数学の研究を始めよう 2016/dec
君はオイラー 完全数をみたか ; 前編
新しい完全数の世界

飯高 茂

平成 28 年 8 月 17 日

1　究極の完全数とその平行移動

本編の目的はオイラー 完全数を新しく導入しその基本定理を確立することである。その前に準備として究極の完全数の定義を復習する.

自然数 a の約数の和を $\sigma(a)$ と書きこれを a の関数と見て ユークリッド関数という.

たとえば, $a = 6$ ならその約数は, $1, 2, 3, 6$ なので $\sigma(a) = 12$ となり $\sigma(a) = 2a$ を満たす.

$\sigma(a) = 2a$ を満たす数を完全数というだから 6 は完全数.

数学の好きな小学生, 高校生, 大学生それから熟年世代にいたるまで完全数は人気のあるテーマである.

「496 が完全数であることを示せ.」 と言われてできる大学生は少ないと思う.

一方, プロの数学者は完全数を歓迎しない. たとえば A.Weil は『数論　歴史からのアプローチ』 足立恒雄・三宅克哉訳、日本評論社、1987 年。p6, 第 1 章 § III, で次のように完全数を軽んじる発言をしている.

ギリシャのみならずそれ以前においても, 完全性という観念が, そのすべての約数の和が自分自身と一致するような整数に結び付けられていた. ユークリッドの数論に関する巻の最後の定理において $2^n(2^{n+1} - 1)$ はその第二因子が素数であるときには完全数であることが主張されている; 著者自身も, これがその数論的な諸結果の中の白眉であると見ているように思える.　この題目とそれに伴って現れるいくつかのものは, 後世の著作にも散発的に顔を出す; 恐らくこれらの概念に付された呼称が特別な興味を惹くのだろう. フェルマの同時代の人達、メルセンヌやフェルニクル、それにフェルマ自身も結構面白がっており、彼の初期の研究においてはそれなりの位置を占めていたことも事実である.(中略) しかし理論的にはほとんど意味のないものであり, このような歴史的事実がなければ, ここに取り上げる必要もなかったろう.

私は大学を退職後, 一般の市民を対象に「数学の研究をはじめよう」をスローガンにして公開の数学研究講座を開いている. そこでも完全数に関連した話しは歓迎される.

さて P を素数とし固定して考える. 与えられた整数 m に関して $\sigma(P^e)+m$ が素数 q のとき $a=P^eq$ を m だけ平行移動した底が P の (狭義の) 究極の完全数と呼ぶ.

これは次式を満たす.

$$\overline{P}\sigma(a)-Pa=(P-2)\mathrm{Maxp}(a)-m(P-1). \tag{1}$$

$\mathrm{Maxp}(a)$ は a の最大素因子を指している.

これを m だけ平行移動した底が P の狭義の究極の完全数の方程式という.

またこの式を満たす a を m だけ平行移動した底が P の (広義の) 究極の完全数と呼ぶ.

$P=2$ のとき $\mathrm{Maxp}(a)$ が消えて方程式は

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

となる.

$m=0$ のときにあてはめると $\sigma(a)-2a=0$ の解 (すなわち広義の完全数) は狭義の完全数になるか, という古来からある数学界の難問になる.

2 完全数の数表

ここで古典的な 完全数の数表を紹介する.

表 1: 完全数の場合

$e \bmod 4$	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 (1456)	6
0	16	17	$2^{16}*131071$	8589869056 (Cataldi,1588)	6
2	18	19	$2^{18}*524287$	137438691328 (Cataldi,1588)	8
2	30	31	$2^{30}*2147483647$	A (Euler, 1772)	8

$A=2305843008139952128$

完全数の定義がなされ 4 つの完全数 (6,28,496,8128) が発見されたのは紀元前のことであった. それから 1500 年以上かかって, 1456 年に第 5 の完全数が発見された. さらに 100 年以上の歳月を経て第 6,7 の完全数が発見され, さらに 100 年以上かかって第 8 の完全数がオイラー (1772 年) によって発見さた.

完全数の末尾の数は 6 または 8 であることは古来から注目されていた.

