

# 書泉グランデ

## 高校生もわかる新しい数論研究

### 第1期 予稿2; 完全数の水平展開2

飯高 茂

2016 年 10 月 28 日

#### 1 完全数の水平展開の俯瞰

$a \leq 2000$  について  $m$  が小さい場合の数表を最初に見てみよう.

この数表を毎日睨んでいるとある日数表の方から「これは面白いですよ」と言ってくるに違いない.

$a \leq 2000$  に制限しているのはエクセルで処理したせいである. これを見て目星をつけたら, 1 千万または 2 千万以下について wxmaxima による数表を開いて確認することができる.

## 1.1 $m = 42, 50$

表 1:  $m = 42, 50$

$a$	factor	$\sigma(a)$	$m$
106	[2, 53]	162	50
1264	[2 <sup>4</sup> , 79]	2480	48
225	[3 <sup>2</sup> , 5 <sup>2</sup> ]	403	47
47	[47]	48	46
65	[5, 13]	84	46
212	[2 <sup>2</sup> , 53]	378	46
488	[2 <sup>3</sup> , 61]	930	46
94	[2, 47]	144	44
238	[2, 7, 17]	432	44
310	[2, 5, 31]	576	44
472	[2 <sup>3</sup> , 59]	900	44
43	[43]	44	42
69	[3, 23]	96	42
99	[3 <sup>2</sup> , 11]	156	42
165	[3, 5, 11]	288	42
1168	[2 <sup>4</sup> , 73]	2294	42
1365	[3, 5, 7, 13]	2688	42

$m = 42$  のとき, 解が多いので  $a$  が 千万まで調べてみた.

表 2:  $m = 42$  追加分

$a$	factor
1365	$3 * 5 * 7 * 13$
2139136	$2^{10} * 2089$

## 1.2 $m = 24, 41$

表 3:

$a$	factor	$\sigma(a)$	$m$
49	$[7^2]$	57	41
81	$[3^4]$	121	41
41	$[41]$	42	40
86	$[2, 43]$	132	40
188	$[2^2, 47]$	336	40
290	$[2, 5, 29]$	540	40
950	$[2, 5^2, 19]$	1860	40
1136	$[2^4, 71]$	2232	40
1196	$[2^2, 13, 23]$	2352	40
1364	$[2^2, 11, 31]$	2688	40
55	$[5, 11]$	72	38
82	$[2, 41]$	126	38
424	$[2^3, 53]$	810	38
484	$[2^2, 11^2]$	931	37
37	$[37]$	38	36
172	$[2^2, 43]$	308	36
1072	$[2^4, 67]$	2108	36
57	$[3, 19]$	80	34
74	$[2, 37]$	114	34
164	$[2^2, 41]$	294	34

表 4:  $m = 40$  追加分

$a$	factor
260084	$2^2 * 11 * 23 * 257$
544256	$2^9 * 1063$
2137088	$2^{10} * 2087$

### 1.3 $m = 26, \dots, 32$

表 5:

$a$	factor	$\sigma(a)$	$m$
250	$[2, 5^3]$	468	32
376	$[2^3, 47]$	720	32
1276	$[2^2, 11, 29]$	2520	32
31	$[31]$	32	30
51	$[3, 17]$	72	30
135	$[3^3, 5]$	240	30
148	$[2^2, 37]$	266	30
976	$[2^4, 61]$	1922	30
29	$[29]$	30	28
62	$[2, 31]$	96	28
182	$[2, 7, 13]$	336	28
230	$[2, 5, 23]$	432	28
344	$[2^3, 43]$	660	28
944	$[2^4, 59]$	1860	28
58	$[2, 29]$	90	26
75	$[3, 5^2]$	124	26
328	$[2^3, 41]$	630	26
850	$[2, 5^2, 17]$	1674	26
1210	$[2, 5, 11^2]$	2394	26

#### 1.4 $m = 18, \dots, 25$

表 6:

