma(a) = 2a + 12$$

をえる. さてこの式を満たす自然数に $6p$ (p は素数, $p \neq 2, 3$) 以外のものがあるかどうかを問題とする.

1.2　$s(a) = 2$ の場合

この問題に対して 自然数 a の相異なる素因数の個数を $s(a)$ で示し $s(a) = 2$ の場合に解決しよう.

このとき $a = p^e q^f$ と表せる. ここで p, q は素数で $p < q$ を満たすとする.

$\overline{p} = p - 1, \overline{q} = q - 1$ とおくとき, 等比数列の和の公式で $\sigma(p^e) = \frac{p^{e+1}-1}{\overline{p}}, \sigma(q^f) = \frac{q^{f+1}-1}{\overline{q}}$ とかけるので

$$\sigma(a) = \sigma(p^e)\sigma(q^f) = \frac{(p^{e+1}-1)(q^{f+1}-1)}{\overline{p}\overline{q}}$$

を用いて

$$\sigma(a) = \frac{(p^{e+1}-1)(q^{f+1}-1)}{\overline{pq}} = 2a + 12 = 2p^e q^f + 12$$

なので

$$(p^{e+1}-1)(q^{f+1}-1) = 2p^e q^f \overline{pq} + 12\overline{pq}. \tag{2}$$

この方程式を解くことは一見して簡単では無い. 以前ならハナからあきらめていた問題であるが, 恐怖のシナリオを解いた勢いで考えてみた.

まず,$X = p^e, Y = q^f$ とおいて書き直すと

$$(pX-1)(qY-1) = 2\overline{pq}XY + 12\overline{pq}.$$

これより

$$(pq - 2\overline{pq})XY = qY + pX + 12\overline{pq} - 1.$$

$pq - 2\overline{pq} = 2 - (p-2)(q-2)$ であり $p = 2$ なら 2. それ以外は負になる.

しかるに, 上式の右辺は正なので $p = 2$.

1.3 $p = 2$ の場合

このとき 式 (2) は

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

となるので

$$2X(Y-1) = qY + 12\overline{q} - 1 = qY + 12q - 13.$$

よって $qY + 12q - 13 = q(Y-1) + 13q - 13$ と変形して

$$2X = q + \frac{13(q-1)}{q^f - 1} = q + \frac{13}{q^{f-1} + q^{f-2} + \cdots + 1}.$$

13 は素数なので $q^{f-1} + q^{f-2} + \cdots + 1 = 1$ または 13.

$f = 1$ なら $Y = q, 2X = 2^{e+1} = q + 13$. ゆえに $2^{e+1} - 13$ が素数ならそれを q とすれば解 $a = 2^e q$ をえる.

$e = 3$ のとき $2^{e+1} - 13 = 3$. よって $q = 3; a = 2^3 \times 3$.

$e = 4$ のとき $2^{e+1} - 13 = 19$. よって $q = 19; a = 2^4 \times 19$.

$e = 5$ のとき $2^{e+1} - 13 = 51$. これは素数では無い.

$e = 3, 2^{e+1} - 13 = 3$ によって $a = 24 = 2^3 \times 3 = 6 \times 4$ なので 4 は擬素数であり, この 24 を擬素数解という.

$f > 1$ のとき $q = 3, f = 3$ が解になり, このとき $a = 2 \times 3^3 = 54 = 6 \times 3^2$.

表 1: $2^{e+1}-13$ が素数 q,$a=2^e q$

e	q	$a=2^e\times q$
3	3	24
4	19	304
8	499	127744
12	8179	33501184
16	131059	8589082624

1.4 $s(a)=3$ の場合

前の項で $a=6p$ という通常解が得られなかった.$p>4$ なら $s(a)=3$ を満たす. そこで $s(a)=3$ の場合に解を求める問題を解決しよう.

このとき $a=p^e q^f r^g$ と表せる. ここで p,q,r は素数で $p<q<r$ を満たすとする.

$\overline{p}=p-1,\overline{q}=q-1,\overline{r}=r-1$ とおくとき,

$$\sigma(a)=\sigma(p^e)\sigma(q^f)\sigma(r^g)=\frac{(p^{e+1}-1)(q^{f+1}-1)(r^{g+1}-1)}{\overline{pqr}}$$

を変形して

$$(p^{e+1}-1)(q^{f+1}-1)(r^{g+1}-1)=2p^e q^f r^g\overline{pqr}+12\overline{pqr}. \tag{3}$$

まず,$X=p^e,Y=q^f,Z=r^g$ とおいて書き直すと

$$(pX-1)(qY-1)(rZ-1)=2\overline{pqr}XYZ+12\overline{pqr}. \tag{4}$$

ここにおいて $X\geq p,Y\geq q,Z\geq r$ に注意する.期待できる解は$p=2,q=3,X=2,Y=3,Z=r$ であってその結果 $a=6r$ となるはずである.

これを正攻法で解くことは多くの困難がありそうなので, 解けるところから考える.

1.$p=2,q=3,X=2,Y=3,Z\geq r$ のもとで $Z=r$ を示す.

式 (4) は

$$3\times 8(rZ-1)=4\overline{r}(6Z+6)$$

になるので $rZ-1=\overline{r}(Z+1)$. ゆえに, $Z=r$.

2.$p=2,q=3,X=2,Y\geq 3^2,Z\geq r$ のもとで矛盾を導く. 式 (4) より

$$3(3Y-1)(rZ-1)=8\overline{r}(YZ+3).$$

$$Y((r+8)Z-9)=24\overline{r}+3(rZ-1).$$

$Y\geq 3^2$ によって

$$24\overline{r}+3(rZ-1)\geq 9((r+8)Z-9).$$

3 で割って

$$8\overline{r}+(rZ-1)\geq 3((r+8)Z-9)=3rZ-24Z-27.$$

$Z \geq r \geq 5$ により

$$13 + 4\overline{r} \geq (r+12)Z \geq 5(r+12) = 5\overline{r} + 65.$$

よって

$$-52 \geq \overline{r}.$$

矛盾.

（つづく）

2　ユークリッド陪関数

自然数 a に対してオイラー陪関数 $\widetilde{\varphi}(a)$ は a の異なる素因子の個数 s を用いてオイラー関数 $\varphi(a)$ を 2^s で割って定義された. 簡単な定義の変更だがえられた結果は期待以上に多かった. ユークリッド関数 $\sigma(a)$ の陪関数 $\widetilde{\sigma}(a)$ を $\sigma(a)/2^s$ で定義よう.

この関数について今までの研究の参考にしつつ実例をあげながら, 類似の性質を調べてみたい.

2.1 $\widetilde{\sigma}(a)$ の数表

パソコン君に $\widetilde{\sigma}(a)$ の数表を作ってもらった.

表 2: $\widetilde{\sigma}(a)$ の数表 ;$\sigma(a) = 2^E \cdots$

a	factor	$\sigma(a)$	$\widetilde{\sigma}(a)$	E	$s(a)$	$E - s(a)$
2	[2]	3	1.5	0	1	-1
3	[3]	4	2	3	1	2
4	$[2^2]$	7	3.5	0	1	-1
5	[5]	6	3	1	1	0
6	[2, 3]	12	3	2	2	0
7	[7]	8	4	4	1	3
8	$[2^3]$	15	7.5	0	1	-1
9	$[3^2]$	13	6.5	0	1	-1
10	[2, 5]	18	4.5	1	2	-1
11	[11]	12	6	2	1	1
12	$[2^2, 3]$	28	7	2	2	0
13	[13]	14	7	1	1	0
14	[2, 7]	24	6	3	2	1
15	[3, 5]	24	6	3	2	1
16	$[2^4]$	31	15.5	0	1	-1
17	[17]	18	9	1	1	0
18	$[2, 3^2]$	39	9.75	0	2	-2
19	[19]	20	10	2	1	1

$\sigma(a) = 2^E \cdots$ とする. $E - s(a)$ は $\widetilde{\sigma}(a)$ を素因数分解したときの 2 での指数である. $a = 18 = 2 \cdot 3^2$ のとき $E - s(a) = -2$. したがって, 小数部が 0.75.