3　オイラー関数と ユークリッド関数

$m=2$ のときは $\sigma(a)-2a=-2$ の解は $a=2^eq, (q=2^{e+1}+1$:フェルマ素数) と書けるか, という問題になりこれも難問で未だに解けない.

$m=4$ のときは 広義の完全数で狭義の完全数にならないものはたくさんある. このとき 広義の完全数は $a=2^eq$ または $a=2^eqr$ (ここで q,r : 素数) と表せるかという問題がありこれも全く解けない.

そこでいささかセコイのだが, 解けそうな問題を別に考える.

自然数 a と互いに素で a 未満の自然数の個数を $\varphi(a)$ で示しこれをオイラー関数という.

オイラー関数とユークリッド関数とはその本質において親和性がある. たとえば, 両者は乗法をもつ.

乗法性

a,b が互いに素な整数なら, $\varphi(ab)=\varphi(a)\varphi(b)$, $\sigma(ab)=\sigma(a)\sigma(b)$.

素数判定法

$a>1$ のとき,$a-\varphi(a)=1$ は a が素数になる必要十分条件. そこでオイラー余関数 $\mathrm{co}\varphi(a)=a-\varphi(a)$ を導入する.

$a>1$ のとき,$a-\sigma(a)=-1$ は a が素数になる必要十分条件. そこでユークリッド余関数 $\mathrm{co}\sigma(a)=\sigma(a)-a$ を導入する.

完全数

$2a=\sigma(a)$ のとき a を 完全数という.

$a=2\varphi(a)$ のとき a は 2 の累乗. 逆も正しい.

a は 2 の累乗のとき $2a=\sigma(a)+1$. しかしこの逆が正しいかどうかは不明.

3.1　ドグマ

次の大いなるなるドグマは信じるに値すると思う.

ドグマ

$\sigma(a)$ を用いた式や予想は $\varphi(a)$ を用いて適当に修正するとより解きやすい問題ができる.

1 つだけ例をあげる.

3.2　$a=2p$ 問題

p : 奇素数とするとき $a=2p$ は $2\sigma(a)=3a+6$ を満たす. 逆に方程式 $2\sigma(a)=3a+6$ を満たす a は $2p$ または 8.

これのオイラー関数版は次の通り.

p : 奇素数とするとき $a = 2p$ は $2\varphi(a) = a - 2$ を満たす. 逆に方程式 $2\varphi(a) = a - 2$ を満たす a は $a = 2p$.

$\sigma(a)$ のときに出てきた例外の 8 が $\varphi(a)$ のときは消えてしまう.

これは簡単な問題だが $a = 6p$ 問題を同じように考える $\sigma(a)$ で定式化するとこの問題はきわめて難しい. 古典的な奇数完全数問題よりも難しくさらに興味深い問題と思われる. ここで完全数 6 が出たことに数学における深淵を感じる.

しかし $a = 6p$ 問題を $\varphi(a)$ で定式化するときわめて簡単に解ける.

4 オイラー φ 完全数

ドグマにしたがって, ユークリッド関数の代わりにオイラー関数を使って完全数と類似した概念を定義しよう.

オイラー関数のとき $\varphi(P^e), (e > 1)$ は合成数になるので完全数の定義をそのままは使えない. そこで, 1 を加えて $\varphi(P^e) + 1$ が素数 q になるとき $a = P^e q$ をもって P を底とする (狭義) のオイラー φ **完全数**と定義する.

本文の題は「君はオイラー完全数をみたか」であるがこれは著者が細々と研究を続けてきて「書泉グランデの公開講座」で数学好きの方たちに話しただけで, 一般に公表するのは今回がはじめてである. 「オイラー完全数なんて聞いたことがない」というのが一般の方のご意見であろう.

さて最も簡単な $P = 2$ の場合を定義に沿ってパソコンで計算してみる.

