

新規まき直し 第一期2017年10月13日  
素数べきと完全数の平行移動

飯高 茂

平成 29 年 8 月 29 日

目 次

1	スーパー完全数	2
2	平行移動 $m$ のスーパー完全数	3
2.1	$m = 0$ のとき	4
2.2	$m = 2$ のとき	5
2.3	$m = 4$ のとき	5
2.4	$m = 4$ のとき	6
2.5	$m = -2$ のとき	7
3	素数解 $p$	9
4	究極のスーパー完全数 I 型	10
4.1	超完全数からスーパー完全数へ	11
4.2	数値例	12
5	究極のスーパー完全数 II 型	14
6	スーパー型のオイラー完全数	16
6.1	数値例	17
7	メルセンヌ数	18
8	究極のスーパーオイラー完全数 I 型	19
9	究極のスーパーオイラー完全数 II 型	21
10	$P = 2$ の場合	21
10.1	$m$ : 偶数	21
10.2	$m$ : 奇数	22
10.3	$m = -3$ :	22
10.4	$m = -5$ :	23

# 1 スーパー完全数

D.Suryanarayana は 1969 年にスーパー完全数 (superperfect numbers) を定義して基本定理を確立した.

Suryanarayana, D. "Super Perfect Numbers." Elem. Math. 24, 16-17, 1969.

Suryanarayana, D. "There Is No Odd Super Perfect Number of the Form  $p^{(2\alpha)}$ ." Elem. Math. 24, 148-150, 1973.

$a = 2^e$  とおくと  $\sigma(a) = 2^{e+1} - 1$  となる. これを素数と仮定し  $q$  とおく.

$\sigma(q) = q + 1 = 2^{e+1} = 2a$  になる.

$q = \sigma(a)$  を代入すると,

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

が成り立つ. 記号  $\sigma^2(a) = \sigma(\sigma(a))$  を用いると

$$\sigma^2(a) = 2a$$

と書き直せる. これを満たす  $a$  をスーパー完全数と呼ぶ.

定義だけみると何をふざけているのですか, と言いたくなる.

しかし ここでもオイラーの定理が成り立つ, ことに注目したい. しかも証明は簡単だ.

定理 1.

$$\sigma^2(a) = 2a$$

を満たす  $a$  は偶数のとき  $2^{p-1}$  とかける. ここで  $2^p - 1$  はメルセンヌ素数.

Proof.

仮定により,  $e > 0$  があり  $a = 2^e L$ , ( $L$ : 奇数) となる.  $N = 2^{e+1} - 1$  とおくと  $\sigma(a) = N\sigma(L)$ .

1).  $L = 1$

$a = 2^e$  により  $\sigma(a) = N$ .  $\sigma^2(a) = \sigma(N)$ .  $\sigma^2(a) = 2a = N + 1$  によれば  $\sigma(N) = N + 1$ . それゆえ  $N$  は素数.  $N = 2^{e+1} - 1$  はメルセンヌ素数.  $a = 2^e$ .

したがって,  $e + 1$  も素数.

2).  $L > 2$

$N > 1$  なので,  $\sigma(L)$  は  $\sigma(a) = N\sigma(L)$  の真の約数. よって  $1, \sigma(L), N\sigma(L)$  は相異なる約数ゆえに

$$\sigma^2(a) \geq 1 + \sigma(L) + N\sigma(L).$$

$\sigma^2(a) = 2a$  なので  $2a \geq 1 + \sigma(L) + N\sigma(L)$ .

$2a = 2^{e+1}L = (N + 1)L$  によれば

$$(N + 1)L \geq 1 + \sigma(L) + N\sigma(L) \geq 1 + (N + 1)L.$$

これは矛盾.

## 2 平行移動 $m$ のスーパー完全数

平行移動  $m$  の狭義の完全数  $\alpha$  は  $q = 2^{e+1} - 1 + m$ :素数, により  $\alpha = 2^e q$  と書ける.

$N = 2^{e+1} - 1$  とする.  $q = N + m$  を満たす.  $a = 2^e$  とおくと,  $\sigma(a) = 2^{e+1} - 1 = N$  なので  $q = N + m$ :素数 により  $\sigma(q) = q + 1$ .

$$q + 1 = \sigma(q) = \sigma(N + m) = \sigma(\sigma(a) + m),$$

$$\sigma(\sigma(a) + m) = q + 1 = 2^{e+1} + m = 2a + m.$$

かくて

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

これを平行移動  $m$  のスーパー完全数の方程式といいこの解  $a$  を平行移動  $m$  のスーパー完全数という.