$a$	factor	$\sigma(a)$	$m$
98	$[2, 7^2]$	171	25
124	$[2^2, 31]$	224	24
23	$[23]$	24	22
35	$[5, 7]$	48	22
39	$[3, 13]$	56	22
63	$[3^2, 7]$	104	22
116	$[2^2, 29]$	210	22
296	$[2^3, 37]$	570	22
848	$[2^4, 53]$	1674	22
46	$[2, 23]$	72	20
154	$[2, 7, 11]$	288	20
190	$[2, 5, 19]$	360	20
25	$[5^2]$	31	19
19	$[19]$	20	18
33	$[3, 11]$	48	18
105	$[3, 5, 7]$	192	18

### 1.5 $m = 10, \dots, 25$

表 7:  $m = 22$  追加分

$a$	factor	$\sigma(a)$	$m$
848	$2^4 * 53$		22
9536	$2^6 * 149$		22
35456	$2^7 * 277$		22
2118656	$2^{10} * 2069$		22

**1.6**  $m = 1, \dots, 6$

表 8:

$a$	factor	$\sigma(a)$	$m$
17	[17]	18	16
38	[2, 19]	60	16
92	[2 <sup>2</sup> , 23]	168	16
170	[2, 5, 17]	324	16
248	[2 <sup>3</sup> , 31]	480	16
752	[2 <sup>4</sup> , 47]	1488	16
988	[2 <sup>2</sup> , 13, 19]	1960	16
27	[3 <sup>3</sup> ]	40	14
34	[2, 17]	54	14
232	[2 <sup>3</sup> , 29]	450	14
13	[13]	14	12
45	[3 <sup>2</sup> , 5]	78	12
76	[2 <sup>2</sup> , 19]	140	12
688	[2 <sup>4</sup> , 43]	1364	12
11	[11]	12	10
21	[3, 7]	32	10
26	[2, 13]	42	10
68	[2 <sup>2</sup> , 17]	126	10
656	[2 <sup>4</sup> , 41]	1302	10

**1.7**  $m = -8, \dots, 0$



表 9:

$a$	factor	$\sigma(a)$	$m$
22	[2, 11]	36	8
130	[2, 5, 13]	252	8
184	[2 <sup>3</sup> , 23]	360	8
1012	[2 <sup>2</sup> , 11, 23]	2016	8
50	[2, 5 <sup>2</sup> ]	93	7
7	[7]	8	6
15	[3, 5]	24	6
52	[2 <sup>2</sup> , 13]	98	6
315	[3 <sup>2</sup> , 5, 7]	624	6
592	[2 <sup>4</sup> , 37]	1178	6
1155	[3, 5, 7, 11]	2304	6
9	[3 <sup>2</sup> ]	13	5
5	[5]	6	4
14	[2, 7]	24	4
44	[2 <sup>2</sup> , 11]	84	4
110	[2, 5, 11]	216	4
152	[2 <sup>3</sup> , 19]	300	4
884	[2 <sup>2</sup> , 13, 17]	1764	4
3	[3]	4	2
10	[2, 5]	18	2
136	[2 <sup>3</sup> , 17]	270	2
2	[2]	3	1
2 <sup>e</sup>	[2 <sup>e</sup> ]	2 <sup>e+1</sup> - 1	1

1.8  $m = -10, \dots, -19$

表 10:

$a$	factor	$\sigma(a)$	$m$
6	[2, 3]	12	0
28	[2 <sup>2</sup> , 7]	56	0
496	[2 <sup>4</sup> , 31]	992	0
20	[2 <sup>2</sup> , 5]	42	-2
104	[2 <sup>3</sup> , 13]	210	-2
464	[2 <sup>4</sup> , 29]	930	-2
650	[2, 5 <sup>2</sup> , 13]	1302	-2
1952	[2 <sup>5</sup> , 61]	3906	-2
18	[2, 3 <sup>2</sup> ]	39	-3
12	[2 <sup>2</sup> , 3]	28	-4
70	[2, 5, 7]	144	-4
88	[2 <sup>3</sup> , 11]	180	-4
1888	[2 <sup>5</sup> , 59]	3780	-4
196	[2 <sup>2</sup> , 7 <sup>2</sup> ]	399	-7
56	[2 <sup>3</sup> , 7]	120	-8
368	[2 <sup>4</sup> , 23]	744	-8
836	[2 <sup>2</sup> , 11, 19]	1680	-8