表 2: 2 を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	12	$2^2 * 3$	4
3	40	$2^3 * 5$	16
5	544	$2^5 * 17$	256
9	131584	$2^9 * 257$	65536
17	8590065664	$2^{17} * 65537$	4294967296

この結果をみると,a の素数部分には 3,5,17,257,65537 のようにフェルマ素数が並んでいるではないか. これには最初びっくりした. そして心が躍った. 冷静になって, 定義に戻り考える:

$q = \varphi(P^e) + 1 = 2^{e-1} + 1$ が素数という条件なので $e - 1 = 2^m$ と書けて結果として q がフェルマ素数になるのは当然である.

完全数の場合のようにこれら q と a の末尾の数をみてみよう. 10 を法としてみればよい.

$e > 4$ なら $e \equiv 1 \mod 4; q \equiv 7; a \equiv 4$; $\varphi(a) \equiv 6 \mod 10$ が成り立つ.

5 つのフェルマー素数に応じて 5 つの φ 完全数ができた. これらはフェルマ素数にちなんでフェルマ φ 完全数 と呼ぶ方がよいかもしれない. 後で一般化されたオイラー φ 完全数が導入されるであろう.

5 φ 弱完全数

$k > 0$ に関して,$e = 1 + 4k, q_k = 2^{4k} + 1, a_k = 2^e q_k$ とおき,
a_k を 2 を底とする φ 弱完全数 という.

表 3: 2 を底とする φ 弱完全数

$e = 1 + 4k$	q_k	factor	a
5	17	17	544
9	257	257	131584
13	4097	$17 * 241$	33562624
17	65537	65537	8590065664
21	1048577	$17 * 61681$	2199025352704
25	16777217	$97 * 257 * 673$	562949986975744
29	268435457	$17 * 15790321$	144115188612726784
33	4294967297	$641 * 6700417$	36893488156009037824
37	68719476737	$17 * 241 * 433 * 38737$	9444732965876729380864

これから次がわかる.
φ 弱完全数 の末尾 2 桁の数は 44,84,24,64,04 が繰り返される
$q = 2^{4k} + 1$ の末尾 2 桁の数は 17,57,97,37,77 が繰り返される

5.1 3 を底とするとき

$P = 3$ の場合も計算してみる.

$$q = 2 * 3^{e-1} + 1, a = 3^e q.$$

表 4: $P = 3$ を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	63	$3^2 * 7$	36
3	513	$3^3 * 19$	324
5	39609	$3^5 * 163$	26244
6	355023	$3^6 * 487$	236196
7	3190833	$3^7 * 1459$	2125764
10	2324581983	$3^{10} * 39367$	1549681956
17	11118121262251209	$3^{17} * 86093443$	7412080755407364
18	100063090585419903	$3^{18} * 258280327$	66708726798666276

定義には自然に出てくる $q = 2 * 3^{e-1} + 1$: 素数, という条件は今まで扱ったことがない.
ここで登場する素数 $7, 19, 163, 487, 1459, \cdots$ は比較的数が多く興味深いものである.
花束を持って彼らまたは 彼女ら (素数を擬人化して呼んでいる) を歓迎しよう. [1]

- $e \equiv 2 \bmod 4$ のとき $q \equiv 7, a \equiv 3 \bmod 10$.
- $e \equiv 1 \bmod 4$ のとき $q \equiv 3, a \equiv 9 \bmod 10$.
- $e \equiv 3 \bmod 4$ のとき $q \equiv 9, a \equiv 3 \bmod 10$.

紙数の関係で証明は略する.

[1] アメリカの大学では he,she のように性別の出る単語を嫌って代わりに ze を使うのだそうだ. 新しく登場した素数を英語で書くときは ze を使うといいだろう. ze の複数形は they だそうだ (笑)

6　オイラー φ 完全数の平行移動

m だけ平行移動した オイラー φ 完全数の定義は次の通り.

$\varphi(P^e)+1+m,(e>1)$ が素数 q になるとき $a=P^eq,(e\geq 2)$ を (P を底とする) m だけ平行移動した (狭義の) オイラー φ 完全数の定義とする.

特にこれを満たす a を (φ,m) 完全数とも言う.

6.1　$e=1$ の場合

この定義では, $e=1$ の場合を除外している.

実際 $e=1$ の場合 $\varphi(P^e)=\varphi(P)=P-1$ なので, $q=\varphi(P^e)+1+m=P+m$ は素数になることが条件である.