**命題 1.**  $a = 2^e$  が平行移動  $m$  のスーパー完全数ならば  $q = 2^{e+1} - 1 + m$  は素数となる.

とくに  $2^e q$  は平行移動  $m$  の狭義の完全数になる.

Proof.

式  $\sigma(\sigma(a) + m) = 2a + m$  に  $a = 2^e$  を代入すると

$$\sigma(2^{e+1} - 1 + m) = 2^{e+1} + m.$$

$k = 2^{e+1} - 1 + m$  とおくと,  $\sigma(k) = k + 1$ . よって,  $k$ : 素数.

**注意 1.** 実例にあたり,  $a = 2^e$  の仮定を弱めて,  $a$  が偶数の仮定だけでも  $a = 2^e$  が導ける可能性がある.

## 2.1 $m = 0$ のとき.

$m = 0$  のとき解は元祖完全数のみ

奇数のスーパー完全数があるか?が課題になる. 難問かもしれないし, 案外解けるかもしれない.

表 1:  $\sigma^2(a) = 2a$

$a$	素因数分解
16	$2^4$
64	$2^6$
4096	$2^{12}$
65536	$2^{16}$
262144	$2^{18}$

これらの解を  $a$  とおくととき,  $p = 2a - 1$  は素数, とくにメルセンヌ素数. 実際にやってみよう.

表 2:  $\sigma^2(a) = 2a$

$a$	素因数分解	$2a - 1$
16	$2^4$	31
64	$2^6$	127
4096	$2^{12}$	8191
65536	$2^{16}$	131071
262144	$2^{18}$	524287

## 2.2 $m = 2$ のとき.

スーパー完全数と言っても変わり映えしない.  $m = 2$  のとき, の結果を表示させて見た. 驚天動地の世界があった.

表 3:  $\sigma(\sigma(a) + 2) = 2a + 2$

$a$	素因数分解	Fermat 素数
1	$2^0$	$3 = 2 + 1$
2	$2^1$	$5 = 2^2 + 1$
8	$2^3$	$17 = 2^4 + 1$
11	11	
41	41	
65	$5 * 13$	
107	107	
128	$2^7$	$257 = 2^8 + 1$
149	149	
881	881	
959	$7 * 137$	
2141	2141	
14363	$53 * 271$	
21119	$7^2 * 431$	
32768	$2^{15}$	$65537 = 2^{32} + 1$
238895	$5 * 47779$	
967679	$23 * 42073$	

表を眺めた結果

- $a$  が偶数なら 2 のべきになり,  $2a + 1$  にはフェルマ素数が並ぶ.
- $a$  が奇数の場合は, 11, 41, 107 などの素数が出る一方, 65, 959 などの合成数が並ぶ.

$a$  が偶数なら 2 のべきになる一方,  $a$  が奇数の場合はわがもの顔に素数や合成数が出ている. これらの奇数にこう言ってやりたいと思った.

入場料は払いましたか?

## 2.3 $m = 4$ のとき.

$m = 4$  のとき解は

## 2.4 $m = 4$ のとき.

$m = 4$  のとき.

表 4:  $\sigma(\sigma(a) + 4) = 2a + 4$

$a$	素因数分解
1	1
2	2
4	$2^2$
8	$2^3$
32	$2^5$
47	47
64	$2^6$
341	$11 * 31$
587	587
2048	$2^{11}$
16384	$2^{14}$
32768	$2^{15}$
131072	$2^{17}$
249793	$19 * 13147$
1309933	$277 * 4729$
2102267	2102267

$m = 4$  のとき解は

- 1) 偶数の解  $2^e$  は  $q = 2^{e+1} + 3$ : 素数, となる. (ただし証明はできない)
- 2) 奇数の解は数多くある.

## 2.5 $m = -2$ のとき.

$m = -2$  のとき.

