数学の研究をはじめよう 2017/april
オイラーの(*) 完全数
前編 オイラーもびっくり

飯高 茂

平成 28 年 11 月 14 日

1 オイラーの (*) 完全数

底 P で 平行移動のパラメータ m の オイラー φ 完全数 についての方程式は次のとおり:

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

いささか苦闘はしたが,$m \geq -2$ のとき基本定理ができた. これは望外の成功であった. また $m < 0$ のときオイラー φ 完全数の方程式を解くことができ個々の具体例の計算が可能になった.

$P = 2$ のときの φ 完全数の方程式は

$$a - 2\varphi(a) = 2(q - m - 1)$$

となりこれを a : についての方程式とみる.

これから解 a : は偶数 が自動的にでてくる. ここで $q = \mathrm{Maxp}(a) = a$ の最大素因子.

$m = -2$ のときは方程式

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

満たし解は $a = 2^e q(q = 2^{e-1} - 1$:素数) の形になる.

$\varepsilon = e - 2$ とおくと, $q = 2^{\varepsilon+1} - 1, a = 2^e q = 4 * 2^\varepsilon q$.

$a' = 2^\varepsilon q$ はユークリッドの完全数. $a = 4a'$ になりこれはユークリッドの完全数 a' の 4 倍になる.

表 1: $P=2, m=-2$

a	素因数分解	a'
24	$2^3 * 3$	6
112	$2^4 * 7$	28
1984	$2^6 * 31$	496
32512	$2^8 * 127$	8128
134201344	$2^{14} * 8191$	

これは美しい結果と言ってよいが,4 倍になるのがいささか気になるところである.

そこでオイラーの φ 完全数の定義をわずかばかり変更してオイラーの $(*)$ 完全数を導入する.

素数 P を固定して考え, これを底とする

定義: $q=\varphi(P^{e+1})+1+m,(e>1)$ が素数になるとき $a=P^{e-1}q$ を (底 P で平行移動のパラメータ m の) オイラーの $(*)$ 完全数とよぶ.

さて

$$q=\varphi(P^{e+1})+1+m=P^e\overline{P}+1+m,$$
$$\varphi(a)=\varphi(P^{e-1}q)=P^{e-2}\overline{P}(q-1)$$

に注意して

$$\begin{aligned}P^2\varphi(a)&=P^e\overline{P}(q-1)\\&=P^eq\overline{P}-P^e\overline{P}\\&=P\overline{P}a-(q-1-m).\end{aligned}$$

かくして $\mathrm{Maxp}(a)=q$ に注意し

$$P^2\varphi(a)=P\overline{P}a-\mathrm{Maxp}(a)+1+m. \tag{1}$$

これが底 P で 平行移動のパラメータ m のオイラー $(*)$ 完全数の方程式である.

オイラーの φ 完全数の方程式の場合とは異なり解 a は P の倍数とは言えない. 実際, これが成り立たない例は枚挙に暇がないほどある.

$P=2$ の場合の方程式は

$$4\varphi(a) = 2a - \mathrm{Maxp}(a) + 1 + m. \tag{2}$$

以後 $q = \mathrm{Maxp}(a)$ とおく. 方程式は

$$4\varphi(a) - 2a = m + 1 - q \tag{3}$$

になるため, $m+1-q$ は偶数になる. よって, $q > 2$ のとき m : 偶数である.

一方, 方程式 $4\varphi(a) - 2a = m + 1 - q$ においては m : 奇数の場合も考える. このとき, q : 偶数になるので $q = 2$. 結局 解は $a = 2^e$ しか無い. $a = 2^e$ のとき, $4\varphi(a) - 2a = 0$. よって, $m = 1$. この結果を次にまとめる:

命題 1 方程式

$$4\varphi(a) = 2a - Maxp(a) + (1 + m). \tag{4}$$

において m : 奇数なら $m = 1$. このとき解は $a = 2^e$.

オイラーの φ 完全数の方程式の場合 m : 奇数のとき興味ある結果が出たのにくらべて何と寂しいことだろう.

2 簡単な例

2.1 $[P=2, m=-2]$ の $(*)$ 完全数

表 2: $[P=2, m=-2]$

a	素因数分解	$\varphi(a)$
6	$[2,3]$	2
28	$[2^2,7]$	12
496	$[2^4,31]$	240
8128	$[2^6,127]$	4032

この場合, 解にユークリッドの完全数 6,28,496,8128 が並んでいる.