$a=P^eq=Pq=P(P+m)$ が狭義のオイラー φ 完全数 となって簡単になり過ぎて面白みに欠ける.

$P=2,e=1$ の場合は $q=2+m$ が素数なら $a=2(2+m)$ を m だけ平行移動した狭義のオイラー φ 完全数 になる.

いろいろやってみると $e=1$ の場合を除外するのは不自然なことでこの場合も取り入れておくのがよいようだ.

6.2　$P=2,m=-2$

もっとも簡単な $P=2.m=-2$ の場合を計算してみる.

表 5: $P=2,m=-2$

a	素因数分解
24	2^3*3
112	2^4*7
1984	2^6*31
32512	2^8*127
134201344	$2^{14}*8191$
34359476224	$2^{18}*131071$
549754765312	$2^{20}*524287$
9223372032559808512	$2^{32}*2147483647$

$q=\varphi(P^e)+1=2^{e-1}+1-2=2^{e-1}-1$ が素数という条件なので, q はメルセンヌ素数になり, ここでの $a=2^eq$ はおしなべて, ユークリッド完全数の 4 倍である.

オイラー φ 完全数を定義してみたらまたユークリッド完全数が出てきた.

6.3 $P = 2, m = 0$

次に $m = 0$ の場合を計算する.

表 6: $P = 2, m = 0$

a	素因数分解
12	$2^2 * 3$
40	$2^3 * 5$
544	$2^5 * 17$
131584	$2^9 * 257$
8590065664	$2^{17} * 65537$

素数部分は フェルマ素数である.

12,40 はともに $m = 0$ のときのオイラー完全数である. 40 歳になったら第 2 オイラー完全数の祝いをするといい.

7 φ 完全数の方程式

$q = \varphi(P^e) + 1 + m, e > 1$ が素数になるとき $a = P^e q$ とする. (m が負の場合もいれているので, $q > P$ を仮定する.)

$$\varphi(a) = \varphi(P^e q) = P^{e-1}\overline{P}\overline{q}$$

に P を掛けて

$$P\varphi(a) = P^e\overline{P}\overline{q} = P^e\overline{P}(q-1)$$

により

$$P\varphi(a) = P^e\overline{P}(q-1) = P^e\overline{P}q - P^e\overline{P}.$$

一方

$q = \varphi(P^e) + 1 + m = P^{e-1}\overline{P} + 1 + m$ なので $P^{e-1}\overline{P} = q - 1 - m$.

ゆえに

$$P^e\overline{P} = P(q - 1 - m).$$

かくして

$$P\varphi(a) = \overline{P}a - P\overline{\mathrm{Maxp}(a)} + Pm. \tag{2}$$

が得られた.

これが m だけ平行移動した オイラー φ 完全数の方程式である.

オイラー φ 完全数の方程式を満たす解が m だけ平行移動した広義のオイラー φ 完全数と呼ばれる.

$P=2$ の場合は簡単になる.

$$2\varphi(a)=a-2\overline{\mathrm{Maxp}(a)}+2m. \tag{3}$$

φ 完全数の方程式 $(*)$ で定義された数は必ずしも φ 完全数になるわけではない.

φ 完全数においては $q=\varphi(P^e)+1+m$ が素数になると仮定されているので $1+m$ は P で割れない.

φ 完全数の方程式 自身を扱うとき $1+m$ は P で割れない, などのことにこだわらない. 実際に $m=P-1$ の場合が重要な結果を与えるのである.

8　計算例

広義のオイラー φ 完全数は狭義のオイラー φ 完全数に比べてどの程度異質なものがあるか調べよう. 定義にしたがって誠をつくして計算するほかない.

9　m : 偶数

m : 偶数という条件は健全なものである.

オイラー φ 完全数の方程式の解を全数調査の方法で探す. $a < 1000000$ について

$$2\varphi(a) = a - 2\overline{\mathrm{Maxp}(a)} + 2m$$

を満たす a とその素因数分解を求める.

計算時間の関係で a は 1000 万未満で探している.