表 5:  $\sigma(\sigma(a) - 2) = 2a - 2$

$a$	素因数分解
4	$2^2$
7	7
8	$2^3$
16	$2^4$
29	29
32	$2^5$
253	$11 * 23$
256	$2^8$
512	$2^9$
889	$7 * 127$
2048	$2^{11}$
8192	$2^{13}$
111097	$7 * 59 * 269$
178741	$47 * 3803$
282385	$5 * 56477$
524288	$2^{19}$

$m = -2$  のときの解は

- 1) 偶数の解は  $2^e$  となり  $q = 2^{e+1} - 3$ : 素数 を満たす. (ただし証明はできない)
- 2) 奇数の解は数多くある.

平行移動  $m = -2$  の解

`factor(20)=2^2*5`

`factor(104)=2^3*13`

`factor(464)=2^4*29`

`factor(650)=2*5^2*13`

`factor(1952)=2^5*61`

`factor(130304)=2^8*509`

`factor(522752)=2^9*1021`

表 6:  $\sigma(\sigma(a) - 4) = 2a - 4$

$a$	素因数分解
4	$2^2$
8	$2^3$
23	23
32	$2^5$
107	107
128	$2^7$
242	$2 * 11^2$
467	467
512	$2^9$
653	653
2048	$2^{11}$
3077	$17 * 181$
6728	$2^3 * 29^2$
9953	$37 * 269$
131072	$2^{17}$
440897	$353 * 1249$
524288	$2^{19}$
130307	130307

$m = -4$  のとき解は

1) 偶数の解は  $2^e$  となり  $q = 2^{e+1} - 5$ : 素数 を満たす. (ただし証明はできない)

2) 奇数の解は数多くある.

`factor(12)=2^2*3`

`factor(70)=2*5*7`

`factor(88)=2^3*11`

`factor(1888)=2^5*59`

`factor(4030)=2*5*13*31`

`factor(5830)=2*5*11*53`

`factor(32128)=2^7*251`

`factor(521728)=2^9*1019`



### 3 素数解 $p$

$\sigma(\sigma(a)+m) = 2a+m$  に素数の解  $p$  があるとする. すると定義より  $\sigma(p+1+m) = 2p+m$  を満たす.

与えられた  $m$  に対し上式の解となる素数  $p$  を探した.

$$m = 2 \text{ のとき, } \sigma(p+3) = 2p+2$$

$$p = 11, 41, 107, 149, 881, 2141, 8381, 18629, 116621 \text{ (petit Fermat 素数)}$$

i). 最初の解  $p = 11$ .  $b = p+1+m = p+3 = 14 = 2Q$ . とおくとき  $Q = 11$ . ここで  $Q = 11$  を伏せておき,

$p+3 = 2Q, a = p = 2Q-3$ .  $\sigma(\sigma(a)+m) = \sigma(2Q) = 3(Q+1), 2a+2 = 4Q-6+2 = 4Q-4$  なので  $3(Q+1) = 4Q-4$ . これより  $Q = 7; a = 2Q-3 = 14-3 = 11$

ii).  $p = 41$   $p+1+2 = 4*11 = 4Q$ .  $\sigma(4Q) = 7(Q+1) = 7Q+7, 7Q+7 = 2a+2 = 2(4Q-3)+2 = 8Q-4$ .  $Q=11$ .

iii).  $p = 107$ .  $p+1+2 = 10*11 = 10Q$ .  $\sigma(10Q) = 18Q+18$ .  $a = 10Q-3$ .  $2a+2 = 20Q-4$ .

$$18Q+18 = 20Q-4 \text{ により } Q = 11, a = p = 10Q-3 = 110-3 = 107.$$

$$m = 4$$

$$p = 47, 587.$$

$$m = -2$$

$$p = 7, 29, 497, 8129$$

$$m = -4$$

$$p = 23, 107, 467, 653, 1955, 130307, 522755$$

## 4 究極のスーパー完全数 I 型

底が奇素数  $P$  のとき 狭義のスーパー完全数の平行移動  $m$  を行う.

$r = P^{f+1} - P + 1 + m$ : 素数,  $\alpha = P^f r$ : 狭義の超完全数

$a = P^f, W = P^{f+1} - 1$  とおくと  $r = W - P + 2 + m = aP - P + 1 + m, \sigma(a) = \frac{W}{\bar{P}}, W = \sigma(a)\bar{P}$ .

$$\sigma(r) = \sigma(\sigma(a)\bar{P} - P + 2 + m).$$

一方,  $W = P^{f+1} - 1 = aP - 1$  により

$$r = W - P + 2 + m = \sigma(a)\bar{P} - P + 2 + m.$$

$r$  は素数なので  $\sigma(r) = r + 1$ .