オイラー陪関数の値は半整数になる場合があった. しかしユークリッド 陪関数 $\widetilde{\sigma}(a)$ の値は整数や半整数どころではなく, 分母が 2 のべきである有理数なのである. これには参ったといわざるをえない.

いくつかの場合に $\widetilde{\sigma}(a)$ の素因数分解での 2 の指数が負の場合順に並べてその様子をさぐってみよう.

表 3:

a	factor	$\sigma(a)$	factor	$\widetilde{\sigma}(a)$	$E; \sigma(a) = 2^E \cdots$	$s(a)$	$E - s(a)$
882	$[2, 3^2, 7^2]$	2223	$[3^2, 13, 19]$	277.875	0	3	-3
900	$[2^2, 3^2, 5^2]$	2821	$[7, 13, 31]$	352.625	0	3	-3
18	$[2, 3^2]$	39	$[3, 13]$	9.75	0	2	-2
36	$[2^2, 3^2]$	91	$[7, 13]$	22.75	0	2	-2
50	$[2, 5^2]$	93	$[3, 31]$	23.25	0	2	-2
72	$[2^3, 3^2]$	195	$[3, 5, 13]$	48.75	0	2	-2
90	$[2, 3^2, 5]$	234	$[2, 3^2, 13]$	29.25	1	3	-2
98	$[2, 7^2]$	171	$[3^2, 19]$	42.75	0	2	-2
100	$[2^2, 5^2]$	217	$[7, 31]$	54.25	0	2	-2
v 2	$[2]$	3	$[3]$	1.5	0	1	-1
4	$[2^2]$	7	$[7]$	3.5	0	1	-1
8	$[2^3]$	15	$[3, 5]$	7.5	0	1	-1
9	$[3^2]$	13	$[13]$	6.5	0	1	-1
10	$[2, 5]$	18	$[2, 3^2]$	4.5	1	2	-1

この表を見ながら値の小数部が 0.5 になる場合を一般化してみた. また例をあげよう.

$\langle 1 \rangle$ $\widetilde{\sigma}(2^e) = \frac{2^{e+1}-1}{2} = \cdots .5$

$\langle 2 \rangle$ $\widetilde{\sigma}(2p^{2e}) = \frac{3}{2} \cdot \frac{1+p+p^2+\cdots+p^{2e+1}}{2} = \cdots .75; \cdots .25, p(:$ 奇素数$)$.

$\langle 3 \rangle$ $\widetilde{\sigma}(2 \times 3^2 \times 5^2 \times 7^2) = 4307.0625 = \cdots .0625$

$\langle 4 \rangle$ $\widetilde{\sigma}(2 \times p) = \frac{p+1}{4} = \cdots .5$, $(p \equiv 1 \bmod 4)$.

3　a が素数の場合

$a=p$ を奇素数とすると $\widetilde{\sigma}(a)=\frac{p+1}{2}$ により $2\widetilde{\sigma}(a)=a+1$ となる．そこで一般に $2\widetilde{\sigma}(a)-a$ を求め順に並べてみると, 正負のどちらも沢山出てくる．驚かざるをえない．

表 4: $2\widetilde{\sigma}(a)-a$ が -2 から 1 まで

a	factor	σ	factor	$\widetilde{\sigma}(a)$	E	$s(a)$	$E-s(a)$	$2\widetilde{\sigma}(a)-a$
44	$[2^2,11]$	84	$[2^2,3,7]$	21	2	2	0	-2
152	$[2^3,19]$	300	$[2^2,3,5^2]$	75	2	2	0	-2
10	$[2,5]$	18	$[2,3^2]$	4.5	1	2	-1	-1
136	$[2^3,17]$	270	$[2,3^3,5]$	67.5	1	2	-1	-1
6	$[2,3]$	12	$[2^2,3]$	3	2	2	0	0
28	$[2^2,7]$	56	$[2^3,7]$	14	3	2	1	0
496	$[2^4,31]$	992	$[2^5,31]$	248	5	2	3	0
2	$[2]$	3	$[3]$	1.5	0	1	-1	1
3	$[3]$	4	$[2^2]$	2	3	1	2	1
5	$[5]$	6	$[2,3]$	3	1	1	0	1
7	$[7]$	8	$[2^3]$	4	4	1	3	1
11	$[11]$	12	$[2^2,3]$	6	2	1	1	1
13	$[13]$	14	$[2,7]$	7	1	1	0	1
17	$[17]$	18	$[2,3^2]$	9	1	1	0	1
19	$[19]$	20	$[2^2,5]$	10	2	1	1	1
20	$[2^2,5]$	42	$[2,3,7]$	10.5	1	2	-1	1
23	$[23]$	24	$[2^3,3]$	12	3	1	2	1
104	$[2^3,13]$	210	$[2,3,5,7]$	52.5	1	2	-1	1

この表をよく見ると実に面白い．

たとえば a が素数なら $2\widetilde{\sigma}(a)-a=1$ になっているが, $a=2^2\times 5$ でも 1 になっている．その先を探すと $a=2^3\times 13$ でも 1 なのである．

$2\widetilde{\sigma}(a)-a=1$ による素数の判定ができない! これはショックである．

余関数の値はいつも正でそれが 1 になるとき, 素数になるという $\sigma(a)$ やオイラー関数, 陪関数の持っていた秩序が壊れている．われわれは楽園から追放されたのであろうか．

4　$2\widetilde{\sigma}(a)-a$ の値

$2\widetilde{\sigma}(a)-a=-1$ のときは $a=10$,$a=136$ でその素因数分解はそれぞれ $[2,5]$ と $[2^3,17]$.

$p=5,17$ はフェルマー素数である．

そこでフェルマー素数 p をとる．すなわち $2^{e+1}+1=p(p:$ 素数$)$ とかけると仮定し $a=2^e p$ としてみる．[1]

[1] このとき $e+1=2^m$ と書ける．p をフェルマー素数という．

$$\widetilde{\sigma}(a)=\widetilde{\sigma}(2^e p)=\frac{(2^{e+1}-1)(p+1)}{4}=\frac{(p-2)(2^{e+1}+2)}{4}=\frac{(p-2)(2^e+1)}{2}$$

これより

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

したがって, フェルマー素数は次式を満たす: $2\widetilde{\sigma}(a)-a=-1$

これはうれしい事態である. フェルマー素数は楽園から追放された私たちを励ましにでてきたのであろうか.

4.1 $2\widetilde{\sigma}(a)-a=-1$ の場合

この逆が言えるだろうか. すなわち 非素数 a が $2\widetilde{\sigma}(a)-a=-1$ を満たすなら $a=2^e p, (2^{e+1}+1=p$: 素数) と書けるか? を考えてみよう.

1). $s=s(a)=1$ のとき, $a=p^e$ とおく.

$2\widetilde{\sigma}(a)=\frac{p^{e+1}-1}{p-1}$ なので $2\widetilde{\sigma}(a)=a-1$ によって $p^{e+1}-1=(p-1)(p^e-1)$. これより $p+p^e=2$. したがって矛盾.