**1.9**  $m = -20, \dots, -39$

**1.10**  $m = -50, \dots, -40$

表 11:

$a$	factor	$\sigma(a)$	$m$
40	$[2^3, 5]$	90	-10
1696	$[2^5, 53]$	3402	-10
24	$[2^3, 3]$	60	-12
30	$[2, 3, 5]$	72	-12
42	$[2, 3, 7]$	96	-12
54	$[2, 3^3]$	120	-12
$6p$	$[2, 3, p]$	$12(p+1)$	-12
304	$[2^4, 19]$	620	-12
550	$[2, 5^2, 11]$	1116	-16
748	$[2^2, 11, 17]$	1512	-16
1504	$[2^5, 47]$	3024	-16
100	$[2^2, 5^2]$	217	-17
208	$[2^4, 13]$	434	-18
36	$[2^2, 3^2]$	91	-19

表 12:

$a$	factor	$\sigma(a)$	$m$
176	$[2^4, 11]$	372	-20
1376	$[2^5, 43]$	2772	-20
1312	$[2^5, 41]$	2646	-22
112	$[2^4, 7]$	248	-24
80	$[2^4, 5]$	186	-26
1184	$[2^5, 37]$	2394	-26
48	$[2^4, 3]$	124	-28
945	$[3^3, 5, 7]$	1920	-30
572	$[2^2, 11, 13]$	1176	-32
992	$[2^5, 31]$	2016	-32
928	$[2^5, 29]$	1890	-34
162	$[2, 3^4]$	363	-39

表 13:

$a$	factor	$\sigma(a)$	$m$
736	$[2^5, 23]$	1512	-40
1352	$[2^3, 13^2]$	2745	-41
350	$[2, 5^2, 7]$	744	-44
608	$[2^5, 19]$	1260	-44
490	$[2, 5, 7^2]$	1026	-46
544	$[2^5, 17]$	1134	-46
60	$[2^2, 3, 5]$	168	-48
416	$[2^5, 13]$	882	-50

## 2 $m \geq 0$ の場合

$m = 0$  なら完全数の式である.

$m = 2$  ならフェルマ素数が出てくる.

### 2.1 $[P = 2, m = 0]$ 完全数

次の結果はパソコンで  $\sigma(a)$  の定義をそのまま用いて完全数の方程式  $\sigma(a) - 2a = 0$  について  $a$  を 2 から 10,000,000 までについて調べた結果である.

表 14:  $[P = 2, m = 0]$  完全数

$a$	素因数分解
6	$2 * 3$
28	$2^2 * 7$
496	$2^4 * 31$
8128	$2^6 * 127$

$a = 2^e q, (q = 2^{e+1} - 1 : \text{メルセンヌ素数})$  の形.

一般に解  $a = 2^e q, (q : \text{素数})$  の形になす解を正規形とよぶ.

正規形  $2^e q$  が  $\sigma(a) = 2a - m$  を満たすなら  $q = 2^{e+1} - 1 + m : \text{素数}$  となる.

$m = 0$  のとき広義の完全数は正規形になる, というのが古代の数学者の抱いた夢の 1 つで, 偶数の場合に解決したのがオイラーである.

これは言い方を変えれば広義の完全数は狭義の完全数になるという予想になる.

### 2.2 $[P = 2, m = 2]$ 完全数

表 15:  $[P = 2, m = 2]$  完全数

$a$	素因数分解
3	3
10	$2 * 5$
136	$2^3 * 17$
32896	$2^7 * 257$
2147516416	$2^{15} * 65537$

$a = 2^e q, (q = 2^{e+1} + 1 : \text{フェルマ素数})$

フェルマ素数 3,5,17,257,65537 が出てくる. これらはいわゆるフェルマ素数 5 兄弟である.