$W = P^{f+1} - 1 = aP - 1$  により  $r + 1 = W - P + 3 + m = aP - P + 2 + m$ .

以上を総合すれば

$$\sigma(r) = \sigma(\bar{P}\sigma(a) - P + 2 + m) = r + 1 = aP - P + 2 + m.$$

左と中を抜いて

$$\sigma(\bar{P}\sigma(a) - P + 2 + m) = aP - P + 2 + m.$$

この式を 究極のスーパー完全数 I 型 という.

この解を 究極のスーパー完全数 (ultimate superperfect numbers) という.

**補題 1** (素数性のレンマ).  $a = P^e$  が究極の I 型スーパー完全数とする.  $A = aP - (P-1) + m$  は素数

したがって,  $\alpha = aA = P^e A$  は平行移動  $m$  の超完全数.

Proof.

$N = P^{e+1} - 1$  とおく.  $A = \bar{P}\sigma(a) - P + 2 + m$  は  $\sigma(A) = A + 1$  を示す.

$A = \bar{P}\sigma(a) - P + 2 + m = N - P + 2 + m$  により  $aP - P + 2 + m = P^{e+1} - P + 2 + m = N - P + 3 + m = A + 1$ .

究極のスーパー完全数の定義式より,  $\sigma(\bar{P}\sigma(a) - P + 2 + m) = \sigma(A), aP - P + 2 + m = A + 1$ .

ゆえに,  $\sigma(A) = A + 1$ .  $A$  は素数.  $A = aP - P + 1 + m$  が素数になるのでこれはメルセンヌ素数の一般化.

$A$  がメルセンヌ素数の一般化なら  $\alpha = aA = P^e A$  は完全数の一般化になるに違いない.  $N = P^{e+1} - 1$  なので,  $A = aP - P + 1 + m = P^{e+1} - P + 1 + m$  が素数であり, 定義により  $\alpha = P^e A$  は平行移動  $m$  の超完全数である.

#### 4.1 超完全数からスーパー完全数へ

$\alpha$  は平行移動  $m$  の超完全数の解で正規形とする.  $Q$  を素数として  $\alpha = P^e Q$  と書けるのである.

超完全数の方程式は  $\bar{P}\sigma(\alpha) = P\alpha - P + 2 + m$ .  $N = P^{e+1} - 1$  を用いると,  $\bar{P}\sigma(\alpha) = N(Q + 1)$ ,  $P\alpha = (N + 1)Q$ .

$$\bar{P}\sigma(\alpha) - P\alpha = N - Q \text{ により } N - Q = P - 2 - m.$$

$$Q = N - P + 2 + m = P^{e+1} - P + 1 + m \text{ は素数なので } \sigma(Q) = Q + 1.$$

これより,  $a = P^e$  とおくと,  $\bar{P}\sigma(a) = N$ .  $\bar{P}\sigma(a) - P + 2 + m = N - P + 2 + m = Q$  に注意して

$$\sigma(\bar{P}\sigma(a) - P + 2 + m = N - P + 2 + m) = \sigma(Q) = Q + 1 = N - P + 2 + m + 1 = aP - P + 2 + m.$$

これはスーパー完全数の公式であり,  $a = P^e$  がスーパー完全数になった.

## 4.2 数値例

表 7: スーパー完全数  $P = 3, m = 0$

$a$	factor
3	3
7	7
19	19
55	$5 * 11$
27	$3^3$
79	79
81	$3^4$
241	241
139	139
415	$5 * 83$
243	$3^5$
727	727
6561	$3^8$
19681	19681

3 のべきの解  $3, 3^3, 3^5, 3^8$

表 8: 超完全数  $P = 3, m = 0$

$a$	factor
21	$3 * 7$
2133	$3^3 * 79$
19521	$3^4 * 241$
176661	$3^5 * 727$

解はすべて A 型

表 9: スーパー完全数  $P = 3, m = 4$

$a$	factor	
3	3	3
11	11	
9	$3^2$	$3^2$
29	29	
23	23	
71	71	
27	$3^3$	$3^3$
83	83	
559	$13 * 43$	
1679	$23 * 73$	
2159	$17 * 127$	
6479	$11 * 19 * 31$	
2187	$3^7$	$3^7$
6563	6563	
10163	10163	
30491	30491	
19683	$3^9$	$3^7$
59051	59051	
34319	34319	
102959	$149 * 691$	
51839	51839	
155519	$7 * 13 * 1709$	
592127	$17 * 61 * 571$	
1776383	$7 * 253769$	

