

書泉グランデでの講義 第二期
高校生も十分わかる新しい数論研究 , 2015 年 2 月 3 月

飯高 茂

平成 27 年 12 月 15 日

目次

0.1	開講の辞	1
0.2	開講の辞 2	1
0.3	完全数の歴史	1
第 1 章	完全数と 3 点セット	3
1.1	素数べき	3
1.1.1	等比数列の和	4
1.1.2	概完全数問題の $s(a) = 1, 2$ での解決	5
1.2	3 点セット	6
1.3	完全数	7
1.3.1	オイラーによる証明	8
1.3.2	Dickson にある完全数の証明	9
1.3.3	$\sigma(a) - a = 1$	9
1.3.4	疑似完全数	9
1.3.5	素数べきの約数の和	10
1.3.6	フェルマーとオイラーの結果	11
1.3.7	ラグランジュの結果	11
1.3.8	等比数列の和の公式	12
1.3.9	$s(a) = 2$ のときの完全数の証明	13
1.4	完全数の平行移動	14
1.5	完全数の数表	15
1.6	m だけ並行移動した場合の数表	19
1.6.1	$m = 2$	19
1.7	オイラーの反例	20
1.7.1	例	23
1.7.2	$m = 4$	24
1.7.3	$m = 6$	26
1.7.4	$m = 8$	26
1.7.5	$m = -2$	27
1.7.6	$m = -4$	29
1.7.7	$m = -6$	30
1.7.8	$m = -8$	31
1.8	m だけ平行移動した方程式の解	32

1.9	$s(a) = 2$ のときの証明	33
1.10	例	34
1.10.1	$\sigma(a) = 2a - 2$	34
1.10.2	$\sigma(a) = 2a - 4$	35
1.10.3	$\sigma(a) = 2a - 6$	36
1.10.4	$\sigma(a) = 2a - 8$	36
1.10.5	$\sigma(a) = 2a - 32$	37
1.10.6	$\sigma(a) = 2a - 64$	37
1.10.7	$\sigma(a) = 2a + 2$	38
1.10.8	$\sigma(a) = 2a + 4$	38
1.10.9	$\sigma(a) = 2a + 6$	39
1.10.10	$\sigma(a) = 2a + 8$	39
1.10.11	$\sigma(a) = 2a + 32$	39
1.11	微小解	40
1.12	$a = 2^e qr$ 型の解	41
1.12.1	$p = 2, m = 4; a = 2^e qr$	42
1.12.2	$p = 2, m = 8; a = 2^e qr$	42
1.12.3	$p = 2, m = -8; a = 2^e qr$	43
1.12.4	$p = 2, m = 32; a = 2^e qr$	44
第 2 章	底が 3 のとき	45
2.1	$a = 3^e$ の場合	45
2.1.1	数値計算例	45
2.1.2	$s(a) = 2$ のときの証明	46
2.2	$2\sigma(a) - 3a$ の値	47
2.3	$2\sigma(a) - 3a = 1$ の場合	49
2.4	亜完全数	51
2.5	亜完全度	51
2.5.1	亜完全度が奇数の場合	51
2.5.2	奇数の例	52
2.5.3	亜完全度が偶数の場合	53
2.5.4	例	56
2.5.5	亜完全度 2,6 の場合	58
2.6	3 のべきとそのユークリッド関数の値	61
2.6.1	フェルマーとオイラーの結果	61
2.6.2	オイラーとラグランジュの結果	62
2.6.3	証明	64
2.7	3 を底とする完全数	64
2.7.1	3 を底とする完全数の数表	65
2.7.2	$s(a) = 1$ のときの証明	66

2.7.3	$s(a) = 2$ のときの証明	66
2.7.4	3 を底とする完全数の方程式	69
2.8	3 を底とする完全数の平行移動	69
2.8.1	$p = 3, m = 1$	70
2.8.2	3 を底とするフェルマー素数	71
2.9	底が 3 のフェルマー数	71
2.9.1	$p = 3, m = 3$	73
2.9.2	$p = 3, m = 4$	73
2.9.3	$p = 3, m = 7$	74
2.9.4	$p = 3, m = 9$	75
2.9.5	$p = 3, m = -2$	75
2.9.6	$p = 3, m = -3$	77
2.9.7	$p = 3, m = -5$	78
2.9.8	$p = 3, m = -6$	79
2.9.9	$p = 3, m = -8$	79
2.9.10	$p = 3, m = -9$	79
2.10	m だけ平行移動した完全数の方程式	80
2.11	方程式を満たす解	81
2.11.1	$m = 0$ のとき	81
2.11.2	$m = 1$ のとき	82
2.11.3	$m = 3$ のとき	82
2.11.4	$m = 4$ のとき	83
2.11.5	$m = 6$ のとき	83
2.11.6	$m = 7$ のとき	83
2.11.7	$m = 9$ のとき	84
2.11.8	$m = -1$ のとき	84
2.11.9	$m = -2$ のとき	84
2.11.10	$m = -3$ のとき	85
2.11.11	$m = -5$ のとき	85
2.11.12	$m = -6$ のとき	85
2.11.13	$m = -8$ のとき	86
2.11.14	$m = -9$ のとき	86
2.12	$a = 3^{eqr}$ の解	87
2.12.1	$m = -2$ のとき	87
2.12.2	$m = 4$ のとき	88
2.12.3	$m = 8$ のとき	88
2.12.4	$m = -8$ のとき	89
2.12.5	$m = -5$ のとき	89
2.12.6	$m = 2$ のとき	90
2.12.7	$m = -1$ のとき	90

2.13	Maxp(a) について	91
第 3 章	究極の完全数	93
3.1	$a = 5^e$ の場合	93
3.1.1	$s(a) = 2$ のときの証明	93
3.1.2	$\sigma(5^e)$ が素数になる場合	95
3.1.3	フェルマーとオイラーの結果	96
3.2	オイラーとラグランジュの結果	97
3.3	例	97
3.3.1	$P = 3$	98
3.3.2	$P = 5$	98
3.3.3	$P = 7$	100
3.3.4	$P = 11$	101
3.3.5	$P = 13$	101
3.4	q を底に持つフェルマー素数	102
3.5	5 が底の完全数	102
3.5.1	$s(a) = 2$ の場合	103
3.6	究極の完全数とその平行移動	106
3.7	例	106
3.7.1	$[p = 5, m = 0]$	106
3.7.2	$[p = 5, m = 1]$	108
3.7.3	$[p = 7, m = 0]$	110
3.7.4	$[p = 11, m = 0]$	111
3.7.5	$[p = 13, m = 0]$	112
3.8	究極の完全数の満たす方程式	113
3.8.1	究極の完全数の基本問題	113
3.9	諸例	114
3.9.1	$[P = 5, m = 0]$	114
3.9.2	$[P = 7, m = 0]$	114
3.9.3	$[P = 43, m = 0]$	114
3.10	微小解	115
3.10.1	微小解の存在する素数	116
3.10.2	$s(a) = 2$ の場合に解く (未完)	117
3.11	例	119
3.11.1	$[m = p - 1]$ の解	119
3.11.2	$[p = 5, m = 1]$	120
3.11.3	$[p = 5, m = 3]$	120
3.11.4	$[p = 5, m = 4]$	120
3.11.5	$[p = 5, m = -2]$	121
3.11.6	$[p = 7, m = 1]$	121

3.11.7	$[p = 7, m = 2]$	121
3.11.8	$[p = 7, m = 3]$	121
3.12	p が一般で解が $a = p^e qr$ の場合	123
3.13	例	124
3.13.1	$p = 5, m = -2; a = 5^e qr$	127
3.13.2	$p = 7, m = 2; a = 7^e qr$	130
3.13.3	$p = 7, m = 3; a = 7^e qr$	130
3.13.4	$p = 7, m = 4; a = 7^e qr$	131
3.13.5	$p = 7, m = -1; a = 7^e qr$	132
第 4 章	P を底とする弱完全数	133
4.0.6	$P = 2$	133
4.0.7	末尾の数	135
4.0.8	$P = 3$	136
4.0.9	末尾の数	138
4.0.10	$P = 5$	139
4.0.11	末尾の数	140
4.0.12	$P = 7$	141
4.1	フェルマーとオイラーの結果	143
4.1.1	実例	144
第 5 章	P を底とするフェルマーの完全数	145
5.1	オイラーの結果の一般化	145
5.2	例	147
5.2.1	$P = 2$	147
5.2.2	$P = 3$	148
5.2.3	$P = 5$	149
5.2.4	$P = 7$	152
5.2.5	$P = 11$	152
5.3	フェルマーの完全数の方程式	155
5.4	例	155
5.4.1	$P = 3$ のとき	155
5.4.2	$P = 5$ のとき	155
5.5	$a = P^e qr$ の解	156
第 6 章	P を底とする概完全数	158
6.1	$P = 5$ の場合	158
6.1.1	$s(a) = 2$ のときの証明	158
6.2	$p = 7$ の場合	160
6.3	pq 形の概完全数	161
6.3.1	非べき概完全数の数表	162

6.4	$s(a) = 3, a = p^e qr$ の場合	163
6.4.1	$p = 2$ のとき	163
6.4.2	$a = p^e qr$ のときの計算例	163
第 7 章	亜完全数	165
7.1	p を底とする亜完全数	165
7.1.1	$p = 3, m = 3$ の例	165
7.1.2	$p = 3, m = 5$ の例	166
7.1.3	$p = 3, m = -3$ の例	166
7.1.4	$p = 5, m = 3$ の例	167
7.1.5	$p = 5, m = -3$ の例	167
7.2	$m = -1$ の例	167
7.2.1	$p = 3, m = -1$ の例	167
7.2.2	$p = 5, m = -1$ の例	168
7.2.3	$p = 7, m = -1$ の例	168
7.2.4	$p = 11, m = -1$ の例	169
7.2.5	$p = 13, m = -1$ の例	169
7.2.6	$p = 17, m = -1$ の例	169
7.3	亜完全度	170
7.3.1	$p = 3, W = 1$ の例	170
7.3.2	$p = 5, W = 1$ の例	170
7.3.3	$p = 7, W = 1$ の例	170
7.3.4	$p = 11, W = 1$ の例	171
7.3.5	$p = 13, W = 1$ の例	171
7.4	亜完全度 1 の微小解	172
7.5	$a = p^e qr$ 型の亜完全数	173
第 8 章	素数べきの方程式変位	175
8.0.1	$m = -2$ の例	176
8.0.2	$s(a) = 2$ の解	176
8.0.3	$m = -2$	177
8.0.4	$m = 1$ の例	178
8.0.5	$m = 2$ の例	179
8.0.6	$P = 5, m = 2$ は解が多い	180
8.0.7	$m = -3$	181
8.0.8	$m = 3$	182
8.0.9	$m = qr$ の解	183
8.0.10	例	184

第 9 章 疑似完全数	190
9.1 疑似完全数の定義	190
9.1.1 $X = 0$	190
9.1.2 $X = 1$	190
9.1.3 $X = 2$	192
9.1.4 $X = -1$	192
9.1.5 $X = -2$	193
第 10 章 オイラー関数と素数兄弟	195
10.1 オイラー関数	195
10.2 オイラー関数の基本性質	195
10.2.1 オイラー関数数表	196
10.2.2 オイラーの公式	197
10.2.3 乗法性	198
10.2.4 乗法性の証明	198
10.3 オイラー関数について 3 点セット	199
10.4 フェルマー数	199
10.4.1 部分的証明	200
10.4.2 不存在性	201
10.5 見事な解	202
10.6 $a = P^e$	202
10.6.1 $a = P^e$ の 3 点セット	202
10.6.2 $P = 3$ のときの 3 点セット	202
10.6.3 5 点セット	203
10.7 $P = 3$ のときのフェルマー素数	204
10.7.1 フェルマー素数の仕組み	206
10.8 再び, オイラー	207
10.8.1 2 素数の追加	208
10.8.2 例題	208
10.8.3 素数の追加	208
10.8.4 1 素数の追加の追加	209
10.8.5 2 素数の追加の追加	209
10.8.6 計算例	210
10.9 $P = 5$ のときのフェルマー素数	210
10.10 $P = 7$ のときのフェルマー素数	211
10.11 $a = pqr$ のときの証明	213
10.12 $p = 11$	214
10.12.1 $p \geq 13$.	215
10.13 素数 3 姉妹の一般形	216
10.13.1 素数 3 姉妹の探索	217

10.13.2 $g = 180$	218
10.13.3 $g = 430$	218
10.13.4 $g = 936$	219
10.14 素数 4 姉妹の場合	220
10.14.1 養女登場	220
10.14.2 $3\varphi(a) = 2a + 2$ の解	221
10.14.3 $7\varphi(a) - 6a = 6$ を満たす a	223
10.15 素数親子の探索	223
10.15.1 数値例	223
10.15.2 $a_0 = g - 1$	223
10.16 $5\varphi(a) = 3(a + 1)$ の解	226
10.16.1 $a = 3L$ の場合	227
10.16.2 $a = 3^2L$ の場合	228
10.17 素数おひとりの世界	230
10.17.1 数値解の例	230
10.17.2 $s(a) = 2$ の解	232
10.18 素数ひとりの別の世界	234
10.19 P が 11 を超えた世界	237
10.20 6^e の場合	238
10.20.1 $3\varphi(a) - a = 1$ の場合	240
10.20.2 $3\varphi(a) - a = 4$ の場合	240
10.20.3 $3\varphi(a) - a = 8, 16$	242
10.21 変位のある素数べき方程式	242
10.21.1 例	243
第 11 章 φ 完全数	245
11.1 p を底とする φ 完全数の例	246
11.1.1 2 を底とするとき	246
11.1.2 3 を底とするとき	247
11.1.3 5 を底とするとき	249
11.1.4 7 を底とするとき	250
11.1.5 11 を底とするとき	251
11.1.6 13 を底とするとき	252
11.1.7 17 を底とするとき	253
11.2 φ 完全数の平行移動	254
11.2.1 $[p = 2, m = 2]$	254
11.2.2 $[p = 2, m = 4]$	254
11.2.3 $[p = 2, m = -2]$	255
11.2.4 $[p = 2, m = -4]$	255
11.2.5 $[p = 3, m = 4]$	255

11.2.6	$[p = 3, m = 6]$	256
11.2.7	$[p = 3, m = -2]$	257
11.2.8	$[p = 3, m = -8]$	258
11.2.9	$[p = 5, m = 2]$	258
11.2.10	$[p = 5, m = 6]$	259
11.3	φ 完全数の平行移動の方程式	260
11.3.1	φ 完全数の方程式 (*) の解	261
11.3.2	2 を底とするとき	261
11.3.3	3 を底とするとき	261
11.3.4	5 を底とするとき	262
11.3.5	7 を底とするとき	262
11.3.6	11 を底とするとき	262
11.3.7	13 を底とするとき	263
11.4	$p \geq 3, m > 0$ の場合	263
11.4.1	$m = 2$ の場合	263
11.4.2	$m = 4$ の場合	264
11.4.3	$m = 6$ の場合	265
11.4.4	$m = 8$ の場合	265
11.5	微小解	266
11.5.1	$p = 2, m = 0$ のときの予想	267
11.6	予想の解決	267
11.7	定理と証明	268
11.8	諸例	269
11.8.1	$p = 2, m = -4$ のとき	269
11.9	$p = 2, m = -q$; (奇素数) のとき	270
11.9.1	$p = 2, m = -3$ のとき	270
11.9.2	$p = 2, m = -5$ のとき	270
11.9.3	$p = 2, m = -7$ のとき	271
11.9.4	$p = 2, m = -11$ のとき	272
11.9.5	$p = 2, m = -13$ のとき	272
11.9.6	$p = 2, m = -19$ のとき	272
11.9.7	$p = 2, m = -23$ のとき	273
11.9.8	$p = 2, m = -29$ のとき	273
11.9.9	$p = 2, m = -31$ のとき	273
11.9.10	$p = 2, m = -37$ のとき	274
11.9.11	$p = 2, m = -41$ のとき	274
11.9.12	$p = 2, m = -43$ のとき	274
11.9.13	copm の表	274
11.10	$p = 2, m = -s$: 奇素数	275
11.11	$p = 3, m \neq 0$ のとき	277

11.11.1 $p = 3, m = -3$ のとき	277
11.11.2 $p = 3, m = -2$ のとき	277
11.12 $p = 5, m \neq 0$ のとき	278
11.12.1 $p = 5, m = -2$ のとき	278
11.12.2 $p = 5, m = 2$ のとき	278
11.13 $\text{co}\varphi(a) - \text{Maxp}(a)$ の値変化	278
11.14 $\text{co}\sigma(a) - \text{Maxp}(a)$ の値変化	280
11.15 素数べきの問題	280
11.15.1 $s(a) > 1$ の場合	281
11.15.2 ソフィーの素数	281
11.15.3 最後の定理	282

はじめに

0.1 開講の辞

本日(2014年11月14日)ここに集って下さった紳士淑女のみなさま,あつくお礼申し上げます。私がこの連続講義でしようとしていることは,画期的な試みです。高校の数学で十分理解できる素材で方法も初等的なものですが,数学の長い歴史を振り返りつつ新しくできつつある数学の理論を紹介します。受講者の皆様もこの数学研究に参加できるのです。

ここで紹介する「高校生も十分わかる新しい数論研究」は以下の節で説明するようなわけで私が1年余り努力を積み重ねて発展させてきたものですから十分練られたモノではありません。ですから証明も可能な限り詳しくいたします。証明に欠陥があるかもしれません。またより一般的な定理に組み込まれるべき命題も数多くあるでしょう。

受講者の方々には覚悟を求めます。講師は受講者との真剣勝負をしたいと思っております。

0.2 開講の辞 2

この本屋さんの7階で「高校生も十分わかる新しい数論研究」がスタートして2ヶ月あまり,驚いたことに多くの参加者が集い企画として大成功といってよいものとなった。これは私にとっても想像外のことであった。10名程度で始まり参加者も減り続け2度ほどで中止となるであろう,という悲観的な想念にとらわれていた。

しかし,受付を開始すると定員20名をすぐに超える申し込みがあり書店は30名に増員したがそれもオーバーした。そのため会場に椅子を詰め込みノートをとる机もなかった。「高校生も十分わかる」という触れ込みではじめたが高校生の参加はなかった。しかし,小学生しかも1年生の参加者があり熱心に聴いてよく質問してくれた。これはまったく想定外であった。

書店の希望により今回から,1回1000円の参加費を集めることになった。ご負担をかけることは申し訳ないが,書店にも事情があり参加者のご理解をお願いしたい。(2015年2月13日)

0.3 完全数の歴史

L.E.Dickson 著の History of the theory of Numbers I,1919/20(Dover, Chelsea Publishing Company 版 1992)の第1章を参考にして完全数の歴史について書いて簡単にふれる。

ユークリッドは原論 IX,prop.36 において $p = 1 + 2 + 2^2 + \dots + 2^n$ が素数なら $a = 2^np$ は完全数になることを示した。

a の約数は

$$1, 2, 2^2, \dots, 2^n, 1 \cdot p, 2 \cdot p, 2^2 \cdot p, \dots, 2^n \cdot p$$

であってこれらの和は等比数列の和の公式を使うと $2a$ になる.

AD 100 年の頃 Nichomachus はすべての偶数を 過剰数 ($\sigma(a) - a > a$), 不足数 ($\sigma(a) - a < a$), 完全数 ($\sigma(a) - a = a$) に分類した.

完全数には稀少性があり, 6, 28, 496, 8128, などではこれらの末尾の数が 6 または 8 であることに注目が集まった. (6, 8 は交互にきて、さらに桁が上がる度に 1 つずつあることを観察した. しかしこれらは正しくなかったことが後にわかった).

1456 年の文書に 5 番目の完全数 33550336 が記載された.

Luca Paciolo (1494 年?) は $1 + 2 + 2^2 + \dots + 2^n$ が素数になることは実行して初めてわかることだが無限にあるだろう、と述べた.

Cardan (1501–1576) は完全数はユークリッドが与えた方法ですべて構成されるだろう.

Tartaglia (1506–1559) $1 + 2 + 4, 1 + 2 + 4 + 8, 1 + 2 + 4 + 8 + 16, \dots$ は交互に素数が合成数になる、と述べた.

F. Maurolicus (1494–1575) は完全数は三角数になることを注意した.

$q = 2^{e+1} - 1$ とおくと $q + 1 = 2 * 2^e$ によって

$$1 + 2 + 3 + \dots + q = \frac{q(q+1)}{2} = 2^e q = a$$

等比数列の和で定義された完全数が等差数列の和としての三角数になった. 不思議なことである.

R. Descartes は 1638 年の Mersenne への手紙で偶数完全数はユークリッドが与えた形になることは証明できたと思う. しかし奇数完全数は ps^2 の形になると述べた.

Fermat は 1640 年の Mersenne への手紙で n が合成数なら $2^n - 1$ も合成数. n が素数なら $2^n - 2$ は $2n$ で割れると述べた.

L. Euler は 1752 年の Goldbach への手紙で 7 個の完全数は $2^{p-1}(2^p - 1)$, $p = 2, 3, 5, 7, 13, 17, 19$ となるが $p = 31$ のときは分からない、と述べた.

L. Euler は Bernoulli への手紙で $p = 31$ のときは完全数であることを確認した.

L. Euler は死後出された論文で 偶数完全数は $2^{p-1}(2^p - 1)$ と表せることの証明を与えた.

Sylvester はオイラーの証明を確認した.

Servais とともに奇数の完全数は 4 個以上の素因子を持つ事を示した.

第1章 完全数と3点セット

1.1 素数べき

2 を公比とし初項 1 の等比数列 $1, 2, 2^2 = 4, 2^3 = 8, \dots$ は数学において基本的で大切な数列である。

3 を公比とする等比数列 $1, 3, 3^2 = 9, 3^3 = 27, \dots$ も大切である。

さて、自然数 a の約数の和を $\sigma(a)$ で表すことは現在ほぼ確定した記号であるが、これを a の関数と見てユークリッド関数と言いたい。

たとえば、 $a = p^3$ (p : 素数) ならその約数は $1, p, p^2, p^3$ 。この和 $1 + p + p^2 + p^3$ が $\sigma(a)$ である。

$S = 1 + p + p^2 + p^3$ とおくと、 $pS = p + p^2 + p^3 + p^4$ 。 $pS - S$ を作るとうまく消し合って $pS - S = p^4 - 1$ 。

$p > 1$ なので $S = \frac{p^4 - 1}{p - 1}$ 。

これから一般に $a = p^e$ のとき $\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}$ がわかる。

2 個以上の素因子を持つときは次のように考えるとよい。

$a = p^2 q^2$ の約数は $1, p, p^2, q, pq, p^2 q, q^2, pq^2, p^2 q^2$ 。これらの和は

$$(1 + p + p^2) + (1 + p + p^2)q + (1 + p + p^2)q^2 = (1 + p + p^2)(1 + q + q^2) = \sigma(p^2)\sigma(q^2).$$

$a = p^e q^f$ の約数は素因子分解の一意性より $p^r q^s$, ($r \leq e, s \leq f$) と書ける。したがって

$$\sigma(a) = \sigma(p^e)\sigma(q^f). \quad (1.1)$$

一般には a, b が互いに素ならば

$$\sigma(ab) = \sigma(a)\sigma(b)$$

が成り立つ。これを $\sigma(a)$ は乗法性を持つと言う。素因数分解の一意性によって乗法性が成り立つことが証明される。一方、素因数分解の一意性は割り算による互除法によって古代ギリシャで証明されていた。

$\sigma(a)$ が奇数になるのは少ない。

$\sigma(a)$ に出てこない数として 9,10,11 があり,12 になる数として 6,11 があげられる. これらを表によらないで数学的に証明するにはどうしたらよいか.

$\sigma(a) = 72$ の方程式と解け

(解は 5 個)

1.1.1 等比数列の和

$a = 2^e$ とし, 等比数列の和の公式を用いると

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

と書けるから $a = 2^e$ なら $\sigma(a) = 2a - 1$ を満たす.

これはごく初等的なことであるが, 等比数列の和の公式が用いられていることに注意を払いたい. そこで数学の世界によくあることだが, この逆を問題として考える.

$\sigma(a) = 2a - 1$ を満たす自然数 a は $a = 2^e$ に限るか?

ごく自然な発想で生まれた問題である. 一般に $\sigma(a) - 2a = -1$ を満たす自然数 a を概完全数 (almost perfect number) と呼ぶそうだ. そこで 200 までの範囲で概完全数をパソコン君に探してもらおうと次の表ができた.

表 1.1:

a	$\sigma(a)$	素因数分解
2	3	[2]
4	7	[2 ²]
8	15	[2 ³]
16	31	[2 ⁴]
32	63	[2 ⁵]
64	127	[2 ⁶]
128	255	[2 ⁷]

概完全数の数表をとって 2 のべきがでてきた. しかし 2 のべき以外に概完全数があるかは, 未だに解決されることなく, 一見やさしそうでも意外に難しい問題として残されている.