$m = 2$  のとき広義の完全数は狭義の完全数になる, ということは正しそうである.

$a$  が偶数に限ってでもこのことを証明したいができない.

以下広義の完全数に限って計算した結果を載せる.

### 2.3 $[P = 2, m = 4]$ 完全数

表 16:  $[P = 2, m = 4]$  完全数

$a$	素因数分解
5	5
14	$2 * 7$
44	$2^2 * 11$
110	$2 * 5 * 11$
152	$2^3 * 19$
884	$2^2 * 13 * 17$
2144	$2^5 * 67$
8384	$2^6 * 131$
18632	$2^3 * 17 * 137$
116624	$2^4 * 37 * 197$

正規形  $2^e q$  以外に非正規形の解が次のように登場する.

$$a = 884 = 2^2 * 13 * 17$$

$$a = 18632 = 2^3 * 17 * 137$$

$$a = 116624 = 2^4 * 37 * 197$$

これらは  $2^e r q (r < q : \text{primes})$  形であり  $\sigma(a) = 2a - 4$  を満たすが正規形ではない.

かくして,  $m = 4$  の場合は広義の完全数で狭義の完全数にならないものが出てきた.

$m = 0, 2$  の場合のように, 広義の完全数は狭義の完全数になるという予想は  $m = 4$  では成立せず反例がいくつもでてきた.

これを安易に予想をたてるものではない, という理解につなげてはいけない.

$m = 4$  の場合は予想を少し修正して,  $m = 4$  のとき広義の完全数は  $2^e q, 2^e r q$  と書ける. とすることができる.

コンピュータの計算によると千万以下の  $a$  については正しい. 果たして一般に成り立つだろうか? これは大難問であると思う.

## 2.4 解 $a = 2^e qr$ を求めるアルゴリズム

$\sigma(a) = 2a - m$  の解として  $a = 2^e qr (2 < q < r: \text{素数})$  があるとする.

$$\sigma(a) = (2^{e+1} - 1)\tilde{q}\tilde{r}, 2a - m = 2^{e+1}qr - m$$

により  $N = 2^{e+1} - 1, \Delta = q + r$  を使うと

$$N\tilde{q}\tilde{r} = 2^{e+1}qr - m.$$

$\tilde{q}\tilde{r} = qr + \Delta + 1$  なので

$$N(qr + \Delta + 1) = (N + 1)qr - m.$$

ゆえに

$$-qr + N(\Delta + 1) = m$$

$q_0 = q - N, r_0 = r - N$  を用いると  $q_0 r_0 = qr - N\Delta + N^2$  なので,

$$q_0 r_0 = N(N + 1) + m.$$

$D = N(N + 1) + m$ , とおけば,  $q_0 r_0 = D$ .

そこで与えられた  $e, m$  に対し,  $D = N(N + 1) + m$ , とおき,  $q_0 r_0 = D$  となる  $q_0, r_0$  について,  $q = q_0 + N, r = r_0 + N$  がともに素数になれば  $a = 2^e qr$  が解.

$N + 1 = 2^{e+1}$  は 4 の倍数なので  $N(N + 1)$  も 4 の倍数.  $q_0, r_0$  はともに偶数なので  $q_0 r_0$  も 4 の倍数. したがって  $m$  も 4 の倍数. だから,  $m = 2$  や  $m = 6$  の場合には  $a = 2^e qr$  型の解はない.

はじめに手計算で求める.

i.  $e = 1, N = 3, D = 16, r_0 = 2, q_0 = 8, r = 5, q = 13.$

ii.  $e = 2, N = 7, D = 60, r_0 = 6, q_0 = 10, r = 13, q = 17.$

iii.  $e = 3, N = 15, D = 244, r_0 = 2, q_0 = 122, r = 17, q = 137.$

アルゴリズムを基に swiprolog で作ったプログラムによる解は次のとおり.

$$a = 2^2 * 13 * 17 = 884$$

$$a = 2^3 * 17 * 137 = 18632$$

$$a = 2^4 * 37 * 197 = 116624$$

$$a = 2^6 * 137 * 1753 = 15370304$$

$$a = 2^7 * 293 * 1973 = 73995392$$

$e < 15$  まで調べたが解はこれ以上見つからない.