表 10: 超完全数  $P = 3, m = 4$

$a$	factor
5	5
33	$3 * 11$
261	$3^2 * 29$
385	$5 * 7 * 11$
897	$3 * 13 * 23$
2241	$3^3 * 83$
26937	$3^2 * 41 * 73$
46593	$3^2 * 31 * 167$

## 5 究極のスーパー完全数 II 型

底が奇素数  $P$  のとき スーパー完全数の平行移動  $m$  を行う.  
 $q = \sigma(P^e) + m$  を素数とし,  $a = P^e$ ,  $N = P^{e+1} - 1$  とおくと,

$$q = \sigma(a) + m, q = \frac{N}{\bar{P}} + m.$$

$$\text{これより, } q - m = \frac{N}{\bar{P}}.$$

$$\text{そこで } \sigma(q) = \sigma(\sigma(a) + m), \sigma(q) = q + 1.$$

$$\sigma(\sigma(a) + m) = q + 1 = \frac{N}{\bar{P}} + m + 1 = \frac{aP - 2 + P}{\bar{P}} + m.$$

分母を取り去って

$$\sigma(\sigma(a) + m) = \frac{aP - 2 + P}{\bar{P}} + m.$$

$$\bar{P}(\sigma(\sigma(a) + m) - m) = aP + P - 2.$$

これが底が奇素数  $P$ , 平行移動  $m$  のときのスーパー完全数の方程式である.

これを一般に II 型の究極のスーパー完全数 (ultimate superperfect numbers) の方程式という.

この解を II 型の究極のスーパー完全数 (ultimate superperfect numbers) という.  
 $m = 0$  のとき,

$$\bar{P}(\sigma(\sigma(a))) = aP + P - 2.$$

$$P = 3 \text{ なら } 2\sigma(\sigma(a)) = 3a + 1.$$

$$P = 5 \text{ なら } 4\sigma(\sigma(a)) = 5a + 3.$$

**補題 2.**  $a = P^e$  が究極の II 型スーパー完全数とする.  $B = \frac{aP - 1}{\bar{P}} + m$  は素数

特に,  $\alpha = aB = P^e B$  は

Proof.

$N = P^{e+1} - 1$  とおく.  $B = \sigma(a) + m = \sigma(P^e) + m$  は  $\sigma(B) = B + 1$  を示す.

究極の II 型スーパー完全数の定義式を  $\bar{P}$  で割ると

$$\sigma(\sigma(a) + m) - m = \frac{aP + P - 2}{\bar{P}}.$$

$$\sigma(a) = \frac{N}{\bar{P}} = \frac{aP - 1}{\bar{P}} \text{ により, } \bar{P}\sigma(a) = aP - 1.$$

スーパー完全数の定義式の右辺を計算する.

$$aP + P - 2 = aP - 1 + \bar{P} = (\sigma(a) + 1)\bar{P} = (B - m + 1)\bar{P},$$

により

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

$\sigma(B) - m = B - m + 1$  によると  $\sigma(B) = B + 1$ .  $B$  は偶数.

$B = \sigma(a) + m = \frac{aP - 1}{\overline{P}} + m$  は一般化された Mersenne 素数.

$\alpha = aB = P^e B$  は平行移動  $m$  の究極の完全数である.

$a = P^e$  なら  $B = \frac{aP - 1}{\overline{P}} + m$  となり素数であることがわかったが  $a = P^e$  と書けない  
なら  $B = \sigma(a) + m$  の意義は不明.