これはオイラー関数を用いたユークリッドの完全数の提示と言うことができる.

$m=-2$ のときなのでオイラー $(*)$ 完全数の方程式は

$$4\varphi(a)=2a-\mathrm{Maxp}(a)-1$$

となる. この式から a : 偶数 を示すことができればいいのだが難しそうなのでこれ以上考えることは放棄した.

そこで a : 偶数 を仮定する. このとき $a=2^eL, (L$: 奇数$)$ と書けるので

$$2^{e+1}\varphi(L)=2^{e+1}L-\mathrm{Maxp}(a)-1.$$

これより

$$2^{e+1}(\mathrm{co}\varphi(L))=q+1, q=\mathrm{Maxp}(L).$$

$\mathrm{co}\varphi(L)=1$ のとき L : 素数で

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

ここで q はメルセンヌ素数, $a=2^eq$ はユークリッド完全数.

L : 非素数のとき,$\mathrm{co}\varphi(L)\geq q$. これより

$$q+1=2^{e+1}\mathrm{co}\varphi(L)\geq 2^{e+1}q\geq 4q.$$

矛盾.

以上によって分かったことは $P=2, m=-2$ の場合, オイラー $(*)$ 完全数の方程式の解 a は a が偶数の場合はユークリッドの完全数になるということである.

これはオイラーが示した「偶数の完全数はユークリッドの完全数になる」という結果はオイラー $(*)$ 完全数の場合にも同じく成り立つのである．これにはオイラーもびっくりするだろう.

簡単な場合：$a = 3^e qr, r < q$: 素数, なら解にならないことは容易にわかる.

3　$(*)$ 条件

m だけ平行移動した オイラーの $(*)$ 完全数の方程式

$$P^2\varphi(a) - P\overline{P}a = m + 1 - \mathrm{Maxp}(a). \tag{5}$$

において $\mathrm{Maxp}(a)$ は P の倍数であることは分る. しかし, a が P の倍数であるとまでは言えない.

オイラーの φ 完全数の方程式にくらべて $(*)$ 完全数の方程式は一段と難しい方程式である.

そこで話しを簡単にするため

「$\mathrm{Maxp}(a) - (1 + m) \equiv 0 \mod P^2$ を満たすとき $(*)$ 条件を満たす」

ということにし, 以下この場合を主な研究対象とする.

すると, $(*)$ 条件を満たす方程式の解 a は P の倍数となる. その結果, $\varepsilon > 0$ があり $a = P^{\varepsilon}L, (L : P$ で割れない$)$, の形にかける.

$$P^2\varphi(a) = P(P^{\varepsilon}\overline{P}\varphi(L)), P\overline{P}a = P(P^{\varepsilon}\overline{P}L)$$

よって, オイラー余関数　$\mathrm{co}\varphi(L) = L - \varphi(L)$ を用いて変形すると:

$$P^{\varepsilon+1}\overline{P}\mathrm{co}\varphi(L) = q - m - 1. \tag{6}$$

次にこれを解く: ただし $m \geq -2$ を仮定する.

$L = 1$ なら $a = P^{\varepsilon}, q = m + 1, P = q$. よって方程式は

$$P^2\varphi(a) - P\overline{P} = 0.$$

$q = m + 1, P = q$ のとき解は P^{ε}.

$L > 1$ なら $\mathrm{co}\varphi(L) = 1$ のとき L : 素数. $P^{\varepsilon+1}\overline{P} = q - m - 1$ を変形して $q = P^{\varepsilon+1}\overline{P} + 1 + m$; という条件になる.

このとき $a = P^{\varepsilon}q$ がオイラーの $(*)$ 完全数の方程式の解になる. ただし $q = \varphi(P^{\varepsilon+2}) + 1 + m$ が素数.

L : 非素数なら $\mathrm{co}\varphi(L) \geq \mathrm{Maxp}(a)$ を満たす. よって,

$a = P^{\varepsilon}L$ において $\pi = \mathrm{Maxp}(L)$ とおく.

a) $P > \pi$ のとき. $q = \mathrm{Maxp}(a) = P$ になるので

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

これより,$q-m-1>q$. 整数条件より $q-m-1\geq q+1$. $m\geq -2$ を仮定したので

$$P^{\varepsilon+1}\overline{P}\mathrm{co}\varphi(L)=P^{\varepsilon+1}\overline{P}\pi=q+1=P+1.$$

$\varepsilon+1=1, P=2, \mathrm{co}\varphi(L)=1$. これは矛盾.

b) $P<\pi$ のとき. $q=\mathrm{Maxp}(a)=\pi$ になるので

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

これは矛盾.