1.1.2 概完全数問題の $s(a) = 1, 2$ での解決

$\sigma(a) - 2a = -1$ を条件 $s(a) = 1, 2$ の下で解いてみよう. ただし $s(a)$ は a の相異なる素因子の数.

$s(a) = 1$ のとき. $a = p^e$ とかける. $\bar{p} = p - 1$ とおくと $\sigma(a) = \frac{p^{e+1}-1}{p-1}$ となるので,

$$\frac{pa-1}{\bar{p}} = 2a-1.$$

よって

$$pa-1 = (2a-1)\bar{p}.$$

$$a(p-2\bar{p}) = 1-\bar{p} = 2-p.$$

$p-2\bar{p} = 2-p$ により

$$2-p = a(2-p).$$

$a > 1$ により, $p = 2$. よって $a = 2^e$.

$s(a) = 2$ のとき. 概完全数はないことを背理法で示す.

$a = p^e q^f$ ($p < q$), $\bar{p} = p - 1, \bar{q} = q - 1$ とおく.

$X = p^e, Y = q^f, A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおくと

$\sigma(a) = \frac{AB}{\rho'}, a = XY$ と書けるので,

$$\frac{AB}{\rho'} = 2XY - 1.$$

これを整理して

$$AB - 2\rho'XY = -\rho'.$$

左辺の XY の係数を R とおくと $R = pq - 2\rho' = 2 - (p-2)(q-2)$.

$$RXY - (pX + qY - 1) = -\rho'. \quad (1.2)$$

しかし $RXY = (pX + qY - 1) - \rho' > q^2 - 1 - \rho' > 0$ により $R > 0$.

$0 < R = 2 - (p-2)(q-2)$ を使うと $p = 2$, よって $\rho' = \bar{q}, R = 2$.

式 (1.2) より

$$2XY - (2X + qY - 1) = -\bar{q}.$$

これを变形して

$$0 = 2XY - (2X + qY) + 1 + \bar{q} = 2XY - (2X + qY) + q.$$

一方 $2XY - (2X + qY) + q = (2X - q)(Y - 1)$ により

$0 = (2X - q)(Y - 1)$. $Y \neq 1$ なので $q = 2X = 2^{e+1}$, 矛盾.

$s(a) \geq 3$ の場合は複雑になりなかなかできない.

1.2 3点セット

関連して次の問題を合わせ考え, $a = 2^e$ に関する3点セットと言う.

- (1) $\sigma(a) - 2a = 0$ を満たす自然数は何か,(これは完全数で次項でふれる)
- (2) $\sigma(a) - 2a = -1$ を満たす自然数は何か, (概完全数)
- (3) $\sigma(a) - 2a = 1$ を満たす自然数は何か.

$\sigma(a) - 2a; a < 2000; |\sigma(a) - 2a| < 10$ の順に並べた表をみて見よう.

研究課題

$p = 2^{e+1} + 3$ が素数なら $a = 2^e p$ は $\sigma(a) - 2a = -4$ を満たす.

表 1.2: $\sigma(a) - 2a$ の値が1桁

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
22	[2, 11]	36	-8 ; 8 だけ平行移動の完全数
130	[2, 5, 13]	252	-8
184	[2 ³ , 23]	360	-8
1012	[2 ² , 11, 23]	2016	-8
50	[2, 5 ²]	93	-7
7	[7]	8	-6 ; 6 だけ平行移動の完全数
15	[3, 5]	24	-6
52	[2 ² , 13]	98	-6
315	[3 ² , 5, 7]	624	-6
592	[2 ⁴ , 37]	1178	-6
1155	[3, 5, 7, 11]	2304	-6
9	[3 ²]	13	-5
5	[5]	6	-4 ; 4 だけ平行移動の完全数
14	[2, 7]	24	-4
44	[2 ² , 11]	84	-4
110	[2, 5, 11]	216	-4
152	[2 ³ , 19]	300	-4
884	[2 ² , 13, 17]	1764	-4
3	[3]	4	-2 ; 2 だけ平行移動の完全数
10	[2, 5]	18	-2
136	[2 ³ , 17]	270	-2
2	[2]	3	-1 ; 2 のべき, 概完全数
4	[2 ²]	7	-1
8	[2 ³]	15	-1
16	[2 ⁴]	31	-1
32	[2 ⁵]	63	-1
64	[2 ⁶]	127	-1
128	[2 ⁷]	255	-1
256	[2 ⁸]	511	-1
512	[2 ⁹]	1023	-1
1024	[2 ¹⁰]	2047	-1

1.3 完全数

完全数 (perfect number) とは $\sigma(a) - 2a = 0$ を満たす自然数 a のことである.

偶数の完全数はオイラーによってその形が決められたが, 完全数は無限にあるか, あるいは奇数

表 1.3: $\sigma(a) - 2a$

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
6	[2, 3]	12	0; 完全数
28	[2 ² , 7]	56	0
496	[2 ⁴ , 31]	992	0
20	[2 ² , 5]	42	2 ; -2 だけ平行移動の完全数
104	[2 ³ , 13]	210	2
464	[2 ⁴ , 29]	930	2
650	[2, 5 ² , 13]	1302	2
1952	[2 ⁵ , 61]	3906	2
18	[2, 3 ²]	39	3
12	[2 ² , 3]	28	4 ; -4 だけ平行移動の完全数
70	[2, 5, 7]	144	4
88	[2 ³ , 11]	180	4
1888	[2 ⁵ , 59]	3780	4
196	[2 ² , 7 ²]	399	7
56	[2 ³ , 7]	120	8 ; -8 だけ平行移動の完全数
368	[2 ⁴ , 23]	744	8
836	[2 ² , 11, 19]	1680	8
40	[2 ³ , 5]	90	10 ; -10 だけ平行移動の完全数
1696	[2 ⁵ , 53]	3402	10

の完全数は存在するかなどは大難問である.

1.3.1 オイラーによる証明

a を偶数の完全数とし, $a = 2^e L (L : \text{奇数})$ の形に書く.

$$\sigma(a) = \sigma(2^e)\sigma(L) = (2^{e+1} - 1)\sigma(L) = 2^{e+1}L$$

となるので $N = 2^{e+1} - 1$ とおけば $N\sigma(L) = (N + 1)L$ となるので

$$N(\sigma(L) - L) = L.$$

$d = \sigma(L) - L$ とおくと $Nd = L$. したがって d は L の約数である. つぎの3つの場合がある.

(1) $d = 1$. $N = L.d = 1 = \sigma(L) - L$ により L は素数 p であり, $p = L = N = 2^{e+1} - 1$. $p = 2^{e+1} - 1$ は素数で $a = 2^e p$. これはユークリッドの与えた完全数の形となっている.

(2) $d = L$. $N = 1 = 2^{e+1} - 1$ になるので $e = 0$. a が奇数になり仮定に反す.

(3) $1 < d < L$. d は $1, L$ 以外の約数なので $\sigma(L) > 1 + L + d$. よって $d = \sigma(L) - L > 1 + d$. これは矛盾.

1.3.2 Dickson にある完全数の証明

$(2^{e+1} - 1)\sigma(L) = 2^{e+1}L$ より

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

左辺は既約分数だから $L = c(2^{e+1} - 1)$, $\sigma(L) = 2^{e+1}c$ を満たす自然数 c がある. $c = 1$ なら $\sigma(L) = L + 1$ になるので L は素数.

$c > 1$ なら c は $1, L$ 以外の L の約数 になり $\sigma(L) \geq 1 + L + c$ を満たすから

$$2^{e+1}c = \sigma(L) \geq 1 + L + c = 1 + c(2^{e+1} - 1) + c = 1 + 2^{e+1}c$$

となってしまう矛盾.

1.3.3 $\sigma(a) - a = 1$

オイラーの証明では $\sigma(a) - a = 1$ なら a は素数ということが有効に使われている.

$\sigma(a) = a + 1$ と書き換えればこれは a の約数は $1, a$ だけということだから定義によって, a は素数.

したがってこのことは当たり前ののだ.

私は高校生への課題として $a = 2p$; $p > 2$ (素数の2倍) になることを $\sigma(a)$ で判定したらどうか. を出してみた. しかし事前に自分でしてみた.

$$\sigma(a) = 3(p + 1) = 3\left(\frac{a}{2} + 1\right)$$

とすると $2\sigma(a) = 3a + 6$ になる. この逆問題を考えた.

$2\sigma(a) = 3a + 6$ を満たすとき, $a = 2p$, および 8.

が証明できた. $a = 2p$ の特徴づけは, 8 を例外としてうまくできた. しかし, $a = 6p, 28p$ などの特徴づけは難しい.

高校生でも解ける問題や, 絶対に解けない数多くの問題があるので, 好都合な問題であった.

1.3.4 疑似完全数

$\sigma(a) - 2a = 1$ を満たす自然数 a は pseudo perfect number (疑似完全数) と呼ばれることがある. これは果たして存在するかどうか問われている.

自然数 a に対し $\sigma(a) - 2a$ を完全度とよぶことにしよう.

完全度 0 なら完全数と呼ばれる。

完全度 -1 なら概完全数と呼ばれるが、2 の累乗 (べき) 以外にあるかは分かっていない。

完全度 1 なら擬似完全数と呼ばれるが、そのような数は無いと予想されているが証明されていない。

完全数の決定問題は 2300 年かかって 48 個発見されたが、無限にあるかどうか、また奇数の完全数はあるかはわかっていない。

完全数の問題は未解決の難問だが、その前後の数の問題 (3 点セット) も未だに解けていない。あえて言うところらの問題は解けないで残されている点に価値がある、

1995 年にフェルマーの大定理の証明が確認されて、350 年におよぶ数論の難問が解けた。そのため目標を失った人は数知れない。しかし 3 点セット問題が手つかずに残されていることは大きな励みになるであろう。

私がこの連続講義で意図していることは 3 点セット問題を解くことでは無い。3 点セット問題をさらに一般にして考えてみることによりこの問題の本質を理解することである。

いろいろ一般化すると、中には解ける問題がみつかって解決できることもある。さらに解決不可能な多くの興味深い問題も出てくる。このようにして数学の広く発展する様を体験できるであろう。

1.3.5 素数べきの約数の和

$\sigma(2^e) = 2^{e+1} - 1$ が素数になるとき、 $e + 1$ も素数である。ここでは $e + 1$ が素数になる場合に限って、 $\sigma(2^e)$ の素因数分解をしている。

$\sigma(2^e)$ が素数になる場合は 7, 31, 127, 8191, 131071, 524287, ... となって意外に多い。

これらを (2 を底とする) メルセンヌ素数という。($e + 1$ は素数と限定した効果である)

表 1.4: $\sigma(2^e) = 2^{e+1} - 1$, $e + 1$: 素数

$2^e = a$	$\sigma(a)$	素因数分解
$2 = 2$	3	[3]
$2^2 = 4$	7	[7]
$2^4 = 16$	31	[31]
$2^6 = 64$	127	[127]
$2^{10} = 1024$	2047	[23, 89]
$2^{12} = 4096$	8191	[8191]
$2^{16} = 65536$	131071	[131071]
$2^{18} = 262144$	524287	[524287]
$2^{22} = 4194304$	8388607	[47, 178481]
$2^{30} = 1073741824$	2147483647	[2147483647]

$\sigma(2^e)$ が素数のとき $2^e \sigma(2^e)$ は完全数になる。例えば

$$2 * 3 = 6, 4 * 7 = 28, 16 * 31 = 496, 64 * 127 = 8128, \dots$$

となり, これらは古代人が発見した4つの完全数である.

実際, $a = 2^e$ に対して $\sigma(a)$ が素数 q のとき $\alpha = aq$ とおき $q = \sigma(2^e) = 2^{e+1} - 1$ より $q + 1 = 2^{e+1} = 2a$ なので

$$\sigma(\alpha) = \sigma(a)\sigma(q) = q(q+1) = 2aq = 2\alpha.$$

したがって α は完全数になる.

1.3.6 フェルマーとオイラーの結果

補題 1 q が素数のとき $2^q - 1$ の素因数 p については $p - 1 = 2Lq$ と書ける.

さらに $p \equiv \pm 1 \pmod{8}$.

Proof.

条件より,

$$2^q \equiv 1 \pmod{p}.$$

q は素数なので 2 の \pmod{p} での位数は q . ゆえに

フェルマーの小定理によると $2^{p-1} \equiv 1 \pmod{p}$. よって, $p - 1 = kq$ と書ける. $p - 1$ は偶数なので k も偶数. よって $k = 2L$ と表せる.

$p - 1 = 2Lq$ により

$$2^{\frac{p-1}{2}} \equiv 2^{Lq} \equiv 1 \pmod{q}.$$

ルジャンドルの記号を用いるとオイラーの基準によって

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)$$

$2^{\frac{p-1}{2}} \equiv 1$ なので $\left(\frac{2}{p}\right) = 1$. 平方剰余の補充法則から

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

ゆえに $p \equiv \pm 1 \pmod{8}$.

例

$q = 11$ とする. $A = 2^{11} - 1$ の素因数分解は $23 * 89$. このとき

$$23 - 1 = 22 = 2 * 11 = 2q, 89 - 1 = 88 = 4 * 11 = 4q.$$

1.3.7 ラグランジュの結果

次の結果はオイラーが予想し 15 年後ラグランジュが証明した.

補題 2 $p > 3$ が奇素数のとき, $M_p = 2^p - 1$ とおく.

$q = 2p + 1$ が素数, かつ $q \equiv \pm 1 \pmod{8}$ のとき, $q = 2p + 1$ は M_p の約数. とくに M_p はメルセンヌ素数にならない.

逆に $q = 2p + 1$ が M_p の因子なら q は素数.

$q = 2p + 1$ が素数なので, $q \equiv 1 \pmod{8}$ は成立しない.

$q = 2p + 1$ が素数になる素数 p を Sophie Germain の素数という.

このとき $q = 2p + 1$ が平方剰余なら M_p の素因子になる.

表 1.5: p : Sophie Germain の素数

p	$q = 2p + 1$	平方剰余	M_p
11	23	+	$23 * 89$
23	47	+	$47 * 178481$
29	59	-	$233 * 1103 * 2089$
41	83	-	$13367 * 164511353$
53	107	-	$6361 * 69431 * 20394401$
83	167	-	$167 * 57912614113275649087721$

$q = 2p + 1$ を法として 2 が平方剰余のとき, q が M_p の因子になっている.

表 1.6:

$2/q$ のルジャンドル	p	$q = 2p + 1$	M_p の素因数分解
(+)	3	7	7
(+)	11	23	$23 * 89$
(+)	23	47	$47 * 178481$
(+)	83	167	$167 * 57912614113275649087721$
(+)	131	263	$263 * 10350794431055162386718619237468234569$
(-)	5	11	31
(-)	29	59	$233 * 1103 * 2089$
(-)	41	83	$13367 * 164511353$
(-)	53	107	$6361 * 69431 * 20394401$
(-)	89	179	$6.1897E+26$
(-)	113	227	$3391 * 23279 * 65993 * 1868569 * 1066818132868207$

1.3.8 等比数列の和の公式

完全数の定義には約数の和が必要である. 素因数分解の一意性と約数の和の公式には, 等比数列の和の公式が不可欠である. とともに, ユークリッドに代表される古代ギリシャの数学者が見いだし

たモノである.

日本の高校生なら誰でも知っている等比数列の和の公式は2500年も前に発見され完全数の理論に使われた. 日本がようやく弥生式の稲作を始めたころ (BC300年頃) 等比数列の和の公式 (ユークリッド BC300-) がすでにできていた.

しかし, 完全数 a は $\sigma(2^e)$ が素数 q になる $a = 2^e$ を用いて必ず $a = 2^e q$ と書けるか?

という問いは依然として解けていない. これが奇数完全数問題である. a の素因子の個数を $s(a)$ とおく.

奇数完全数の非存在問題は a の素因子が7個以下なら解けているらしい.

ここでは完全数 a に対しその相異なる素因子の個数が2の場合に限って解くことにする.

1.3.9 $s(a) = 2$ のときの完全数の証明

$s(a) = 2$ のとき a を素因数分解し $a = p^e q^f$ とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおけば

$$\frac{AB}{\rho'} = 2XY.$$

書き直して

$$AB = 2\rho'XY.$$

$AB - 2\rho'XY$ の XY の係数を R とおくと $R = pq - 2\rho'$ となり

$$RXY = pX + qY - 1.$$

この式を基本等式という.

$R = pq - 2\rho' = 2 - (p - 2)(q - 2)$ であり基本等式から $R > 0$ なので $p = 2$ かつ $R = 2$. したがって $2XY = 2X + qY - 1$ が成り立ち, $Y \geq q$ によって,

$$\begin{aligned} 0 &= 2XY - (2X + qY - 1) = (2X - q)Y - (2X - 1) \\ &\geq (2X - q)q - (2X - 1) \\ &= 2X(q - 1) - (q^2 - 1) \\ &= \bar{q}(2X - q - 1) \end{aligned}$$

よって

$$q + 1 \geq 2X.$$

一方, $(2X - q)Y = (2X - 1)$ によれば $2X - q \geq 1$. すなわち $2X \geq q + 1$. よって $2X = q + 1, q = 2^{e+1} - 1$.

ここで $2X = q + 1$ が成り立ち $Y = q$ が得られた. したがって, $a = XY = 2^e q, q = 2^{e+1} - 1$ になったので a は完全数.

1.4 完全数の平行移動

$q = 2^{e+1} - 1$ が素数のとき $2^e q$ は完全数になる. 完全数の平行移動とは次の意味である.

別のパラメータ m に対して $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した完全数という. ただし m は偶数の整数.

これは概念としては新しいと思う.

1.5 完全数の数表

表 1.7: 完全数の場合

$e \bmod 4$	e	$e + 1$	$2^e * q$	a	$a \bmod 10$
1	1	2	$2 * 3$	6	6
2	2	3	$2^2 * 7$	28	8
0	4	5	$2^4 * 31$	496	6
2	6	7	$2^6 * 127$	8128	8
0	12	13	$2^{12} * 8191$	33550336 (1456)	6
0	16	17	$2^{16} * 131071$	8589869056 (Cataldi,1588)	6
2	18	19	$2^{18} * 524287$	137438691328 (Cataldi,1588)	8
2	30	31	A	B (Euler, 1772)	8
0	60	61	C	D (Pervushin, 1883)	6
0	88	89	E	F (Powers, 1911)	6
0	106	107	G	H (Powers, 1914)	8
2	126	127	I	J (Lucas, 1876)	8
0	520	521	K	-- (Robinson, 1952)	6
2	606	607	L	-- (Robinson, 1952)	8
2	1278	1279	M	-- (Robinson, 1952)	8

$$\begin{aligned}
A &= 2^{30} * 2147483647 \\
B &= 2305843008139952128 \\
C &= 2^{60} * 2305843009213693951 \\
D &= 2658455991569831744654692615953842176 \\
E &= 2^{88} * 618970019642690137449562111 \\
F &= 191561942608236107294793378084303638130997321548169216 \\
G &= 2^{106} * 162259276829213363391578010288127 \\
H &= 13164036458569648337239753460458722910223472318386943117783728128 \\
I &= 2^{126} * 170141183460469231731687303715884105727 \\
J &= 14474011154664524427946373126085988481573677491474835889066354349131199152128. \\
K &= 2^{520} * 6864797660130609714981900799081393217269435300143 \\
&\quad - - 305409394463459185543183397656052122559640661454554977296 \\
&\quad - - 311391480858037121987999716643812574028291115057151. \\
L &= 2^{606} * 5311379928167670986895882065524686273295931 \\
&\quad - - 177270319231994441382004035598608522427391625 \\
&\quad - - 022652292856688893294862465010153465793376527 \\
&\quad - - 072394095199787665873519438312708353932190317 \\
&\quad - - 28127. \\
M &= 2^{1278} * 104079321946643990819252403273640855386152 \\
&\quad - - 622472667048053191123504036080596733602980 \\
&\quad - - 12239441732324184842421613954281007791383 \\
&\quad - - 566248323464908139906605677320762924129509 \\
&\quad - - 3892203457731833496615835504729594205476898 \\
&\quad - - 11211693677147548478866962501384438260291732 \\
&\quad - - 34888531116082853841658502825560466622483189 \\
&\quad - - 09188018470682222031405210266984354887329580 \\
&\quad - - 28878050869736186900714720710555703168729087
\end{aligned}$$

a の末尾の数は 6 か 8. 言い換えると $a \equiv 6$ または $8 \pmod{10}$. これは完全数の持つ周知の性質のひとつ.

Euler が 1772 年に (1707 年に生まれたオイラーはこのとき 65 歳) $2^{31} - 1$ が素数になることを示して 8 番目の完全数 $A = 2^{30} * 2147483647$ をえた. 7 番目の完全数は 1588 年だったのでほぼ 200 年ぶりの記録更新であった. 次の完全数の発見は 1876 年 (Lukas) だったので彼の記録は 100 年以上持ちこたえた.

Lucas は $2^{127} - 1$ が素数になることを示して一挙に記録を更新しこの素数は電子計算機が用いられる以前の人類が知りえた最大の素数としての記録を誇った. オイラーとルカの発見した完全数の間に 3 個の完全数が隠れていたことは 20 世紀になって明らかにされた.

2015 年現在, 知られている最大素数は $2^{57885161} - 1$ で桁数が 17425170 であるという.

数表を観察すると次の結果がわかる. ただし, ここで $e > 1$ の場合しか扱わない.

$e = 1$ は例外の場合として考える.

- $e \equiv 0 \pmod{4}$ なら $q \equiv 1 \pmod{10}$. $a \equiv 6 \pmod{10}$.

- $e \equiv 2 \pmod{4}$ なら $q \equiv 7 \pmod{10}$. $a \equiv 8 \pmod{10}$.

Proof. (金子元さんの援助による)

$2^4 = 16 \equiv 1 \pmod{5}$ を以下用いる.

1). $e = 4k$. $q = 2^{e+1} - 1 \equiv 1 \pmod{5}$ によって $q = 1 + 5L$. q は奇数なので L は偶数. $q \equiv 1 \pmod{10}$.

$$a = 2^e q \equiv q \equiv 1 \pmod{5}; a = 1 + 5L. a \text{ は偶数なので } L = 2m + 1. a = 1 + 5(2m + 1) \equiv 6 \pmod{10}.$$

2). $e = 4k + 1$. $c = 2^{2k+1}$ とおくと

$q = 2^{e+1} - 1 = 2^{4k+2} - 1 = c^2 - 1 = (c - 1)(c + 1)$ は素数なので $c - 1 = 1$. ゆえに $q = 3, k = 0, e = 1$. $a = 2 * q = 6$. これは例外的な場合.

3). $e = 4k + 2$. $q = 2^{e+1} - 1 \equiv 2 \pmod{5}$ によって $q = 2 + 5L$. L は奇数になり, $q \equiv 7 \pmod{10}$.

$a = 2^e q \equiv -q \equiv 3 \pmod{5}; a = 3 + 5L$. a は偶数なので $L = 2m + 1$. $a = 3 + 5(2m + 1) \equiv 8 \pmod{10}$.

4). $e = 4k + 3$. $q = 2^{e+1} - 1 \equiv 0 \pmod{5}$ によって $q = 5$. $q = 2^{e+1} - 1 = 5$ とは矛盾する.

末尾の1桁は6, または8になるという結果はやさしいが完全数の美しい性質である.
 q の末尾の1桁は1(最初だけ3), または7になるという性質は完全数の歴史では取り上げられていなかった.

次の表はメルセンヌ素数の表である.

表 1.8:

a	q
1	3
2	7
3	31
4	127
5	8191
6	131071
7	524287
8	2147483647
9	2305843009213693951
10	618970019642690137449562111
11	162259276829213363391578010288127
12	170141183460469231731687303715884105727

1.6 m だけ並行移動した場合の数表

1.6.1 $m = 2$

2 だけ並行移動した場合を見てみよう. $q = 2^{e+1} + 1$ が素数の場合になる. $e+1 = 2^m$ と表せる.

表 1.9: $q = 2^{e+1} + 1$ が素数

e	$e+1$	$e \bmod 4$	$2^e * q$	a
0	1	0	3	3
1	2	1	$2 * 5$	10
3	4	3	$2^3 * 17$	136
7	8	3	$2^7 * 257$	32896
15	16	3	$2^{15} * 65537$	2147516416

3,5,17,257,65537 らは5個のフェルマー素数である.

$2^e * q = 3, 10, 136, 32896, 2147516416$ を2だけ平行移動したフェルマーの完全数と呼んでやりたい.

$e \geq 3$ のとき $q \equiv 7, a \equiv 6 \pmod{10}$.

とくに a の末尾の数は6.

Proof. $e+1 = 2^r$ により $r \geq 2$ なら $e+1 = 4N$ と書けるので

$q = 2^{e+1} + 1 \equiv 2 \pmod{5}$. 一方, q は奇数により $2^e \equiv 3 \times 2^{e+1} \pmod{10}$ になる

ので

$q \equiv 7 \pmod{10}$.

$a = 2^e * q \equiv 3 * q \equiv 6 \pmod{5}$, a は偶数なので $a \equiv 6 \pmod{10}$.

