数学の研究をはじめよう 2017/dec 真正フェルマ完全数　前編

飯高 茂

1　フェルマ完全数

2 だけ平行移動した狭義の完全数は, $q = 2^{2^m} + 1$ が素数のとき $a = 2^{2^m-1}q$ になる．ここにおいて, $q = F_m = 2^{2^m} + 1$ はフェルマ素数なので $a = 2^{2^m-1}q$ をフェルマ完全数という.

フェルマ素数は 5 個しか知られていないので素数条件をはずして, フェルマ数について考えた場合 $a = 2^{2^m-1}q$ をフェルマー弱完全数という.

P が奇素数の場合 $L_m = \dfrac{P^{2^m} + 1}{2}$ が素数のとき, $a_m = P^{2^m-1}L_m$ を底が P のフェルマ完全数という．素数条件をはずして底が P のフェルマ弱完全数を考えてもよい．この場合, フェルマ完全数の方程式は考えなくてもよい.

1.1 例

表 1: $P = 2$; Fermat 弱完全数

m	2^m	a_m	(F_m)=素因数分解
0	1	3	(3)=3
1	2	10	(5)=5
2	4	136	(17)=17
3	8	32896	(257)=257
4	16	2147516416	(65537)=65537
5	32	9223372039002259456	$(4294967297) = 641 * 6700417$
6	64	A	B

$A = 170141183460469231740910675752738881536$
$B = (18446744073709551617) = 274177 * 67280421310721$

2　P を底とするフェルマの(弱)完全数

Fermat 完全数を底の概念を導入して一般化しよう.

P を奇素数とし $E > 0$ について $R = P^E + 1$ とおく. これ は偶数なので $L_E = \frac{R}{2}$ とする. L_E を素数とすると, E は 2 のべきになるので $E = 2^m, (m > 0)$ とかける.

一般に $E = 2^m$ とかけるとき L_E は奇数であることが証明できる.

実際,L_E は偶数であると仮定する. すなわち $L_E = \frac{R}{2} = 2L'$ とすると $R = 4L'$ なので

$$R = P^E + 1 = 4L' \equiv 0 \mod 4.$$

ゆえに, $P^E \equiv -1$. 一方, $P = 2k + 1$ とおくとき

$$P^E = (2k + 1)^{2^m} \equiv 1 \mod 4.$$

これで前の式に矛盾した.

以上を踏まえて, $E = 2^m$ のとき $L_m = \frac{P^E+1}{2}$ とおく.

これは奇数であり, P を底とするフェルマ数と理解する.

ただし,$P = 2$ のとき $E = 2^m, L_m = F_m = P^E + 1$ とおく.

補題 1 $e > 1$ について L_m の素因子 Q は $P - 1$ の因子にならない.

$a_m = P^{2^m-1}L_m$ を P が **底のフェルマの弱完全数**と定義する.

L_m が素数の場合なら, a_m を P が**底のフェルマの完全数**と呼ぶ.

フェルマの弱完全数はフェルマの完全数に比べて豊富な例を持っている. しかも, フェルマの完全数で言えたことは弱完全数でも成り立つ事がある.

一般の底の場合でもフェルマの完全数は数が少ない. 研究対象が少ないのは研究上不利だ.

一方, 弱完全数は無限にあるので研究材料として有利である.

2.1 $P = 3$

$P = 3$ のときの Fermat 弱完全数を計算してみよう.
ここで面白い例が出なければ, 底を一般化する試みは失敗したとも言える.