2). $s=2$ のとき.

i. $a=2^e q^f; (q>2$: 奇素数, $f>0$) とすると

$$2\widetilde{\sigma}(a)=\frac{(2^{e+1}-1)(q^{f+1}-1)}{2\overline{q}}=a-1=2^e q^f-1$$

によって,

$$(2^{e+1}-1)(q^{f+1}-1)=(2^{e+1}q^f-2)\overline{q}.$$

これより $N=2^{e+1}-1$ とおくと

$$N(q^{f+1}-1)=(Nq^f+q^f-2)\overline{q}.$$

になり $N(q^f-1)=(q^f-1-1)\overline{q}$. さらに書き換えて

$$N=\overline{q}-\frac{q-1}{q^f-1}.$$

$\frac{q-1}{q^f-1}$ は整数なので $f=1$. よって $a=2^e p, 2^{e+1}+1=p.(p:$ 素数).

ii. $a=p^e q^f; (q>p>2$: 奇素数, $f>0$) とする. 以下では $\overline{p}=p-1, \overline{q}=q-1, X=p^e, Y=q^f$ を使う.

$4\widetilde{\sigma}(a)=\frac{(p^{e+1}-1)(q^{f+1}-1)}{\overline{p}\overline{q}}=\frac{(pX-1)(qY-1)}{\overline{p}\overline{q}}, a=p^e q^f=XY$ なので, とりあえず $4\widetilde{\sigma}(a)<2a-4$ を証明する.

$$\begin{aligned}2a-4-4\widetilde{\sigma}(a)&=2XY-4-\frac{(pX-1)(qY-1)}{\overline{p}\overline{q}}\\&=\frac{2\overline{p}\overline{q}XY-4\overline{p}\overline{q}-(pX-1)(qY-1)}{\overline{p}\overline{q}}\end{aligned}$$

$R = 2\overline{pq} - pq = (p-2)(q-2) - 2$ とおくとき, 上式の分子 B は

$$B = RXY + pX + qY - 1 - 4\overline{pq} \geq RXY + p^2 + q^2 - 1 - 4\overline{pq}.$$

$p = 3, q = 5$ のとき, $R = 1, X = 3, Y = 5, 4\overline{pq} = 32$. よって、$RXY + p^2 + q^2 - 1 - 4\overline{pq} \geq 16$.

このほかの場合は $p = 3, q = 7$ のとき $R = 3$. だから $B > 50$ は示される.

かくて $2\widetilde{\sigma}(a) < a - 2$ が示されたので, $2\widetilde{\sigma}(a) = a - 1$ を満たすことはない.

3) $s \geq 3$. a が s 個の素因子 $p_1, p_2, \cdots, p_s$ を持ち, それらに応じて指数 $e_1, e_2, \cdots, e_s$ があり $Q_1 = p^{e_1}, \cdots, Q_s = p^{e_s}$ によって $a = Q_1 \cdots Q_s$ と書ける.

条件式 $2\widetilde{\sigma}(a) = a - 1$ を変形すると $\sigma(a) = 2^{s-1}(a-1)$. よって

$$\sigma(a) = \frac{(q_1Q_1 - 1)\cdots(q_sQ_s - 1)}{\overline{q_1}\cdots\overline{q_s}}$$

により

$$(q_1Q_1 - 1)\cdots(q_sQ_s - 1) = 2^{s-1}(Q_1\cdots Q_s - 1)\overline{q_1}\cdots\overline{q_s}.$$

5 不等式

$2 \leq q_1 < q_2 < \cdots < q_s, 2 \leq s$ とするとき不等式

$$(q_1Q_1 - 1)\cdots(q_sQ_s - 1) \leq 2^{s-1}(Q_1\cdots Q_s - 2)\overline{q_1}\cdots\overline{q_s}$$

が成り立つことを s に関しての数学的帰納法で証明しよう.

ただし, $s = 2, q_1 = 2$ のときは除外する.

$s = 2, q_1 > 2$ のときは不等式は成立している. したがって, $s = 3, q_1 = 2$ のとき最初に証明しておく.

目的の不等式は $2 = q_1 < q_2 < q_3$ のとき

$$(2Q_1 - 1)(q_2Q_2 - 1)(q_3Q_3 - 1) < 4(Q_1Q_2Q_3 - 2)\overline{q_2q_3} \tag{5}$$

である. $s = 2$ の場合の不等式

$$(q_2Q_2 - 1)(q_3Q_3 - 1) < 2(Q_2Q_3 - 2)\overline{q_2q_3}$$

に対して $2Q_1 - 1$ を掛ける.

$$(2Q_1 - 1)(q_2Q_2 - 1)(q_3Q_3 - 1) < 2(2Q_1 - 1)(Q_2Q_3 - 2)\overline{q_2q_3}$$

に対して

$$4(Q_1Q_2Q_3 - 2)\overline{q_2q_3} > 2(2Q_1 - 1)(Q_2Q_3 - 2)\overline{q_2q_3}$$

をしめせば良いのだが, 書き直すと

$$2(Q_1Q_2Q_3 - 2) > (2Q_1 - 1)(Q_2Q_3 - 2)$$

なので $\alpha = Q_1, \beta = Q_2Q_3$ とおけば $2(\alpha\beta - 2) > (2\alpha - 1)(\beta - 2)$. これは $4\alpha + \beta > 6$ なので当然成立.

次に $s-1$ の場合を仮定して s の場合を示す.

記号の簡単化のために $\widetilde{Q} = Q_1 \cdots Q_{s-1}, q^* = \overline{q_1} \cdots \overline{q_{s-1}}$ とおく.

帰納法の仮定によって次式は成立している.

$$(q_1Q_1 - 1) \cdots (q_{s-1}Q_{s-1} - 1) < 2^{s-2}(\widetilde{Q} - 2)q^*$$

なので $q_sQ_s - 1$ を掛けて

$$(q_1Q_1 - 1) \cdots (q_{s-1}Q_{s-1} - 1) \cdot (q_sQ_s - 1) < 2^{s-2}(\widetilde{Q} - 2)q^*(q_sQ_s - 1).$$

これから

$$2^{s-1}(Q_1 \cdots Q_s - 2)\overline{q_1} \cdots \overline{q_s} = 2^{s-1}(\widetilde{Q}Q_s - 2)q^*\overline{q_s}$$

によって

$$2^{s-1}(\widetilde{Q}Q_s - 2)q^*\overline{q_s} - 2^{s-2}(\widetilde{Q} - 2)q^*(q_sQ_s - 1) > 0$$

を示せばよい.

2^{s-2} と q^* をはずせば

$$2(\widetilde{Q}Q_s - 2)\overline{q_s} - (\widetilde{Q} - 2)(q_sQ_s - 1) > 0$$

となる.

$$\begin{aligned}
2(\widetilde{Q}Q_s - 2)\overline{q_s} - (\widetilde{Q} - 2)(q_sQ_s - 1) &= 2(\widetilde{Q}Q_s - 2)(q_s - 1) - (\widetilde{Q} - 2)(q_sQ_s - 1) \\
&= q_s(\widetilde{Q}Q_s + 2Q_s - 4) - 2\widetilde{Q}Q_s + 4 + \widetilde{Q} - 2 \\
&\geq 5(\widetilde{Q}Q_s + 2Q_s - 4) - 2\widetilde{Q}Q_s + \widetilde{Q} + 2 \\
&= 3\widetilde{Q}Q_s + 10(Q_s - 1) + \widetilde{Q} + 1 \\
&> 3 \cdot 6 \cdot 5 + 5 \cdot 3 + 7 \\
&> 100.
\end{aligned}$$

かくして陪関数についての有力な評価式が次のように得られた.

定理 1 $2 \leq q_1 < q_2 < \cdots < q_s, 2 \leq s$ とするとき $2\widetilde{\sigma}(a) < a - 2$ を満たす.

ただし, $s = 2, q_1 = 2$ は除外する.

これより次の定理が得られた.

定理 2 $2\widetilde{\sigma}(a) - a = -1$ を満たすとき $a = 2^e p$ と書ける. ここで $p = 2^{e+1} + 1$ は素数である.

このとき $e + 1$ は 2^m となる. $F_m = 2^{2^m} + 1$ はフェルマー数と呼ばれる.