フェルマ素数 5 兄弟のように,  $2^e qr$  と書ける解はこれら 5 個しかないかもしれない.

しかしこれが正しい根拠はなにもない.



## 2.5 $[P = 2, m = 6]$ 完全数

表 17:  $[P = 2, m = 6]$  完全数

$a$	素因数分解
7	7
15	$3 * 5$
52	$2^2 * 13$
315	$3^2 * 5 * 7$
592	$2^4 * 37$
1155	$3 * 5 * 7 * 11$
2102272	$2^{10} * 2053$

驚いたことにこの解は非常に特色があり本当に面白い.

正規形の解は  $a = 52 = 2^2 * 13, 592 = 2^4 * 37, 2102272 = 2^{10} * 205$  で意外に少ない.

無理して探すと正規形の解はまだある (たぶん無数にある).

$a = 9903520314283394042913882112 = 2^{46} * 140737488355333$

さらに非正規形の解がいくつか登場する.

$a = 7$  ( $a$  が素数の場合は後でふれる)

$a = 15 = 3 * 5$  ( $a = pq$  は  $p < q, p, q$ : 素数の場合は後でふれる)

これは易しい解である.

非正規形の解:

$a = 315 = 3^2 * 5 * 7, 1155 = 3 * 5 * 7 * 11$  が2つ出てきた.

これは正規形の解とは全く異なり、今までにない新種の解である. これにはびっくりポン. そこで、これら新種の解をモンスターと呼んでみたい.

$a = 315 = 3^2 * 5 * 7$  はモンスター 315 であるが ニックネームとしてシチゴサンと呼ぶ.

これは奇数で  $3^e r q$  の形に書ける.

一方  $a = 1155 = 3 * 5 * 7 * 11$  は小さいほうから奇素数4つの積であり、その姿形が美しい. これは和服の帯を連想させるものがあるのでオビと命名しよう.

## 2.6 オビ 1155 の特徴づけ

i.  $a = 3 * 5rq (5 < r < q)$ : 素数を仮定すると,  $r = 7, q = 11$ .

Proof

$\sigma(a) = 24\tilde{r}\tilde{q}, 2a - 6 = 30rq - 6$  により

$$4\tilde{r}\tilde{q} = 5rq - 1.$$

$r \geq 7$  になる.

a.  $r = 7$  のとき

$32\tilde{q} = 35q - 1$  により  $32 = 3q - 1$ . これより  $q = 11$ .

b.  $r \geq 11$  のとき

$4r\tilde{q} + 4\tilde{q} = 5rq - 1$  によって

$$4\tilde{q} + 1 = r(5q - 4\tilde{q}) = r(q - 1) \geq 11q - 44.$$

$4q + 49 \geq 11q$  により  $49 \geq 7q$ .  $q \leq 7$ .  $q > r \geq 11$  に矛盾.

ii.  $a = 3qrs, (3 < q < r < s: \text{素数})$  を仮定するとき,  $q = 5, q = 7, r = 11$ .

Proof

$q = 5$  は前に扱ったので  $q \geq 7$  を仮定して矛盾を導く.

