

数学の研究をはじめよう 2017/sept

劣完全数の素敵な世界 前編

飯高 茂

1 ユークリッドの完全数

ユークリッドの完全数の定義は次のとおり.

$p = 2^{e+1} - 1$ が偶数のとき $a = 2^e p$ をユークリッドの完全数という.

m だけ平行移動した場合も考える.

$p = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e p$ を m だけ平行移動したユークリッドの完全数という.

$\sigma(a)$ で自然数 a の約数の和を示しこれを. ユークリッドの関数という.

a が m だけ平行移動したユークリッドの完全数のとき $\sigma(a) = 2a - m$ を満たす.

与えられた m について $\sigma(a) = 2a - m$ を満たす a がどのくらいあるかを調べることは非常に困難な課題である. $m = 0$ の場合が完全数の決定問題で現代数学では解決できないのではないかと思うほど難しい.

2 劣完全数

ここで $p = 2^{e+1} - 1 + m$ の 2 を奇素数 P に変更し $q = P^{e+1} - 1 + m$ が素数のとき $a = P^e q$ を底 P , 平行移動 m の狭義の劣完全数 (subperfect number) といひ, このときの q をサブ素数 (subprime number) という.

さて劣完全数の満たす方程式の導入を行う. $\bar{P} = P - 1$ という記号は今後もよく使う.

劣完全数 $a = P^e q$ について

$$\bar{P}\sigma(a) = \bar{P}\sigma(P^e q) = (P^{e+1} - 1)(q + 1)$$

$N = P^{e+1} - 1$ とおくと, $q = P^{e+1} - 1 + m = N + m$.
 $\overline{P}\sigma(a) = N(q+1) = Nq + N$ になるが $Nq + N = P^{e+1}q - q + N = Pa - q + N$,
 $q + N = m$ なので

$$\overline{P}\sigma(a) = Pa - m.$$

究極の完全数の場合の方程式に比べて簡明な式になった.

この方程式の解を底 P , 平行移動 m の広義の劣完全数 (subperfect number with translation parameter m) というのである. 広義の劣完全数を簡単に劣完全数という.

$P > 2$ なら, $m = 0$ のとき $q = P^{e+1} - 1 + m$ は素数にならない. しかし, 例外が 1 つだけある. $e = 0, P = 3$ のとき, $q = 2$ は素数で $a = 2$ となる.

m によっては $P^{e+1} - 1 + m$ は素数になりうるのでこのように劣完全数を定義しても一向構わないである.

$e > 0$ のとき $q = P^{e+1} - 1$ は素数にならないという難点を克服するために $P^{e+1} - 1$ の代わりに $\sigma(P^e)$ を使うこともできる. $q = \sigma(P^e) + m$ が素数のとき $a = P^e q$ を考えればよく, これを究極の完全数という.

劣完全数の研究は現在進行中であり, 興味ある結果が多数得られている.

次の結果は小学校算数のようなものだが私は知らなかった. オイラーが使ったらしい.

補題 1 a, b, c, d が自然数で, $\frac{a}{b} = \frac{c}{d}$ が成り立つ. $\frac{a}{b}$ が既約分数なら, 自然数 k があり $c = ka, d = kb$ となる.

Proof.

$da = bc$, $\text{GCD}(a, b) = 1$ かつ $a|bc$ より $a|c$. ゆえに $c = ka$. これから $d = kb$. (記号 $a|c$ は a が c の約数を意味する.)

3 $P \geq 3$, 平行移動 $m = 0$ の劣完全数

狭義の劣完全数の場合, $q = P^{e+1} - 1 + m$ が素数なので, $P \geq 3$ であれば, m は奇数になる.

$\sigma(a) - a$ を $\text{co}\sigma(a)$ と書きユークリッド余関数という. 以下でもよく使われることになる.

広義の劣完全数ではあえて, m が偶数の場合も考える. とくに $m = 0$ の場合は興味があり, 次の結果が得られている.

命題 1 $P \geq 3$, 平行移動 $m = 0$ の広義の劣完全数は $P = 3$ の場合の $a = 2$.

Proof.