5.1 $2\widetilde{\sigma}(a)-a=0$ の場合

表によると $2\widetilde{\sigma}(a)-a=0$ のとき $a=6,28,496$ であるがこれは偶数完全数の最初の 3 個である．
そこで $a=2^e p, 2^{e+1}-1=p(p:$ 素数$)$ としてみる．

$$\widetilde{\sigma}(a)=\widetilde{\sigma}(2^e p)=\frac{(2^{e+1}-1)(p+1)}{4}=\frac{p}{2}2^e=\frac{a}{2}$$

ゆえに $2\widetilde{\sigma}(a)-a=0$. よって偶数完全数 a は $2\widetilde{\sigma}(a)-a=0$ を満たすことがわかった. しかし驚くべきことにこの逆が成立する．

定理 3 $2\widetilde{\sigma}(a)-a=0$ を満たすとき $a=2^e p$ と書ける．ここで $p=2^{e+1}-1$ は素数である．

このとき a は偶数完全数になる．また $p=2^{e+1}-1$ を**メルセンヌ素数**という．

証明はフェルマー数の場合とほぼ同じであるが繰り返しをいとわず証明することにしよう．
少し一般化して次の結果を示す．

定理 4 $2\widetilde{\sigma}(a)-a=m$ を満たし $a=2^e q^f$ と書けるとする．このとき $\dfrac{(2m+1)(q-1)}{q^f-1}$ は整数である．
とくに, $m=-2,-1,0,1,2$ のとき $f=1$.

proof.
$a=2^e q^f$ なので,$Q=q^f$ とおけば

$$2\widetilde{\sigma}(a)=\frac{(2^{e+1}-1)(qQ-1)}{2\overline{q}}=2^e Q+m.$$

$N=2^{e+1}-1$ とおくと

$$(2^{e+1}-1)(qQ-1)=N(qQ-1)=2\overline{q}(2^e Q+m)=(N+1)\overline{q}Q+2m\overline{q}.$$

$N(Q-1)=2m(q-1)+(q-1)Q$ となるのでこれを変形した

$$N=(2m+1)\frac{q-1}{Q-1}+q-1$$

の右辺も整数なので $\frac{(2m+1)(q-1)}{q^f-1}$ は整数.
とくに, $m=-2,-1,0,1,2$ のとき $f=1$ になるので $q=Q$. $N=2m+q$.

- $m=0$ のとき $q=N=2^{e+1}-1$,
- $m=-1$ のとき $q=N=2^{e+1}+1$,
- $m=1$ のとき $q=N=2^{e+1}-3$.

結果として, a は偶数の完全数となる．
本来の完全数の定義は $\sigma(a)-2a=0$ を満たす自然数 a である．
$2\widetilde{\sigma}(a)=a$ は陪関数による完全数 (まがい) の定義と考えて良い．これを書き直すと $s=s(a)$ とおけば $\sigma(a)=2^{s-1}a$ となる．
とくに偶数の完全数となることが簡単に示されたのである．

6 素数の場合

$a=p$ が素数の場合, $\widetilde{\sigma}(p)=\frac{p+1}{2}$ なので $2\widetilde{\sigma}(p)-p=1$ が成り立つ. よって $p-\widetilde{\sigma}(p)=p-\frac{p+1}{2}=\frac{p-1}{2}$.

したがって $a-\widetilde{\sigma}(a)$ は 正の値はとるが, その値が 1 であることが素数の判定に使えない.

$y=\widetilde{\sigma}(a), x=a$ とおくとき, $y<x$ は成り立ち, $x=2^e$ ならば $x=y+0.5$.

7 擬素数

a が素数であれば $2\widetilde{\sigma}(a)-a=1$ が成り立つ. この逆は成り立つだろうか.

$2\widetilde{\sigma}(a)-a=1$ が成り立つ場合をパソコン君に調べてもらった.

表 5: $2\widetilde{\sigma}(a)-a=1$

a	factor	$\sigma(a)$	$\widetilde{\sigma}(a)$	$2\widetilde{\sigma}(a)-a$
2	[2]	3	1.5	1
3	[3]	4	2	1
5	[5]	6	3	1
7	[7]	8	4	1
11	[11]	12	6	1
13	[13]	14	7	1
17	[17]	18	9	1
19	[19]	20	10	1
20	$[2^2,5]$	42	10.5	1
23	[23]	24	12	1
29	[29]	30	15	1
31	[31]	32	16	1
37	[37]	38	19	1

解 a には素数以外に $20=2^2\times 5$ と $104=2^3\times 13$ が出てきた. これらは素数ではないが素数のふりをしている. そこでこれらを擬素数と呼んでも問題はないだろう. さらに擬素数を探すため $2^e\cdot p$ の形をした $2\widetilde{\sigma}(a)-a=1$ の解を探そう.

$a=2^e\cdot p, (p>2)$ とすると $2\widetilde{\sigma}(a)=(2^{e+1}-1)\times\frac{p+1}{2}$ になるので $2\widetilde{\sigma}(a)=a+1$ を用いて

$$(2^{e+1}-1)\cdot(p+1)=2^{e+1}p+2$$

$2^{e+1}p+2=(2^{e+1}-1)p+2+p$ としてから右辺に移項すれば $2^{e+1}-1=p+2$. よって $p=2^{e+1}-3$.

そこでパソコン君に $2^{e+1}-3$ が素数になる場合を探してもらった.

この表から意外にも多くの擬素数があることがわかった. とくに最初のうちは $e=2,3,4,5$ と最初の 4 つが出てくるところがすごい. これはフェルマー数の最初の 5 つが素数であることに匹敵するおもしろい事実である.

これらの擬素数はたぶん無限に存在する. しかし, このようなことは現代数学では証明できないに違いない. これも不思議なことである.

表 6: 擬素数の表

e	$2^{e+1}-3=p$	$2^e \times p = a$
2	$2^3-3=5$	$2^2 \times 5 = 20$
3	$2^4-3=13$	$2^3 \times 13 = 104$
4	$2^5-3=29$	$2^4 \times 29 = 464$
5	$2^6-3=61$	$2^5 \times 61 = 1952$
8	$2^9-3=509$	$2^8 \times 509 = 130304$
9	$2^{10}-3=1021$	$2^9 \times 1021 = 522752$
11	$2^{12}-3=4093$	$2^{11} \times 4093 = 8382464$
13	$2^{14}-3=16381$	$2^{13} \times 16381 = 134193152$

7.1 陪関数での素数判定

ここで $2^{e+1}-3$ が素数 p になる場合, $2^e \cdot p$ を指数 e の**擬素数**とよび $\mathbf{p}_e$ で記す.

定理 5 自然数 a が $2\tilde{\sigma}(a)=a+1$ を満たすとき $a=p$ *(p:素数)* または $a=2^e p$ と書ける. ここで $p=2^{e+1}-3$ は素数.

proof.
$s(a)=1$ とする. $a=p^e$ とするとき $2\tilde{\sigma}(a)=\frac{p^{e+1}-1}{p-1}$ になり, 仮定 $2\tilde{\sigma}(a)=a+1$ によれば $p=p^e$. となり結果として簡単な結果 $a=p$ に至った.

$s(a)=2$ とする. $a=p^e q^f$ とするとき,$q>p>2$ なら不等式によって矛盾.
$a=2^e q^f$ とすると $f=1, q=2^{e+1}-3$ とかける. $q=2^{e+1}-3$ は素数.

$s(a)\geq 3$ とすると不等式 $2\tilde{\sigma}(a)<a-2$ を使うと仮定 $2\tilde{\sigma}(a)=a-1$ と矛盾する.

このようにして, 陪関数を使う素数の判定法は擬素数も出てくるという意外な形で決着がついた.
$2\tilde{\sigma}(a)-a=0,-1,1$ の値に応じてメルセンヌ素数と フェルマー素数, 擬素数が出ることが証明できた.
これらの詳しい研究はこの後に回して, 視覚から研究のヒントをえるためグラフを描いてみよう.