$\sigma(a) = 4\tilde{q}\tilde{r}\tilde{s}, 2a - 6 = 6qrs - 6$  により 2 で割って

$$2\tilde{q}\tilde{r}\tilde{s} = 3qrs - 3.$$

$A = \tilde{r}\tilde{s}, B = rs$  とおくとき

$$2(q + 1)A = 3qB - 3.$$

これより  $q(3B - 2A) = 2A + 3$ .  $q \geq 7$  を思い出してしたがって

$$2A + 3 = q(3B - 2A) \geq 7(3B - 2A) = 21B - 14A.$$

変形して

$$16A + 3 \geq 21B.$$

$\Delta = r + s$  を用いて

$$16(B + \Delta + 1) + 3 \geq 21B.$$

ゆえに

$$16(\Delta + 1) + 3 \geq 5B.$$

$r, s$  を用いて書き直すと

$$16(r + s + 1) + 3 \geq 5rs.$$

$r \geq 11$  でまとめると

$$16s + 19 \geq r(5s - 16) \geq 11(5s - 16) = 55s - 176.$$

これより

$195 \geq 39s$ . よって  $s < 5$ ;  $s \geq r + 2 \geq 13$  に矛盾.

iii.  $a = pqrs$ , ( $2 < p < q < r < s$ :素数) を仮定するとき,  $p = 3, q = 5, q = 7, r = 11$ .

Proof

$p = 3$  のときは ii で示したので  $p \geq 5$  を仮定して矛盾を導く.

$\sigma(a) = \widetilde{pqr}s, 2a - 6 = 2pqrs - 6$  により

$A = \widetilde{qr}s, B = qrs$  とおくと  $\sigma(a) = (p + 1)A, pqrs = pB$ .

$\sigma(a) = 2a - 6$  により  $(p + 1)A = 2pB - 6$  なので

$$p(2B - A) = A + 6.$$

これより  $2B - A > 0$  なので  $p \geq 5$  により

$$p(2B - A) = A + 6 \geq 5(2B - A) = 10B - 5A.$$

$$6A + 6 \geq 10B.$$

2 で割って

$$3A + 3 \geq 5B.$$

$C = \widetilde{rs}, D = rs$  とおくと  $A = (q + 1)C, B = qD$ .

よって,

$$3(q + 1)C + 3 \geq 5qD.$$

ゆえに

$$3C + 3 \geq q(5D - 3C).$$

$q \geq p + 2 \geq 7$  により

$$3C + 3 \geq q(5D - 3C) \geq 7(5D - 3C) = 35D - 21C.$$

$$3 + 24C \geq 35D.$$

$\Delta = r + s$  とおくととき  $C = D + \Delta + 1$  になり

$$3 + 24(D + \Delta + 1) \geq 35D.$$

よって,

$$3 + 24(\Delta + 1) = 24\Delta + 27 \geq 11D.$$

$$24(r + s) + 27 \geq 11rs$$

となり  $s \geq r + 2$  を用いて

$$24r + 27 \geq 11rs - 24s = (11r - 24)s \geq (11r - 24)(r + 2) = 11r^2 - 22r - 48.$$

よって,

$$24r + 27 \geq 11r^2 - 22r - 48.$$

これより

$$75 \geq 11r^2 - 46r = r(11r - 46).$$

これを解くと  $r < 7$ .

$r > q \geq 11$  なのでこれは成り立たない.

かくして 6 だけ平行移動した完全数で、4つの素数の積にかけるものはオビに限る、ことが証明できた。(できてみれば簡単だが最初はオビの特徴づけはあきらめていた)

## 2.7 ナガオビの特徴づけ

(水谷一さんの示唆によるところ大, 記して感謝する.)

3 から初めて順に素数の積  $a = 3 * 5 * 7 * \dots$  を一般にナガオビという.

**命題 1** 長さ  $r$  のナガオビを  $a = q_1 * q_2 * \dots * q_r$  と書く.

$M = -\sigma(a) + 2a$  とし  $M > 0$  を仮定する.

素数の積  $b = p_1 < p_2 < \dots < p_r$  があり  $M = -\sigma(b) + 2b$  を満たすとき,  $b = a$

Proof  $p_j \geq q_j$  なので  $b = \prod_{j=1}^r p_j \geq a = \prod_{j=1}^r q_j$ .  
 $\sigma(a) = 2a - M$  の両辺を  $a$  で割ると,

$$\prod_{j=1}^r \left(1 + \frac{1}{q_j}\right) = 2 - \frac{M}{a}.$$

$\prod_{j=1}^r \left(1 + \frac{1}{q_j}\right) \geq \prod_{j=1}^r \left(1 + \frac{1}{p_j}\right)$  によって

$$-\frac{M}{a} \geq -\frac{M}{b}.$$

ゆえに,  $\frac{1}{a} \geq -\frac{1}{b}$ . よって  $a \geq b$ . これより,  $a = b$ .