## 6 スーパー型のオイラー完全数

スーパー完全数の類似を狙って、 $\sigma(a)$  の代わりに  $\varphi(a)$  を用いてみよう。

$a = 2^e$  とするとき  $q = 2\varphi(a) + 1 = 2^e + 1$ .  $q$  が素数なら  $q$  はフェルマ素数である。

$q$  が素数のとき、 $\varphi(q) = q - 1$  なので、 $\varphi(q) = \varphi(2\varphi(a) + 1) = q - 1, q - 1 = 2^e = a$  により

$$\varphi(2\varphi(a) + 1) = a.$$

$a = 2^e$  は上の式を満たすが逆を簡単に示すことができる。

**補題 3.** 究極の完全数が正規形なら、その  $P^e$  はスーパー完全数

Proof.

平行移動  $m$  の究極の完全数の方程式は



## 6.1 数値例

表 11:  $2\sigma(\sigma(a)) = 3a + 1$ , II 型

$a$	素因数分解
9	$3^2$
729	$3^6$
531441	$3^{12}$

表 12:  $2(\sigma(\sigma(a) + 3) - 3) = 3a + 5$ , II 型

$a$	素因数分解
3	3
27	$3^3$
243	$3^5$
19683	$3^9$

表 13:  $4\sigma^2(a) = 5a + 3$ , II 型

$a$	素因数分解
25	$5^2$
15625	$5^6$

計算例から推測する.

$P \geq 3, m = 0$  のとき解はすべて微小解  $P^e$

**命題 2.**  $\bar{P}(\sigma(\sigma(a) + m) - m) = aP + P - 2$  の解  $P^e$  があるとす.  $Q = \sigma(P^e) + m$  は素数になる.

Proof.

$a = P^e$  を代入する,  $N = P^{e+1} - 1$  とおくとき  $\sigma(P^e) = \frac{N}{P}$ .

$Q = \sigma(P^e) + m = \frac{N}{P} + m$  とおくとき

$$\bar{P}(\sigma(\frac{N}{P} + m) - m) = N + 1 + P - 2.$$

$\sigma(\frac{N}{P} + m) - m = \sigma(Q) - m$  を用いて

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

$\overline{P}$  で割ると

$$\sigma(Q) - m = \frac{N}{\overline{P}} + 1.$$

変形して

$$\sigma(Q) = \frac{N}{\overline{P}} + m + 1 = Q + 1.$$

$Q$  は素数になった.

$Q = \sigma(a) + m$  を一般メルセンヌ数という.  $a = P^e$  なら  $Q = \frac{aP}{P} + m$  となり素数である.

$a = P^e$  と書けないときは  $Q = \sigma(a) + m$  の意味はまったく分からない.

## 7 メルセンヌ数

表 14:  $P = 2, m = 2$

$a$	mersenne	$a$ の素因数分解
2	5	2
8	17	$2^3$
11	14	11
41	44	41
65	86	$5 * 13$
107	110	107
128	257	$2^7$
149	152	149
881	884	881
959	1106	$7 * 137$
2141	2144	2141
14363	14690	$53 * 271$
21119	24626	$7^2 * 431$
32768	65537	$2^{15}$

表 15:  $P = 2, m = 2$

$a$	$a$ factor	mer	$Mer$ の factor
1	1	3	3
2	2	5	5
8	$2^3$	17	17
11	11	23	23
41	41	83	83
65	$5 * 13$	131	131
107	107	215	$5 * 43$
128	$2^7$	257	257
149	149	299	$13 * 23$
881	881	1763	$41 * 43$
959	$7 * 137$	1919	$19 * 101$
2141	2141	4283	4283
14363	$53 * 271$	28727	$23 * 1249$
21119	$7^2 * 431$	42239	42239
32768	$2^{15}$	65537	65537
238895	$5 * 47779$	1935359	477791

表 16:  $P = 3, m = 3$

$a$	mersenne	$a$ の素因数分解
3	7	3
27	43	$3^3$
243	367	$3^5$
19683	29527	$3^9$

## 8 究極のスーパーオイラー完全数 I 型

底の素数  $P$ , 平行移動  $m$  に関する究極のスーパーオイラー完全数 I 型の定義をする.

$q = \varphi(P^e) + 1 + m$  は素数とする.