与えられた m, $e < 100$ について指数分を動かし, $q = 2^{e-1} + 1 + m$ が素数となる場合を調べる $a = 2^e q$ とおくことに比較するとはなはだ能率が悪い.

9.1　$P = 2, m = -2; m = 0$

表 7: $P = 2, m = -2; m = -4$

$m = -2$		$m = 0$	
a	素因数分解	a	素因数分解
24	$2^3 * 3$	12	$2^2 * 3$
112	$2^4 * 7$	40	$2^3 * 5$
1984	$2^6 * 31$	544	$2^5 * 17$
32512	$2^8 * 127$	131584	$2^9 * 257$

$m = -2$ のときメルセンヌ 素数　3,7,31,127 が並ぶ.

$m = 0$ のとき とフェルマ 素数 3,5,17,257 が並ぶ.

9.2 $P = 2, m = 2; m = 4$

表 8: $P = 2, m = 2; m = 4$

$m = 2$		$m = 4$	
a	素因数分解	a	素因数分解
20	$2^2 * 5$	28	$2^2 * 7$
56	$2^3 * 7$	208	$2^4 * 13$
176	$2^4 * 11$	2368	$2^6 * 37$
608	$2^5 * 19$		
8576	$2^7 * 67$		
33536	$2^8 * 131$		

$m = -2, 0, 2, 4$ とした場合, 解 a は $a = 2^e q, (q = 2^{e-1} + 1 + m$:素数) の形なので想定された形の解が出てくるのみである.

せっかく広義のオイラ完全数を定義しても新しいものがでてこない. これは不思議なのでそのことの証明を試みる.

10　オイラー φ 完全数の方程式の解

φ 完全数の方程式

$$P\varphi(a) = \overline{P}a - P\overline{\mathrm{Maxp}(a)} + Pm$$

について P を法としてみると, $\overline{P}a \equiv 0 \mod P$ が直ちに出るので a は P の倍数になり $a = P^e L, (L$ は,P で割れない) と書ける. この e は重要な数である.

11　微小解

$m = 0, e = 1$ のとき $a = Pq_0 (P > q_0$: 素数), は

$$P\varphi(a) = \overline{P}a - P\overline{\mathrm{Maxp}(a)}$$

の解になることは一般的に証明できる.

実際, $\mathrm{Maxp}(a) = P$ によって

$$P\varphi(a) - \overline{P}a = P\overline{P}\overline{q_0} - \overline{P}Pq_0 = -\overline{P}P.$$

$m = 0$ のときの解 $a = Pq_0 (P > q_0$: 素数) を微小解という. 微小解は φ 完全数の方程式 $(*)$ に特有の解である.

逆に, $m = 0, e = 1$ のときの解は微小解になることを示すことができる.

$a = PL, (L$ は,P で割れない) と書けるので $P\varphi(a) = P\overline{P}\varphi(L)$,

$$\overline{P}a - P\overline{\mathrm{Maxp}(a)} = \overline{P}PL - P\overline{q}.$$

よって,

$$P\overline{P}\varphi(L) = \overline{P}PL - P\overline{q}.$$

オイラーの余関数 $\mathrm{co}\varphi(L) = L - \varphi(L)$ を使うと

$$\overline{P}\mathrm{co}\varphi(L) = q - 1.$$

そこで $\pi = \mathrm{Maxp}(L)$ とおく.

1) L が素数なら $\mathrm{co}\varphi(L) = 1$ なので $\overline{P} = q - 1$. ゆえに $P = q$. L は素数なので q_0 と書くと, $P = q = \mathrm{Maxp}(a)$ により $P > q_0$. $a = Pq_0$ が解になる.

2) L が非素数なら $\mathrm{co}\varphi(L) \geq \pi$.

$\overline{P}\mathrm{co}\varphi(L) = q - 1$　によって

$$q - 1 = \overline{P}\mathrm{co}\varphi(L) \geq \overline{P}\pi.$$

a) $P > \pi$ のとき. $q = P$ になり

$$P-1=q-1=\overline{P}\mathrm{co}\varphi(L)\geq\overline{P}\pi\geq 2\overline{P}.$$

矛盾.

b) $P<\pi$ のとき. $q=\pi$ になり

$$q-1\geq\overline{P}\pi=\overline{P}q\geq q.$$

矛盾.