1.7 オイラーの反例

フェルマーの期待に反して, $m \geq 5$ のときフェルマー素数は発見されていない.

オイラーは, 次の結果を証明しこれを用いて F_5 の素因数 641 を発見した.

補題 3 F_m の素因数 Q は $1 + 2^{m+1}K$ と書ける.

Proof

$2^{2^m} + 1 \equiv 0 \pmod{Q}$ なので $2^{2^m} \equiv -1 \pmod{Q}$.

\pmod{Q} での 2 の位数 u は 2^{m+1} の約数である.

$u = 2^s$ とおくと $s \leq 2^{m+1}$ だが $2^{2^m} \equiv -1$ により $s = 2^{m+1}$.

$2^{Q-1} \equiv 1 \pmod{Q}$ によれば $Q-1$ は 2^{m+1} の倍数なので $Q = 1 + 2^{m+1}k$.

補題 4 $Q = 1 + 2^{m+1}k$ において k は偶数である.

$Q = 1 + 2^{m+2}k'$ と書ける.

$2^{\frac{Q-1}{2}} = 2^m k$ となりオイラーの基準によって

$$2^{\frac{Q-1}{2}} \equiv \left(\frac{2}{q}\right) \pmod{Q}.$$

$$2^{\frac{Q-1}{2}} = 2^{2^m k} \equiv (-1)^k \pmod{Q}.$$

k : 偶数 $k = 2k'$.

k : 奇数. $\left(\frac{2}{Q}\right) = -1$ になり $Q \equiv \pm 3 \pmod{8}$.

$Q = 1 + 2^m k, Q = \pm 3 + 8L$ のとき $2^m k = -1 + \pm 3 + 8L$.

(+) なら $2^m k = 2 + 8L. 2^{m-1}k = 1 + 4L. m > 1$ なら矛盾.

(-) なら $2^m k = -4 + 8L. 2^{m-1}k = -2 + 4L. m > 1$ なら矛盾.

$m = 5$ なら $Q = 1 + 128k'. k = 5$ のとき $Q = 641$.

$F_5 = 641 * 6700417$ が素因数分解. $6700417 - 1 = 6700416 = 2^7 * 3 * 17449$.

1.7.1 例

$m = 5$ なら $Q = 1 + 64k$. $k = 10$ のとき $Q = 641$.

$F_5 = 4294967297 = 641 * 6700417$ が素因数分解.

$641 - 1 = 640 = 2^7 * 5$; $2^7 = 2^{5+2}$.

$6700417 - 1 = 6700416 = 2^7 * 3 * 17449$

$F_6 = 18446744073709551617 = 274177 * 67280421310721$ が素因数分解.

$F_7 = 340282366920938463463374607431768211457$

$F_7 = 59649589127497217 * 5704689200685129054721$ が素因数分解.

各素因子について, フェルマーの結果を確認する.

```

m=6
?- A=274177, B is A-1,factorize(B,C),exps(C,D),write(B),put(9),write(D),nl.
274176 [2^8,3^2,7,17] ;2^8=2^{6+2}.
A = 274177,
B = 274176,
D = [2^8, 3^2, 7, 17].

?- A=67280421310721, B is A-1,factorize(B,C),exps(C,D),write(B),put(9),write(D),nl.
67280421310720 [2^8,5,47,373,2998279]
A = 67280421310721,
B = 67280421310720,
D = [2^8, 5, 47, 373, 2998279].

?- A=59649589127497217, B is A-1,factorize(B,C),exps(C,D),write(B),put(9),write(D),nl.
59649589127497216 [2^9,116503103764643]
A = 59649589127497217,
B = 59649589127497216,
D = [2^9, 116503103764643].

```

1.7.2 $m = 4$

$q = 2^{e+1} + 3$ が素数の場合

表 1.10: $p = 2, m = 4$

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
1	5	$2^5 * 67$	2144	4
2	6	$2^6 * 131$	8384	4
3	11	$2^{11} * 4099$	8394752	2
2	14	$2^{14} * 32771$	536920064	4
3	15	$2^{15} * 65539$	2147581952	2
1	17	$2^{17} * 262147$	34360131584	4
3	27	A	B	2
1	29	C	D	4
2	54	E	F	4
2	66	G	H	4
3	83	I	J	2
2	98	K	L	4

$A = 2^{27} * 268435459, B = 36028797421617152$

$$C = 2^{29} * 1073741827, D = 576460753914036224$$

$$E = 2^{54} * 36028797018963971, F = 576460753914036224$$

$$G = 2^{66} * 147573952589676412931$$

$$H = 649037107316853507609507569598464$$

$$I = 2^{83} * 19342813113834066795298819$$

$$J = 187072209578355573530071687601903897267059558449152$$

$$K = 2^{98} * 633825300114114700748351602691$$

$$L = 200867255532373784442745261543596063265446546273971631816704$$

(
表を見ると

- $e \equiv 1 \pmod{4}$ なら $q \equiv 7, a \equiv 4 \pmod{10}$.
- $e \equiv 2 \pmod{4}$ なら $q \equiv 1, a \equiv 4 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ なら $q \equiv 9, a \equiv 2 \pmod{10}$.

Proof.

$e = 4k + 1$ のとき,

$$q \equiv 4 + 3 \equiv 7 \pmod{5}, q \equiv 7 \pmod{10}.$$

$$a = 2^e q \equiv 2 * 7 = 14 \equiv 4 \pmod{5}, a \equiv 4 \pmod{10}.$$

$e = 4k + 2$ のとき,

$$q \equiv -2 + 3 \equiv 1 \pmod{5}, q \equiv 1 \pmod{10}.$$

$$a = 2^e q \equiv 4 * q \equiv 4 \pmod{5}, a \equiv 4 \pmod{10}.$$

$e = 4k + 3$ のとき,

$$q \equiv 1 + 3 \equiv 4 \pmod{5}, q \equiv 9 \pmod{10}.$$

$$a = 2^e q \equiv 3 * 4 = 12 \equiv 2 \pmod{5}, a \equiv 2 \pmod{10}.$$

1.7.3 $m = 6$

$q = 2^{e+1} + 5$ が素数の場合

表 1.11: $p = 2, m = 6$

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
2	2	$2^2 * 13$	52	2
0	4	$2^4 * 37$	592	2
2	10	$2^{10} * 2053$	2102272	2
2	46	A	B	2
0	52	C	D	2

$$A = 2^{46} * 140737488355333$$

$$B = 9903520314283394042913882112$$

$$C = 2^{52} * 9007199254740997$$

$$D = 40564819207303363365892639424512$$

1.7.4 $m = 8$

$q = 2^{e+1} + 7$ が素数の場合

表 1.12: $p = 2, m = 8$

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
3	3	$2^3 * 23$	184	4
1	5	$2^5 * 71$	2272	2
3	7	$2^7 * 263$	33664	4
1	9	$2^9 * 1031$	527872	2
3	15	$2^{15} * 65543$	2147713024	4
1	17	$2^{17} * 262151$	34360655872	2
3	19	$2^{19} * 1048583$	549759483904	4

1.7.5 $m = -2$

$q = 2^{e+1} - 3$ が素数の場合これらは指数 e の擬素数 p_e である. 完全数のときと比べると素数の数が断然多い.

表 1.13: $q = 2^{e+1} - 3$ が素数

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
2	2	$2^2 * 5$	20	0
3	3	$2^3 * 13$	104	4
0	4	$2^4 * 29$	464	4
1	5	$2^5 * 61$	1952	2
0	8	$2^8 * 509$	130304	4
1	9	$2^9 * 1021$	522752	2
3	11	$2^{11} * 4093$	8382464	4
1	13	$2^{13} * 16381$	134193152	2
3	19	A	B	4
1	21	C	D	2
3	23	E	F	4
0	28	G	H	4
1	93	I	J	2

$$A = 2^{19} * 1048573, B = 549754241024$$

$$C = 2^{21} * 4194301, D = 8796086730752$$

$$E = 2^{23} * 16777213, F = 140737463189504$$

$$G = 2^{28} * 536870909, H = 144115187270549504$$

$$I = 2^{93} * 19807040628566084398385987581$$

$$J = 196159429230833773869868419445529014560349481041922097152$$

表を見ると

- $e \equiv 1 \pmod{4}$ なら $q \equiv 1, a \equiv 2 \pmod{10}$.
- $e \equiv 0 \pmod{4}$ なら $q \equiv 9, a \equiv 4 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ なら $q \equiv 3, a \equiv 4 \pmod{10}$.

Proof.

$e = 4k + 1$ のとき,

$$q = 2^{e+1} - 3 \equiv 4 - 3 \equiv 1 \pmod{5}, q \equiv 1 \pmod{10}.$$

$$a = 2^e q \equiv 2 * 1 = 2 \pmod{5}, a \equiv 2 \pmod{10}.$$

$e = 4k$ のとき,

$$q = 2^{e+1} - 3 \equiv 2 - 3 \equiv 4 \pmod{5}, q \equiv 9 \pmod{10}.$$
$$a = 2^e q \equiv 9 \equiv 4 \pmod{5}, a \equiv 4 \pmod{10}.$$

$$e = 4k + 3 \text{ のとき,}$$
$$q \equiv 1 - 3 \equiv 3 \pmod{5}, q \equiv 3 \pmod{10}.$$
$$a = 2^e q \equiv 9 \equiv 4 \pmod{5}, a \equiv 4 \pmod{10}.$$

$$e = 4k + 2 \text{ のとき,}$$
$$q = 2^{e+1} - 3 \equiv 3 - 3 \equiv 0 \pmod{5}. q = 5.$$
$$q = 2^{e+1} - 3 = 5; e = 2. a = 2^e q = 4 * 5 = 20.$$

1.7.6 $m = -4$

$q = 2^{e+1} - 5$ が素数の場合

表 1.14: $q = 2^{e+1} - 5$

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
3	3	$2^3 * 11$	88	8
1	5	$2^5 * 59$	1888	8
3	7	$2^7 * 251$	32128	8
1	9	$2^9 * 1019$	521728	8
3	11	$2^{11} * 4091$	8378368	8
1	17	$2^{17} * 262139$	34359083008	8
3	19	$2^{19} * 1048571$	549753192448	8
1	25	$2^{25} * 67108859$	2251799645913088	8
3	31	$2^{31} * 4294967291$	9223372026117357568	8
3	35	$2^{35} * 68719476731$	2361183241263023915008	8
3	50	$2^{50} * 72057594037927931$	A	8
3	65	$2^{65} * 73786976294838206459$	B	8

$A = 81129638414606676066289470930944$

$B = 2722258935367507707522529418717050175488$

指数 e が奇数になることの証明

偶数になる, すなわち $e = 2N$ と仮定して矛盾を導く.

$q = 2^{2N+1} - 5$ が素数とする. 3 を法としてみる. $2^{2N+1} = 4^N \times 2 \equiv 2, 5 \equiv 2 \pmod{3}$.

これらにより $q = 2^{2N+1} - 5 \equiv 0 \pmod{3}$ したがって q が 3 の倍数; 矛盾が導かれた.

表を見ると

• $e \equiv 1 \pmod{4}$ なら $q \equiv 9, a \equiv 8 \pmod{10}$.

• $e \equiv 3 \pmod{4}$ なら $q \equiv 1, a \equiv 8 \pmod{10}$.

Proof.

$e = 4k + 1$ のとき,

$q \equiv 4 \pmod{5}, q \equiv 9 \pmod{10}$.

$a = 2^e q \equiv 2 * 9 \equiv 3 \pmod{5}, a \equiv 8 \pmod{10}$.

$e = 4k + 3$ のとき,

$q \equiv 1 \pmod{5}, q \equiv 1 \pmod{10}$.

$a = 2^e q \equiv 3 * 1 \pmod{5}, a \equiv 8 \pmod{10}$.

1.7.7 $m = -6$

$q = 2^{e+1} - 7$ が素数の場合

表 1.15: $q = 2^{e+1} - 7$ が素数

$e \pmod 4$	e	$2^e * q$	a	$a \pmod{10}$
2	2	$2^2 * 1$	4	4
2	38	$2^{38} * 549755813881$	151115727449904501489664	4
2	714	A	B	4
2	1982	C	D	4
2	2318	E	F	4

$$A = 2^{714} * 172364133221937103085272756482[156digits]353486799545737272878084128761$$

$$B = 148546972106748408784527026025[371digits]871159239450829038055508148224$$

$$C = 2^{1982} * 875954204768565768610254822675[537digits]949667135757182722184637841401$$

$$D = 383647884425865224359990619773[1134digits]165116463409179288256647266304$$

$$E = 2^{2318} * 122619614032433428311834616579[639digits]105574484775025248995836428281$$

$$F = 51778487273147246081979595282[1336digits]568219992473923005215055806464$$

(

$a = 4$ のとき, $\tilde{\sigma}(4) = \frac{7}{2}$ なので $4 - 2\tilde{\sigma}(4) = -3$. (1 が素数のフリをしている)

$q = 2^{e+1} - 7$ が素数になる場合がきわめて少ない.

a の末尾の数は 4.

e が偶数の証明

$e = 2k + 1$ として矛盾を導く.

$$q = 2^{e+1} - 7 = (2^2)^{k+1} - 7 \equiv 1 - 1 = 0 \pmod 3 \text{ なので矛盾.}$$

$e = 4k + 2$ の証明

$e = 4k$ として矛盾を導く.

$$q = 2^{e+1} - 7 = (2^4)^k \times 2 - 7 \equiv 2 - 2 = 0 \pmod 5 \text{ なので矛盾.}$$

$q = 2^{e+1} - 7$ が素数となる場合を探すには e が初項 2, 公差 4 の等差数列となることを使えば, 効率の向上が期待できる.

1.7.8 $m = -8$ $q = 2^{e+1} - 9$ が素数の場合表 1.16: $p = 2, m = -8$

$e \bmod 4$	e	$2^e * q$	a
0	4	$2^4 * 23$	368
0	8	$2^8 * 503$	128768
2	10	$2^{10} * 2039$	2087936
0	16	$2^{16} * 131063$	8589344768
0	32	$2^{32} * 8589934583$	36893488108764397568
0	124	$2^{124} * 42535295865117307932921825928971026423$	A
0	140	B	C

$$A = 904625697166532776746648320380374279912262923807289020860114158381451706368$$

$$B = 2^{140} * 2787593149816327892691964784081045188247543$$

$$C = 3885337784451458141838923813647037813284801133935104869028107705636280205707069882368$$

1.8 m だけ平行移動した方程式の解

パラメータ m に対して $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した完全数ということにしたがこれの満たす方程式を求めよう. ただし m は偶数の整数.(実際には1桁程度に留めるのがよいだろう)

$\sigma(a) = \sigma(2^e q) = (2^{e+1} - 1)(q + 1)$, $q + 1 = 2^{e+1} + m$ に注意して次の式変形を行う.

$$\begin{aligned}\sigma(a) &= \sigma(2^e q) \\ &= (2^{e+1} - 1)(q + 1) \\ &= (q - m)(2^{e+1} + m) \\ &= q(2^{e+1} + m) - m(2^{e+1} + m) \\ &= 2a + qm - m(q + 1) \\ &= 2a - m.\end{aligned}$$

かくして $\sigma(a) = 2a - m$ がえられた.

方程式 $\sigma(a) = 2a - m$ の解は偶数完全数の平行移動としてできるか?

という問題を建てる.

m が少し大きいと反例が出やすい.

$m = 2$ では反例が出なかった

1.9 $s(a) = 2$ のときの証明

方程式 $\sigma(a) = 2a - m$ を満たす解を $|m| \leq 8$ の場合に $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した完全数と書けることを次に証明する.

a を素因数分解し $a = p^e q^f$ とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる.

$\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおけば

$$\frac{AB}{\rho'} = 2XY - m.$$

書き直して

$$AB = 2\rho'XY - m\rho'.$$

$AB - 2\rho'XY$ の XY の係数を R とおくと $R = pq - 2\rho'$ となり

$$RXY = pX + qY - 1 - \rho'm.$$

この式を基本等式という.

$m \leq 8$ のとき $pX + qY - 1 - \rho'm > 0$ を次に示す.

$$pX + qY - 1 - \rho'm > p^2 + q^2 - 1 - \rho'm \geq 0.$$

最初に $p = 2, q = 3$ としてみる.

$$p^2 + q^2 - 1 - \rho'm = 12 - 2m = 2(6 - m) \text{ なので } m \leq 6 \text{ ならよい.}$$

$p = 2, q = 3, m = 8$ とおくと

$$RXY = 2XY, pX + qY - 1 - \rho'm = 2X + 3Y - 1 - 16$$

により, $2XY + 17 = 2X + 3Y$.

$(2X - 3)Y = 2X - 17$ により

$$Y = 1 - \frac{14}{2X - 3} < 1.$$

$p = 2, q = 5, m = 8$ とおくと $2XY = 2X + 5Y - 1 - 32$. やはり解がない.

$pX + qY - 1 - \rho'm > 0$ が示されたので

基本等式から $R > 0$ なので $p = 2$ かつ $R = 2$. したがって

$$2XY = 2X + qY - 1 - \bar{q}m.$$

$Y = q$ のとき $2Xq = 2X + q^2 - 1 - \bar{q}m$.

$$2X\bar{q} = \bar{q}\bar{q} - \bar{q}m.$$

よって

$$2X = \tilde{q} - m.$$

$Y > q$ のとき $Y \geq q^2$ なので

$$(2X - q)Y = 2X - 1 - \bar{q}m \geq (2X - q)q^2.$$

$$2X(1 - q^2) - \bar{q}m \geq 1 - q^3.$$

\bar{q} で割ると

$$2X\tilde{q} + m < q^2 + q + 1.$$

$2X - q > 1$ と組み合わせると

$$\tilde{q}^2 + m < 2X\tilde{q} + m < q^2 + q + 1 = \tilde{q}^2 - q.$$

よって $m < -q$.

m が負の値になるとどうなるか?

1.10 例

1.10.1 $\sigma(a) = 2a - 2$

$m = 2$ すなわち, $\sigma(a) = 2a - 2$ を満たす解の表を作った.

表 1.17: $\sigma(a) = 2a - 2$

a	素因数分解	$\sigma(a)$
3	[3]	4
10	[2, 5]	18
136	[2 ³ , 17]	270
32896	[2 ⁷ , 257]	65790
2147516416	[2 ¹⁵ , 65537]	

たぶん解はこれだけ.

[研究課題]

$\sigma(a) = 2a - 2$ で a が偶数なら $s(a) = 2$ を満たすか? (オイラーの証明を真似てもうまくいかな
いだろう)

$s(a) = 3$ を満たす解があるか.

次に $m = 4$ の場合を扱う.

1.10.2 $\sigma(a) = 2a - 4$

$\sigma(a) = 2a - 4$ を満たす解の表を作った.

表 1.18: $\sigma(a) = 2a - 4$

a	素因数分解	$\sigma(a)$
5	[5]	6
14	[2, 7]	24
44	[2 ² , 11]	84
110	[2, 5, 11]	216
152	[2 ³ , 19]	300
884	[2 ² , 13, 17]	1764
2144	[2 ⁵ , 67]	4284
8384	[2 ⁶ , 131]	16764
18632	[2 ³ , 17, 137]	37260

$a = 5$ は $s(a) = 1$ なので反例になる. この例は微小解として後で扱うことになる.
 $a = 110, 884, 18632$ は $s(a) = 3$ なので反例になる. 反例はさらにありそうである.

[研究課題]

$\sigma(a) = 2a - 4$ で a が偶数なら $s(a) = 2, 3$ を満たすか?

$s(a) = 3$ を満たす解をすべて求めよ.

1.10.3 $\sigma(a) = 2a - 6$

$m = 6$; $\sigma(a) = 2a - 6$ を満たす解の表を作った.

表 1.19: $\sigma(a) = 2a - 6$

a	素因数分解	$\sigma(a)$
7	[7]	8
15	[3, 5]	24
52	[2 ² , 13]	98
315	[3 ² , 5, 7]	624
592	[2 ⁴ , 37]	1178
1155	[3, 5, 7, 11]	2304

微小解 $a = 7$, $s(a) = 2$ の解は識られているとおりだが $s(a) = 3$ の解 315 ([3², 5, 7]) に続けて $s(a) = 4$ の解 1155 ([3, 5, 7, 11]) が後を追う.

$a = 2^e qr$ 型の解はないらしい.

1.10.4 $\sigma(a) = 2a - 8$

$m = 8$; $\sigma(a) = 2a - 8$ を満たす解の表を作った.

表 1.20: $\sigma(a) = 2a - 8$

a	素因数分解	$\sigma(a)$
22	[2, 11]	36
130	[2, 5, 13]	252
184	[2 ³ , 23]	360
1012	[2 ² , 11, 23]	2016
2272	[2 ⁵ , 71]	4536
18904	[2 ³ , 17, 139]	37800
33664	[2 ⁷ , 263]	67320
70564	[2 ² , 13, 23, 59]	141120
85936	[2 ⁴ , 41, 131]	171864

$2^e qr$ がたの解 184 ([2³, 23]), 2272 ([2⁵, 71]), 33664 [2⁷, 263] に注目.
 $s(a) = 4$ の解 70564 ([2², 13, 23, 59]) が登場.

m が大きい場合も計算してみた.

1.10.5 $\sigma(a) = 2a - 32$

$m = 32$; $\sigma(a) = 2a - 32$ を満たす解の表を作った.

表 1.21: $\sigma(a) = 2a - 32$

a	素因数分解	$\sigma(a)$
572	1176	$[2^2, 11, 13]$
992	2016	$[2^5, 31]$
7544	15120	$[2^3, 23, 41]$
10184	20400	$[2^3, 19, 67]$
28544	57120	$[2^7, 223]$
83312	166656	$[2^4, 41, 127]$
113072	226176	$[2^4, 37, 191]$
122624	245280	$[2^8, 479]$

$2^e q, 3^e q r$ の解のみなのうれしい.

1.10.6 $\sigma(a) = 2a - 64$

$m = 64$; $\sigma(a) = 2a - 64$ を満たす解の表を作った.

表 1.22: $\sigma(a) = 2a - 64$

a	素因数分解	$\sigma(a)$
108	280	$[2^2, 3^3]$
220	504	$[2^2, 5, 11]$
6808	13680	$[2^3, 23, 37]$
8968	18000	$[2^3, 19, 59]$
14008	28080	$[2^3, 17, 103]$
24448	48960	$[2^7, 191]$
66928	133920	$[2^4, 47, 89]$

ついに $a = 2^2 * 3^3$ として $s(a) = 2$ で $2^e q$ と書けない解が登場.
 $m = 64$ のときこれだけが反例かもしれない.

1.10.7 $\sigma(a) = 2a + 2$

$m = -2$; $\sigma(a) = 2a + 2$ を満たす解の表を作った.

表 1.23: $\sigma(a) = 2a + 2$

a	素因数分解	$\sigma(a)$
20	$[2^2, 5]$	42
104	$[2^3, 13]$	210
464	$[2^4, 29]$	930
650	$[2, 5^2, 13]$	1302
1952	$[2^5, 61]$	3906

解 650 ($[2, 5^2, 13]$) はひねくれている.

1.10.8 $\sigma(a) = 2a + 4$

$m = -4$; $\sigma(a) = 2a + 4$ を満たす解の表を作った.

表 1.24: $\sigma(a) = 2a + 4$

a	素因数分解	$\sigma(a)$
12	$[2^2, 3]$	28
70	$[2, 5, 7]$	144
88	$[2^3, 11]$	180
1888	$[2^5, 59]$	3780
4030	$[2, 5, 13, 31]$	8064
5830	$[2, 5, 11, 53]$	11664
32128	$[2^7, 251]$	64260

$s(a) = 4$ の解が複数個ある.

1.10.9 $\sigma(a) = 2a + 6$

$\sigma(a) = 2a + 6$ を満たす解の表を作った.

表 1.25: $\sigma(a) = 2a + 6$

a	素因数分解	$\sigma(a)$
8925	$[3, 5^2, 7, 17]$	17856
32445	$[3^2, 5, 7, 103]$	64896

$s(a) = 4$ の解は複数個ありしかもひねくれている.

1.10.10 $\sigma(a) = 2a + 8$ 表 1.26: $\sigma(a) = 2a + 8$

a	素因数分解	$\sigma(a)$
56	$[2^3, 7]$	120
368	$[2^4, 23]$	744
836	$[2^2, 11, 19]$	1680
11096	$[2^3, 19, 73]$	22200
17816	$[2^3, 17, 131]$	35640
45356	$[2^2, 17, 23, 29]$	90720
77744	$[2^4, 43, 113]$	155496
91388	$[2^2, 11, 31, 67]$	182784

$s(a) = 3, 4$ の解が普通にでている.

1.10.11 $\sigma(a) = 2a + 32$

$s(a) = 2$ で $2^e q$ 形でない解 $a = 250 = 2 * 5^3$ があつた.