7.2 $\widetilde{\sigma}(a)$ のグラフ

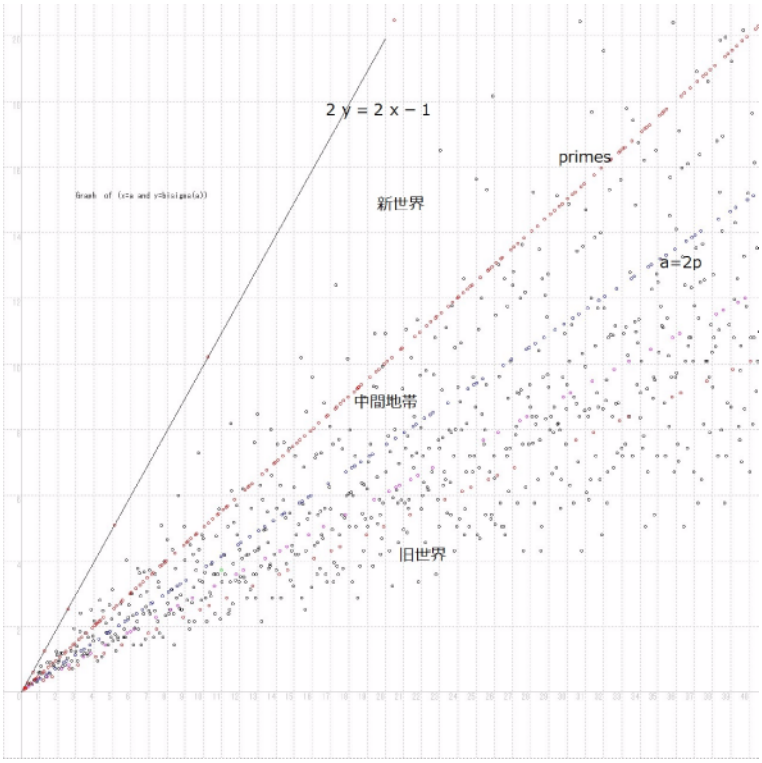

図 1: $\widetilde{\sigma}(a)$ のグラフ

$x = a, y = \widetilde{\sigma}(a)$ とおく.

$2y = 2x - 1$ が成り立つのは $a = 2^e$ のときのみでこれを除くと $y < x - \frac{1}{2}$ を満たす.

$a = p$ が素数なら $2\widetilde{\sigma}(a) = 1 + p = 1 + a$ なので $y = \frac{x+1}{2}$ の上にある.

$y \leq x - \frac{1}{2}, y \geq \frac{x+1}{2}$ の定める領域は, これまでの $b = \sigma(a)$ や $b = \varphi(a)$, さらに $b = \widetilde{\varphi}(a)$ などでは無かった所なので**新世界**と命名しよう.

$y \leq \frac{x-2}{2}$ の定める領域を**旧世界**, その間を**中間地帯**と命名する.

中間地帯は $y < \frac{x+1}{2}$ と $y \geq \frac{x-2}{2}$ で定められた帯状の領域で $a = 2^e q^f, e > 2, f > 0$ と書ける.

8　$\widetilde{\sigma}(a)$ の余関数

$\widetilde{\sigma}(a)$ のグラフから予想できる結果は $a > \widetilde{\sigma}(a)$ である．数表の結果からは $a = 2^e$ のときに限って $a - \widetilde{\sigma}(a) = \frac{1}{2}$ でありこのときが $a - \widetilde{\sigma}(a)$ の最小値になりそうである．最初にこのことを証明しよう．

記号を整理して研究に役立てるため $a - \widetilde{\sigma}(a)$ を $\widetilde{\sigma}(a)$ の余関数ということにして記号 $co\widetilde{\sigma}(a)$ を用いる．すなわち $co\widetilde{\sigma}(a) = a - \widetilde{\sigma}(a)$ と定める．

9 余関数の p^e での値

$a=p$ が素数なら $\widetilde{\sigma}(a)=\frac{1+p}{2}$ なので $co\widetilde{\sigma}(a)=\frac{p-1}{2}\geq\frac{1}{2}$.
$p=2$ ならば $co\widetilde{\sigma}(p)=\frac{1}{2}$.
$p=3$ ならば $co\widetilde{\sigma}(p)=\frac{3-1}{2}=1$.
$p\geq 5$ ならば $co\widetilde{\sigma}(p)=\frac{p-1}{2}\geq 2$.
$a=p^e$. ここで p が素数, かつ $e>1$ なら $co\widetilde{\sigma}(a)=\frac{p^e(p-2)+1}{2(p-1)}$ なので
$p=2$ ならば $co\widetilde{\sigma}(2^e)=\frac{1}{2}$.
$p=3$ ならば $co\widetilde{\sigma}(3^e)=\frac{3^e+1}{4}\geq 4$.
$p\geq 5$ ならば $co\widetilde{\sigma}(p)=\frac{p^e(p-2)+1}{2(p-1)}\geq\frac{5^e\times 3+1}{8}>8$.
これを用いて $co\widetilde{\sigma}(a)$ の値を小さい方から決定しよう.

a を素因数分解して $a=Q_1Q_2\cdots Q_s$ と書く. ここで各 Q_i は素数 p_i の累乗, その指数は e_i とおく. p_i 等は相異なり, $1<s, p_1<\cdots<p_s$ と仮定しておく.

$R_i=\widetilde{\sigma}(Q_i), \theta_i=co\widetilde{\sigma}(Q_i)$ とおけば $Q_i=\theta_i+R_i$.

$co\widetilde{\sigma}(a)=a=Q_1Q_2\cdots Q_s-R_1R_2\cdots R_s=(R_1+\theta_1)(R_2+\theta_2)\cdots(R_s+\theta_s)-R_1R_2\cdots R_s\geq(R_1+\theta_1)(R_2+\theta_2)-R_1R_2=R_1\theta_2+R_2\theta_1+\theta_1\theta_2$.

ここで $p_1=2$ なら $R_1=\frac{2^{e+1}}{2}\geq\frac{3}{2}, \theta_1\geq\frac{1}{2}, R_2>1, \theta_2\geq 1$. 故に $co\widetilde{\sigma}(a)>1$.

表 7: $co\widetilde{\sigma}(a)$ の数表

a	factor	$\sigma(a)$	$\widetilde{\sigma}(a)$	$co\widetilde{\sigma}(a)$
2	[2]	3	1.5	0.5
4	$[2^2]$	7	3.5	0.5
8	$[2^3]$	15	7.5	0.5
16	$[2^4]$	31	15.5	0.5
32	$[2^5]$	63	31.5	0.5
64	$[2^6]$	127	63.5	0.5
128	$[2^7]$	255	127.5	0.5
256	$[2^8]$	511	255.5	0.5
512	$[2^9]$	1023	511.5	0.5
3	[3]	4	2	1
5	[5]	6	3	2
9	$[3^2]$	13	6.5	2.5
6	[2, 3]	12	3	3
7	[7]	8	4	3
11	[11]	12	6	5
12	$[2^2, 3]$	28	7	5
10	[2, 5]	18	4.5	5.5