表 2: $P = 3$; Fermat 弱完全数

m	2^m	a	(L_m)=素因数分解
1	2	15	(5)=5
2	4	1107	(41)=41
3	8	7175547	$(3281) = 17 * 193$
4	16	308836705316427	(21523361)=21523361
5	32	A	B
6	64	C	D
7	128	E	F

$A = 5722806367154190562796729901 87$
$B = (926510094425921) = 926510094425921$
$C = 196503076295643052858681214356932539158308401746008315969 7707$
$D = (171684191010146256242328924544641) = 171684191010146256242328924544641$
$E = 23168075396190788794156631131 6[62 digits]771379200003876302731668088747$
$F = (589509228886929158576043643070625933283910579613792055454 8481)$
$= 257{*}275201{*}138424618868737{*}3913786281514524929{*}153849834853910661121$
L_m を底 $P = 3$ のときの Fermat 数という.
$L_1 = 5, L_2 = 41$ は素数 ($P = 3$ のときの Fermat 素数) であるが,
$L_3 = 3281 = 17 * 193$ は合成数. しかし,
$L_4 = 21523361, L_5 = 926510094425921, L_6 = 926510094425921,$
$L_7 = 171684191010146256242328924544641$ はみな素数である.
$P = 3$ のとき多くの Fermat 素数が出てきたことに感動.

3　真正 Fermat 完全数

奇素数 P を底, 平行移動 m の真正 Fermat 完全数を次のように定義する.
$q=\dfrac{P^{e+1}+1}{2}+m$: 素数と仮定する. すると, $2(q-m)=P^{e+1}+1$.
$a=P^eq$ を底 P, 平行移動 m の狭義の真正 Fermat 完全数という.
$N=P^{e+1}-1$ とおくとき, $a=P^eq$ について,

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

なので分母を払い,

$$\overline{P}\sigma(a)=N(q+1)=(N+1)q+N-q.$$

$(N+1)q=Pa, 2(q-m)-1=P^{e+1}=N+1$ によれば, $N=2(q-m-1)$.
ゆえに,

$$\overline{P}\sigma(a)-Pa=(N+1)q+N-q-(N+1)q=N-q=q-2(m+1).$$

$q=$Maxp(a) を用いて

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

これを底 P, 平行移動 m の真正 Fermat 完全数の方程式といい, これを満たす a を底 P, 平行移動 m の広義の真正 Fermat 完全数という.

底 P, 平行移動 m の劣完全数の方程式は $\overline{P}\sigma(a)-Pa=-m$.

ついでに底 P, 平行移動 m の究極の完全数とは $q=\sigma(P^e)+m$: 素数と仮定する. $a=P^eq$ を底 P, 平行移動 m の究極の完全数という.

実際, $N=P^{e+1}-1$ とおくとき, $N=\overline{P}\sigma(P^e)$. 定義より $q-m=\sigma(P^e)=\dfrac{N}{\overline{P}}$.
よって, $N=(q-m)\overline{P}$.
$a=P^eq$ について,

$$\overline{P}\sigma(a)=N\sigma(q)=Nq+N=Pa-q+N.$$

これより

$$\overline{P}\sigma(a)-Pa=N-q=(q-m)\overline{P}-q=q(P-2)-m\overline{P}.$$

したがって, 底 P, 平行移動 m の究極の完全数の方程式は $\overline{P}\sigma(a)-Pa=(P-2)q-m\overline{P}$.

q を Maxp(a) で置き換えると

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

3.1 3種の方程式

これまでに出てきた方程式を並べてみてみよう.

1. 劣完全数の方程式は $\overline{P}\sigma(a) - Pa = -m$.
2. 真正 Fermat 完全数の方程式は $\overline{P}\sigma(a) - Pa = Maxp(a) - 2(m+1)$.
3. 究極の完全数の方程式は $\overline{P}\sigma(a) - Pa = (P-2)Maxp(a) - m\overline{P}$.

$P = 3$ に特化すると,

1. 劣完全数の方程式は $2\sigma(a) - 3a = -m$.
2. 真正 Fermat 完全数の方程式は $2\sigma(a) - 3a = Maxp(a) - 2(m+1)$.
3. 究極の完全数の方程式は $2\sigma(a) - 3a = Maxp(a) - 2m$.

驚いたことに, $P = 3$ のとき, 真正 Fermat 完全数の方程式において, $m+1$ を m に置き換えると, 究極の完全数の方程式になる. 何ということだ! 私は思わず笑ってしまった.