次の結果が基本定理になる.

定理 1 $(*)$ 条件を満たすと仮定する.

$$P^2\varphi(a)-P\overline{P}a=m+1-Maxp(a) \tag{7}$$

の解 a は $m\geq -2$ のとき $a=P^{\varepsilon}q$ となる. これはオイラーの $(*)$ 完全数になる.

ただし $q=\varphi(P^{\varepsilon+2})+1+m$ が素数. よって解はオイラーの $(*)$ 完全数になる. これが基本定理である.

3.1 $[P=2, m=0]$ の $(*)$ 完全数の解

$m=0$ なので方程式は

$$4\varphi(a)=2a-q+1.$$

表 3: $[P=2, m=0]$

a	素因数分解	q	$q-1$
10	$[2,5]$	5	4
136	$[2^3,17]$	17	16
165	$[3,5,11]$	11	10 *
15561	$[3^2,7,13,19]$	19	18 *
16215	$[3,5,23,47]$	47	46 *
32896	$[2^7,257]$	257	256
1600125	$[3,5^3,17,251]$	251	250 *

上の表はパソコンで $a<2,000,000$ の範囲の解を調べた結果である.

* は $q-m-1$ が 4 の倍数ではない場合, すなわち $q-m-1\equiv 2 \bmod 4$ の場合. だから $(*)$ 条件を満たさない場合である.

これらの結果は非常に興味深い:

a : 偶数なら $a=2^e q, (q=2^{e+1}+1$:素数$)$ とかける.

a : 奇数の解は 4 個あり,

$a=65=[3,5,11]$,$a=15561=[3^2,7,13,19]$,$a=16215=[3,5,23,47]$ $a=1600125=[3,5^3,17,251]$ となっている.

奇数の解は他にあるだろうか. このときは $(*)$ 条件を満たさない場合である.

$m=0$ のときなので $(*)$ 完全数の方程式は

$$4\varphi(a)=2a-\mathrm{Maxp}(a)+1$$

1.

a : 偶数 を仮定する. $a=2^e L, (L:$ 奇数$)$ と書けるので (基本定理の特別な場合だが, この場合を再度証明する)

$$2^{e+1}\varphi(L)=2^{e+1}L-\mathrm{Maxp}(a)+1.$$

$q=\mathrm{Maxp}(L)$ とすると

$$2^{e+1}\mathrm{co}\varphi(L)=q-1.$$

$\mathrm{co}\varphi(L) = 1$ のとき
L : 素数, $L = q$ となり $q = 2^{e+1} + 1$: 素数. これはもちろんフェルマ素数.

L : 非素数のとき
$\mathrm{co}\varphi(L) \geq q$ となり

$$2^{e+1}q \leq 2^{e+1}(\mathrm{co}\varphi(L)) = q - 1$$

これは矛盾.

完全数の場合と同じく a : 偶数を (オイラーのように) 仮定すれば $a = 2^e q, (q = 2^{e+1} + 1$:素数) と書けるという結果は美しい結果というしかない.

2. 奇数の解

この場合は奇数の解がいくつかあり 相異なる素因子の個数 $s(a)$ が 3 と 4 の例を与えている.

強引に解釈すれば, 奇数の解は奇数完全数の類似である.

定義だけで姿がみえない奇数完全数が $m = 0$ のときのオイラー $(*)$ 完全数の解としてこの世に現れて下さったと勝手に思い込み幸せになろう.

3.2 $3^e rq$ の型の解

一般に奇数解の決定は困難な課題である.

ここでは解 $a = 165 = [3, 5, 11]$ に着目して $a = 3^e rq (3 < r < q$: 素数) の場合に解を探すことにする.