課題 $a\neq 2^e$ のとき

$$co\widetilde{\sigma}(a)>\sqrt{a}.$$

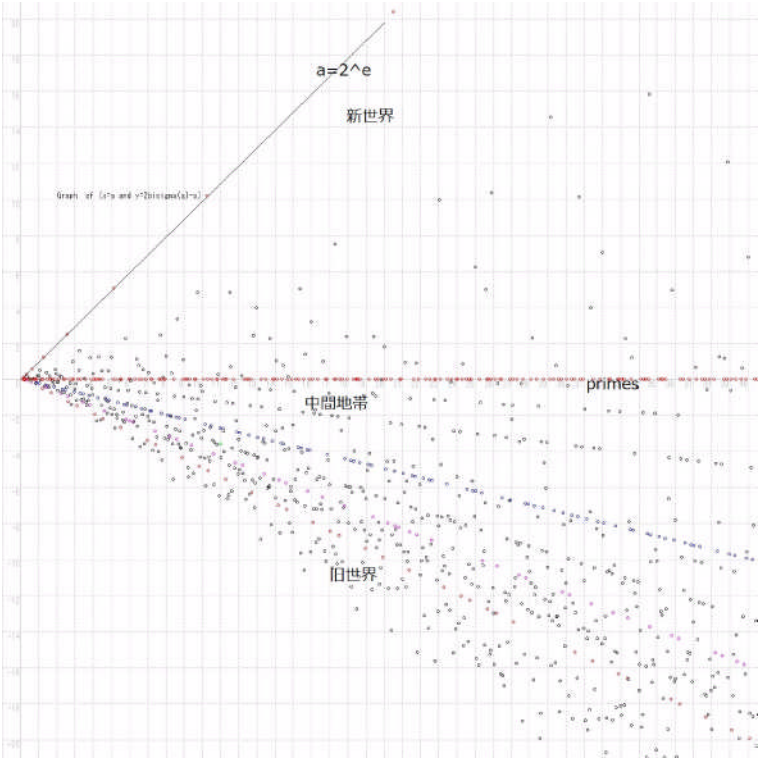

図 2: 余関数のグラフ

10　陪関数のグラフ

11　$a = mp$ 問題

簡単な場合で練習しよう．

$a = 2p(p:$ 奇数$)$ とするとき $2\widetilde{\sigma}(a) = 2\widetilde{\sigma}(2p) = 3\widetilde{\sigma}(p) = \frac{3p+3}{2} = \frac{3a+6}{4}$ によって

$$8\widetilde{\sigma}(a) = 3a + 6.$$

$a < 200000$ の範囲まで調べても $2p$(通常解) 以外の解は 180 だけである．

12　$a = qp$ 問題

q を p と異なる素数として $a = qp$ の場合を調べる．これまでの経験によればこの場合は最も易しい場合であり非通常解はめったに出ない．ユークリッド陪関数ではどうなるだろうか．

便宜上 $\widetilde{q} = q + 1$ とおく．

$2\widetilde{\sigma}(a) = 2\widetilde{\sigma}(qp) = \widetilde{q}\widetilde{\sigma}(p) = \widetilde{q}\frac{p+1}{2}$ と変形すると

$$4q\widetilde{\sigma}(a) = \widetilde{q}(a + q). \tag{6}$$

これが $a = qp$ 問題のユークリッド陪関数での方程式でこれを解 a について解くのが課題である．最初にパソコンでやってみる．最初に $q = 3$ で確認してみる．

擬素数を復習しておく．

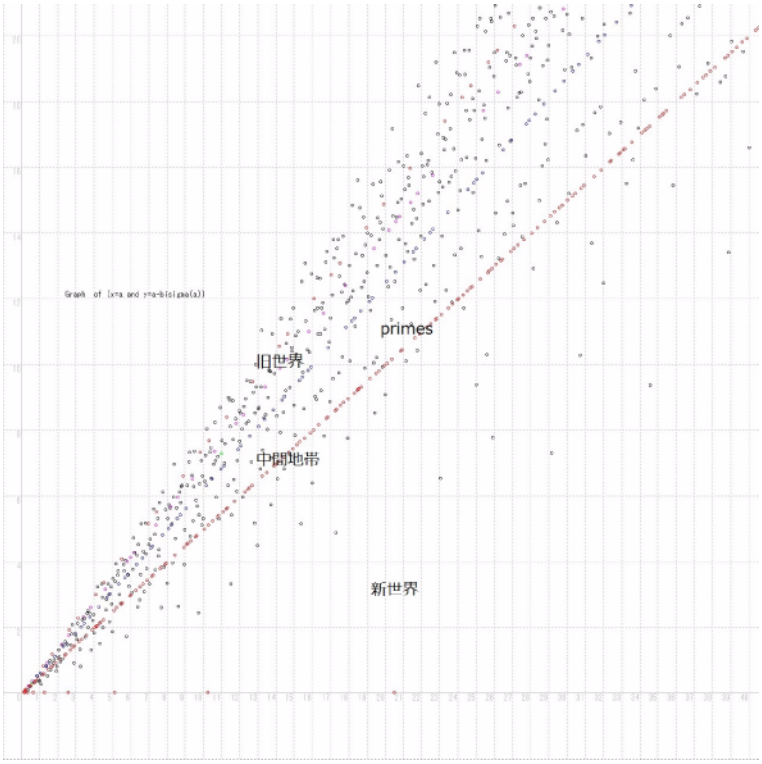

図 3: 2bi

- $2^2 \times 5 = 20 = \mathbf{p}_2$
- $2^3 \times 13 = 104 = \mathbf{p}_3$
- $2^4 \times 29 = 464 = \mathbf{p}_4$
- $2^5 \times 61 = 1952 = \mathbf{p}_5$

非通常解 60$= [2^2, 3, 5]$ も $3 \times \mathbf{p}_2$ と書ける.

ついで $q = 5$ のときは非通常解だけを記録してみた. $a < 10000$ 以下では次の 4 個だけである. 後半の 3 個は 擬素数の 5 倍であり, これらの解も擬素数からできた非通常解である. エイリアン解とまでは呼べない.

最初の非通常解は 150 で $5 \times \mathbf{p}_2 = 100$ とは異なる. 5 倍の 5 と $2^2 \times 5 = 20 = \mathbf{p}_2$ が混戦して数学の方が混乱しているようだ.

13 と $2^3 \times 13 = 104 = \mathbf{p}_3$ に出ている 13 が混戦してこれに対応する非通常解が消滅した.

23 の場合は $a < 100000$ まで非通常解を求めた.

$a = qp$ 問題は最も簡単な場合で, $\sigma(a)$ なら非通常解は $a = q^3$ だけで, これらしか無いことは証明できている.

オイラー関数, 陪関数の場合は $a = qp$ 問題に非通常解は存在しない. 美しい調和の世界とも言えるが, 平和すぎてつまらないとも思われる.

来たれ, 荒ぶるエイリアンたち. 私はこのように密かなつぶやき声を発した.

表 8:

a	factor	$\widetilde{\sigma}(a)$
2	[2]	1.5
6	[2,3]	3
10	[2,5]	4.5
14	[2,7]	6
22	[2,11]	9
26	[2,13]	10.5
34	[2,17]	13.5
38	[2,19]	15
46	[2,23]	18
58	[2,29]	22.5
62	[2,31]	24
74	[2,37]	28.5
82	[2,41]	31.5
86	[2,43]	33
94	[2,47]	36
106	[2,53]	40.5
118	[2,59]	45
122	[2,61]	46.5
134	[2,67]	51
142	[2,71]	54
146	[2,73]	55.5
158	[2,79]	60
166	[2,83]	63
178	[2,89]	67.5
180	$[2^2, 3^2, 5]$	68.25

しかし, $a = q^{\varepsilon}p$ 問題ではエイリアン解がでてきてそれらは, エイリアンの卵からできている. これは良い. 現象の解明は進んでも証明が追いつかない.

$\widetilde{\sigma}(a)$ の場合は擬素数が堂々と出てくる. 本当のエイリアンは少なく, 飼い慣らせる擬素数解が多いのは不思議なことだ. しかし, 証明がほとんどできないことを告白しておく.

パソコンでの探索を精密化して広げれば思いがけないエイリアンにぶつかる可能性はある.