表 1.27: $\sigma(a) = 2a + 16$

a	素因数分解	$\sigma(a)$
550	$[2, 5^2, 11]$	---
748	$[2^2, 11, 17]$	---
1504	$[2^5, 47]$	---
7192	$[2^3, 29, 31]$	---
7912	$[2^3, 23, 43]$	---
10792	$[2^3, 19, 71]$	---
17272	$[2^3, 17, 127]$	---
30592	$[2^7, 239]$	---

表 1.28: $\sigma(a) = 2a + 32$

a	素因数分解	$\sigma(a)$
250	468	$[2, 5^3]$
376	720	$[2^3, 47]$
1276	2520	$[2^2, 11, 29]$
12616	25200	$[2^3, 19, 83]$
20536	41040	$[2^3, 17, 151]$

1.11 微小解

$\sigma(a) = 2a - m$ の解に $a = p^e$ があるとする.

$$m = 2a - \sigma(a) = 2p^e - (1 + p + \cdots + p^e) = p^e - (1 + p + \cdots + p^{e-1})$$

を満たす.

$e = 1$ のとき $m = p - 1$ なので $m + 1$ が素数 p になるとき p は微小解.

$m = 2, 4, 6, 10, 16$ のとき微小解 $p = 3, 5, 7, 11, 17$ がそれぞれあるが $m = 8, 32$ のとき微小解はない.

$e = 2$ のとき $m = p^2 - 1 - p$. $p > 2$ になるがこのとき m は奇数なので一応除外する.

$e = 3$ のとき $m = p^3 - 1 - p - p^2$. $p = 3$ のとき $m = 14$.

例

表 1.29: $\sigma(a) = 2a - 14$

a	素因数分解	$\sigma(a)$
27	40	$[3^3]$
34	54	$[2, 17]$
232	450	$[2^3, 29]$
34432	68850	$[2^7, 269]$

1.12 $a = 2^e qr$ 型の解

$a = 2^e qr$ 型の解.

$\sigma(a) = 2a + m$ に解 $a = 2^e qr$ ($2 < q < r$:素数) があるとする.

$\sigma(a) = \sigma(2^e qr) = (2^{e+1} - 1)\tilde{q}\tilde{r}$, $2a = 2^{e+1}qr$ により $\Delta = q + r$ を用いて

$$2^{e+1}(\Delta + 1) - (qr + \Delta + 1) = -m,$$

により

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

$\Gamma = 2^{e+1} - 1$ を用いると

$$qr = \Gamma\Delta + \Gamma + m.$$

$q_0 = q - \Gamma, r_0 = r - \Gamma$ に置き換えると

$$q_0 r_0 = \Gamma^2 + \Gamma + m. \tag{1.3}$$

与えられた $e > 0$ に対して $\Gamma = 2^{e+1} - 1, D = \Gamma^2 + \Gamma + m$ とおき $D = q_0 r_0$ と2組の積に因数分解して $q = q_0 + \Gamma, r = r_0 + \Gamma$ がともに素数となる q, r を選択すると $a = 2^e qr$ 型の解が得られる.

これはアルゴリズムとしては優秀である.

実行例

$2^e = 2^4, m = 4(e = 4)$ と初期値を入れる.

$D = 996, U(\Gamma) = 31$

$D = 996$ を分解する.

$a=1$ $b=996$ $a1=32$ $32=[2,2,2,2]$ ($a1$: 素数ではない)

$a=2$ $b=498$ $a1=33$ $33=[3,11]$

$a=3$ $b=332$ $a1=34$ $34=[2,17]$

$a=4$ $b=249$ $a1=35$ $35=[5,7]$

$a=5$ $b=199$ $a=6$ $b=166$ $a1=37$ $37=[37]$ $a = 37$ は素数

$197=[197]$ $b = 197$ も素数.

解 $a = 2^4 * 37 * 197$ を発見 $\sigma = 233244$.

次の解を探す.

$a=7$ $b=142$; $a=8$ $b=124$; $a=9$ $b=110$; $a=10$ $b=99$; $a=11$ $b=90$; $a=12$ $b=83$; $a=1=43$ $43=[43]$
 $a = 43$ は素数.

$114=[2,3,19]$ しかし $b = 114$ は素数ではない.

次の解を探す.

$a=13$ $b=76$; $a=14$ $b=71$; $a=15$ $b=66$; $a=16$ $b=62$; $a=17$ $b=58$; $a=18$ $b=55$; $a=19$ $b=52$;
 $a=20$ $b=49$; $a=21$ $b=47$; $a=22$ $b=45$; $a=23$ $b=43$; $a=24$ $b=41$; $a=25$ $b=39$; $a=26$ $b=38$;
 $a=27$ $b=36$; $a=28$ $b=35$; $a=29$ $b=34$; $a=30$ $b=33$; $a=31$ $b=32$ 解にはならず.

1.12.1 $p = 2, m = 4; a = 2^e qr$

表 1.30: $p = 2, m = 4; a = 2^e qr$

a	素因数分解	$\sigma(a)$
110	$2 * 5 * 11$	216
884	$2^2 * 13 * 17$	1764
18632	$2^3 * 17 * 137$	37260
116624	$2^4 * 37 * 197$	233244
15370304	$2^6 * 137 * 1753$	30740604
73995392	$2^7 * 293 * 1973$	147990780

$a = 2^e qr$ 型の解からなる表を見る.

最初の1行を無視するとみな a の末尾の数は 2,4.

1.12.2 $p = 2, m = 8; a = 2^e qr$

最初の1行を無視するとみな a の末尾の数は 2,4,6.

表 1.31: $p = 2, m = 8; a = 2^e qr$

a	素因数分解	$\sigma(a)$
130	$2^1 * 5 * 13$	252
1012	$2^2 * 11 * 23$	2016
18904	$2^3 * 17 * 139$	37800
85936	$2^4 * 41 * 131$	171864
1090912	$2^5 * 73 * 467$	2181816
952413274955776	$2^{13} * 16421 * 7080043$	1904826549911544
120646991405056	$2^{13} * 16693 * 882251$	241293982810104
99249696661504	$2^{13} * 16763 * 722749$	198499393323000
144141578099802112	$2^{14} * 32771 * 268460033$	288283156199604216
4611826763432034304	$2^{15} * 65537 * 2147516419$	9223653526864068600
304811774955304517632	$2^{18} * 524411 * 2217277373$	609623549910609035256

1.12.3 $p = 2, m = -8; a = 2^e qr$ 表 1.32: $p = 2, m = -8; a = 2^e qr$

a	素因数分解	$\sigma(a)$
836	$2^2 * 11 * 19$	1680
17816	$2^3 * 17 * 131$	35640
11096	$2^3 * 19 * 73$	22200
77744	$2^4 * 43 * 113$	155496
2291936	$2^5 * 67 * 1069$	4583880
13174976	$2^6 * 139 * 1481$	26349960
45335936	$2^7 * 337 * 1051$	90671880
35021696	$2^7 * 419 * 653$	70043400
4856970752	$2^9 * 1171 * 8101$	9713941512
1461083549696	$2^{12} * 10939 * 32609$	2922167099400
144141575952121856	$2^{14} * 32771 * 268460029$	288283151904243720
933386556194816	$2^{14} * 33409 * 1705211$	1866773112389640
417857739454939136	$2^{18} * 673469 * 2366851$	835715478909878280

a の末尾の数は 2,4,6.

1.12.4 $p = 2, m = 32; a = 2^e qr$ 表 1.33: $p = 2, m = 32; a = 2^e qr$

a	素因数分解	$\sigma(a)$
170	$2^1 * 5 * 17$	324
988	$2^2 * 13 * 19$	1960
12008	$2^3 * 19 * 79$	24000
8648	$2^3 * 23 * 47$	17280
117808	$2^4 * 37 * 199$	235600
63248	$2^4 * 59 * 67$	126480
1292768	$2^5 * 71 * 569$	2585520
526688	$2^5 * 109 * 151$	1053360
13192768	$2^6 * 139 * 1483$	26385520
4495808	$2^6 * 199 * 353$	8991600
169371008	$2^7 * 269 * 4919$	338742000
33653888	$2^7 * 467 * 563$	67307760
883927808	$2^8 * 557 * 6199$	1767855600
293947648	$2^8 * 787 * 1459$	587895280
69662739968	$2^9 * 1031 * 131969$	139325479920
2493705728	$2^9 * 1489 * 3271$	4987411440
1473186024448	$2^{10} * 2053 * 700759$	2946372048880
217898810368	$2^{10} * 2089 * 101863$	435797620720
1282330216448	$2^{11} * 4211 * 148691$	2564660432880
1020401174528	$2^{11} * 4243 * 117427$	2040802349040
546409576448	$2^{11} * 4391 * 60761$	1092819152880
1290987160936448	$2^{13} * 16411 * 9602779$	2581974321872880
8041132207751168	$2^{14} * 32839 * 14945393$	16082264415502320
219521427324928	$2^{14} * 35923 * 372979$	439042854649840
2306054126720811008	$2^{15} * 65539 * 1073790979$	4612108253441622000
2306054126720811008	$2^{15} * 65539 * 1073790979$	4612108253441622000
419512906614407168	$2^{15} * 65557 * 195288343$	839025813228814320
1824454941114368	$2^{15} * 71563 * 778027$	3648909882228720
5544305213636608	$2^{16} * 182899 * 462547$	11088610427273200
295163668022862675968	$2^{17} * 262151 * 8590163969$	590327336045725351920

第2章 底が3のとき

2.1 $a = 3^e$ の場合

完全数では2のべきが基本であったがここでは3のべきの場合を扱う。

$a = 3^e$ とおくと $\sigma(a) = \sigma(3^e) = \frac{3^{e+1}-1}{2}$, なので $2\sigma(a) = 3^{e+1} - 1 = 3a - 1$.

そこで $2\sigma(a) - 3a = -1$ を満たす a は何かを問題とする。これだけを単独で考えるのはもったいないので3点セットにして

- (1) $2\sigma(a) - 3a = -1$ を満たす自然数は何か,
- (2) $2\sigma(a) - 3a = 1$ を満たす自然数は何か,
- (3) $2\sigma(a) - 3a = 0$ を満たす自然数は何か

を問題にする。

2.1.1 数値計算例

$2\sigma(a) - 3a = -1$ を満たす自然数についてパソコン君に計算してもらおう。

表 2.1: $2\sigma(a) - 3a = -1$

a	$\sigma(a)$	素因数分解
3	4	[3]
9	13	[3 ²]
27	40	[3 ³]
81	121	[3 ⁴]
243	364	[3 ⁵]
729	1093	[3 ⁶]
2187	3280	[3 ⁷]
6561	9841	[3 ⁸]
19683	29524	[3 ⁹]

この場合は期待に応じて3のべきが並んで出てきた。言い換えれば $s(a) = 1$ の解だけである。 $s(a) = 1$ を仮定したとき a が3のべきになることはすぐわかる。

2.1.2 $s(a) = 2$ のときの証明

$s(a) = 2$ を仮定して $2\sigma(a) = 3a - 1$ を満たすとき矛盾を導こう.

最初に a は奇数であることを確認する. なぜなら -1 は奇数で, $2\sigma(a)$ は偶数だから.

$s(a) = 2$ のときなので a を素因数分解し $a = p^e q^f$ ($2 < p < q$) とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおけば

$$\frac{2AB}{\rho'} = (3a - 1) = 3XY - 1.$$

書き直して

$$2AB = 3\rho'XY - \rho'.$$

$2AB - 3\rho'XY$ の XY の係数を R とおけば

$$R = 2pq - 3\rho' = 6 - (p - 3)(q - 3).$$

$-\rho' + pX + qY - 1 = RXY$ によって $R > 0$.

$p \geq 3$ なので $0 < R = 6 - (p - 3)(q - 3)$ により $p = 3, R = 6, \rho' = 2\bar{q}$.

$$-2\bar{q} = 6XY - 2(3X + qY - 1)$$

を2で割って

$$-\bar{q} = 3XY - (3X + qY - 1) = (3X - q)Y - 3X + 1.$$

移項して $(3X - q)Y - 3X + 1 + \bar{q} = 0$ により

$$(3X - q)Y - 3X + q = (3X - q)(Y - 1) = 0.$$

$3X = q$ となり矛盾.

$s(a) = 3$ のときも矛盾が導けるとよいのだが, 面倒くさそうである.

$s(a) \geq 3$ なら解のないことの証明は難しそうなので, どちらかというとなら解がある方に私は1票入りたい.

2.2 $2\sigma(a) - 3a$ の値

パソコン君に $2\sigma(a) - 3a$ の値を調べて表をつくってもらった. 便宜上 $2\sigma(a) - 3a$ を ω 完全度という.

この表の観察の結果興味ある結果が見えたら証明してみよう. うまく行けば自分の定理が見つかるかもしれない.

表 2.2: $2\sigma(a) - 3a$ (ω 完全度) の表

ω 完全度	a	素因数分解	$\sigma(a)$
-5	7	[7]	8
-5	39	[3, 13]	56
-5	279	[3 ² , 31]	416
-5	178119	[3 ⁵ , 733]	--
-3	5	[5]	6
-3	33	[3, 11]	48
-3	261	[3 ² , 29]	390
-3	385	[5, 7, 11]	576
-3	897	[3, 13, 23]	1344
-3	2241	[3 ³ , 83]	--
-3	269371	[3 ² , 41, 73]	--
-1	3	[3]	4(3 の累乗)
-1	9	[3 ²]	13
-1	27	[3 ³]	40
-1	81	[3 ⁴]	121
-1	243	[3 ⁵]	364
-1	729	[3 ⁶]	1093
0	2	[2]	3

ここの観察からいろいろな結果が想定できる.

表 2.3:

亜完全度	a	素因数分解	$\sigma(a)$
1	21	[3, 7]	32
2	4	[2 ²]	7
3	15	[3, 5]	24
3	207	[3 ² , 23]	312
3	1023	[3, 11, 31]	1536
6	6	[2, 3]	12
6	8	[2 ³]	15 (擬素数)
6	10	[2, 5]	18(2の奇素数倍)
6	14	[2, 7]	24
6	22	[2, 11]	36
6	26	[2, 13]	42
6	34	[2, 17]	54
6	38	[2, 19]	60
6	46	[2, 23]	72
6	58	[2, 29]	90
6	62	[2, 31]	96
6	74	[2, 37]	114
6	82	[2, 41]	126
6	86	[2, 43]	132

表によれば $2\sigma(a) = 3a$ を満たす a は2だけらしい. 証明を試みたら簡単にきた. そこで定理とした.

定理 1 $2\sigma(a) = 3a$ を満たすとき $a = 2$.

Proof.

$2\sigma(a) = 3a$ により a は偶数なので $a = 2^e L$ とおき L は奇数とする.

$$2\sigma(a) = 2(2^{e+1} - 1)\sigma(L) = 3 * 2^e L$$

これより $N = 2^{e+1} - 1$ とおき両辺を2倍する.

$$4N\sigma(L) = 3 * 2^{e+1} L = 3(N + 1)L$$

$L > 1$ なら $\sigma(L) > L$ なので

$$3(N + 1)L = 4N\sigma(L) > 4N(L + 1)$$

$3L > NL + 4N$, $N \geq 3$ なので矛盾.

よって $L = 1$. $a = 2^e$ になって $4N = 3(N + 1)$. ゆえに $N = 3, e = 1$. したがって $a = 2$.

3点セットのうち1つは解けてしまった. これはうれしい.

2.3 $2\sigma(a) - 3a = 1$ の場合

すなわち亜完全度が1の場合, パソコン君に数値例をだしてもらい次の表ができた.

表 2.4: $2\sigma(a) - 3a = 1$

a	$\sigma(a)$	素因数分解
21	32	$[3, 7]$
2133	3200	$[3^3, 79]$
19521	29282	$[3^4, 241]$
176661	264992	$[3^5, 727]$
129127041	193690562	$[3^8, 19681]$

この解の素因数分解は $3^e * q$ の形になっている. このような形の解があるとしてその形を決めよう.

$a = 3^e * q$, ($q > 3$: 素数) として代入すると

$$2\sigma(a) = (3^{e+1} - 1)(q + 1) = 3a + 1 = 3^{e+1}q + 1.$$

これより

$$(3^{e+1} - 1)(q + 1) = (3^{e+1} - 1)q + 3^{e+1} - 1 = 3^{e+1}q + 1.$$

$3^{e+1}q$ が両辺から消えて

$$-q + 3^{e+1} - 1 = 1.$$

書き直して $q = 3^{e+1} - 2$. そこで $3^{e+1} - 2$ が素数になるときそれを q とおき $a = 3^e * q$ と定義すると $2\sigma(a) - 3a = 1$ を満たす.

2.4 亜完全数

$q = 3^{e+1} - 2$ が素数になるとき $a = 3^e * q$ を (3 を底とする) 亜完全数とよぼう. 亜完全数は $2\sigma(a) - 3a = 1$ を満たす.

逆に $2\sigma(a) - 3a = 1$ を満たすときそれは亜完全数か, という問題を考える. これは難しい問題であろう.

2.5 亜完全度

$W = 2\sigma(a) - 3a$ とおき W は完全度であり亜完全数の 亜完全度は 1 である.

与えられた W は適当に小さいとして $W = 2\sigma(a) - 3a$ を満たす a を仮定 $s(a) = 2$ の下でこれを求めよう.

a を素因数分解し $a = p^e q^f$ とする.

2.5.1 亜完全度が奇数の場合

W は奇数と仮定する.

$W = 2\sigma(a) - 3a$ によって a は奇数. したがって $2 < p < q$ となる.

$X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\overline{pq}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \overline{pq}$ とおけば

$$\frac{2AB}{\rho'} = 3XY + W.$$

書き直して

$$2AB = \rho'(3XY + W)$$

$2AB - 3\rho'XY$ の XY の係数を R とおくと $R = 2pq - 3\rho'$ になりさらに

$$\begin{aligned} R &= 2pq - 3\rho' \\ &= -pq + 3(p + q - 1) \\ &= -(p - 3)(q - 3) + 6. \end{aligned}$$

それから

$$\rho'W = RXY - 2(pX + qY - 1).$$

$\rho'W + 2(pX + qY - 1) = RXY$ によって $RXY > \rho'W + 2(p^2 + q^2 - 1) > 0$ により $R > 0$ なので $p \geq 3$ に注意し $p = 3, R = 6$.

このとき $\rho' = 2\overline{q}$ になり

$$2\bar{q}W = 6XY - 2(3X + qY - 1).$$

移項して

$$\bar{q}W = (3X - q)Y - 3X + 1.$$

(1) $Y = q$ と仮定すると

$$\bar{q}W = (3X - q)q - 3X + 1 = 3X\bar{q} - \bar{q}(q + 1)$$

により, \bar{q} を払うことによって

$$W = 3X - (q + 1).$$

ここで話を逆転させる. $3X - W - 1$ が素数のときこれを q とおいて $a = 3^e q$ を定めれば亜完全度 W の数 a を得るのである.

とくに $W = -1$ なら $3X = q$ が素数なのでこの場合は起きない.

$W = 1$ なら $q = 3^{e+1} - 2$ が素数なので, 亜完全数の場合である.

(2) $Y = q^2$ のとき.

$$\bar{q}W = (3X - q)q^2 - 3X + 1 = 3X(q^2 - 1) + 1 - q^3 = \bar{q}(3X(q + 1) - (q^2 + q + 1)).$$

これより \bar{q} を払うと

$$W = 3X(q + 1) - (q^2 + q + 1).$$

$W > 0$ のとき $3X \geq q + 1$ が成り立つので

$$W = 3X(q + 1) - (q^2 + q + 1) \geq (q + 1)^2 - (q^2 + q + 1) \geq q \geq p + 2 \geq 5.$$

この場合 $W > 1$ になる. 亜完全数にならない.

$Y \geq q^3$ ならますます $2\sigma(a) - 3a$ は大きくなるであろう.

したがって, $s(a) = 2, W = 1$ のとき $Y = q$ となり亜完全数になる.

2.5.2 奇数の例

$q = 5, f = 2, X = 3$ とおくと $a = 5^2 * 3 = 75$.

$W = 3X(q + 1) - (q^2 + q + 1) = 9 * 6 - (q^2 + q + 1) = 23$.

$W = 23$ なら $a = 75$ になるか?

$q = 5, f = 2, X = 3^2$ とおくと $a = 5^2 * 3^2 = 225$

$W = 3X(q + 1) - (q^2 + q + 1) = 27 * 6 - (q^2 + q + 1) = 131$

この場合 $s(a) = 3$ の解も出てきた.

$q = 5, f = 2, X = 3^3$ とおくと $a = 5^2 * 3^3 = 675$.

表 2.5: $W = 23$ の場合

a	$\sigma(a)$	素因数分解
75	124	$[3, 5^2]$

表 2.6: $W = 131$ の場合

a	$\sigma(a)$	素因数分解
225	403	$[3^2, 5^2]$
1407	2176	$[3, 7, 67]$

$$W = 3X(q+1) - (q^2 + q + 1) = 27 \times 6 - (q^2 + q + 1) = 455.$$

表 2.7: $W = 455$ の場合

a	$\sigma(a)$	素因数分解
675	1240	$[3^3, 5^2]$
819	1456	$[3^2, 7, 13]$

この場合も解が2つしかないらしいが分からない。

2.5.3 亜完全度が偶数の場合

亜完全度 W は偶数 $2m$ と仮定する. $2\sigma(a) - 3a = 2m$ により a は偶数.

$s(a) = 2$ の場合に計算しよう. a を素因数分解すると $a = 2^e q^f$, $2 < q$ となる.

$X = 2^e$, $Y = q^f$ とおくと $a = XY$. すると

$$\sigma(a) = \frac{(2X-1)(qY-1)}{\bar{q}}$$

であり, $A = 2X - 1$, $B = qY - 1$, $\rho' = \bar{q}$ とおけば

$$\frac{2AB}{\rho'} = 3XY + 2m.$$

書き直して

$$2AB = \rho'(3XY + 2m)$$

$R = 4q - 3\rho'$ とおくと $R = q + 3$.

$$2\rho'm = 2\bar{q}m = RXY - 2(2X + qY - 1) = (RX - 2q)Y - 4X + 2.$$

(1) $Y = q$.

$(RX - 2q)Y - 4X + 2 = (RX - 2q)q - 4X + 2 = (Rq - 4)X + 2(1 - q^2)$ と
 $Rq - 4 = q(q + 3) - 4 = (q + 4)\bar{q}$ により

$$2\bar{q}m = (q + 4)\bar{q}X - 2(q + 1)\bar{q}.$$

よって

$$2m = (q + 4)X + 2(q + 1).$$

これより

$$X = \frac{2m + 2q + 8 - 6}{q + 4} = 2 + \frac{2(m - 3)}{q + 4}.$$

$X = 2^e \geq 2$ に注意すると $m \geq 3$. かつ $m = 3$ なら $a = 2q$. これは通常解.
 $e > 1$ のとき

$$X - 2 = 2^e - 2 = \frac{2(m - 3)}{q + 4}.$$

これを書き換えれば

$$2(m - 3) = (q + 4)(2^e - 2). \quad (2.1)$$

与えられた $2m$ について上記の式を満たす q, e を探す. m が小さければいいが, 一般の解をすべて見つけるのは容易ではない.

(i) $e = 2$ のとき $a = 2^2q$.

$m - 3 = q + 4$ により, $q = 3, 5, 7, 11$ に応じて $m = 10, 12, 14, 18$. 亜完全度 W は $20, 24, 28, 36$

表 2.8: $W = 20$ の場合

a	$\sigma(a)$	素因数分解
12	28	$[2^2, 3]$

表 2.9: $W = 24$ の場合

a	$\sigma(a)$	素因数分解
18	39	$[2, 3^2]$
20	42	$[2^2, 5]$

表 2.10: $W = 28$ の場合

a	$\sigma(a)$	素因数分解
28	56	$[2^2, 7]$

表 2.11: $W = 36$ の場合

a	$\sigma(a)$	素因数分解
44	84	$[2^2, 11]$
50	93	$[2, 5^2]$

(ii) $e = 3$ のとき $a = 2^3q$.

$2(m - 3) = 6(q + 4)$ から $m = 3(q + 5)$.

$q = 3, 5, 7$ に応じて $m = 24, 30, 36$. 亜完全度 W は 48, 60, 72

表 2.12: $W = 48$ の場合

a	$\sigma(a)$	素因数分解
24	60	$[2^3, 3]$
68	126	$[2^2, 17]$
98	171	$[2, 7^2]$

表 2.13: $W = 60$ の場合

a	$\sigma(a)$	素因数分解
40	90	$[2^3, 5]$
92	168	$[2^2, 23]$

(2) $Y = q^2$.

$(RX - 2q)Y - 4X + 2 = (RX - 2q)q^2 - 4X + 2 = (Rq^2 - 4)X + 2(1 - q^3)$ と $Rq^2 - 4 = q^2(q + 3) - 4 = (q^2 + 4q + 4)\bar{q}$ により

$$2\bar{q}m = \bar{q}(q^2 + 4q + 4)X - 2\bar{q}(q^2 + q + 1).$$

よって

$$2m = (q+2)^2 X - 2(q^2 + q + 1).$$

書き換えると

$$(X-2)q^2 + (4X-2)q + 4X - 2 = 2m.$$

$X=2$ のとき $3(q+3) = m$,

例 $m = 36X = 2, q = 11, Y = 121$.