表 18: ナガオビの例

$a$	素因数分解	$m = -\sigma(a) + 2a$
105	$3 * 5 * 7$	18
1155	$3 * 5 * 7 * 11$	6
15015	$3 * 5 * 7 * 11 * 13$	-2226
255255	$3 * 5 * 7 * 11 * 13 * 17$	-70098

ここで 15015, 255255 は  $m$  が負になるので使えない.

表 19:  $[P = 2, m = 6]$  完全数

$a$	素因数分解
7	7
15	$3 * 5$
52	$2^2 * 13$
315	$3^2 * 5 * 7$
592	$2^4 * 37$
1155	$3 * 5 * 7 * 11$
2102272	$2^{10} * 2053$

## 2.8 シチゴサン $a = 315 = 3^2 * 5 * 7$ の特徴づけ

$a = 3^e qr$  ( $3 < q < r$  : 素数) とおくとき  $e = 2, q = 5, r = 7$  を示す.

Proof

$$\sigma(a) = \sigma(3^e qr) = \frac{3^{e+1} - 1}{2} \widetilde{qr}, 2a - 6 = 2 * 3^e qr - 6 \text{ なので}$$

$$(3^{e+1} - 1) \widetilde{qr} = 4 * 3^e qr - 12.$$

$$N = 3^{e+1} - 1, \Delta = q + r \text{ とおけば, } \widetilde{qr} = qr + \Delta + 1.$$

$$N \widetilde{qr} = 4 * 3^e qr - 12 = \frac{4(N + 1)qr}{3} - 12.$$

3倍して

$$3N \widetilde{qr} = 4(N + 1)qr - 36.$$

整理して

$$3N(\Delta + 1) = (N + 4)qr - 36.$$

$N$  で括ると

$$N(3(\Delta + 1) - qr) = 4(qr - 9).$$

$q_0 = q - 3, r_0 = r - 3$  とおくとき  $q_0 r_0 = qr - 3\Delta + 9$ . これを用いて  $qr - 3(\Delta + 1) = q_0 r_0 - 12$ . それゆえ

$$N(12 - q_0 r_0) = 4(qr - 9).$$

$r \geq q + 2 \geq 5 + 2, q \geq 5$  なので  $4(qr - 9) > 0$ .

これより  $12 > q_0 r_0$ . ここから  $q_0 = 2, 3, 4$  に応じて各個撃破する.

i.  $q_0 = 2$ .  $q = 5$  かつ  $12 > q_0 r_0 = 2r_0$  により  $6 > r_0 = r - 3$ .  $9 > r \geq q + 2 = 7$ .  $q = 5$  なので  $r_0 \geq q_0 + 2 = 2 + 2 = 4$ . ゆえに  $r \geq 7$ . したがって  $q = 5, r = 7$ .  $N(12 - q_0 r_0) = 4(qr - 9)$  により,  $12 - q_0 r_0 = 12 - 4 * 2 = 4, qr - 9 = 35 - 9 = 26$ .  $N = 26 = 27 - 1 = 3^3 - 1, N = 3^{e+1} - 1$  によれば  $e = 2$ . したがって  $a = 3^2 * 5 * 7$ .

ii.  $q_0 = 3$ .  $q = 3 + 3 = 6$ . 素数ではない.

iii.  $q_0 = 4$ .  $12 - q_0 r_0 = 12 - 4 * r_0$  によって,  $r_0 < 3$ . しかし  $r_0 > q_0 = 4$  に矛盾する.

伏字法を用いてより一般の場合を考える.

$a = p^e qr$  ( $2 < p < q < r$  : 素数) とおくとき  $\sigma(a) = 2a - 6$  を満たすなら  $e = 2, p = 3, q = 5, r = 7$  を示す.