表 9: $a = 3p$ 問題の解

a	素因数分解
3	[3]
6	[2,3]
15	[3,5]
21	[3,7]
33	[3,11]
39	[3,13]
51	[3,17]
57	[3,19]
60	$[2^2, 3, 5] = 3 \times \mathbf{p}_2$
69	[3,23]
87	[3,29]
93	[3,31]
111	[3,37]

表 10: $a = 5p$ 問題の非通常解

a	素因数分解
150	$[2, 3, 5^2]$
520	$[2^3, 5, 13] = 5 \times \mathbf{p}_3$
2320	$[2^4, 5, 29] = 5 \times \mathbf{p}_4$
9760	$[2^5, 5, 61] = 5 \times \mathbf{p}_5$

表 11: $a = 7p$ 問題の非通常解

a	素因数分解
140	$[2^2, 5, 7] = 7 \times \mathbf{p}_2$
728	$[2^3, 7, 13] = 7 \times \mathbf{p}_3$
3248	$[2^4, 7, 29] = 7 \times \mathbf{p}_4$
13664	$[2^5, 7, 61] = 7 \times \mathbf{p}_5$

表 12: $a = 11p$ 問題の非通常解

a	素因数分解
220	$[2^2, 5, 11] = 11 \times \mathbf{p}_2$
1144	$[2^3, 11, 13] = 11 \times \mathbf{p}_3$
5104	$[2^4, 11, 29] = 11 \times \mathbf{p}_4$

表 13: $a = 13p$ 問題の非通常解

a	素因数分解
260	$[2^2, 5, 13] = 13 \times \mathbf{p}_2$
6032	$[2^4, 13, 29] = 13 \times \mathbf{p}_4$

表 14: $a = 17p$ 問題の非通常解

a	素因数分解
340	$[2^2, 5, 17] = 17 \times \mathbf{p}_2$
1768	$[2^3, 13, 17] = 17 \times \mathbf{p}_3$
7888	$[2^4, 17, 29] = 17 \times \mathbf{p}_4$

表 15: $a = 19p$ 問題の非通常解

a	素因数分解
380	$[2^2, 5, 19] = 19 \times \mathbf{p}_2$
1976	$[2^3, 13, 19] = 19 \times \mathbf{p}_3$
8816	$[2^4, 19, 29] = 19 \times \mathbf{p}_4$

表 16: $a = 23p$ 問題の非通常解

a	素因数分解
460	$[2^2, 5, 23] = 23 \times \mathbf{p}_2$
2392	$[2^3, 13, 23] = 23 \times \mathbf{p}_3$
10672	$[2^4, 23, 29] = 23 \times \mathbf{p}_4$
44896	$[2^5, 23, 61] = 23 \times \mathbf{p}_5$

12.1 $2\widetilde{\sigma}(a) - a$ の平行移動

$2\widetilde{\sigma}(a) - a$ の平行移動問題を考えてみよう.

表 17: $2\widetilde{\sigma}(a) - a = 0, -1, -2, -3$

a	factor	$\sigma(a)$	$\widetilde{\sigma}(a)$	$2\widetilde{\sigma}(a) - a$
15	$[3, 5]$	24	6	-3
52	$[2^2, 13]$	98	24.5	-3
592	$[2^4, 37]$	1178	294.5	-3
14	$[2, 7]$	24	6	-2
44	$[2^2, 11]$	84	21	-2
152	$[2^3, 19]$	300	75	-2
10	$[2, 5]$	18	4.5	-1
136	$[2^3, 17]$	270	67.5	-1
6	$[2, 3]$	12	3	0
28	$[2^2, 7]$	56	14	0
496	$[2^4, 31]$	992	248	0

表 18: $2\widetilde{\sigma}(a) - a = 2, 3, 4$

a	factor	$\sigma(a)$	$\widetilde{\sigma}(a)$	$2\widetilde{\sigma}(a) - a$
12	$[2^2, 3]$	28	7	2
88	$[2^3, 11]$	180	45	2
4	$[2^2]$	7	3.5	3
9	$[3^2]$	13	6.5	4
56	$[2^3, 7]$	120	30	4
368	$[2^4, 23]$	744	186	4

13　ユークリッドとオイラー

$a > 1$ のとき $\sigma(a) - \varphi(a) \geq 2$ が成り立ち, 等号の成立は a : 素数の場合だけである.
これは

$$\sigma(a) - a \geq 1, a - \varphi(a) \geq 1$$

を左右の不等式を足せば得られる. 等号の成立は a : 素数の場合だけなことも明らかであろう.

表 19: $\sigma(a) - \varphi(a)$ の順に

a	factor	$\sigma - \varphi$	$\tilde{\sigma}(a) - \tilde{\varphi}(a)$
4	$[2^2]$	5	2.5
9	$[3^2]$	7	3.5
6	$[2, 3]$	10	2.5
8	$[2^3]$	11	5.5
25	$[5^2]$	11	5.5
10	$[2, 5]$	14	3.5
49	$[7^2]$	15	7.5
15	$[3, 5]$	16	4
14	$[2, 7]$	18	4.5
21	$[3, 7]$	20	5
27	$[3^3]$	22	11
16	$[2^4]$	23	11.5
121	$[11^2]$	23	11.5
12	$[2^2, 3]$	24	6
35	$[5, 7]$	24	6
22	$[2, 11]$	26	6.5
169	$[13^2]$	27	13.5
33	$[3, 11]$	28	7
26	$[2, 13]$	30	7.5

14　$a = mp$ 問題

一般に $a = mp$ とおきここで p は素数 m は p で割れない自然数とする.

$$\varphi(a) = \varphi(m)\varphi(p) = \varphi(m)(p-1) = \varphi(m)(\frac{a}{m} - 1)$$

を変形して

$$\frac{\varphi(a)}{\varphi(m)} = \frac{a}{m} - 1 \tag{7}$$

式 (1) から 式 (7) を引くと

$$\frac{\sigma(a)}{\sigma(m)} - \frac{\varphi(a)}{\varphi(m)} = 2. \tag{8}$$

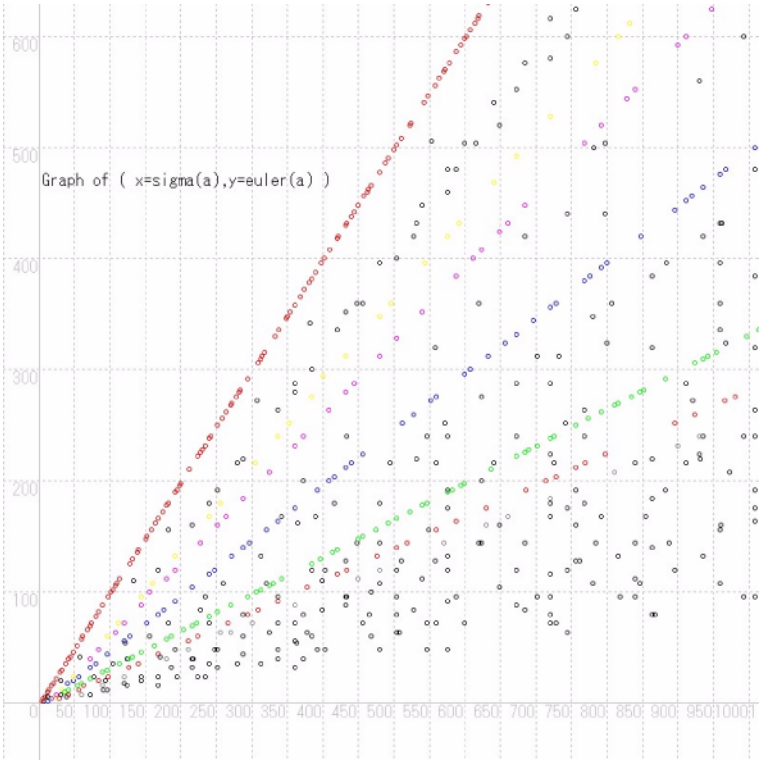

図 4:

これが $\sigma(a)$ と $\varphi(a)$ についての $a = mp$ 問題の基本方程式である.