$a = 242, \sigma(a) = 399. 2\sigma(a) - 3a = 2 \times 399 - 3 \times 242 = 72 = W$.

(3) $Y = q^3$ などについても考えるべきである

2.5.4 例

ここでは $W = 72$ の場合の a を決定するとき $Y = q$ を仮定する.

$$2(m-3) = (q+4)(2^e - 2).$$

$m = 36 = W/2$ により $m-3 = 33$, $2(m-3) = 2 \times 3 \times 11 = (q+4)(2^e - 2)$ を解くと $2(m-3) = 33 \times 2 = 11 \times 6$ のそれぞれの分解に応じて (1),(2) の解が出るが, $Y = q^2$ の場合もあった.

(1) $q+4 = 11(q=7), 2^e - 2 = 6(e=3)$.

(2) $q+4 = 33(q=29), 2^e - 2 = 2(e=2)$

(3) $Y = 11^2, X = 2$.

表 2.14: $W = 72$ の場合

a	$\sigma(a)$	素因数分解
56	120	$[2^3, 7]$
116	210	$[2^2, 29]$
242	399	$[2, 11^2]$

このようにして複数解の場合はまことに興味深い.

表 2.15: $X = 2$ の場合

q	$4X - 2$	$W = 2m$	m
3	6	24	12
5	6	36	18
7	6	48	24
11	6	72	36
13	6	84	42
17	6	108	54
19	6	120	60

$X = 4$ のとき $q^2 + 7q + 7 = m$,

表 2.16: $X = 4$ の場合

q	$4X - 2$	$W = 2m$	m
3	14	62	31
5	14	94	47
7	14	126	63
11	14	190	95

$X = 8$ のとき $3(q^2 + 5q + 5) = m$,

表 2.17: $X = 8$ の場合

q	$4X - 2$	$W = 2m$	m
3	30	138	69
5	30	210	105

2.5.5 亜完全度 2,6 の場合

最初に亜完全度が偶数 $2m$ の場合を扱う.

$2\sigma(a) - 3a = 2m$ を満たすので a は偶数である. a の素因数分解で 2 の指数部分を e とし奇数 L により $a = 2^e L$ と表す.

$2\sigma(a) - 3a = 2(2^{e+1} - 1)\sigma(L) - 3 \cdot 2^e L$ により

$$(2^{e+1} - 1)\sigma(L) - 3 \cdot 2^{e-1} L = m. \quad (2.2)$$

移項して

$$(2^{e+1} - 1)\sigma(L) = 3 \cdot 2^{e-1} L + m.$$

$m \leq 3$ と仮定する.

$L = 1$ の場合.

$$2^{e+1} - 1 - 3 \cdot 2^{e-1} = 2^{e-1} - 1 = m \leq 3$$

により $2^{e-1} \leq 4$. したがって $e - 1 \leq 2$.

$e = 3$ なら $a = 8$. このとき $2\sigma(a) - 3a = 6$.

$e = 2$ なら $a = 4$. このとき $2\sigma(a) - 3a = 2$.

$L > 1$ の場合. $\sigma(L) \geq L + 1$ によって

$$3 \cdot 2^{e-1}L + m = (2^{e+1} - 1)\sigma(L) \geq (2^{e+1} - 1)(L + 1).$$

$3 \cdot 2^{e-1}L$ を右辺に移して

$$3 \geq m \geq (2^{e+1} - 1)(L + 1) - 3 \cdot 2^{e-1}L = (2^{e-1} - 1)L + 2^{e+1} - 1.$$

$L \geq 3$ により

$$3 \geq (2^{e-1} - 1)L + 2^{e+1} - 1 \geq (2^{e-1} - 1)3 + 2^{e+1} - 1 = 2^{e-1} - 4.$$

かくして $7 \geq 2^{e-1}$. よって $e - 1 \leq 2$. かくて $e = 1, 2, 3$.

式 (2.2) に $e = 1$ を代入すると,

$$3\sigma(L) = 3 \cdot L + m \leq 3(L + 1).$$

ゆえに $\sigma(L) = L + 1$. L は素数で $a = 2L$.

式 (2.2) に $e = 2$ を代入すると

$$7(L + 1) \leq 7\sigma(L) = 3 \cdot 2L + m = 6L + m \leq 6L + 3.$$

これは矛盾.

$e = 3$ を代入しても矛盾がでる.

以上によって亜完全度 $W = 6$ なら $a = 2p$, (p : 奇素数) または $a = 8$.

$W = 2$ なら $a = 4$.

2.6 3のべきとそのユークリッド関数の値

3のべき 3^e について $e+1$ が素数の場合 $\sigma(a)$ の素因数分解を行う。

表 2.18: $3^e = a$

$3^e = a$	$\sigma(a)$	の素因数分解
$3^2 = 9$	13	[13]
$3^4 = 81$	121	[11 ²]
$3^6 = 729$	1093	[1093]
$3^{10} = 59049$	88573	[23, 3851]
$3^{12} = 531441$	797161	[797161]
$3^{16} = 43046721$	64570081	[1871, 34511]
$3^{18} = 387420489$	581130733	[1597, 363889]
$3^{22} = 31381059609$	47071589413	[47, 1001523179]
$3^{28} = 22876792454961$	34315188682441	[59, 28537, 20381027]
$3^{30} = 205891132094649$	308836698141973	[683, 102673, 4404047]

$\sigma(3^e)$ が素数になるのは 13, 1093, 797161 であり数少ない。これらを **3** を底としたメルセンヌ素数という。

2.6.1 フェルマーとオイラーの結果

補題 5 k が奇数のとき $3^k - 1 = 2L$ と書ける。ここで L は奇数

Proof.

L は偶数 $2L'$ とする。

$$3^k - 1 = 2L = 4L' \equiv 0 \pmod{4}.$$

$3^k - 1 \equiv (-1)^k - 1 = -2 \pmod{4}$, により矛盾。

3を底としたメルセンヌ数についてもフェルマーとオイラーの結果は成立する。

補題 6 q が素数のとき $3^q - 1$ の奇数素因数 p については $p - 1 = 2Lq$ と書ける。

さらに $p \equiv \pm 1 \pmod{12}$.

Proof.

条件より,

$$3^q \equiv 1 \pmod{p}.$$

q は素数なので 3 の \pmod{p} での位数は q .

フェルマーの小定理によると $3^{p-1} \equiv 1 \pmod{p}$. よって, $p-1 = kq$ と書ける. $p-1$ は偶数なので k も偶数. よって $k = 2L$ と表せることによって $p-1 = 2Lq$ と書ける.

$$3^{\frac{p-1}{2}} \equiv 3^{Lq} \equiv 1 \pmod{p}.$$

ルジャンドルの記号を用いるとオイラーの基準によって

$$3^{\frac{p-1}{2}} \equiv \left(\frac{3}{p}\right)$$

$3^{\frac{p-1}{2}} \equiv 1$ なので $\left(\frac{3}{p}\right) = 1$. 平方剰余の補充法則から $p \equiv \pm 1 \pmod{12}$.

例 $q = 17$ のとき $A = 3^{17} - 1 = 129140162$. この素因子分解 [2, 1871, 34511].

$p_1 = 1871$ とおくと $p_1 - 1$ の素因子分解 [2, 5, 11, 17].

$p_2 = 34511$ とおくと $p_2 - 1$ の素因子分解 [2, 5, 7, 17, 29].

奇数素因数 p については $p = 1 + 2Lq$ と書ける. $L = 1$ の場合が最小なのでこれが $3^q - 1$ の最小の奇数素因数になる.

このとき $p = 1 + 2q$ が素数なので q は Sophie Germain 素数.

2.6.2 オイラーとラグランジュの結果

オイラーとラグランジュの結果は底が3でも成り立つ. しかも具体例で計算すると, 底が2のときより結果が断然良い. これは驚くべき結果であった.

補題 7 p を素数とし, $q = 2p + 1$ も素数とする. $N_p = 3^p - 1$ とおくと, q を法として3が平方剰余とする. このとき q は N_p の素因子である.

Proof.

仮定から $3 \equiv n^2 \pmod{q}$ を満たす整数 n がある. フェルマーの小定理を用いて

$$3^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \pmod{q}$$

ゆえに $N_p = 3^p - 1 = qk$ と書けるので, q は N_p の素因子.

(平方剰余の相互法則から $q \equiv \pm 1 \pmod{12}$)

$q = 2p + 1$ も素数なので $q \equiv -1 \pmod{12}$ のみ成り立つ.8

この逆も成立する.

補題 8 p を素数とし, $q = 2p + 1$ が N_p の因子とする. このとき $q = 2p + 1$ も素数.

Proof.

$q = 2p + 1$ は素数でないとする. その最小の素因子をとり q_0 とする. $2p + 1 \geq q_0^2$ を満たす. q_0 も N_p の素因子なので $q_0 \neq 3$.

$$3^p - 1 = N_p \equiv 0 \pmod{q_0}.$$

p は素数なので q_0 を法とした3の位数である. フェルマーの小定理を用いて

$$3^{q_0-1} \equiv 1 \pmod{q_0}.$$

ゆえに, $q_0 - 1$ は p の倍数. とくに $q_0 - 1 > p$ になり

$$2p + 1 \geq q_0^2 = q_0^2 + 2q_0 + 1 > 2(p + 1) + 1.$$

これで矛盾した.

p : Sophie Germain 素数について, q はすべて $q + 1 = 12L$ を満たし結果としてすべて q は N_p の因子となっていた. これは感動の結果である.

表 2.19: $q = 2p + 1$: 素数

p	$q = 2p + 1$	$q + 1$	$q + 1 \pmod{12}$	N_p 素因数分解
5	11	12	0	$2 * 11^2$
11	23	24	0	$2 * 23 * 3851$
23	47	48	0	$2 * 47 * 1001523179$
29	59	60	0	$2 * 59 * 28537 * 20381027$
41	83	84	0	$2 * 83 * 2526913 * 86950696619$
53	107	108	0	$2 * 107 * 24169 * 3747607031112307667$
83	167	168	0	A
89	179	180	0	B
113	227	228	0	C
131	263	264	0	D
173	347	348	0	E
178	359	360	0	F
190	383	384	0	G

$$A = 2 * 167 * 12119 * 1036745531 * 950996059627210897943351$$

$$B = 2 * 179 * 1611479891519807 * 5042939439565996049162197$$

$$C = 2 * 227 * 1583 * 2172539 * 526256453012063980796131127321354599535039$$

$$D = 2 * 263 * 605199588591144003100881306574406851660288427740394885828171$$

$$E = 2 * 347 * 762239 * 2125048865543 * 30985428700388045508959018054392810762033149280306907746766819$$

$$F = 2 * 359 * 56207 * 100957 * 19510643 * 291066066130451 * 6779963644378513811 * 1618686647444916557058589635943$$

$$G = 2 * 383 * 311713 * 9593931911 * 5890868591760365434332005074929710400548909181468214858888003483695003$$

2.6.3 証明

参加者の水谷氏の指摘により, 次の結果を証明する.

補題 9 p を素数とし, $q = 2p + 1$ も素数とする. このとき q を法として 3 は平方剰余である.

素数 q を mod12 で分類すると $q \equiv 1, 5, 7, 11 \pmod{12}$ である.

1. $q \equiv 1 \pmod{12}$ とすると $q = 1 + 12k$. $q = 2p + 1$ なので $1 + 12k = 2p + 1$. よって $p = 6k$. 矛盾.

2. $q \equiv 5 \pmod{12}$ とすると $q = 5 + 12k = 2p + 1$. よって $p = 4 + 6k$. 矛盾.

3. $q \equiv 7 \pmod{12}$ とすると $q = 7 + 12k = 2p + 1$. よって $p = 3 + 6k$. 矛盾.

$q \equiv 11 \pmod{12}$ のみ生き残り, このとき q を法として 3 は平方剰余.

2.7 3を底とする完全数

$a = 3^e$ に対して $\sigma(3^e) = \frac{3^{e+1} - 1}{2}$ が素数 q になったとする. このとき $\alpha = aq$ を **3** を底とする完全数とすることにする.

2.7.1 3を底とする完全数の数表

表 2.20: 3を底とする完全数

$e \pmod 4$	e	素因数分解	$q \pmod{10}$	a	$a \pmod{10}$
2	2	$3^2 * 13$	3	117	7
2	6	$3^6 * 1093$	3	796797	7
0	12	$3^{12} * 797161$	1	423644039001	1
2	70	A	3	B	7
2	102	C	3	D	7
0	540	$3^{540} * E$	1	--	--

$$A = 3^{70} * 3754733257489862401973357979128773$$

$$B = 9398681223266955568884336291512894246732289173595197254503404033277$$

$$C = 3^{102} * 6957596529882152968992225251835887181478451547013$$

$$D = 322720996484187844746619306273472246597518644973851120620$$

$$-- 67563800310073569424269938090581449997117$$

$$E = 66308439547181843673169185149975450335546563790474079717256778$$

$$-- 4209623516341640238400510288503463008441736852119221000000301102$$

$$-- 9079481693984080146458143761582514901416066165280887590649954106$$

$$-- 12765793960501606910585490086339893058591064091241255832207903808201.$$

これらから次の結論を導くことができる。

- $e \equiv 2 \pmod 4$ のとき q の末尾の数は 3, a の末尾の数は 7.
- $e \equiv 0 \pmod 4$ のとき q の末尾の数は 1, a の末尾の数は 1.

普通の完全数では末尾の数が 4 または 6 であったが 3 を底とする完全数では末尾の数が 7 または 1 になる。

Proof.

$3^2 = 9 \equiv -1 \pmod 5$ により $3^4 \equiv 1 \pmod 5$. これを以下使う.

$2q = 3^{e+1} - 1$ となる素数 q についてその末尾の数は 3 または 1 を示す.

1. $e = 4k + 2$ のとき

$$2q = 3^{e+1} - 1 = 3^{4k+3} - 1 \equiv -3 - 1 \equiv 1 \equiv 6 \pmod 5.$$

よって $q \equiv 3 \pmod 5$. $q = 3 + 5L$ となるが q は素数なので奇数. L は偶数になるので $q \equiv 3 \pmod{10}$.

$$a = 3^e q \equiv 3^2 q \equiv -q \equiv 2 \pmod 5 \text{ により } a = 2 + 5L.$$

a は素数なので L は奇数. よって $a \equiv 7 \pmod{10}$.

2. $e = 4k$ のとき

$$2q = 3^{e+1} - 1 = 3^{4k+1} - 1 \equiv 3 - 1 \equiv 2 \pmod{5}.$$

よって $q \equiv 1 \pmod{5}$. $q = 1 + 5L$ となるが q は奇数. L は偶数になるので $q \equiv 1 \pmod{10}$.
 $a = 3^e q \equiv q \equiv 1 \pmod{5}$ により 1 は奇数なので $a \equiv 1 \pmod{10}$.

3. $e = 4k + 3$ のとき $A = 3^{k+1}$ とおくと

$$2q = 3^{e+1} - 1 = 3^{4k+4} - 1 = A^4 - 1 = (A-1)(A^3 + A^2 + A + 1).$$

$A - 1 = 3^{k+1} - 1 = 2(3^k + 3^{k-1} + \dots + 1)$ なので $k > 0$ なら $\frac{A-1}{2} > 1$. よって q が素数に矛盾.
 $k = 0$ なら $e = 3$ なので $2q = 3^4 - 1 = 80$. $q = 40$; これは矛盾.

4. $e = 4k + 1$ のとき $A = 3^{2k+1}$ とおくと

$$2q = 3^{e+1} - 1 = 3^{4k+2} - 1 = A^2 - 1 = (A-1)(A+1).$$

$$A - 1 = 3^{2k+1} - 1 = 2(3^{2k} + 3^{2k-1} + \dots + 1)$$

$$q = (A^2 - 1)/2 = (A-1)/2(A+1) = (3^{2k} + 3^{2k-1} + \dots + 1)(A+1).$$

q が素数に矛盾.

2.7.2 $s(a) = 1$ のときの証明

3 を底とする完全数の基本問題を $s(a) = 1$ の場合だけ扱う.

$a = q^f$ が $2\sigma(a) = 3a + \text{Maxp}(a)$ を満たすと仮定する.

$Y = q^f$ とおくと

$$\frac{2(qY - 1)}{\bar{q}} = 3Y + q.$$

これより

$$Y(2q - 3\bar{q}) = 2 + q\bar{q}.$$

$2q - 3\bar{q} > 0$ により, $q = 2$.

$Y(2q - 3\bar{q}) = 2 + q\bar{q}$ に $q = 2$ を代入すると $Y = 4$. よって $a = 4$.

このような解を微小解という.

2.7.3 $s(a) = 2$ のときの証明

3 を底とする完全数の基本問題を $s(a) = 2$ の場合だけ扱う.

$2\sigma(a) = 3a + \text{Maxp}(a)$ を満たすと仮定する.

ここで a は奇数である. なぜなら $\text{Maxp}(a)$ は奇数で, $2\sigma(a)$ は偶数だから.

a を素因数分解し $a = p^e q^f$ ($2 < p < q$) とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおけば

$\text{Maxp}(a) = q$ なので

$$\frac{2AB}{\rho'} = 3XY + q.$$

書き直して

$$2AB = 3\rho'XY + q\rho'.$$

$2AB - 3\rho'XY$ の XY の係数を R とおけば

$$R = 2pq - 3\rho' = 6 - (p - 3)(q - 3).$$

$q\rho' = RXY - (pX + qY - 1)$ によって $R > 0$.

$0 < R = 6 - (p - 3)(q - 3)$ により, a は奇数になるので $p = 3, R = 6, \rho' = 2\bar{q}$.

$$2\bar{q}q = RXY - 2(3X + qY - 1)$$

を2で割って

$$\bar{q}q = 3XY - (3X + qY - 1) = (3X - q)Y - 3X + 1.$$

$3X > q$ かつ $Y \geq q$ によって

$$\bar{q}q \geq (3X - q)q - 3X + 1 = 3X\bar{q} - \tilde{q}\bar{q}.$$

$\bar{q}q \geq 3X\bar{q} - \tilde{q}\bar{q}$ から \bar{q} を消すと

$$q \geq 3X - \tilde{q}.$$

よって

$$2q + 1 \geq 3X.$$

ここで $Y = q$ を仮定すると $2q + 1 = 3X$ が成り立ち $q = \frac{3^{e+1}-1}{2} = \sigma(3^e)$ は素数. $a = 3^e q$ は3を底とした完全数になる.

$Y > q$ のとき $Y \geq q^2$ になる.

$$\begin{aligned} \bar{q}q &= (3X - q)Y - 3X + 1 \\ &= (3X - q)Y - 3X + q + 1 - q \\ &= (3X - q)(Y - 1) + 1 - q \\ &\geq (3X - q)(q^2 - 1) + 1 - q \\ &\geq (3X - q)\bar{q}\tilde{q} - \bar{q}. \end{aligned}$$

よって

$$q \geq (3X - q)\tilde{q} - 1.$$

1 を移項すると $\tilde{q} \geq (3X - q)\tilde{q}$ になるので \tilde{q} で割ると

$$1 \geq (3X - q) > 0.$$

ゆえに $3X - q = 1$. しかし $q = 3X - 1 = 3^{e+1} - 1 = 2\sigma(3^e)$ の右端は素数ではない. これは矛盾.

2.7.4 3を底とする完全数の方程式

普通の完全数の定義では $\sigma(a) - 2a = 0$ を満たす数のことでこれが偶数の場合はオイラーにより $a = 2^e \sigma(2^e)$; (ただし, $\sigma(2^e)$ は素数) が証明された.

ここではオイラーの与えた形から出発し $\sigma(3^e)$ が素数 q のとき $a = 3^e q$ を **3** を底とする完全数と呼ぶことにした. ここが少しずるい.

$$q = \sigma(3^e) = \frac{3^{e+1} - 1}{2} \text{ より } q + 1 = \frac{3^{e+1} + 1}{2} \text{ なので}$$

$$\begin{aligned} 2\sigma(a) &= 2\sigma(3^e)\sigma(q) \\ &= (3^{e+1} - 1)(q + 1) \\ &= q(3^{e+1} + 1) \\ &= 3a + q \end{aligned}$$

ここから q を消すことができないので a の最大素因子を $\text{Maxp}(a)$ と書く記号を導入すると次の方程式の形にまとめられる.

$$2\sigma(\alpha) = 3\alpha + \text{Maxp}(\alpha).$$

次の大きな問題はこの方程式を満たす α は $\sigma(3^e)$ が素数 q になるのをういて $\alpha = aq$ と書くことができるか, である.

とりあえず, この問題を **3** を底とする完全数の基本問題と呼ぶ. これは難しそうな問題だが逆に反例をつくりやすいかもしれない.

2.8 3を底とする完全数の平行移動

定義によれば $q = \sigma(3^e) = \frac{3^{e+1} - 1}{2}$ が素数 q のとき $a = 3^e q$ が **3** を底とする完全数である. これを m だけ平行移動することを考える.

$$q = \frac{3^{e+1} - 1}{2} + m \text{ が素数 } q \text{ のとき } a = 3^e q \text{ を } m \text{ だけ平行移動した } \mathbf{3} \text{ を底とする完全数という.}$$

これらが存在しなければ意味がないのでパソコンで確認する.

2.8.1 $p = 3, m = 1$

$p = 3, m = 1$ のとき $q = \frac{3^{e+1}+1}{2}$ は素数になる場合を調べる.

表 2.21: $m = 1$

$e \bmod 4$	e	素因数分解	$q \bmod 10$	a	$a \bmod 10$
1	1	$3 * 5$	5	15	7
3	3	$3^3 * 41$	1	1107	7
3	15	$3^{15} * 21523361$	1	308836705316427	7
3	31	$3^{31} * 926510094425921$	1	X	7
3	63	A	1	B	7

$$X = 572280636715419056279672990187$$

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

$$B = 1965030762956430528586812143569325391583084017460083159697707$$

q の末尾の数は 1, a の末尾の数は 7.

Proof.

$m = 1$ なので $2q = 3^{e+1} + 1$ になる.

1. $e = 4k + 3$.

$$2q = 3^{e+1} + 1 = 3^{4k+4} + 1 \equiv 2 \pmod{5}.$$

$q = 1 + 5L$ となり L は偶数なので $q \equiv 1 \pmod{10}$.

$$a = 3^e q \equiv 2q \equiv 2 \pmod{5}.$$

$a = 2 + 5L'$ となるが a は奇数なので L' も奇数. よって $a \equiv 7 \pmod{10}$.

2. $e = 4k + 1, B = 3^{2k+1} = -(-3)^{2k+1}$.

$$2q = 3^{e+1} + 1 = 3^{4k+2} + 1 = 1 - (-3)^{2k+1} = 4D, D = (-3)^{2k} + \dots + 1.$$

q は素数に反する.

3. $e = 4k + 2$.

$$2q = 3^{e+1} + 1 = 3^{4k+3} + 1 \equiv -2 \pmod{5}.$$

今のところここから矛盾が出ない. 計算例が 4 つしかないので, 何とも言えない.

2.8.2 3を底とするフェルマー素数

$m = 1$ の場合 $e + 1 = 2, 4, 16, 64$ などではこれらは2の指数が2のべきである.

$q = \frac{3^{e+1} + 1}{2}$ は次のとおり.

- i) 5,
- ii) 41,
- iii) 21523361,
- iv) 926510094425921
- v) 1716841910146256242328924544641

これらはフェルマーの素数に類似している. そこで

3を底とするフェルマー素数という.

5を除外すると末尾の数は1.

本来のフェルマー素数と同じく5個あるのが不思議でならない.

この場合の a は次のとおり.

- i) $15 = 3 * 5,$
- ii) $1107 = 3^3 * 41,$
- iii) $308836705316427 = 3^{15} * 21523361,$
- iv) $3^{31} * 926510094425921$
- v) $3^{63} * 1716841910146256242328924544641$

これらを3を底とするフェルマーの完全数という.

15を除外すると末尾の数は7である. 人間は正直な者で名前がつくと研究したくなる.

このようなフェルマーの完全数を研究した人はいないと思う. 研究の処女地と言って良い.

2.9 底が3のフェルマー数

$3^{e+1} + 1 = 2N_{e+1}$ とおくと N_{e+1} が素数になるとき, $e + 1 = 2^m$ と書ける. 一般に $G_m = (3^{2^m} + 1)/2$ とおき, これを底が3のフェルマー数, これが素数のとき底が3のフェルマー素数という.

オイラーの結果と類似した結果が成り立つ.

補題 10 G_m の素因数 Q は $1 + 2^{m+1}K$ と書ける.

$3^{2^m} + 1 \equiv 0 \pmod{Q}$ なので $3^{2^m} \equiv -1 \pmod{Q}$.

\pmod{Q} での3の位数 u は 2^{m+1} の約数である.