$m = 0$ なので $\overline{P}\sigma(a) = Pa$ により

$$\frac{\overline{P}}{P} = \frac{a}{\sigma(a)}.$$

$\frac{\overline{P}}{P}$ は既約分数なので, 自然数 k があり $a = k\overline{P}, \sigma(a) = kP$ となる.

$$\sigma(a) = kP = k(\overline{P} + 1) = k\overline{P} + k = a + k.$$

$\text{co}\sigma(a) = \sigma(a) - a$ を使うと $\text{co}\sigma(a) = k$ かつ k は a の約数なので, $k = 1, a$ は素数.

なぜなら, $k > 1$ とすると, これらは a と異なる約数なので $\text{co}\sigma(a) \geq 1 + k$. これは $\text{co}\sigma(a) = k$ に矛盾する.

$\text{co}\sigma(a) = 1$ になり, a は素数 $a = k\overline{P}$ は素数なので, $k = 1, \overline{P} = 2$. よって $P = 3, a = 2$.

水谷一氏の指摘により, 元の証明よりはるかに簡易化できた.

(この証明は オイラーが行った, 「偶数完全数はユークリッドの完全数になる」証明と酷似している. そこに幾ばくかの興味がある)

4 $P \geq 3$, 平行移動 $m = P - 1$ の劣完全数

命題 2 $P \geq 3$, 平行移動 $m = \overline{P}$ の劣完全数は存在しない.

Proof.

$\overline{P}\sigma(a) - Pa = -\overline{P}$ によって, $\overline{P}(\sigma(a) + 1) = Pa$ になるので,

$$\frac{\overline{P}}{P} = \frac{a}{\sigma(a) + 1}.$$

$\frac{\overline{P}}{P}$ は既約分数なので, 自然数 k があり $a = k\overline{P}, \sigma(a) + 1 = kP$ となる.

$$\sigma(a) + 1 = kP = k(\overline{P} + 1) = k\overline{P} + k = a + k.$$

よって,

$$\sigma(a) - a = \text{co}\sigma(a) = k - 1.$$

k は a の約数なので $k - 1 = \sigma(a) - a \geq k$. これは矛盾.

この論法によれば, $m = \nu\overline{P}, \nu > 0$ の場合は劣完全数が存在しないことがわかる.

注意 $P = 2$ のとき, $m = -1$ だけ平行移動した場合の方程式は $\sigma(a) = 2a + 1$ になる. この場合は解が存在しないと思われているが今でも証明できない. しかし劣完全数の場合 $\bar{P}(\sigma(a) + 1) = Pa$ の解を考える. 解の不存在が簡単に証明できる. これほどうまく行くと思わず「劣完全数の素敵な世界」と叫びたくなる.

5 $P \geq 3$, 平行移動 $m = -\bar{P}$ の劣完全数

定理 1 $P \geq 3$, 平行移動 $m = -\bar{P}$ の劣完全数は $P = 3, a = 2^2$.

Proof. 定義によって $\bar{P}\sigma(a) - Pa = \bar{P}$ になるので $\bar{P}(\sigma(a) - 1) = Pa$. よって,

$$\frac{\bar{P}}{P} = \frac{a}{\sigma(a) - 1}.$$

$\frac{\bar{P}}{P}$ は既約分数なので, 自然数 k があり $a = k\bar{P}, \sigma(a) - 1 = kP$ となる.

$$\sigma(a) - 1 = kP = k(\bar{P} + 1) = k\bar{P} + k = a + k.$$

よって,

$$c\sigma(a) = \sigma(a) - a = k + 1.$$

$a = k\bar{P}$ に注目し場合を分ける.

1) $k = 1. \sigma(a) - a = 2$.

ユークリッド余関数 $c\sigma(a) = \sigma(a) - a$ の値は 2 にならないことが知られているから矛盾.

2) $k > 1. k \neq \bar{P}$.

$k, \bar{P}, 1$ は a の真の約数なので

$$\sigma(a) - a = k + 1 \geq k + \bar{P} + 1$$

. これは矛盾.

3) $k > 1. k = \bar{P}$.

$a = k^2$ なので $\sigma(a) = k^2 + k + 1$. このとき k は素数. $k = \bar{P}$ も素数なので, $P = 3, a = k^2 = 4$.