12 定理と証明

次の結果が基本定理である.

定理 1 $m\geq 0$ のとき

$$P\varphi(a)=\overline{P}a+Pm-P\overline{Maxp(a)}$$

を満たす解は

$\langle 1\rangle$ $m=0,e=1$ のとき微小解 $a=Pq_0(P>q_0)$ となる.

$\langle 2\rangle$ $m=P-1$ のときの微小解 $a=P^e$ となる.

$\langle 3\rangle$ $e>1$ のとき a は $(\varphi,m)-$ 完全数.

$\langle 4\rangle$ $e=1$ のとき $a=Pq$, $q=P+m$ は素数.

証明.

$a=P^eL(P,L$ は互いに素) と書けくとき次式を満たす:

$$P\varphi(a)=P^e\overline{P}\varphi(L),\overline{P}a=P^e\overline{P}L.$$

$q=\mathrm{Maxp}(a)$ とおくとこれより

$$P^e\overline{P}\varphi(L)=P^e\overline{P}L+Pm-P\overline{q}$$

余関数 $\mathrm{co}\varphi(L)=L-\varphi(L)$ を用いて,

$$P^e\overline{P}\mathrm{co}\varphi(L)=P\overline{q}-Pm.$$

P で割って

$$P^{e-1}\overline{P}\mathrm{co}\varphi(L)=\overline{q}-m.$$

$L=1$ のとき $a=P^e,q=P.$ さらに $\mathrm{co}\varphi(L)=0.$ よって, $q-1=m$ により, $P=q$ なので $m=P-1.$

$m=P-1$ のとき, $a=P^e$ も微小解という.

$L \geq 2$ のとき $a = P^e L \geq 2P^e$.

$$P^{e-1}\overline{P}\mathrm{co}\varphi(L) = \overline{q} - m.$$

において

(1) L : 素数なら $\mathrm{co}\varphi(L) = 1$ によって, $P^{e-1}\overline{P} = \overline{q} - m = q - 1 - m$.
$q = P^{e-1}\overline{P} + 1 + m$ が素数になり $a = P^e q$ は狭義のオイラー完全数.
すなわち a は $(\varphi, m)-$ 完全数.

(2) L が素数でないとき. $\pi = \mathrm{Maxp}(L)$ とおく.
$\mathrm{co}\varphi(L) \geq \pi$ を用いて

$$P^{e-1}\overline{P}\mathrm{co}\varphi(L) = \overline{q} - m \geq P^{e-1}\overline{P}\pi.$$

これより,

$$\overline{q} - m \geq P^{e-1}\overline{P}\pi.$$

(a) $P > \pi$ の場合,$q = \mathrm{Maxp}(a) = P, \pi \geq 2$. これより

$$\overline{q} - m = P - 1 - m \geq P^{e-1}\overline{P} \times 2.$$

$m \geq 0$ によって

$$\overline{P} = P - 1 \geq P - 1 - m \geq P^{e-1}\overline{P} \times 2.$$

これは矛盾.

(b) $P < \pi$ の場合,$q = \mathrm{Maxp}(a) = \pi \geq 2$.
これより

$$\overline{q} - m = \pi - 1 - m \geq P^{e-1}\overline{P}\pi \geq 2\pi.$$

$m \geq 0$ によって

$$\pi - 1 - m \geq 2\pi.$$

これは矛盾.

かくて $e = 1$ のとき $q = P + m$ が素数なら $a = Pq$ は解. これも微小解という. 微小解は形が単純で条件も確かめやすいが, 普通の解に比べて芸のない解なのである.

このようにして, $m \geq 0$ の場合にはオイラーの φ 完全数の基本問題は解決した.
しかし解決しても困ることがある. 問題がなくなって失業状態になるから.
そこで $m < 0$ の場合について詳しく調べることにした.
$P = 2$ の場合に限っても興味ある結果がいろいろ出てきて, 思いのほか豊穣の大地が広がっていたのである.