$a = P^e$  とおく.  $q = \varphi(a) + 1 + m$ ,  $\varphi(q) = q - 1$  なので

$\varphi(q) = \varphi(\varphi(a) + 1 + m)$ . 一方,  $q - 1 = \varphi(P^e) + m = \varphi(a) + m$ . これを組み合わせると,

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

これから中抜きして

$$\varphi(\varphi(a) + 1 + m) = \varphi(a) + m.$$

$$a = P^e \text{ により } \varphi(a) = P^{e-1}\bar{P} = \frac{P^e\bar{P}}{P} = \frac{a\bar{P}}{P}.$$

表 17:  $P = 2, m = 0$

$a$	mersenne	$a$ の素因数分解
2	3	2
4	7	$2^2$
16	31	$2^4$
64	127	$2^6$
4096	8191	$2^{12}$
65536	131071	$2^{16}$
262144	524287	$2^{18}$

$$P\varphi(\varphi(a) + 1 + m) = \bar{P}a + mP.$$

これを  $a$  についての方程式と見て, 究極のスーパーオイラー完全数の I 型定義方程式という. この解を 究極のスーパーオイラー完全数と呼ぶ.

$P = 2$  のとき, スーパーオイラー完全数の I 型定義方程式は

$$2\varphi(\varphi(a) + 1 + m) = a + 2m.$$

**定理 2.**  $P\varphi(\varphi(a) + 1 + m) = \bar{P}a + mP$  の解は  $a = P^e$  となる.

Proof.

$$P\varphi(\varphi(a) + 1 + m) = \bar{P}a + mP \text{ の式により } a \equiv 0 \pmod{P}.$$

$a = P^e L, ((P, L) = 1)$ , と書ける.  $L = 1$  を示す.

$a = \varphi(P^e L) = P^{e-1} \bar{P} \varphi(L)$  を式に代入する.

$$P\varphi(\varphi(a) + 1 + m) = P\varphi(P^{e-1} \bar{P} \varphi(L) + 1 + m), \bar{P}a + mP = P(\bar{P}P^{e-1} + m) \text{ により}$$

$$P\varphi(P^{e-1} \bar{P} \varphi(L) + 1 + m) = P(\bar{P}P^{e-1} + m).$$

よって,

$$\varphi(P^{e-1} \bar{P} \varphi(L) + 1 + m) = \bar{P}P^{e-1}L + m.$$

$P^{e-1} \bar{P} = \varphi(P^e)$  によって,

$$\varphi(\varphi(P^e) \varphi(L) + 1 + m) = \bar{P}P^{e-1}L + m.$$

一般に  $x > 1$  なら  $x - 1 \geq \varphi(x)$ . これを  $x = \varphi(P^e) \varphi(L) + 1 + m$  について使うと

$$\begin{aligned} x - 1 &= \varphi(P^e) \varphi(L) + m \\ &\geq \varphi(\varphi(P^e) + \varphi(L) + 1 + m) \\ &= \bar{P}P^{e-1}L + m \end{aligned}$$

$$\varphi(P^e)\varphi(L) + m \geq \overline{P}P^{e-1}L + m.$$

よって

$$\varphi(P^e)\varphi(L) \geq \overline{P}P^{e-1}L = \varphi(P^e)L.$$

$\varphi(P^e)(\varphi(L) - L) \geq 0$  になるので  $0 \geq \varphi(L) - L \geq 0$ . これより,  $L = 1; a = P^e$ .

$q = \varphi(a) + 1 + m = \overline{P}P^{e-1} + 1 + m$  は素数なのでこれをオイラー型 Mersenne 素数という.

例  $P = 3, m = 3$

## 9 究極のスーパーオイラー完全数 II 型

底の素数  $P$ , 平行移動  $m$  に関する究極のスーパーオイラー完全数 II 型を定義する.

$q_0 = P\varphi(P^e) + 1 + m$  は素数とする.

$a = P^e$  とおく.  $\varphi(q_0) = q_0 - 1$  なので  $\varphi(q_0) = \varphi(P\varphi(a) + 1 + m)$ .

一方,  $q_0 - 1 = P\varphi(P^e) + m = a\overline{P} + m$ . これを組み合わせると,

$$\varphi(P\varphi(a) + 1 + m) = a\overline{P} + m.$$

これを 究極のスーパーオイラー完全数 II 型の定義式といいこの解を究極のスーパーオイラー II 型完全数という.