$u = 2^s$ とおくと $s \leq m + 1$ だが $3^{2^m} \equiv -1$ により $s = m + 1$. 結局 $u = 2^{m+1}$.

$3^{Q-1} \equiv 1 \pmod{Q}$ によれば $Q - 1$ は 2^{m+1} の倍数なので $Q = 1 + 2^{m+1}k$.

$G_m = (3^{2^m} + 1)/2$ について $m = 1, 2, 4, 5, 6$ は素数になる.

$m = 7$ のとき $2^m = 128$. よって $Q = 1 + 256K$.

$$3^{128} + 1 = 2 * 257 * 275201 * 138424618868737 * 3913786281514524929 * 153849834853910661121$$

?- A is 257-1, factorize(A,B), exps(B,C).

A = 256,

C = [2^8].

?- A is 275201-1, factorize(A,B), exps(B,C).

A = 275200,

C = [2^8, 5^2, 43].

?- A is 138424618868737-1, factorize(A,B), exps(B,C).

A = 138424618868736,

C = [2^13, 3, 2131, 2643131].

?- A is 3913786281514524929-1, factorize(A,B), exps(B,C).

A = 3913786281514524928,

C = [2^8, 31, 787, 3919, 159898891].

?- A is 153849834853910661121-1, factorize(A,B), exps(B,C).

A = 153849834853910661120,

C = [2^11, 3, 5, 433, 19801, 584118287].

これらは数値例とはいえ、実に見事な美しい結果である。

$m = 2$ なら解無し。これは当然である。 $q = \frac{3^{e+1}+3}{3}$ の右辺は3の倍数だから、素数にならない。

2.9.1 $p = 3, m = 3$ 表 2.22: $p = 3, m = 3$

$e \pmod 4$	e	素因数分解	a
1	1	$3 * 7$	21
3	3	$3^3 * 43$	1161
1	5	$3^5 * 367$	89181
1	9	$3^9 * 29527$	581179941
1	59	A	B
1	65	C	D
1	99	E	F
1	143	$3^{143} * G$	--
1	155	$3^{155} * H$	--

$$A = 3^{59} * 21195579137608101757147216603,$$

$$B = 299501716652405201735529971620260138517926107518220545401$$

$$C = 3^{65} * 15451577191316306180960320901767$$

$$D = 159167491799470872815531783629094754615308050339358788840978581$$

$$E = 3^{99} * 257688760366005665518230564882810636351053761003$$

$$F = 44268998145979128223130220339296604471538908$$

$$-- 775995230596372503065712466091688381559649206109001$$

$$G = 253764393028207800359877079870848178454371125095831943631813721057443$$

$$H = 134860802795303781631053435203643426805969445092054023955634715732487236763$$

[研究課題]

$q \equiv 3, 7; a \equiv 1 \pmod{10}$ を示す.

2.9.2 $p = 3, m = 4$

$$A = 3^{74} * 304133393856678854559841996309430657$$

$$B = 61664747505854495487450130408616108074056769063871156275495392272296233$$

表 2.23: $p = 3, m = 4$

$e \bmod 4$	e	素因数分解	a
2	2	$3^2 * 17$	153
2	6	$3^6 * 1097$	799713
2	74	A	B
2	190	C	--
2	394	D	--

$C = 3^{190} * 6747294337140546901864078698261942458701251147$
 -- 015050957033352683510961004453136793029129177
 $D = 3^{394} * 145166236803607666075029365382581885219152159697093$
 -- 24231043461565691787150531467933452530561614636658056574554
 -- 49081397363517073931519024006052367992891671955307824800900
 -- 41796692270130317057
 $p = 3, m = 6$

表 2.24: $p = 3, m = 6$

$e \bmod 4$	e	素因数分解	a
2	2	$3^2 * 19$	171
0	4	$3^4 * 127$	10287
0	32	$3^{32} * 2779530283277767$	5150525730438778918597812319047
0	40	A	B
0	136	C	D

$A = 3^{40} * 18236498188585393207$
 $B = 221713244121518885040991975334388054807$
 $C = 3^{136} * 116033101521814266282522670265591302448272119385382690275177741687$
 $D = 897578709918110413192788237560[70digits]066886376017053855629213351127$

2.9.3 $p = 3, m = 7$

$A = 3^{69} * 1251577752496620800657785993042931$
 $B = 1044297913696328396542704032390327145538043226491913729549236194473$
 $C = 3^{93} * 353482524507552353248601597918807457271678691$
 $D = 83299930088154900023013317262493116774089521865276753817089242886050887332772275251707993$

表 2.25: $p = 3, m = 7$

$e \pmod 4$	e	素因数分解	a
1	1	$3^1 * 11$	33
3	3	$3^3 * 47$	1269
1	9	$3^9 * 29531$	581258673
1	13	$3^{13} * 2391491$	3812809105593
1	69	A	B
1	93	C	D

2.9.4 $p = 3, m = 9$

表 2.26: $p = 3, m = 9$

$e \pmod 4$	e	素因数分解	a
1	1	$3^1 * 13$	39
1	5	$3^5 * 373$	90639
3	11	$3^{11} * 265729$	47073095163
1	65	A	B

$$A = 3^{65} * 15451577191316306180960320901773$$

$$B = 159167491799470872815531783629156560924073315564082630124585639$$

2.9.5 $p = 3, m = -2$

表 2.27: $p = 3, m = -2$

$e \pmod 4$	e	素因数分解	a
2	2	$3^2 * 11$	99
2	6	$3^6 * 1091$	795339
0	8	$3^8 * 9839$	64553679
2	30	$3^{30} * 308836698141971$	B
0	44	C	D
0	48	E	F
2	126	G	H

$$A = 3^{30} * 308836698141971$$

$$B = 63586737412823790543611413179$$

$$C = 3^{44} * 1477156353275416849319$$

$$D = 1454660594681285404312770985990662195258039$$

$$E = 3^{48} * 119649664615308764795039$$

$$F = 9544028161703913537712043727700109165060666079$$

$$G = 2^{126} * 1965030762956430528586812143568753110946368598712640184849491$$

$$H = 257423059957675431046184790351[61\text{digits}]969067117567366322276523388539$$

解が急に増えた.

2.9.6 $p = 3, m = -3$

$p = 3, m = 3$ のときは $q = \frac{3^{e+1}-7}{2}$.

表 2.28: $m = -3$

$e \pmod 4$	e	素因数分解	a
3	3	$3^3 * 37$	999
3	11	$3^{11} * 265717$	47070969399
1	17	$3^{17} * 193710241$	25015772097509283
1	25	$3^{25} * 1270932914161$	1076846981534813373022323
1	105	A	B
3	163	C	D

$A = 3^{105} * 187855106306818130162790081799568953899918191769361$

$B = 235263606436972938820285474273[41\text{digits}]232655623244560699998326360723$

$C = 3^{163} * 884821727139988111281341588371104523273965529248966451172919369920848760385637$

$D = 521939659212661049190964243666[96\text{digits}]293165758751776686426411496999$

さて

- $e \equiv 3 \pmod 4$ なら q の末尾の数は 7. a の末尾の数は 9
- $e \equiv 1 \pmod 4$ なら q の末尾の数は 1. a の末尾の数は 3.

正しいか? 証明を試みる.

$2q = 3^{e+1} - 7, a = 3^e q$ が成り立つ.

1. $e = 4k + 3$.

$2q = 3^{e+1} - 7 \equiv 1 - 7 = -6 \equiv 4 \pmod 5$ によって $q \equiv 2 \pmod 5$. q は奇数なので $q = 2 + 5(2L + 1) = 7 + 10L$. したがって $q \equiv 7 \pmod{10}$.

$a = 3^e q \equiv -3 \times 7 = -21 \equiv 4 \pmod 5$.

だから $a = 4 + 5L = 4 + 5(2L' + 1) \equiv 9 \pmod{10}$.

2. $e = 4k + 1$.

$2q = 3^{e+1} - 7 \equiv -1 - 7 = -8 \equiv 2 \pmod 5$ によって $q \equiv 1 \pmod 5$. q は偶数なので $q = 1 + 5(2L)$. したがって $q \equiv 1 \pmod{10}$.

$a = 3^e q \equiv 3 \pmod 5$.

だから $a = 3 + 5L = 3 + 5(2L') \equiv 3 \pmod{10}$.

$e = 4k + 1, 4k + 3$ の場合は起きるかどうかわからない.

2.9.7 $p = 3, m = -5$

表 2.29: $p = 3, m = -5$

$e \bmod 4$	e	素因数分解	a
1	5	$3^5 * 359$	87237
1	17	$3^{17} * 193710239$	25015771839228957
1	25	$3^{25} * 1270932914159$	1076846981533118795803437
1	41	$3^{41} * 54709494565756179599$	A
1	49	B	C
1	89	D	E

$$A = 1995419197093669964566521857711735192397$$

$$B = 3^{49} * 358948993845926294385119$$

$$C = 85896253455335221839408872147959443720605174877$$

$$D = 3^{89} * 4363981784043856212945698739738363670020719$$

$$E = 12696224674311065389881621286769260291737450899132657959860813489930810516505382927$$

2.9.8 $p = 3, m = -6$

表 2.30: $p = 3, m = -6$

$e \bmod 4$	e	素因数分解	a
2	2	$3^2 * 7$	63
2	6	$3^6 * 1087$	792423
2	50	A	B

$$A = 3^{50} * 554982727552690459387051173677544966279709650584584460722776607952622367$$

$$B = 205337218587882563986989041073[84digits]838531020939300449909200485383$$

2.9.9 $p = 3, m = -8$

表 2.31: $p = 3, m = -8$

$e \bmod 4$	e	素因数分解	a
2	2	$3^2 * 5$	45
0	4	$3^4 * 113$	9153
0	8	$3^8 * 9833$	64514313
0	28	$3^{28} * 34315188682433$	785021449540846353084400113

2.9.10 $p = 3, m = -9$

表 2.32: $p = 3, m = -9$

$e \bmod 4$	e	素因数分解	a
3	3	$3^3 * 31$	837
3	7	$3^7 * 3271$	7153677
3	11	$3^{11} * 265711$	47069906517
3	15	$3^{15} * 21523351$	308836561827357
3	99	A	B

$$A = 3^{99} * 257688760366005665518230564882810636351053760991$$

$$B = 442689981459791282231302203392966044715389087739337205$$

$$-- 13444457741566621572625896468840776020997$$

2.10 m だけ平行移動した完全数の方程式

$q = \frac{3^{e+1}-1}{2} + m$ が素数 q のとき $a = 3^e q$ とおく. これが満たす完全数の方程式を決定しよう.
 $q + 1 = \frac{3^{e+1}+1}{2} + m$ に注意して,

$$\begin{aligned}\sigma(a) &= \sigma(3^e q) \\ &= (3^{e+1} - 1)/2 * (q + 1)\end{aligned}$$

によって

$$\begin{aligned}2\sigma(a) &= (3^{e+1} - 1)(q + 1) \\ &= 2(q - m)(q + 1) \\ &= 2q(q + 1) - 2m(q + 1) \\ &= q(3^{e+1} + 1 + 2m) - 2mq - 2m \\ &= 3a + q - 2m\end{aligned}$$

かくして $q = \text{Maxp}(a)$ を使うと方程式

$$2\sigma(a) = 3a + \text{Maxp}(a) - 2m$$

がえられた.

この方程式を満たす解を探す. 一種の逆問題を考えることになる.

2.11 方程式を満たす解

$a \leq 200000$ の範囲で解を探索する.

2.11.1 $m = 0$ のとき

$m = 0$ のとき $2\sigma(a) = 3a + \text{Maxp}(a)$.

表 2.33: $[p = 3, m = 0]$

a	素因数分解	$\sigma(a)$
4	$[2^2]$	7
117	$[3^2, 13]$	182
796797	$[3^6, 1093]$	--

117 は最も小さい 3 を底とする完全数であるがさらに小さい解 4 が出てきた.

2.11.2 $m = 1$ のとき

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

表 2.34: $[p = 3, m = 1]$

a	素因数分解	$\sigma(a)$
2	[2]	3
15	[3, 5]	24
741	[3, 13, 19]	1120
1107	$[3^3, 41]$	1680
14883	$[3, 11^2, 41]$	22344
38781	$[3^2, 31, 139]$	58240

3 を底とするフェルマー完全数は 15, 1107 などであるが $2\sigma(a) = 3a + \text{Maxp}(a) - 2$ の解は拡張された 3 を底とするフェルマー完全数と呼ぶことができる。

フェルマー完全数は 5 しか見つからないが拡張された 3 を底とするフェルマー完全数は多いかも知れない。

2.11.3 $m = 3$ のとき表 2.35: $[p = 3, m = 3]$

a	素因数分解	$\sigma(a)$
21	[3, 7]	32
1161	$[3^3, 43]$	1760
89181	$[3^5, 367]$	133952

2.11.4 $m = 4$ のとき表 2.36: $[p = 3, m = 4]$

a	素因数分解	$\sigma(a)$
5	[5]	6
153	$[3^2, 17]$	234
27639	$[3^2, 37, 83]$	41496
51417	$[3^2, 29, 197]$	77220

2.11.5 $m = 6$ のとき表 2.37: $[p = 3, m = 6]$

a	素因数分解	$\sigma(a)$
7	[7]	8
171	$[3^2, 19]$	260
10287	$[3^4, 127]$	15488

2.11.6 $m = 7$ のとき表 2.38: $[p = 3, m = 7]$

a	素因数分解	$\sigma(a)$
33	[3, 11]	48
385	[5, 7, 11]	576
1269	$[3^3, 47]$	1920
2975	$[5^2, 7, 17]$	4464
53751	[3, 19, 23, 41]	80640

2.11.7 $m = 9$ のとき表 2.39: $[p = 3, m = 9]$

a	素因数分解	$\sigma(a)$
25	$[5^2]$	31
39	$[3, 13]$	56
90639	$[3^5, 373]$	136136

2.11.8 $m = -1$ のとき

$$q = \frac{3^{e+1}-1}{2} - 1 = \frac{3^{e+1}-3}{2} = 3 \times \frac{3^e-1}{2}$$

表 2.40: $[p = 3, m = -1]$

a	素因数分解	$\sigma(a)$
27755	$[5, 7, 13, 61]$	41664

$s(a) = 4$ の解が1つだけでできた. 説明が見つからないであろう.
1つだけの解ということが証明できるだろうか.

2.11.9 $m = -2$ のとき表 2.41: $[p = 3, m = -2]$

a	素因数分解	$\sigma(a)$
8	$[2^3]$	15
99	$[3^2, 11]$	156
759	$[3, 11, 23]$	1152

2.11.10 $m = -3$ のとき表 2.42: $[p = 3, m = -3]$

a	素因数分解	$\sigma(a)$
999	$[3^3, 37]$	1520

2.11.11 $m = -5$ のとき表 2.43: $[p = 3, m = -5]$

a	素因数分解	$\sigma(a)$
663	$[3, 13, 17]$	1008
38223	$[3^2, 31, 137]$	57408
87237	$[3^5, 359]$	131040

2.11.12 $m = -6$ のとき表 2.44: $[p = 3, m = -6]$

a	素因数分解	$\sigma(a)$
16	$[2^4]$	31
63	$[3^2, 7]$	104

2.11.13 $m = -8$ のとき

[p=3,m=-8]

表 2.45: $[p = 3, m = -8]$

a	素因数分解	$\sigma(a)$
45	$[3^2, 5]$	78
9153	$[3^4, 113]$	13794
49851	$[3^2, 29, 191]$	74880

2.11.14 $m = -9$ のとき表 2.46: $[p = 3, m = -9]$

a	素因数分解	$\sigma(a)$
75	$[3, 5^2]$	124
837	$[3^3, 31]$	1280

2.12 $a = 3^e qr$ の解

$m = 1$ のとき $2\sigma(a) = 3a + \text{Maxp}(a) - 2$ になるが、この解 a を素因数分解すると [3, 13, 19] と [3, 11², 41] があったのでこの形の解, $3^e qr$ と書ける解を探す.

一般にして, $2\sigma(a) = 3a + \text{Maxp}(a) - 2m$ の解を $a = 3^e qr (3 < q, r : \text{素数})$ とおくと $\text{Maxp}(a) = r$ になるので

$$(3^{e+1} - 1)(q + 1)(r + 1) = 3^{e+1}qr + r - 2m.$$

$\Delta = q + r$ とすると

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

$q' = q + 1, \Delta' = q' + r = \Delta + 1, \Gamma = 3^{e+1} - 1$ とすると

$$q'r = (3^{e+1} - 1)\Delta' + 2m.$$

$q_0 = q' - \Gamma, r_0 = q - \Gamma$ は次式を満たす

$$q_0 r_0 = \Gamma^2 + 2m.$$

そこで, 与えられた e に対して, $\Gamma = 3^{e+1} - 1, D = \Gamma^2 + 2m$ を求め2因数分解: $q_0 r_0 = D, q_0 < r_0$ を行い, $q = q_0 + \Gamma - 1, r = r_0 + \Gamma$ がともに素数になるものを探す.

次の結果をえ $e = 1, 2, 11$ について解が発見された.

表 2.47: $[p = 3, m = 1]$

a	素因数分解	$\sigma(a)$
741	$a = 3 * 13 * 19$	1120
38781	$a = 3^2 * 31 * 139$	58240
4954286665155815901	$a = 3^{11} * 536917 * 52088299$	7431429997759768000

2.12.1 $m = -2$ のとき

$$2\sigma(a) = 3a + \text{Maxp}(a) + 4$$

この結果を受けて $m = -2$ のとき $a = 3^e qr$ の解を探す.

表 2.48: $[p = 3, m = -2]$

a	素因数分解	$\sigma(a)$
8	$[2^3]$	15
99	$[3^2, 11]$	156
759	$[3, 11, 23]$	1152

表 2.49: $[p = 3, m = -2; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
759	$3^1 * 11 * 23$	1152
19184931	$3^4 * 433 * 547$	28777672
8061750261	$3^5 * 739 * 44893$	12092647840
721889577	$3^5 * 947 * 3137$	1082835936
629690031	$3^5 * 1019 * 2543$	944536320
998897581791	$3^7 * 7331 * 62303$	1498346403840
156372861294706304709	$3^{12} * 1608337 * 182948677$	234559291942150931404
24736154970540283911	$3^{12} * 1692433 * 27502087$	37104232455824176912
43612339225270702734885159	$3^{13} * 4782971 * 5719200505223$	65418508837908913702580352

2.12.2 $m = 4$ のとき

表 2.50: $[p = 3, m = 4; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
51417	$3^2 * 29 * 197$	77220
27639	$3^2 * 37 * 83$	41496
965007	$3^3 * 103 * 347$	1447680
4162847823	$3^5 * 751 * 22811$	6244283136
277979312695831119	$3^{11} * 695047 * 2257691$	416968969044875520

2.12.3 $m = 8$ のとき

表 2.51: $[p = 3, m = 8; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
51939	$3^2 * 29 * 199$	78000
10214836272423	$3^8 * 36821 * 42283$	15322254429768
435027039990994161	$3^{11} * 612671 * 4008253$	652540559988495360
21539587380792522005259	$3^{12} * 1594421 * 25420220719$	32309381071201493118240

2.12.4 $m = -8$ のとき表 2.52: $[p = 3, m = -8; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
49851	$3^2 * 29 * 191$	=74880
50833737	$3^4 * 269 * 2333$	76251780
6111764199	$3^5 * 743 * 33851$	9167663232
7456106388662649	$3^{10} * 328981 * 383821$	11184159583185892
5944032701003008683	$3^{12} * 2449813 * 4565551$	8916049051506795808

2.12.5 $m = -5$ のとき表 2.53: $[p = 3, m = -5; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
663	$3^1 * 13 * 17$	1008
38223	$3^2 * 31 * 137$	57408
1727757	$3^3 * 89 * 719$	2592000
862299	$3^3 * 109 * 293$	1293600
15862743783	$3^5 * 733 * 89057$	23794160208
760262656887	$3^7 * 7669 * 45329$	1140394008000
113629660934874742039491	$3^{14} * 14475463 * 1641200653$	170444491402312933659568

2.12.6 $m = 2$ のとき $m = 2$ のとき

$$2\sigma(a) = 3a + \text{Maxp}(a) - 4.$$

 $a = 3^f$ はこの式を満たす.実際に $2\sigma(a) = 3 * 3^f - 1, 3a + \text{Maxp}(a) - 4 = 3 * 3^f + 3 - 4$.表 2.54: $[p = 3, m = 2]$

a	素因数分解	$\sigma(a)$
3	[3]	4
9	[3 ²]	13
27	[3 ³]	40
81	[3 ⁴]	121
243	[3 ⁵]	364
729	[3 ⁶]	1093
2187	[3 ⁷]	3280
6561	[3 ⁸]	9841
19683	[3 ⁹]	29524
59049	[3 ¹⁰]	88573
99807	[3, 17, 19, 103]	149760
177147	[3 ¹¹]	265720

 $2\sigma(a) = 3a + \text{Maxp}(a) - 4$ のエイリアン解として 99807([3, 17, 19, 103]) が出た.実は $m = 2$ を選ぶのは違反行為である. $s(a) = 2$ のときは $q = \frac{3^{e+1}-1}{2} + m$ が素数になるはずなので $m = 2$ は出てこない.しかし, 方程式が $2\sigma(a) = 3a + \text{Maxp}(a) - 2m$ が得られたとき $m = 2$ を代入するとパソコンが出す結果, 非常に面白い例が出てきた. $s(a) = 2$ の解はないが $s(a) = 1, 4$ の例がでてきた. $m = -1$ も違反であり, $s(a) = 2$ の解はないが $s(a) = 4$ の例を出してきた. この例は何を意味するか私は困惑させられた. このような異常な例をとりこむ理論ができそうにないからである.2.12.7 $m = -1$ のとき表 2.55: $[p = 3, m = -1]$

a	素因数分解	$\sigma(a)$
27755	[5, 7, 13, 61]	41664
19379169	[3 ⁴ , 419, 571]	29069040

$s(a) = 2$ の解はない.

2.13 $\text{Maxp}(a)$ について

底が3の m だけ平行移動した完全数の方程式を移項してえられた

$$2\sigma(a) - 3a - \text{Maxp}(a) = -2m$$

に関して $2\sigma(a) - 3a - \text{Maxp}(a)$ を底が3の完全度という.

底が3の完全度の絶対値が9以下の場合 $a \leq 5000$ について数表を作った.

この結果から面白い性質が見えるだろうか.

表 2.56: 底が3の完全度の絶対値が9以下

a	[5]	$\sigma(a)$	完全度	特性
5	[5]	6	-8	$m = 4$ 平行移動
153	$[3^2, 17]$	234	-8	
26	[2, 13]	42	-7	
21	[3, 7]	32	-6	$m = 3$ 平行移動
1161	$[3^3, 43]$	1760	-6	
22	[2, 11]	36	-5	
3	[3]	4	-4	$m = 2$; 微小解
9	$[3^2]$	13	-4	
27	$[3^3]$	40	-4	
81	$[3^4]$	121	-4	
243	$[3^5]$	364	-4	
729	$[3^6]$	1093	-4	
2187	$[3^7]$	3280	-4	
2	[2]	3	-2	$m = 1$ 平行移動
15	[3, 5]	24	-2	
741	[3, 13, 19]	1120	-2	
1107	$[3^3, 41]$	1680	-2	
14	[2, 7]	24	-1	
4	$[2^2]$	7	0	完全数
117	$[3^2, 13]$	182	0	
10	[2, 5]	18	1	
6	[2, 3]	12	3	
8	$[2^3]$	15	4	$m = -2$ 平行移動
99	$[3^2, 11]$	156	4	
759	[3, 11, 23]	1152	4	
999	$[3^3, 37]$	1520	6	$m = -3$ 平行移動
147	$[3, 7^2]$	228	8	$m = -4$ 平行移動
3185	$[5, 7^2, 13]$	4788	8	

第3章 究極の完全数

3.1 $a = 5^e$ の場合

一般に P を素数とし $E > 0$ について $a = P^E$ とおくと
 $\sigma(a) = \sigma(P^E) = \frac{aP-1}{P}$ によって

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

これが $a = P^E$ に関する方程式である.

$P = 5$ については $4\sigma(a) - 5a = -1$ となる. とりあえず, $a \leq 20000$ についてパソコンで計算して表を作る.

表 3.1: $4\sigma(a) - 5a = -1$

a	$\sigma(a)$	素因数分解
5	6	[5]
25	31	[5 ²]
77	96	[7, 11]
125	156	[5 ³]
625	781	[5 ⁴]
3125	3906	[5 ⁵]
15625	19531	[5 ⁶]

驚いたことに 5 のべきでない数 $77 = 7 * 11$ が登場した. 懐かしの昭和歌謡曲を聞いていたら, そこに桃クロが出てきたような衝撃である.

$s(a) = 1$ を期待していたところに $s(a) = 2$ の例が出てきたのだから.