$4\varphi(a) = 4\varphi(3^e rq) = 8 * 3^{e-1} * \overline{q} * \overline{r}$,
$2a - \mathrm{Maxp}(a) + 1 = 2 * 3^e rq - q + 1$.
これより, $\Delta = q + r$ を用いると

$$8 * 3^{e-1}(qr - \Delta + 1) = 6 * 3^{e-1} rq - q + 1.$$

$$2 * 3^{e-1} qr = 8 * 3^{e-1}(\Delta - 1) - q + 1.$$

$q_0 = q - 4, r_0 = r - 4$ とおけば

$$q_0 r_0 = qr - 4\Delta + 16.$$

これを前の式に代入して

$$2 * 3^{e-1} qr = 2 * 3^{e-1}(q_0 r_0 + 4\Delta - 16) == 8 * 3^e + 1 - q.$$

$$2*3^{e-1}q_0r_0 = 8*3^e + 1 - q.$$

$q_0 = q-4$ によって

$$2*3^{e-1}q_0r_0 = 8*3^e - q_0 - 3.$$

これより

$$q_0(2*3^{e-1}*r_0+1) = 3(8*3^{e-1}-1).$$

変形して

$$2*3^{e-1}(q_0*r_0-12) = 8*3^e-3 = -q_0-3.$$

書き直して

$$2*3^{e-1}(12-q_0*r_0) = q_0+3 > 0.$$

ゆえに $12-q_0*r_0 > 0$. そこで $12 \geq \dfrac{12}{r_0} > q_0$.

1). $r_0 = 1$ のとき,
$12 > q_0 = q-4$ により $q < 16$. q は素数なので $q \leq 13$. ゆえに $q_0 \leq 9$.
$2*3^{e-1}(12-q_0) = q_0+3$ を q_0 で整理すると

$$24*3^{e-1} = 3+q_0(1+2*3^{e-1}) \leq 3+9(1+2*3^{e-1}).$$

よって

$$8*3^{e-1} \leq 1+3(1+2*3^{e-1}).$$

これより,

$$8*3^{e-1}-1 \leq 3(1+2*3^{e-1}) = 3+2*3^e.$$

$$2*3^{e-1} \leq 3+1 = 4.$$

$$2*3^e \leq 12.$$

$3^e \leq 6$ になり $e=1$.
$2*3^{e-1}(12-q_0) = q_0+3$ に $e=1$ を代入して

$$2(12-q_0) = q_0+3.$$

$21 = 3q_0$ によって $q_0 = 7, q = 11$.
こうして解 $a = 3*5*11$ を得られた.

2). $r_0 = r - 4 > 1$ のとき,
$r \geq 7$. よって $r_0 \geq 3$.
$4 = 12/3 \geq \dfrac{12}{r_0} > q_0 = q - 4$ によれば $8 > q$.
$7 \geq q$ によって $q = r$. これは $q > r$ に矛盾

3.3 $p^e rq$ 型の解

少し一般に $a = p^e rq$ 型の解としても $a = 3 * 5 * 11$ になることを示す. これはいわゆる伏字問題である.

前の項の結果によれば $p \geq 5$ として矛盾を導けばよい.

$4\varphi(a) = 4\varphi(p^e rq) = 4p^{e-1}\overline{pqr}$, $2a + 1 - q = 2pp^{e-1}\overline{p}qr + 1 - q$ によって,

$$4p^{e-1}\overline{pqr} = 2pp^{e-1}\overline{p}qr + 1 - q.$$

これより, $A = \overline{qr}, B = qr$ とおくと

$$4p^{e-1}(p-1)A = 2p^e B + 1 - q,$$

$$2p^{e-1}(2(p-1)A - pB) = 1 - q.$$

$\Delta = q + r$ を用いて

$$0 < -2(p-1)A + pB = pB - 2(p-1)A = pB - 2(p-1)(B - \Delta + 1) = (2-p)B + 2(p-1)(\Delta - 1)$$

$$0 < (2-p)B + 2(p-1)(\Delta - 1) = p(-B + 2(\Delta - 1)) + 2(B - \Delta + 1)$$

によって,

$$p(B - 2(\Delta - 1)) < 2(B - \Delta + 1).$$

$p \geq 5$ なので

$$5(B - 2(\Delta - 1)) < 2(B - \Delta + 1).$$

整理して

$$3B < 8(\Delta - 1).$$

$3qr < 8(q+r) - 8$ を変形して

$$q(3r-8) < 8r - 8$$

$q \geq r+2$ により
$(r+2)(3r-8) < 8r-8$ なので
$r(3r-8) < 8$ になるが $r > 5$ でこの不等式は成り立たない.

$s(a) \geq 4$ のときはどうしてよいか皆目わからない.