6 $P = 3, m$ は 偶数の場合

$P = 3$ とする.

$2\sigma(a) - 3a = -m$ になる. m : 偶数の場合, $m > 0$ なら解はないので $-40 \geq m \geq -1$ の範囲についてコンピュータで出力してできた結果は次の通り. ここで

$$m = -40 \quad \text{factor}(52) = 2^2 * 13$$

これを $m = -40$ のときは解が 52 でその素因数分解は $2^2 * 13$ と読む. 以下も同じ.

$m=-36$;factor(44)= $2^2 \cdot 11$,factor(50)= $2 \cdot 5^2$
 $m=-30$;factor(32)= 2^5
 $m=-28$;factor(28)= $2^2 \cdot 7$
 $m=-24$;factor(18)= $2 \cdot 3^2$,factor(20)= $2^2 \cdot 5$
 $m=-20$;factor(12)= $2^2 \cdot 3$
 $m=-14$ factor(16)= 2^4

$m=-6$

factor(6)= $2 \cdot 3$,factor(8)= 2^3 ,factor(10)= $2 \cdot 5$,factor(14)= $2 \cdot 7$
factor(22)= $2 \cdot 11$,factor(26)= $2 \cdot 13$,factor(34)= $2 \cdot 17$

$m = -6$ のとき $a = 2p$. $p > 2$: 素数, $a = 2^3$ の解が出てくる.
 $\sigma(2p) = 3p + 3$ なので $2\sigma(a) - 3a = 6p + 6 - 6p = 6$.
これはいわゆる通常解で,B型の解ともいう.

7 $P = 3$, B型の解

$a = 2p$ のとき $\sigma(2p) = 3p + 3$ を満たす. すると $2\sigma(a) - 3a = 6p + 6 - 6p = 6$.

定理 2 $2\sigma(a) - 3a = 6$ を満たす解 a は $a = 2p$ ($p > 2$: 素数) および $a = 2^3 = 8$.

$a = 2p$ は通常解で,B型の解である.

しかし, 解 $a = 2^3 = 8$ もありこれを擬素数解という.

Proof.

$2\sigma(a) - 3a = 6$ を $2(\sigma(a) - 3) = 3a$ と変形して分数で書くと

$$\frac{2}{3} = \frac{a}{\sigma(a) - 3}$$

$\frac{2}{3}$ は既約なので, k があり $a = 2k, \sigma(a) - 3 = 3k = a + k$ を満たす. ゆえに
 $\sigma(a) - a = 3 + k$.

1) k : 奇数なら, $k > 1$. $a = 2k$ の約数は 少なくとも $1, 2, k, 2k$. $\sigma(a) - a \geq 1 + 2 + k$. ここで等号が成り立つので, $a = 2k$ の約数は $1, 2, k, 2k$ に限る. よって k :素数

2) k : 偶数なら, $k = 2^\varepsilon L, L$: 奇数.

$L \neq 1$ なら, L は $1, 2, k, 2k$ 以外の k の約数. 矛盾.

$L = 1$ なら, $a = 2k = 2^{\varepsilon+1}$. この約数の個数は $2 + \varepsilon$.

$2 + \varepsilon = 4$ より $\varepsilon = 2, k = 4, a = 8$

したがって, $a = 2p, a = 8$.

8 一般のB型の解

$2\sigma(a) - 3a = 6$ の 2 は素数なのでこれを一般にし 素数 Q で置き換える. パラメータ m をとり $Q\sigma(a) - (Q+1)a = m$ の解として $a = Qp (Q \neq p)$ があると仮定する.

$\sigma(a) = (Q+1)p + Q + 1$ なので

$$Q\sigma(a) = (Q+1)Qp + Q(Q+1) = (Q+1)a + Q(Q+1).$$

そこで, $m = Q(Q+1)$ とおけば

$$Q\sigma(\alpha) = (Q+1)\alpha + Q(Q+1).$$

定理 3 Q が素数のとき

$$Q\sigma(\alpha) = (Q+1)\alpha + Q(Q+1)$$

の解は $\alpha = Qp (Q \neq p)$ または $\alpha = Q^3$.

Proof.