3.1.1 $s(a) = 2$ のときの証明

方程式 $4\sigma(a) - 5a = -1$ の解を $s(a) = 2$ のときに求めよう.

a を素因数分解し $a = p^e q^f$ ($2 < p < q$) とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \overline{pq}$ とおけば

$$\frac{4AB}{\rho'} = 5XY - 1.$$

書き直して

$$4AB = 5\rho'XY - \rho'.$$

$4AB - 5\rho'XY$ の XY の係数を R とおけば

$$R = 4pq - 5\rho' = 20 - (p-5)(q-5).$$

$-\rho' + 4(pX + qY - 1) = RXY$ によって $R > 0, 0 < R = 20 - (p-5)(q-5)$ により 次の場合がある.

$$(1) p = 5, R = 20. \rho' = 4\bar{q},$$

$$(2) p = 3, R = 30 + 2q. \rho' = 2\bar{q},$$

$$(3) p = 7, R = 30 - 2q; q = 11, 13. \rho' = 6\bar{q}.$$

次の基本等式

$$RXY - 4(pX + qY - 1) = -\rho'$$

を各場合ごとに調べる.

1. $p = 5, R = 20. \rho' = 4\bar{q}$ の場合.

基本等式を 4 で割って

$$5XY - (5X + qY - 1) = -\bar{q}.$$

$(5X - q)Y - 5X = -\bar{q} - 1 = q$ により

$$(5X - q)(Y - 1) = 0.$$

よって $5X = 5^{f+1} = q$ となり矛盾.

2. $p = 3, R = 30 + 2q. \rho' = 2\bar{q}.$

$R_1 = R/2 = 5 + q$ とおくと

$$R_1XY - 2(3X + qY - 1) = -\bar{q}.$$

変形して

$$(R_1X - 2q)Y = 6X - q - 1.$$

$Y = q$ のとき,

$(R_1X - 2q)q = 6X - q - 1$ によって $X \geq 3$ により

$$(R_1q - 6)X = 2q^2 - q - 1 \geq 3(5 + q)q - 6q = 3q^2 + 15q - 6q = 3q^2 + 9q.$$

これから矛盾が出る.

$Y \geq q^2$ のとき,

$$(R_1X - 2q)Y = 6X - q - 1 \geq (R_1X - 2q)q^2 = ((5+q)X - 2q)q^2 = (5+q)Xq^2 - 2q^3.$$

$$2q^3 - q - 1 \geq 3((5+q)q^2 - 6) = 3q^3 + 15q^2 - 18.$$

これから矛盾が出る.

3. $p = 7, R = 30 - 2q; q = 11, 13; \rho' = 6\bar{q}$.

$$R_1XY - 2(7X + qY - 1) = -3\bar{q}.$$

$q = 11$ のとき, $R_1 = 4$.

$$4XY - 2(7X + 11Y - 1) = -30.$$

$4XY - 2(7X + 11Y) = -32$ を変形して

$$2(2X - 11)Y = 14X - 32 = 7(2X - 11) - 32 = 7(2X - 11) + 45.$$

$(2X - 11)(2Y - 7) = 45$ の解として $2X - 11 = 3, 2Y - 7 = 15$ があり, $X = 7, Y = 11$. ここで $a = 77$. かくして 5 のべきでない解が発見された.

$q = 13$ のとき, $R_1 = 2$.

$$XY - (7X + 13Y) = -25.$$

$(X - 7)(Y - 13) = 91 - 25 = 65$. しかし, X, Y は奇数なので $X - 7, Y - 13$ はともに偶数で矛盾. したがって $s(a) = 2$ のとき $a = 77$.

しかしながら $s(a) = 3$ の解がまだある可能性が残る.

g

3.1.2 $\sigma(5^e)$ が素数になる場合

$\sigma(5^e)$ が素数になるのは 31, 19531, 12207031, 305175781 であり少ない.

$p = 29, q = 2p + 1 = 59$ はともに素数で, $59 + 1 \equiv 0 \pmod{5}$. すなわち $q \equiv \pm 1 \pmod{5}$ なので $\left(\frac{5}{q}\right) = 1$ を満たす.

このとき q は $\sigma(a)$ の約数になることが示される.

表 3.2: $5^e a$ の $\sigma(a)$

$5^e = a$	$\sigma(a)$	素因数分解
$5^2 = 25$	31	[31]
$5^4 = 625$	781	[11, 71]
$5^6 = 15625$	19531	[19531]
$5^{10} = 9765625$	12207031	[12207031]
$5^{12} = 244140625$	305175781	[305175781]
$5^{16} = 152587890625$	190734863281	[409, 466344409]
$5^{18} = 3814697265625$	4768371582031	[191, 6271, 3981071]
$5^{22} = 2384185791015625$	2980232238769531	[8971, 332207361361]
$5^{28} = 37252902984619140625$	46566128730773925781	[59, 35671, 22125996444329]

3.1.3 フェルマーとオイラーの結果

補題 11 $q, k > 1$ が奇数のとき $q^k - 1 = \bar{q}L$ と書ける. ここで L は奇数

Proof.

$$\frac{q^k - 1}{q} = 1 + q + \cdots + q^{k-1} \equiv k \equiv 1 \pmod{2}.$$

奇素数 P を底としたメルセンヌ数についてもフェルマーとオイラーの結果は成立する.

補題 12 q が素数のとき $\frac{P^q - 1}{P}$ の素因数 p は $p - 1 = 2Lq$ と書ける.

$$\left(\frac{P}{p}\right) = 1.$$

さらに $P = 5$ なら $p \equiv \pm 1 \pmod{P}$.

Proof.

条件より,

$$P^q \equiv 1 \pmod{p}.$$

q は素数なので P の $\text{mod } p$ での位数は q .

フェルマーの小定理によると $P^{p-1} \equiv 1 \pmod{p}$. よって, $p - 1 = kq$ と書ける. $p - 1$ は偶数なので k も偶数. よって $k = 2L$ と表せることによって $p - 1 = 2Lq$ と書ける.

$$P^{\frac{p-1}{2}} \equiv P^{Lq} \equiv (P^q)^L \equiv 1 \pmod{q}.$$

ルジャンドルの記号を用いるとオイラーの基準によって

$$P^{\frac{p-1}{2}} \equiv \left(\frac{P}{p}\right)$$

$$P^{\frac{p-1}{2}} \equiv 1 \text{ なので } \left(\frac{P}{p}\right) = 1.$$

$P = 5$ なら平方剰余の法則から $p \equiv \pm 1 \pmod{5}$.

3.2 オイラーとラグランジュの結果

オイラーとラグランジュの結果は底が P でも成り立つ.

補題 13 p を素数とし, $q = 2p + 1$ も素数とする. $L_p = P^p - 1, P \neq p$ とおくと, q を法として P が平方剰余とする. このとき q は L_p の素因子である.

Proof.

仮定から $P \equiv n^2 \pmod{q}$ を満たす整数 n がある. フェルマーの小定理を用いて

$$P^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \pmod{q}$$

ゆえに $L_p = P^p - 1 = qk$ と書けるので, q は L_p の素因子.

(平方剰余の相互法則から $q \equiv \pm 1 \pmod{P}$)

この逆も成立する.

補題 14 p を素数とし, $q = 2p + 1$ が $L_p = P^p - 1$ の因子とする. このとき $q = 2p + 1$ も素数.

Proof.

$q = 2p + 1$ は素数でないとする. その最小の素因子をとり q_0 とする. $2p + 1 \geq q_0^2$ を満たす. q_0 も N_p の素因子なので $q_0 \neq P$.

$$P^p - 1 = N_p \equiv 0 \pmod{q_0}.$$

p は素数なので q_0 を法とした P の位数である. フェルマーの小定理を用いて

$$P^{q_0-1} \equiv 1 \pmod{q_0}.$$

ゆえに, $q_0 - 1$ は p の倍数. とくに $q_0 - 1 > p$ になり

$$2p + 1 \geq q_0^2 > p^2 + 2p + 1 > 2(p + 1) + 1.$$

これで矛盾した.

p, q が素数のとき, $q \pm 1$ が 5 で割れる場合を調べた.

$p = 29, q = 59 \equiv -1 \pmod{5}$ なので q を法として 5 は平方剰余.

$q = 59$ は L_p の素因子.

$B = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 * 231669654363683130095909$

$p = 89, q = 179 \equiv +1 \pmod{5}$ なので q を法として 5 は平方剰余.

$q = 179$ は L_p の素因子.

3.3 例

以下では素数 P に対してその素数べき P^p について $N_p = \frac{P^p - 1}{P - 1}$ が素数にならない場合を扱う. $q = 2p + 1$ も素数になる場合に限定した.

表 3.3: q : 素数

p	$q = 2p + 1$	$q - 1$	$q + 1$	L_p 素因数分解
11	23	22	24	$2^2 * 12207031$
23	47	46	48	$2^2 * 8971 * 332207361361$
29	59	58	60	$2^2 * 59 * 35671 * 22125996444329625552508473588471$
41	83	82	84	A
53	107	106	108	$2^2 * 5960555749 * 17154094481 * 27145365052629449$
89	179	108	180	$2^2 * B$

3.3.1 $P = 3$

表 3.4: $P = 3, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(4) = 2^2$
3	7	$(13) = 13$
5	11	$(121) = 11^2$
11	23	$(88573) = 23 * 3851$
23	47	$(47071589413) = 47 * 1001523179$
29	59	$(34315188682441) = 59 * 28537 * 20381027$
41	83	$(18236498188585393201) = 83 * 2526913 * 86950696619$
53	107	$(9691622833840009948398361) = 107 * 24169 * 3747607031112307667$
83	167	$A = B$
89	179	$C = D$

$$A = (1995419197093669964767123337786174517613)$$

$$B = 167 * 12119 * 1036745531 * 950996059627210897943351$$

$$C = (1454660594681285404315232913246121223340241)$$

$$D = 179 * 1611479891519807 * 5042939439565996049162197$$

$q = 2p + 1$ が N_p の最小素因子となる.

3.3.2 $P = 5$

$$A = (46566128730773925781) = 59 * 35671 * 22125996444329$$

$$B = (11368683772161602973937988281) = 2238236249 * 5079304643216687969$$

$$C = (2775557561562891351059079170227050781) = 960555749 * 17154094481 * 27145365052629449$$

表 3.5: $P = 5, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(6)=2*3$
5	11	$(781)=11*71$
23	47	$(2980232238769531)=8971*332207361361$
29	59	A
41	83	B
53	107	C
83	167	$D = E$
89	179	$F = G$
113	$(227)=227$	$H = I$
131	$(263)=263$	$J = K$

$D = (2584939414228211483973152162718633917393162846565246582031)$
 $E = 20515111 * 1431185706701868962383741 * 88040095945103834627376781$
 $F = (40389678347315804437080502542478654959268169477581977844238281)$
 $G = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 * 231669654363683130095909$
 $H = (2407412430484044816319972428231159148172627060269235244049923494458198547363281)$
 $I = 2939 * 6329 * 129499 * 308491 * 304247586761 * 2084303944451 - *620216264269531 * 8237123176890810696379$
 $J = 918354961579912115600575419704879435795832466228193-3761787122705300134839490056037902832031)$
 $K = 2621 * 23928199 * 34720241 * 16815642611861 * -250805666433416532678429525124977090318975999001796354124089$
 $q = 2p + 1$ が N_p の最小素因子となるのは $q = 11, 179,$
 $p = 23$ での (N_p) の素因数分解 $8971 * 332207361361$ について

```

?- A=8971,B is A-1, factorize(B,BB),exps(BB,J).
A = 8971,
B = 8970,
BB = J, J = [2, 3, 5, 13, 23].

3 ?- A=332207361361,B is A-1, factorize(B,BB),exps(BB,J).
A = 332207361361,
B = 332207361360,
BB = [2, 2, 2, 2, 3, 3, 5, 7, 23|...],
J = [2^4, 3^2, 5, 7, 23, 293, 9781].
    
```

B がどれも 2×23 を因数に持つ.

$p = 29$ での (N_p) の素因数分解 $59 * 35671 * 22125996444329$ について

4 ?- A=59,B is A-1, factorize(B,BB),exps(BB,J).

A = 59,

B = 58,

BB = J, J = [2, 29].

5 ?- A=35671,B is A-1, factorize(B,BB),exps(BB,J).

A = 35671,

B = 35670,

BB = J, J = [2, 3, 5, 29, 41].

6 ?- A=22125996444329,B is A-1, factorize(B,BB),exps(BB,J).

A = 22125996444329,

B = 22125996444328,

BB = [2, 2, 2, 7, 29, 13624382047],

J = [2^3, 7, 29, 13624382047].

B はどれも 2×29 を因数に持つ.

3.3.3 $P = 7$

表 3.6: $P = 7, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(8)=2^3$
3	7	$(57)=3*19$
11	23	$(329554457)=1123*293459$
23	47	$(4561457890013486057)=47*3083*31479823396757$
29	59	$(536650959302196621139601)=59*127540261*71316922984999$
41	83	A
53	107	B = C
83	167	D = E

$A = (7427940054393865983365007662428001) = 83 * 20515909 * 4362139336229068656094783$

$B = (102812251604677061048459359469231621132196401)$

$C = 8269 * 319591 * 8904276017035188056372051839841219$

$D = (2317320324970087447233098679232119852283366872016190787490668645944057)$

$E = 167*66733*76066181*7685542369*62911130477521*303567967057423*18624275418445601$

$q = 2p + 1$ が N_p の最小素因子となるのは $q = 47, 59, 83, 167$.

3.3.4 $P = 11$

表 3.7: $P = 11, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(12)=2^2 * 3$
3	7	$(133)=7*19$
5	11	$(16105)=*3221$
11	23	$(28531167061)=15797*1806113$
23	47	$(89543024325523737224653)=829*28878847*3740221981231$
29	59	$(158630929717149157441443670489)=523*303309617049998388989376043$
41	83	$X = Y$
53	107	$A = B$
83	167	$C = D$

$$X = (497851811249935469864782916383866125124241)$$

$$Y = 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$$

$$A = (1562472251828744662703731061631669238387852269920031433)$$

$$B = 107 * 351497 * 6005113 * 6918082374901313855125397665325977135579$$

$$C = (27264206856132551104041433310203529772397431215022163096159207985879419668700193602213)$$

$$D = 167 * 12119 * 178057577 * 52447614013 * 1442525225996981034595894901431683672700025887063977893738081$$

$q = 2p + 1$ が N_p の最小素因子となるのは $q = 7, 83, 107, 167$

3.3.5 $P = 13$

表 3.8: $P = 13, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(8)=2^3$
3	7	$(57)=3*19$
11	23	$(329554457)=1123*293459$
23	47	$(4561457890013486057)=47*3083*31479823396757$
29	59	$(536650959302196621139601)=59*127540261*71316922984999$
41	83	A
53	107	$B = C$
83	167	$D = E$
89	179	$F = G$

$$A = (7427940054393865983365007662428001) = 83 * 20515909 * 4362139336229068656094783$$

$$B = (102812251604677061048459359469231621132196401)$$

$$C = 8269 * 319591 * 38904276017035188056372051839841219$$

$$D = (2317320324970087447233098679232119852283366872016190787490668645944057)$$

$$E = 167 * 66733 * 76066181 * 7685542369 * 62911130477521 * 303567967057423 * 18624275418445601$$

$$F = (272630418912405818079526826512979668501285829125832829957489675526672381601)$$

$$G = 1805633 * 18489605314740987765913 * 8166146875847876762859119015147004762656450569$$

$$q = 2p + 1 \text{ が } N_p \text{ の最小素因子となるのは } q = 47, 59, 83, 167$$

$$p = 89 \text{ のときの } G = 1805633 * 18489605314740987765913 * 8166146875847876762859119015147004762656450569$$

の各素因数について

?- A=1805633, B is A-1, factorize(B, BB), exps(BB, J).

$$A = 1805633,$$

$$B = 1805632,$$

$$J = [2^6, 89, 317].$$

?- A=18489605314740987765913, B is A-1, factorize(B, BB), exps(BB, J).

$$A = 18489605314740987765913,$$

$$B = 18489605314740987765912,$$

$$J = [2^3, 3, 7, 89, 89839, 13764595178129].$$

B はどちらも 2×89 を因数に持つ.

3.4 q を底に持つフェルマー素数

素数 $q > 2$ に対して $L = q^e + 1$ は偶数であるが $L/2$ が素数になると仮定すると $e = 2^m$ であり, 実際に素数になることもある. このとき q を底に持つフェルマー素数と呼ぶ.

便宜上 L を L_m と書く.

3.5 5が底の完全数

$a = 5^e$ に対して $\sigma(5^e)$ が素数 q になったとする. $\alpha = aq$ とおき $\sigma(\alpha)$ を計算する.

$$\sigma(\alpha) = \sigma(aq) = \sigma(a)\sigma(q) = \sigma(q)(q+1)$$

になる. $q = \sigma(5^e) = \frac{5^{e+1}-1}{4}$ より

$$q+1 = \frac{5^{e+1}+3}{2} = \frac{5a+3}{4}$$

なので

$$\sigma(\alpha) = \sigma(a)(q+1) = \frac{\sigma(a)(5a+3)}{4} = \frac{(5\alpha+3q)}{4}.$$

これから

$$4\sigma(\alpha) = 5\alpha + 3q.$$

ここから q を消すことができないので a の最大素因子を $\text{Maxp}(a)$ と書きこれを使うことにする. すると

$$4\sigma(\alpha) = 5\alpha + 3\text{Maxp}(\alpha)$$

を満たす.

3.5.1 $s(a) = 2$ の場合

$4\sigma(\alpha) = 5\alpha + 3\text{Maxp}(\alpha)$ の解を $s(a) = 2$ の場合に求めよう.

a を素因数分解し $a = p^e q^f$ ($2 < p < q$) とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおけば

$$\frac{4AB}{\rho'} = 5XY + 3q$$

書き直して

$$4AB = 5\rho'XY + 3\rho'q.$$

$4AB - 5\rho'XY$ の XY の係数を R とおけば

$$R = 4pq - 5\rho' = 20 - (p - 5)(q - 5).$$

$3q\rho' + 4(pX + qY - 1) = RXY$ によって $R > 0, 0 < R = 20 - (p - 5)(q - 5)$ により 次なる解がある.

$$(1) p = 5, R = 20. \rho' = 4\bar{q},$$

$$(2) p = 3, R = 30 + 2q. \rho' = 2\bar{q},$$

$$(3) p = 7, R = 30 - 2q; q = 11, 13 \rho' = 6\bar{q}.$$

$$RXY - 4(pX + qY - 1) = 3q\rho'.$$

$$1. p = 5, R = 20. \rho' = 4\bar{q}.$$

$$(20X - 4q)Y - 20X = 12q\bar{q} - 4.$$

4 で割って

$$(5X - q)Y - 5X = (5X - q)Y - (5X - q) - q = 3q\bar{q} - 1.$$

変形して

$$(5X - q)(Y - 1) = 3q\bar{q} + \bar{q}.$$

$Y - 1 \geq \bar{q}$ により

$$3q\bar{q} + \bar{q} \geq (5X - q)\bar{q}$$

\bar{q} を除して

$$3q + 1 \geq (5X - q).$$

i. $Y = q$ なら $3q + 1 = (5X - q)$. ゆえに $q = \frac{5^{e+1}-1}{4}$.

ここで話を逆転し e を動かして $\frac{5^{e+1}-1}{4}$ が素数のときを探して q とおけばよい.

ii. $Y = q^2$ なら

$$(5X - q)(q^2 - 1) = (5X - q)(Y - 1) = 3q\bar{q} + \bar{q}$$

により,

$$(5X - q)(q + 1) = 3q + 1.$$

$5X = q + \frac{3q+1}{q+1} = q + 4 - \frac{2}{q+1}$. しかるに $\frac{2}{q+1}$ は整数になれないから矛盾.

iii. $Y \geq q^3$ なら

$$(5X - q)(Y - 1) = 3q\bar{q} + \bar{q} \geq (5X - q)(q^3 - 1) = (5X - q)(q^2 + q + 1)\bar{q}.$$

\bar{q} を除すると $3q + 1 \geq q^2 + q + 1$; 矛盾.

2. $p = 3, R = 30 + 2q, \rho' = 2\bar{q}$,

$R_1 = 15 + q$ とおくとき

$$R_1XY - 2(3X + qY - 1) = 3q\bar{q} - 2.$$

$Y \geq q$ により

$$(R_1X - 2q)Y = 6X + 3q\bar{q} - 2 \geq (R_1X - 2q)q.$$

$6X + 3q\bar{q} - 2 \geq (R_1X - 2q)q$ により

$$3q\bar{q} - 2 + 2q^2 \geq (R_1q - 6)X.$$

i. $X \geq 3^2 = 9$ のとき

$$3q\bar{q} - 2 + 2q^2 \geq 9(R_1q - 6) = 9(q^2 + 15q - 6).$$

これから矛盾が出る.

ii. $X = 3$ のとき

$$3R_1Y - 2(9 + qY - 1) = 3q\bar{q} - 2.$$

これより

$$Y(3R_1 - 2q) = 3q\bar{q} - 4.$$

$3R_1 - 2q = q + 45$ なので $q_1 = q + 45$ とおいて

$$q_1Y = 3q^2 - 3q - 4 = \bar{q} - 4 = 3q_1^2 - 273q_1 + 6226.$$

$\frac{6226}{q_1}$ は整数で $6226 = 2 * 11 * 283$, $q_1 = q + 45$ は偶数なので $q_1 = q + 45 = 6226, 2 * 283$.

その結果 $q = 6226 - 45 = 6161 = 61 * 11$, $q = 2 * 283 - 45 = 521$. しかし, $a = 3 * 521$ は条件を満たさない.

3. $p = 7, R = 30 - 2q; q = 11, 13 \rho' = 6\bar{q}$.

$p = 7$ より $R_1 = 15 - q$ とおくと

$$R_1XY - 2(7X + qY - 1) = 9q\bar{q}$$

i. $q = 11$ なら

$$4XY - 2(7X + 11Y - 1) = 9q\bar{q} = 90 \times 11.$$

$X_1 = 2X, Y_1 = 2Y$ とすると

$$X_1Y_1 - 7X_1 - 11Y_1 = 9q\bar{q} = 90 \times 11 - 2 = 988.$$

$$X_1(Y_1 - 7) - 11(Y_1 - 7) = (X_1 - 11)(Y_1 - 7) = 988 + 77 = 1065 = 3 * 5 * 71.$$

これより $X_1 = 2X = 11 + 3, Y_1 = 2Y = 7 + 5 * 71$. $X = 7, 2Y = 362, Y = 81 = 3^4$. 矛盾

ii. $q = 13$ なら $R_1 = 2$.

$$4XY - 4(7X + 13Y - 1) = 18q\bar{q} = 2808.$$

$$XY - (7X + 13Y) = 3^2 * 6 * 13 - 1 = 701.$$

$$(X - 13)(Y - 7) = 701 + 13 * 7 = 792 = 8 * 9 * 11.$$

$X - 13 = 36, Y - 7 = 22; Y = 29$. 矛盾

例

3.6 究極の完全数とその平行移動

P を素数とし $\sigma(P^e)$ が素数 q のとき $a = P^e q$ を底が P の究極の完全数と呼ぼう.

このとき $q = \frac{P^{e+1}-1}{P}$ となる. 言葉ができると諒解しやすくまた研究したくなるという効果がある.

究極の完全数を整数 m だけ平行移動しよう.

$q = \frac{P^{e+1}-1}{P} + m$ は素数として $a = P^e q$ を m だけ平行移動した底が P の完全数と呼ぶ.

3.7 例

3.7.1 $[p = 5, m = 0]$

表 3.9: $P = 5, m = 0$

e	素因数分解	a
2	$5^2 * 31$	775
6	$5^6 * 19531$	305171875
10	$5^{10} * 12207031$	119209287109375
12	$5^{12} * 305175781$	74505805908203125
46	$5^{46} * 177635683940025046467781066894531$	A
126	B	C
148	D	--
180	E	--

$A = 25243548967072377773175314089049123822405817918479442596435546875$

$B = 5^{126} * 14693679385278593849609206715278070972733319459651094018859396328480215743184089660644531$

$C = 17272337110188892507727037256[117\text{digits}]661895799450576305389404296875$

$D = 5^{148} * 3503246160812042677309323958224790328200654854691289429392670709724477706714651503716595470$

$E = 5^{180} * 8156630584998155658387867636570684444626455322586208184698295569337154055746857784028620158$

この表によると q の下2桁は, 31 または 81.

$4q = 5^{e+1} - 1$ を利用して, $q \equiv 31 \pmod{50}$ を証明する. $e \geq 2$ により

$$4q = 5^{e+1} - 1 \equiv -1 \pmod{25}$$

6倍して

$$24q \equiv -6 \pmod{25}$$

$24q \equiv -q$ により

$$q \equiv 6 \equiv 31 \pmod{25}$$

q は奇数なので $q \equiv 31 \pmod{50}$.

$e \geq 3$ を仮定する. $a = 5^e * q = 625 * 5^{e-3} * (31 + 50k) = 625K$, K は奇数.

$$a = 625(2s + 1) \equiv 625 \equiv 625 + 50 = 675 \equiv 5 \pmod{25}.$$

よって $q \equiv 31, a \equiv 25 \pmod{50}$.