Proof.

$p = 3$  は前の項で示したので,  $p \geq 5$  を仮定して矛盾を導く.

$$\sigma(a) = \sigma(p^e qr) = \frac{p^{e+1} - 1}{p} \tilde{q}\tilde{r}, 2a - 6 = 2 * p^e qr - 6 \text{ なので}$$

$$(p^{e+1} - 1)\tilde{q}\tilde{r} = 2 * \bar{p} * p^e qr - 6\bar{p}.$$

$$N = p^{e+1} - 1, \Delta = q + r \text{ とおけば, } \tilde{q}\tilde{r} = qr + \Delta + 1.$$

$$N\tilde{q}\tilde{r} = \bar{p}(2 * p^e qr - 6).$$

$$N\tilde{q}\tilde{r} - \bar{p}(2 * p^e qr) = -6\bar{p}.$$

$$p^e(p\tilde{q}\tilde{r} - 2\bar{p}qr) = \tilde{q}\tilde{r} - 6\bar{p}.$$

$A = \tilde{q}\tilde{r}, B = qr$  とおくとき,

$$p\tilde{q}\tilde{r} - 2\bar{p}qr = pA - 2\bar{p}B = p(A - 2B) + 2B.$$

よって,

$$p^e(p(A - 2B) + 2B) = \tilde{q}\tilde{r} - 6\bar{p}.$$

$$A - 2B = -B + \Delta + 1, p(A - 2B) + 2B = (2 - p)B + p(\Delta + 1).$$

かくて次の基本方程式をえる.

$$p^e((2 - p)B + p(\Delta + 1)) = B + \Delta + 1 - 6\bar{p}.$$

**補題 1**  $2 \leq p < q < r$  が素数なら  $B + \Delta - 6\bar{p} \geq 0$ .

Proof

$r \geq q + 2$  により

$$B + \Delta = qr + q + r \geq q(q + 2) + 2q + 2 = (q + 2)^2 - 2.$$

$q \geq p + 1$  により

$$(q + 2)^2 - 2 \geq (p + 3)^2 - 2.$$

$(p + 3)^2 - 2 - 6(p - 1) = p^2 + 13 > 0$ . かくて証明された.



補題 2  $2 < p < q < r$  が素数で  $(2-p)B + p(\Delta + 1) > 0$  なら  $p = 3, q = 5, r = 7$ .

Proof

$(2-p)B + p(\Delta + 1) > 0$  より

$$(2-p)qr + p(q+r+1) > 0.$$

変形して

$$r((2-p)q+p) + p(q+1) > 0.$$

$r \geq q+2$  なので

$$p(q+1) > r((p-2)q-p) \geq (q+2)(p-2)q-p = q^2(p-2) + q(p-4) - 2p.$$

これより

$$3p > q^2(p-2) - 4q.$$

$$3p > q^2(p-2) - 4q = q(q(p-2) - 4).$$

$F(x) = x(x(p-2) - 4)$  とおくと 2 次式の軸は  $x = \frac{2}{p-2} < p+2$ .  $q \geq p+2$  なので  $F(q) \geq F(p+2) = (p+2)(p^2 - 8)$ . ゆえに

$$3p > (p+2)(p^2 - 8).$$

$p = 3$  なら 左辺=9, 右辺=5. よって成立.  $p \geq 5$  なら不成立.

$p = 3$  を  $3p > q^2(p-2) - 4q = q(q(p-2) - 4)$  に代入すると  $q \geq p+2 = 5$  なので  $9 > q^2 - 4q = q(q-4)$  により,  $q = 5$ .

$p = 3, q = 5$  を  $r((2-p)q+p) + p(q+1) > 0$  に代入すると  $r((2-3)5+3) + 18 > 0$  により  $r < 8$ . 結局  $r = 7$

2つの補題によって,  $p = 3, q = 5, r = 7$ . すなわち  $a = 3^2 * 5 * 7$  が示された.