とりあえず $m = q$: 素数, の場合に解を求めよう. すると

$$(q-1)\sigma(a) - (q+1)\varphi(a) = 2(q^2-1)$$

と思いの外きれいな式になった.

$q = 2$ のときは

$$\sigma(a)3\varphi(a) = 6 \tag{9}$$

$q = 3$ のときは

$$\sigma(a) - 2\varphi(a) = 8 \tag{10}$$

エクセルで表を作ると次のようになる.

$45 = 3^2 \times 5$ がエイリアン解

さらに $m = 5, 7$ のとき $a = mp$ 問題の解はすべて mp と書ける通常解だけだとパソコン君は言う.

14.1 $a = 3p$ 問題の解

$s(a) = 2$ を仮定して考える. このとき $a = p^e q^f$ と表せる. ここで p, q は素数で $p < q$ を満たすとする.

表 20: $a = 2p$ 問題の解

a	factor	$\sigma(a)$
6	$[2, 3]$	12
10	$[2, 5]$	18
14	$[2, 7]$	24
22	$[2, 11]$	36
26	$[2, 13]$	42
34	$[2, 17]$	54
38	$[2, 19]$	60
45	$[3^2, 5]$	(エイリアン解) 78
46	$[2, 23]$	72
58	$[2, 29]$	90
62	$[2, 31]$	96
74	$[2, 37]$	114
82	$[2, 41]$	126
86	$[2, 43]$	132
94	$[2, 47]$	144

表 21: $a = 2p$ 問題の解

a	factor	$\sigma(a) = 2$
6	$[2, 3]$	12
15	$[3, 5]$	24
21	$[3, 7]$	32
33	$[3, 11]$	48
39	$[3, 13]$	56
51	$[3, 17]$	72
57	$[3, 19]$	80
69	$[3, 23]$	96
87	$[3, 29]$	120
93	$[3, 31]$	128
111	$[3, 37]$	152
123	$[3, 41]$	168
129	$[3, 43]$	176
141	$[3, 47]$	192
159	$[3, 53]$	216
175	$[5^2, 7]$	エイリアン解 248
177	$[3, 59]$	240
183	$[3, 61]$	248

$\overline{p}=p-1, \overline{q}=q-1$ とすると
とかけるので

$$(p^{e+1}-1)(q^{f+1}-1)=2p^e q^f(\overline{p}\cdot\overline{q})^2+8\overline{p}\cdot\overline{q}. \tag{11}$$

$X=p^e, Y=q^f$ とおいて書き直すと

$$(p^2X-1)(q^2Y-1)=2(\overline{pq})^2XY+8\overline{p}\cdot\overline{q}.$$

これより $A=q^2(p^2X-1)-2(\overline{pq})^2X$ とおくと $A=(p^2q^2-2(\overline{pq})^2)X-q^2$ と書きなおせる．さらに $B=p^2X-1+8\overline{p}\cdot\overline{q}$ とおけば $AY=B$ となる．

$R=p^2q^2-2(\overline{pq})^2$ とおけば $A=RX-q^2$,

$$\begin{aligned}R&=p^2q^2-2(\overline{p}\,\overline{q})^2\\&=p^2q^2-2(p-1)^2\overline{q}^2\\&=Cp^2+(4p-2)\overline{q}^2.\end{aligned}$$

ここで, $C=q^2-2\overline{q}^2=q(4-q)-2$.

14.2 $p=2$ の場合

i. $p=2$.

- $R=4C+6\overline{q}^2=4q^2-2\overline{q}^2=2(q^2+2q-1)$,
- $B=4X-1+8\overline{q}$
- $A=RX-q^2, AY=B$.

によって

$$B=4X-1+8\overline{q}=AY\geq A=RX-q^2=2(q^2+2q-1)X-q^2.$$

$q\geq 3, X\geq 1$ によって

$$q^2-1+8\overline{q}\geq(2q^2+4q-6)X\geq 2q^2+4q-6.$$

結局 2 次不等式に至る．

$q^2-1+8\overline{q}\geq 2q^2+4q-6$ によって $4q-2\geq q^2$. これより $q=3$ になる．

$a=3\times 2=6$ が最小の解.

14.3 $p = 3$ の場合

ii. $p = 3$.

- $C = q^2 - 2\overline{q}^2$,
- $R = 9C + 10\overline{q}^2 = 9q^2 - 8\overline{q}^2 = q^2 + 16q - 8$,
- $B = 9X - 1 + 16\overline{q} = 9X + 16q - 17$,
- $A = RX - q^2, AY = B$.

によって

$$B = 9X - 1 + 16\overline{q} = 9X + 16q - 17 = AY \geq A = RX - q^2.$$

これより

$$q^2 - 1 + 16\overline{q} \geq (R - 9)X = (q^2 + 16q - 17)X.$$

ゆえに $X \leq 1$ がでるので $X = 1$. これから

$$B = 9X - 1 + 16\overline{q} = 16q - 8, A = RX - q^2 = R - q^2 = 16q - 8.$$

一方 $AY = B$ だったから $Y = 1$. $a = 3q$

14.4 $p = 5$ の場合

iii. $p = 5$.

- $R = 25C + 18\overline{q}^2 = 25q^2 - 32\overline{q}^2 = -7q^2 + 64q - 32$,
- $B = 25X - 1 + 32\overline{q} = 25X + 32q - 33$,
- $A = RX - q^2, AY = B$.

$C = q^2 - 2\overline{q}^2$ によると $R = 25C + 18\overline{q}^2 = 25q^2 - 32\overline{q}^2$.
$AY = B > 0, A = RX - q^2$ から $R2 = 5q^2 - 32\overline{q}^2 > 0$.
それゆえ. $\sqrt{\frac{25}{32}} > \frac{q-1}{q} = 1 - \frac{1}{q}$.
無理式の計算によって $q \leq \frac{32+20\sqrt{2}}{7}$. かくして $q \leq 9$. q は 5 より大きい素数なので $q = 7$.
ふたたび計算して $R = 73, A = 73X - 49, B = 25X + 191$.
$AY = (73X - 49)Y = 25X + 191 \geq 73X - 49$ によれば $48X \leq 49 + 191 = 240$. $X \leq 5$.
$X = 5^{e-1}$ により $e = 2, 1$.
$Y = \frac{25X+191}{73X-49}$, であるが $X = 1$ のとき $Y = 9$. しかしこれは $Y = 7^{f-1}$ に矛盾する.
以上によって $X = 5$ のとき $X = 5, a = 5^2 \times 7$. これがエイリアン解.

14.5 $p \geq 7$ の場合

iv. $p \geq 7$.
$C = q^2 - 2\overline{q}^2, R = Cp^2 + (4p-2)\overline{q}^2$ によって

$$R = (q^2 - 2\overline{q}^2)p^2 + (4p-2)\overline{q}^2 = p^2q^2 + (-2p^2 + 4p - 2)\overline{q}^2 > 0.$$

$p^2q^2 > (2p^2 - 4p + 2)\overline{q}^2$ により

$$\frac{p^2}{2p^2 - 4p + 2} > (1 - \frac{1}{q})^2.$$

さらに整理して

$$\frac{1}{q} > 1 - \frac{p}{\sqrt{2p^2 - 4p + 2}}.$$

この右辺の式の逆数を q_0 と書くと $q < q_0$. q_0 を $p = 5, 7, 11, 13, 17, 19$ について計算する.

表 22: q_0 の評価

p	limit of q
5	8.61203875
7	5.712911723
11	4.500803694
13	4.27409509
17	4.020924166
19	3.94306982

これによると $p \geq 7$ なら $q \leq 5$. 矛盾である.