## 10 $P = 2$ の場合

最初に  $P = 2$  の場合を扱う. スーパーオイラー完全数 II 型の定義式は

$$\varphi(2\varphi(a) + 1 + m) = a + m.$$

### 10.1 $m$ :偶数

$m$  を偶数と仮定する.  $\varphi(a)$  は  $a > 2$  なら偶数なので  $a$  も偶数. 奇数の  $L$  によって  $a = 2^e L$  と書ける.  $2\varphi(a) + 1 + m > 1$  を仮定しておく. これは  $m$  が一般の負の場合を扱うので記憶に留めておくとよい.  $x = 2\varphi(a) + 1 + m > 1$  なので,  $\varphi(x) \leq x - 1 = 2\varphi(a) + m$ .

$$a + m = \varphi(2\varphi(a) + 1 + m) = \varphi(x) \leq x - 1 = 2\varphi(a) + m$$

$$2^e L = a + m \leq x - 1 = 2\varphi(a) + m = 2^e \varphi(L) + m.$$

$L \leq \varphi(L)$  により,  $L = 1, a = 2^e$ .  $Q = 2\varphi(a) + 1 + m = 2^e + 1 + m$ ,

$$\varphi(Q) = \varphi(2\varphi(a) + 1 + m) = a + m = 2^e + m = Q - 1.$$

ゆえに  $Q = 2^e + 1 + m$  は素数になった.

$m = 0$  なら  $Q = 2^e + 1$  はフェルマ素数.

$m = -2$  なら  $Q = 2^e - 1$  はメルセンヌ素数.

## 10.2 $m$ :奇数

$m$  を奇数と仮定する.  $\varphi(a)$  は  $a > 2$  なら偶数なので  $a$  も奇数になる. ここでも奇数完全数の不存在問題が連想されて戦意をそがれる思いがする.

とりあえず計算してみると,  $m > -3$  の場合は解が見つからない. しかし  $m = -3, -5, -7, -9 \dots$  になると多くの解が見いだせる.

## 10.3 $m = -3$ :

$$4 = 2^2$$

$a$	$a - 2$
5	3
7	5
13	11
19	17
31	29
43	41
61	59
73	71
103	101
109	107
139	137
151	149
181	179
193	191
199	197

$a = 4$  が先頭の解だが以下はすべて素数. すべての素数ではない.  $a, a - 2$  がともに素数なのでこれらは双子素数になる.

$\varphi(2\varphi(a) + 1 + m) = a + m$  において,  $m = -3$  とおくと  $\varphi(2\varphi(a) - 2) = a - 3$ .

$a = 4$  は確かに解.

$a = 2 + p$  とし  $p, a$  はともに素数とする.

$2\varphi(a) - 2 = 2(a - 1) - 2 = 2a - 4 = 2p$  になり  $\varphi(2p) = p - 1 = a - 3$ .

こうして双子素数の解が確認できた.

10.4  $m = -5$ :

$$9 = 3^2$$

$a$	$a - 3$	$p = (a - 3)/2$
13	10	5
17	14	7
29	26	13
37	34	17
41	38	19
61	58	29
89	86	43
97	94	47
109	106	53
137	134	67
149	146	73
181	178	89
197	194	97
229	226	113
257	254	127
277	274	137
281	278	139

$\varphi(2\varphi(a) + 1 + m) = a + m$  において,  $m = -5$  とおくと  $\varphi(2\varphi(a) - 4) = a - 5$ .

$a > 9$  の解は素数なので  $a$ : 素数なら  $2\varphi(a) - 4 = 2(a - 1) - 4 = 2(a - 3)$

$a - 3$  は偶数なのでこれを 2 で割って表計算をするとこれは素数が並んでいる.

$p = \frac{a-3}{2}$  とおくと  $a = 2p + 3, 2a - 6 = 4p$

$2\varphi(a) - 4 = 2(a - 3) = 4p$  そこで  $\varphi(2a - 6) = \varphi(4p) = 2(p - 1) = a - 5$ .

$p, a = 2p + 3$  がともに素数となる場合は無限にあるかもしれない. かくして双子素数と類似した素数の対についてこれらが無限にあるか, という問題ができた.

$m = -7$  のときは解は  $a = 2^3, 3^2, 13$  が発見された.

$a$	$a - 5$	$p = (a - 5)/2$
17	12	3
25	20	5
73	68	17
97	92	23
193	188	47
241	236	59
337	332	83
409	404	101
433	428	107
457	452	113
601	596	149
673	668	167
769	764	191

$a = 2p + 5, p$  がともに素数ならこれから解ができる.