$Q\sigma(\alpha) = (Q+1)(\alpha+Q)$ によって,

$$\frac{Q}{Q+1} = \frac{\alpha+Q}{\sigma(\alpha)}.$$

よって, k があり

$$Q\alpha + Q = kQ, \sigma(\alpha) = kQ + k.$$

これより

$$\alpha = \bar{k}Q, (\bar{k} = k-1), \sigma(\alpha) = (k-1+1)Q + k-1+1 = \bar{k}Q + \bar{k} + 1.$$

$\sigma(\bar{k}Q) = \bar{k}Q + \bar{k} + 1$ が成り立つので

1) $\bar{k} \neq Q$. $\bar{k} = p$ は素数で, $p \neq Q$ ここで $\alpha = \bar{k}Q = pQ$.

2) $\bar{k} = Q^2$. $\alpha = Q^3$.

$Q\sigma(\alpha) = (Q+1)\alpha + m$ は劣完全数の方程式ではない. 変形劣完全数とでもいうしかない.

$m = 1$ すなわち

$$\overline{P}\sigma(a) = Pa - 1$$

の解には底の素数のべき P^e がある.

実際 $a = P^e$ を代入すると,

$$\overline{P}\sigma(a) - Pa = -1.$$

方程式 $\overline{P}\sigma(a) = Pa - 1$ の解を一般に概完全数 (almost perfect number) と呼ぶ.

$P = 5, m = 1$ のときコンピュータの出力結果

$P=5, m= 1$

`factor(5)=5, factor(25)=5^2, factor(77)=7*11,`

`factor(125)=5^3, factor(625)=5^4`

驚いたことに累乗ではない解 $a = 7 * 11$ が見つかった.

9 一般的な概完全数

$P = 5$ の場合を参考にして $\overline{P}\sigma(a) = Pa - 1$ の解に 2 素数の積, $rq (P < r < q : \text{素数})$, があるとする.

$a = rq, \sigma(a) = (r + 1)(q + 1), A = (r + 1)(q + 1), B = rq, \Delta = r + q$ とおくと
とき $A = B + \Delta + 1$.

$$\overline{P}\sigma(a) = \overline{P}A = \overline{P}(B + \Delta + 1)$$

一方,

$$Pa - 1 = Prq - 1 = PB - 1 \text{ によって,}$$

$$\overline{P}(B + \Delta + 1) = PB - 1 = \overline{P}B + B - 1.$$

$$\overline{P}B + \overline{P}(\Delta + 1) = \overline{P}B + B - 1.$$

$$B - \overline{P}(\Delta + 1) = 1.$$

$r_0 = r - \overline{P}, q_0 = q - \overline{P}, B_0 = r_0q_0$ とおくと

$$B_0 = r_0q_0 = B - \overline{P}\Delta + \overline{P}^2.$$

$$B - \overline{P}\Delta = B_0^2 - \overline{P}^2$$

ゆえに

$$B_0^2 = P^2 - P + 1.$$

ここで、奇素数 P に対して $D = P^2 - P + 1$ とおき因数分解を行い、 $B_0^2 = D$ を満たす、 r_0, q_0 に対して $r = r_0 + \overline{P}, q = q_0 + \overline{P}$ がともに素数となる、 r, q があれば $a = rq$ が解になる。

これによりプログラムを作ると次のように解が数多く見つかる。

表 1: 概完全数の表

P	$D = P^2 - P + 1$	a	a の素因数分解	$\sigma(a)$
$P = 5$	[3, 7]	77	$7 * 11$	96
$P = 11$	[3, 37]	611	$13 * 47$	672
$P = 17$	[3, 7, 13]	2033	$19 * 107$	2160
		1073	$29 * 37$	1140
$P = 31$	[7 ² , 19]	6031	$37 * 163$	6232
$P = 37$	[31, 43]	5293	$67 * 79$	5440
$P = 41$	[3, 547]	25241	$43 * 587$	25872
$P = 47$	[3, 7, 103]	9983	$67 * 149$	10200
$P = 73$	[7, 751]	65017	$79 * 823$	65920
$P = 89$	[3, 7, 373]	50249	$109 * 461$	50820

たとえば $4\sigma(a) - 5a = 4 * 96 - 5 * 77 = 384 - 385 = -1$.