$P = 5$ に特化すると,

1. 劣完全数の方程式は $4\sigma(a) - 5a = -m$.
2. 真正 Fermat 完全数の方程式は $4\sigma(a) - 5a = Maxp(a) - 2(m+1)$.
3. 究極の完全数の方程式は $4\sigma(a) - 5a = 3Maxp(a) - 4m$.

ここでは真正 Fermat 完全数の方程式と究極の完全数の方程式は確かに異なっている.

3.2 計算結果

$P = 3$ のとき $2\sigma(a) - 3a = Maxp(a) - 2(m+1)$.

表 3: $P = 3, m = -5$, のときの解

a	factor
147	$3 * 7^2$
3185	$5 * 7^2 * 13$
50373	$3^2 * 29 * 193$

表 4: $m = -3$, のときの解

a	factor
99	$3^2 * 11$
759	$3 * 11 * 23$
795339	$3^6 * 1091$

表 5: $m = -2$, のときの解

a	factor
27755	$5 * 7 * 13 * 61$
218225	$5^2 * 7 * 29 * 43$

表 6: $m = 0$ のときの解

a	factor
15	$3 * 5$
741	$3 * 13 * 19$
1107	$3^3 * 41$
14883	$3 * 11^2 * 41$
38781	$3^2 * 31 * 139$

$15 = 3 * 5$

$1107 = 3^3 * 41$

正規形以外の解が意外に多い.
第二正規形もそこそこある.

表 7: $P=3, m=1$ のときの解

a	factor
3	3
9	3^2
27	3^3
81	3^4
243	3^5
729	3^6
2187	3^7
6561	3^8
19683	3^9
59049	3^{10}
99807	$3*17*19*103$
177147	3^{11}
531441	3^{12}
603681	$3*13*23*673$
1594323	3^{13}

$m=1$ のときは 3^e は直ちにわかるように解である.
しかしそれ以外の解がでてきた. どれもオビである.

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

において, $a=P^e$
が解と仮定すると $\overline{P}\sigma(a)-Pa=(P^{e+1}-1)-P^{e+1}=-1$ なので

$$-1=P-2(m+1).$$

ゆえに, $m=\frac{P+1}{2}-1=m=\frac{P-1}{2}$
$P=3, m=1$

```
type C for true-Fermat
factor(3)=3
factor(9)=3^2
factor(27)=3^3
factor(81)=3^4
factor(243)=3^5
factor(729)=3^6
factor(2187)=3^7
```

```
factor(6561)=3^8
factor(19683)=3^9
factor(59049)=3^10
factor(99807)=3*17*19*103
factor(177147)=3^11
factor(531441)=3^12
factor(603681)=3*13*23*673
```

$P = 5, m = 2$

```
factor(5)=5
factor(25)=5^2
factor(125)=5^3
factor(625)=5^4
factor(637)=7^2*13
factor(3125)=5^5
factor(15625)=5^6
factor(78125)=5^7
factor(390625)=5^8


\begin{verbatim}
factor(7)=7
factor(49)=7^2
factor(343)=7^3
factor(2401)=7^4
factor(16807)=7^5
factor(117649)=7^6
factor(823543)=7^7

factor(11)=11
factor(121)=11^2
factor(1331)=11^3
factor(14641)=11^4
factor(161051)=11^5

factor(13)=13
factor(169)=13^2
factor(2197)=13^3
factor(28561)=13^4
```

```
factor(371293)=13^5
```

```
factor(17)=17
factor(289)=17^2
factor(4913)=17^3
factor(83521)=17^4
factor(311167)=23*83*163
```

表 8: $P = 5, m = 2$ のときの解

a	factor
25	5^2
125	5^3
625	5^4
637	$7^2 * 13$
3125	5^5
15625	5^6

$7^2 * 13$ は正規解ではない.
$P = 7m = 3$ のときの解は $a = 7^e$ の他の解は未発見.

表 9: $P = 3, m = 2$ のときの解

a	factor
21	$3 * 7$
1161	$3^3 * 43$
89181	$3^5 * 367$

正規解がある.

表 10: $P = 3, m = 3$ のときの解

a	factor
5	5
153	$3^2 * 17$
27639	$3^2 * 37 * 83$
51417	$3^2 * 29 * 197$
799713	$3^6 * 1097$
965007	$3^3 * 103 * 347$

表 11: $P = 3, m = 5$ のときの解

a	factor
7	7
171	$3^2 * 19$
10287	$3^4 * 127$

3.3 正規形の解

表 12: $P = 3, m = 0$ のときの解

a	factor
15	$3 * 5$
1107	$3^3 * 41$
308836705316427	$3^{15} * 21523361$
572280636715419056279672990187	$3^{31} * 926510094425921$
A	B

A=1965030762956430528586812143569325391583084017460083159697707
B=$3^{63} * 1716841910146256242328924544641$

表 13: $P = 3, m = 2$ のときの解

a	factor
21	$3 * 7$
1161	$3^3 * 43$
89181	$3^5 * 367$
581179941	$3^9 * 29527$
C	D

$C = 299501716652405201735529971620260138517926107518220545401$
$D = 3^{59} * 21195579137608101757147216603$

4　真正フェルマ完全数のB型解

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

これを真正 Fermat 完全数の方程式といい, これを満たす a を広義の真正 Fermat 完全数という.

数値実験を繰り返し次の解 (B 型解) を見いだした.

表 14: $P = 5, m = -9, a < 200$ のときの解

a	factor
15	$3 * 5$
21	$3 * 7$
33	$3 * 11$
39	$3 * 13$
51	$3 * 17$
57	$3 * 19$
69	$3 * 23$
87	$3 * 29$
93	$3 * 31$
111	$3 * 37$
123	$3 * 41$
129	$3 * 43$

$a = 3p(p > 3:$ 素数$)$ が解でありこれを通常解という.

4.1　一般化

これを一般にすることを考えてみた.

$Q = P - 2$ を素数と仮定して, $a = Qq, (Q < q:$ 素数$)$ は次の方程式の解とする.

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

$\mathrm{Maxp}(a) = q$ に注意する.

$$\overline{P}\sigma(a) - Pa = q - 2(m+1).$$

$\sigma(a) = (Q+1)(q+1) = (P-1)(q+1) = \overline{P}(q+1)$ により

$\overline{P}\sigma(a) - Pa = \overline{P}^2 q + \overline{P}^2 - P(P-2)q$ なので

$$\overline{P}^2 q + \overline{P}^2 - P(P-2)q = \overline{P}^2 q + \overline{P}^2 - (\overline{P}^2 - 1))q = q - 2(m+1).$$

$\overline{P}^2 q - P(P-2)q = q$ なので, q が消えて

$$\overline{P}^2 = -2(m+1).$$

これを m について解くと

$$m+1 = -\frac{\overline{P}^2}{2}.$$

$P = 5$ なら $Q = 3, m+1 = -8$. よって, $m = -9$.

$Q = P-2$:素数, $m = -\frac{\overline{P}^2}{2} - 1$ とおくとき, $a = Qq, (Q < q$: 素数$)$ が解であり, B 型の解である.

$Q, P = Q+2$ はともに素数を仮定している. (Q, P) はいわゆる双子素数 (twin primes) である. 双子素数は無数にあるという予想されているが未解決.

表 15: B 型解を与える P

twin	P	$Q = P-2$	$(P-1)^2/2$	m
	5	3	8	-9
	7	5	18	-19
x	9	7	32	-33
x	11	9	50	-51
	13	11	72	-73
x	15	13	98	-99
x	17	15	128	-129
	19	17	162	-163
x	21	19	200	-201
x	23	21	242	-243
x	25	23	288	-289
x	27	25	338	-339
x	29	27	392	-393
	31	29	450	-451
x	33	31	512	-513

twin に x が書かれているのは双子素数にならない場合.

数値例をあげる. $P = 13, m = -73$

```
factor(143)=11*13
factor(187)=11*17
factor(209)=11*19
factor(253)=11*23
factor(319)=11*29
factor(341)=11*31
factor(407)=11*37
factor(451)=11*41
factor(473)=11*43
factor(517)=11*47
factor(583)=11*53
factor(649)=11*59
```