表の観察から

- $e \equiv 2 \pmod{4}$ なら $q \equiv 31, a \equiv 75 \pmod{100}$,
- $e \equiv 0 \pmod{4}$ なら $q \equiv 81, a \equiv 25 \pmod{100}$.

しかし証明には至らなかった.

3.7.2 $[p = 5, m = 1]$ 表 3.10: $P = 5, m = 1$

e	素因数分解	a
3	$5^3 * 157$	19625
5	$5^5 * 3907$	12209375
9	$5^9 * 2441407$	4768373046875
11	$5^{11} * 61035157$	2980232275390625
27	$5^{27} * 9313225746154785157$	69388939039072283782064914703369140625
153	A	B

$$A = 5^{153} * 109476442525376333665916373694[48digits]859491143608465790748596191407$$

$$B = 958807317440962217401517959958[154digits]294595676474273204803466796875$$

$q \equiv 7, 32 \pmod{50}$ を以下で証明する.

$$q = \frac{5^{e+1}-1}{4} + 1 = \frac{5^{e+1}+3}{4} \text{ により}$$

$e \geq 2, 5^2 \equiv 0 \pmod{25}$ を用いて

$$4q = 5^{e+1} + 3 \equiv 3 \pmod{25}.$$

6倍して

$$24q \equiv -q \equiv 18 \pmod{25}$$

$q \equiv 7$ により

$$q \equiv 7 \pmod{25}.$$

$q = 7 + 25k$. q は奇数なので k は偶数になり,

$$q \equiv 7 \pmod{50}.$$

$a \equiv 25 \pmod{50}$ は読者への課題.

しかし表の観察から

- $e \equiv 3 \pmod{4}$ なら $q \equiv 57, a \equiv 25 \pmod{100}$,

- $e \equiv 1 \pmod{4}$ なら $q \equiv 7, a \equiv 65 \pmod{100}$.

証明は？

$[p = 5, m = -2]$

表 3.11: $P = 5, m = -2$

e	素因数分解	a
2	$5^2 * 29$	725
10	$5^{10} * 12207029$	119209267578125
14	$5^{14} * 7629394529$	46566128717041015625
26	$5^{26} * 1862645149230957029$	A
32	$5^{32} * 29103830456733703613279$	B
42	$5^{42} * 284217094304040074348449707029$	C

$$A = 2775557561562891347706317901611328125$$

$$B = 677626357803440271254605613648891448974609375$$

$$C = 64623485355705287099328804067454257165081799030303955078125$$

以下で, $q \equiv 9 \pmod{10}$ を示す.

$$q = \frac{5^{e+1}-1}{4} - 2 = \frac{5^{e+1}-9}{4} \text{ により}$$

$$4q = 5^{e+1} - 9 \text{ により}$$

6倍して

$$24q \equiv -q \equiv -54 \equiv -4 \pmod{25}.$$

$$q \equiv 4 \equiv 29 \pmod{25}.$$

$q = 19 + 25k$ となるが, q は奇数なので k は偶数. ゆえに

$$q \equiv 29 \pmod{50}.$$

3.7.3 $[p = 7, m = 0]$

表 3.12: $P = 7, m = 0$

e	素因数分解	a
4	$7^4 * 2801$	6725201
12	$7^{12} * 16148168401$	223511436608353935601
130	A	B
148	C	--

$$A = 7^{130} * 8505346116479680194953954163954280577066639$$

$$-- 2330682673302530819774105141531698707146930307290253537320447270457$$

$$B = 620064964809565522477522001004[160digits]149867511012464186481525314793$$

$$C = 7^{149} * 1385022127101034087007743810331355039266633249933176317292 --27790657325163310341833227775$$

$e \equiv 0 \pmod{4}$ なら a, q は末尾が 1.

$e \equiv 2 \pmod{4}$ なら $q \equiv 7, b \equiv 3 \pmod{10}$.

証明できるか?

$[p = 7, m = 1]$

表 3.13: $P = 7, m = 1$

e	素因数分解	a
3	$7^3 * 401$	137543
5	$7^5 * 19609$	329568463
11	$7^{11} * 2306881201$	4561457891661258343
35	$7^{35} * 441955140976608911963170563601$	X
41	A	B

$$X = 167420868544846506666536922416431932606978335013856009100743$$

$$A = 7^{41} * 51995580380757061883555053636996009$$

$$B = 2317320324970087447233098679232119889423067143985520704315706958084063$$

q の末尾は 1,9 ; a の末尾は 3 .

証明できるか?

3.7.4 $[p = 11, m = 0]$ 表 3.14: $P = 11, m = 0$

e	素因数分解	a
16	$11^{16} * 50544702849929377$	A
18	$11^{18} * 6115909044841454629$	B
72	C	D
138	E	F

$$A = 2322515441988780809505203793273697,$$

$$B = 34003948586157739898684696499226975549.$$

$$C = 11^{72} * 1051153199500053598403188407217590190707671147285551702341089650185945215953$$

$$D = 496393063768024261910916388812210934417238517638790071036123979591088-6247622149100809195553292$$

$$E = 11^{138} * 56700023252179573962582828126717134448680538588121757508114966$$

$$-01630462174655445733557105920797699326519891538336121983348434678610919$$

$$-02034340949$$

$$F = 197570745515252862741089786745[126digits]419090574842472900026072825856$$

 $[p = 11, m = -1]$ 表 3.15: $P = 11, m = -1$

e	素因数分解	a
7	$11^{16} * 21435889$	A
136	B	C

$$A = 984973308935517986686129$$

$$B = 11^{136} * 339670648186281055704283718218[92digits]178162598657497243307737178361$$

$$C = 295894866274296553472802883472[133digits]214577548653064817929088925696$$

3.7.5 $[p = 13, m = 0]$ 表 3.16: $P = 13, m = 0$

e	素因数分解	a
4	$13^4 * 30941$	883705901
6	$13^6 * 5229043$	25239591813787

3.8 究極の完全数の満たす方程式

平行移動も許した究極の完全数の満たす方程式を作る.

$$q = \frac{P^{e+1}-1}{P} + m \text{ であって}$$

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

になり, $q + 1 = \frac{P^{e+1}+P-2}{P} + m$ を用いて次のように式変形する.

$$\begin{aligned} \sigma(a) &= \frac{P^{e+1} - 1}{\overline{P}}(q + 1) \\ &= (q - m)(q + 1) \\ &= q(q + 1) - m(q + 1) \\ &= \frac{q}{P}(P^{e+1} + P - 2) + mq - m(q + 1) \\ &= \frac{Pa + q(P - 2)}{\overline{P}} - m. \end{aligned}$$

これより $q = \text{Maxp}(a)$ を用いて

$$\overline{P}\sigma(a) - Pa = (P - 2)\text{Maxp}(a) - m(P - 1). \quad (3.1)$$

これを m 平行移動した究極の完全数の基本方程式という.

例えば $P = 2$ なら

$$\sigma(a) = 2a - m.$$

$P = 2$ に限って不愉快な $\text{Maxp}(a)$ が消えた.

$P = 3$ なら

$$2\sigma(a) = 3a + \text{Maxp}(a) - 2m.$$

3.8.1 究極の完全数の基本問題

(3.1) を満たすとき

素数 $q = \frac{P^{e+1}-1}{P} + m$ を基にして $a = P^e q$

とかけるか? という問題を究極の完全数の基本問題と言う.

これが一般に成立するはずはない. とりあえず反例を探す.

3.9 諸例

次に方程式を満たす a を表示する.

$a = < 200000$ 程度の範囲で全数検査するので非常に時間がかかる.

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

3.9.1 $[P = 5, m = 0]$

表 3.17: $[P = 5, m = 0]$

a	素因数分解	$\sigma(a)$
775	$[5^2, 31]$	992

微小解は無い.

3.9.2 $[P = 7, m = 0]$

表 3.18: $[P = 7, m = 0]$

a	素因数分解	$\sigma(a)$
9	$[3^2]$	13

$a = 3^2$ は微小解.

3.9.3 $[P = 43, m = 0]$

表 3.19: $[P = 43, m = 0]$

a	素因数分解	$\sigma(a)$
49	$[7^2]$	57

3.10 微小解

平行移動しない場合を扱う. したがって

$$\bar{P}\sigma(a) - Pa = (P - 2)\text{Maxp}(a)$$

を満たすので $s(a) = 1$ のときの解を求めよう. $a = q^f$ が上の式を満たすとする.

平行移動しない場合を扱う. したがって

$$\bar{P}\sigma(a) - Pa = (P - 2)\text{Maxp}(a)$$

を満たす. $s(a) = 1$ のときの解を求めよう. $a = q^f$ が上の式を満たすとする.

$f = 1$ のとき.

$$\bar{P}(q + 1) - Pq = (P - 2)q.$$

これより,

$$P - q - 1 = (P - 2)q.$$

$(P - 1)(q - 1) = 0$ がでて矛盾.

$f \geq 2$ のとき.

$Y = q^f$ とおけば $a = Y, \bar{q}\sigma(a) = qY - 1$ を満たし $\text{Maxp}(a) = q$ によって

$$\frac{\bar{P}(qY - 1)}{\bar{q}} = PY + (P - 2)q.$$

整理して

$$Y(\bar{P}q - P\bar{q}) = \bar{P} + (P - 2)q\bar{q}.$$

これより

$$\bar{P} = Y(P - q) - (P - 2)q\bar{q} = q(q^{f-1}(P - q) - (P - 2)\bar{q}).$$

よって $\bar{P} = wq$ を満たす自然数 w がある. q を払って

$$w = (q^{f-1}(P - q) - (P - 2)\bar{q}) = P(q^{f-1} - \bar{q}) - q^f + 2\bar{q}.$$

よって $P = 1 + wq$

$$w = (1 + wq)(q^{f-1} - \bar{q}) - q^f + 2\bar{q}.$$

$$w(1 - q^f + q\bar{q}) = -q^f + q^{f-1} + \bar{q}.$$

$w = 1$ のとき.

$P = 1 + q$ となり P, q はともに素数だから $q = 2, P = 3, a = Y = 2^f$.

$2\sigma(a) = 3a + 2$ なので $2(2Y - 1) = 3Y + 2$. これより $a = Y = 4$.

$w \geq 2$ のとき.

$$2(q^f - q\bar{q} - 1) \leq w(q^f - q\bar{q} - 1) = q^f - q^{f-1} - \bar{q}.$$

これより

$$q^f - 2q\bar{q} - 2 \leq -q^{f-1} - \bar{q}.$$

$$q^{f-1}(q+1) \leq 2q^2 - 3q + 3.$$

$f \geq 3$ のとき.

$$q^2(q+1) \leq 2q^2 - 3q + 3.$$

変形して

$$q^3 - q^2 \leq 3 - 3q.$$

これは矛盾.

$f = 2$ のとき

$$w(q^2 - q(q-1) - 1) = q^2 - q - (q-1) = \bar{q}^2.$$

$q^2 - q(q-1) - 1 = q-1$, $w\bar{q} = \bar{q}^2$ によって $w = \bar{q}$.

$P-1 = wq = q(q-1)$ により $P = 1 + q(q-1)$.

P, q が素数で $P = 1 + q(q-1)$ を満たすとき方程式で定められた底が P のとき $a = q^2$ が微小解.

微小解が存在するための素数 P の条件が素数 q があって $P = 1 + q(q-1)$ を満たすことである. このような素数として $P = 7, 43$ がある.

$P = 3$ のとき微小解 $q = 2^2$; $P = 7$ のとき微小解 $q = 3^2$; $P = 157$ のとき微小解 $q = 13^2$ などが現れる.

3.10.1 微小解の存在する素数

微小解の存在する素数はほかにあるだろうか. パソコン君に頼むと次のように意外に多くの解を出してきた.

a, b が互いに素な自然数のとき等差数列 $\{an + b\}$ ($n = 1, 2, 3, \dots$) には無限に多くの素数がある. これが有名な Dirichlet の定理である.

しかし, 2 次数列たとえば $\{n^2 + 1\}$ には無限に多くの素数があるに違いない. これは有名な数論における期待であるが証明はできるはずがない, と思われているほど難しい.

$\{n^2 - n + 1\}$ は無限に多くの素数があることは確実だが証明はない.

微小解の存在条件では n を素数に限りつつ $\{n^2 - n + 1\}$ には無限に多くの素数があるか問うている.

表 3.20: P, q が素数

q	P
3	7
7	43
13	157
67	4423
79	6163
139	19183
151	22651
163	26407
193	37057

これは真に難問中の難問である。このような難問が、微小解の存在問題として登場した。実に不思議なことである。

3.10.2 $s(a) = 2$ の場合に解く (未完)

与えられた素数 P と整数 m について次式が満たされるとする。

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

これを $m = 0$ の条件をつけ a の方程式 とみて $s(a) = 2$ の場合に解いてみよう。

$a = p^e q^f, p < q$ はいつもの通りで $X = p^e, Y = q^f, A = pX - 1, B = qY - 1, \rho' = \overline{pq}$ を使う。

$$\frac{\overline{P}AB}{\rho'} - PXY = (P - 2)q$$

が基礎方程式になる。 ρ' をかけて

$$\overline{P}AB - \rho'PXY = \rho'(P - 2)q.$$

左辺の XY の係数を R とおけば

$$R = \overline{P}pq - \rho'P = P(pq - \rho') - pq.$$

$\Delta = p + q$ とおくと $pq - \rho' = \Delta - 1$.

$$R = P(\Delta - 1) - pq = -P + P\Delta - pq = P^2 - P - p'q'.$$

ここで $p' = p - P, q' = q - P$.

$p = P(p' = 0)$ なら $R = P(P - 1)$ 。これが標準的な場合になるが $p > P, p < P$ の場合もあり、ここで一般に考えることは難しい。

実際、 $P = 7$ とすると $R = 42 - p'q'$ 。

- $p = 2$ のとき $R = 7 + 5q$
- $p = 3$ のとき $R = 14 + 4q$
- $p = 5$ のとき $R = 28 + 2q$
- $p = 7$ のとき $q \geq 11, R = 42$
- $p = 11$ のとき $q = 13, 17$.

したがって, ここで小休止.

3.11 例

3.11.1 $[m = p - 1]$ の解

$\overline{P}\sigma(a) - Pa = (P - 2)\text{Maxp}(a) - m(P - 1)$ おいて微小解として $s(a) = 1$ の解 $a = P^e$ があるとする.

$$\overline{P}\sigma(a) - Pa = (P^{e+1} - 1) - P^{e+1} = -1 \text{ により}$$

$$-1 = (P - 2)\text{Maxp}(a) - m(P - 1) = (P - 2)P - m(P - 1).$$

よって $m(P - 1) = (P - 1)^2$. これより $m = P - 1$.

$m = P - 1$ のとき 微小解 P^e 以外の解がどのくらいあるかがわからない

3.11.2 $[p = 5, m = 1]$ 表 3.21: $[p = 5, m = 1]$

a	素因数分解	$\sigma(a)$
2	[2]	3
35	[5, 7]	48
3059	[7, 19, 23]	3840
7469	[7, 11, 97]	9408
19625	$[5^3, 157]$	24648

3.11.3 $[p = 5, m = 3]$ 表 3.22: $[p = 5, m = 3]$

a	素因数分解	$\sigma(a)$
847	$[7, 11^2]$	1064

3.11.4 $[p = 5, m = 4]$ 表 3.23: $[p = 5, m = 4]$

a	素因数分解	$\sigma(a)$
5	[5]	6
25	$[5^2]$	31
125	$[5^3]$	156
625	$[5^4]$	781
3125	$[5^5]$	3906
15625	$[5^6]$	19531
78125	$[5^7]$	97656

表 3.24: $[p = 5, m = -2]$

a	素因数分解	$\sigma(a)$
539	$[7^2, 11]$	684
725	$[5^2, 29]$	930
12905	$[5, 29, 89]$	16200

3.11.5 $[p = 5, m = -2]$ **3.11.6** $[p = 7, m = 1]$ 表 3.25: $[p = 7, m = 1]$

a	素因数分解	$\sigma(a)$
2	$[2]$	3
126293	$[17^2, 19, 23]$	--
137543	$[7^3, 401]$	--

3.11.7 $[p = 7, m = 2]$ $[p=7,m=2]$

表 3.26:

a	素因数分解	$\sigma(a)$
3	$[3]$	4
2891	$[7^2, 59]$	3420
59171	$[7, 79, 107]$	69120

3.11.8 $[p = 7, m = 3]$

表 3.27:

a	素因数分解	$\sigma(a)$
77	[7, 11]	96
13651	[11, 17, 73]	15984

3.12 p が一般で解が $a = p^e qr$ の場合

整数 m と素数 p に付いての方程式

$$\bar{p}\sigma(a) - pa = (p-2)\text{Maxp}(a) - m(p-1)$$

の解を $p^e qr$ ($p < q, r$: 素数) の形に限って求めよう.

$\bar{p}\sigma(a) = (p^{e+1} - 1)\tilde{q}\tilde{r}$, $pa = (p^e - 1)qr$, $(p-2)\text{Maxp}(a) - m(p-1) = (p-2)r - m(p-1)$ によって

$\Delta = q + r$, $\Gamma = p^{e+1} - 1$ を用いて

$$\begin{aligned}\bar{p}\sigma(a) - pa &= \Gamma(qr + \Delta + 1) - (\Gamma + 1)qr \\ &= \Gamma\Delta + \Gamma - qr &= (p-2)r - m(p-1)\end{aligned}$$

整理して

$$\Gamma\Delta + \Gamma + m(p-1) = (p-2)r + qr = (p-2+q)r.$$

$q' = q + p - 2$, $\Delta' = q' + r$ とおくと $\Gamma = q + r = q' + 2 - p + r = \Gamma' - p + 2$ によると $D = \Gamma^2 + \Gamma(3-p) + m\bar{p}$ を用いて

$$q'r = \Gamma\Delta' + \Gamma(3-p) + m\bar{p}$$

から $q_0 = q' - \Gamma$, $r_0 = r - \Gamma$ より

$$q_0 r_0 = \Gamma^2 + \Gamma(3-p) + m\bar{p} = D.$$

実際には与えられた p, m に対して自然数 e を動かしながら $\Gamma = p^{e+1} - 1$ を用いて $D = \Gamma^2 + \Gamma(3-p) + m\bar{p}$ を異なる2因数 $q_0 r_0$ に分解して $q = q' + 2 - p = q_0 + \Gamma + 2 - p$, $r = r_0 + \Gamma$ がともに素数のものを選べば良い.

3.13 例

表 3.28: $p = 3, m = 1; a = 3^e qr$

a	素因数分解	$\sigma(a)$
741	$3^1 * 13 * 19$	1120
38781	$3^2 * 31 * 139$	58240
4954286665155815901	$3^{11} * 536917 * 52088299$	7431429997759768000

表 3.29: $p = 3, m = -2; a = 3^e qr$

a	素因数分解	$\sigma(a)$
759	$3^1 * 11 * 23$	1152
19184931	$3^4 * 433 * 547$	28777672
8061750261	$3^5 * 739 * 44893$	12092647840
721889577	$3^5 * 947 * 3137$	1082835936
629690031	$3^5 * 1019 * 2543$	944536320
998897581791	$3^7 * 7331 * 62303$	1498346403840

表 3.30: $p = 3, m = 4; a = 3^e qr$

a	素因数分解	$\sigma(a)$
51417	$3^2 * 29 * 197$	77220
27639	$3^2 * 37 * 83$	41496
965007	$3^3 * 103 * 347$	1447680
4162847823	$3^5 * 751 * 22811$	6244283136
277979312695831119	$3^{11} * 695047 * 2257691$	416968969044875520

表 3.31: $p = 3, m = -4; a = 3^e qr$

a	素因数分解	$\sigma(a)$
50373	$3^2 * 29 * 193$	75660
283176230906781	$3^9 * 100511 * 143137$	424764346431744

表 3.32: $p = 3, m = -5; a = 3^e qr$

a	素因数分解	$\sigma(a)$
663	$3^1 * 13 * 17$	1008
38223	$3^2 * 31 * 137$	57408
1727757	$3^3 * 89 * 719$	2592000
862299	$3^3 * 109 * 293$	1293600
15862743783	$3^5 * 733 * 89057$	23794160208
760262656887	$3^7 * 7669 * 45329$	1140394008000

3.13.1 $p = 5, m = -2; a = 5^e qr$ 表 3.33: $p = 5, m = -2; a = 5^e qr$

a	素因数分解	$\sigma(a)$
12905	$5^1 * 29 * 89$	16200
3661325	$5^2 * 137 * 1069$	4577460
22529978346875	$5^5 * 16189 * 445339$	28162473267600
465804347839109375	$5^6 * 78137 * 381528319$	582255435085032960
66707089798390625	$5^6 * 78233 * 54571009$	83383862288916540
14285072369594921875	$5^8 * 2215201 * 16508563$	17856340462006033768
6249195223516796875	$5^8 * 3215137 * 4975819$	7811494029399727960

表 3.34: $p = 5, m = 2; a = 5^e qr$

a	素因数分解	$\sigma(a)$
244917625	$5^3 * 853 * 2297$	306148752

表 3.35: $p = 5, m = -2; a = 5^e qr$

a	素因数分解	$\sigma(a)$
12905	$5^1 * 29 * 89$	16200
3661325	$5^2 * 137 * 1069$	4577460
22529978346875	$5^5 * 16189 * 445339$	28162473267600
465804347839109375	$5^6 * 78137 * 381528319$	582255435085032960
66707089798390625	$5^6 * 78233 * 54571009$	83383862288916540
14285072369594921875	$5^8 * 2215201 * 16508563$	17856340462006033768
6249195223516796875	$5^8 * 3215137 * 4975819$	7811494029399727960
5546067393132418478515625	$5^9 * 9765949 * 290764011289$	6932584241415741171153000
30068550191905103515625	$5^9 * 9826877 * 1566631769$	37585687739882554368360
766585572748771484375	$5^9 * 16727981 * 23463191$	958231965935981952864

表 3.36: $p = 5, m = -7; a = 5^e qr$

a	素因数分解	$\sigma(a)$
1604823625	$5^3 * 641 * 20029$	2006044560
3118158090625	$5^5 * 27241 * 36629$	3897697640760
6118684191916796875	$5^8 * 3365093 * 4654799$	7648355239899487200

3.13.2 $p = 7, m = 2; a = 7^e qr$ 表 3.37: $p = 7, m = 2; a = 7^e qr$

a	素因数分解	$\sigma(a)$
59171	$7 * 79 * 107$	69120
A	$7^8 * 43244809 * 603583009$	B

$$A = 150471866868680839759081$$

$$B = 175550511346794816038100$$

3.13.3 $p = 7, m = 3; a = 7^e qr$ 表 3.38: $p = 7, m = 3; a = 7^e qr$

a	素因数分解	$\sigma(a)$
147394439384689	$7^4 * 16879 * 3636991$	171960182312960
4412913789067	$7^4 * 20731 * 88657$	5148399494456
323545312034623637	$7^6 * 1475431 * 1863923$	377469530708614176

3.13.4 $p = 7, m = 4; a = 7^e qr$ 表 3.39: $p = 7, m = 4; a = 7^e qr$

a	素因数分解	$\sigma(a)$
64253	$7^1 * 67 * 137$	75072
44138857	$7^2 * 397 * 2269$	51497220
69612772327	$7^3 * 2467 * 82267$	81214969600

3.13.5 $p = 7, m = -1; a = 7^e qr$ 表 3.40: $p = 7, m = -1; a = 7^e qr$

a	素因数分解	$\sigma(a)$
64570497397	$7^3 * 2473 * 76123$	75332310400
19060639997	$7^3 * 2713 * 20483$	22237430400

表 3.41: $p = 7, m = -6; a = 7^e qr$

a	素因数分解	$\sigma(a)$
324579681723559549	$7^6 * 1458697 * 1891333$	378676295345728924

表 3.42: $p = 7, m = -7; a = 7^e qr$

a	素因数分解	$\sigma(a)$
69601	$7^1 * 61 * 163$	81344

第4章 P を底とする弱完全数

P を奇素数とし, $p = e + 1$ が素数のとき, $q = \frac{P^p - 1}{P}$ に関して $a = p^e q$ を P を底とする弱完全数という.

しかしながら $P = 2$ のときは $p = e + 1$ が素数の場合, $q = 2^p - 1$ に関して $a = p^e q$ を P を底とする弱完全数という.

数値例

4.0.6 $P = 2$

表 4.1: $P = 2$

p	$(2p + 1) =$	$2^p - 1 =$ 分解	a
3	(7)=7	(7)=7	28
5	(11)=11	(31)=31	496
7	(15)=3*5	(127)=127	8128
11	(23)=23	(2047)=23*89	2096128
13	(27) = 3 ³	(8191)=8191	33550336
17	(35)=5*7	(131071)=131071	8589869056
19	(39)=3*13	(524287)=524287	137438691328
23	(47)=47	(8388607)=47*178481	35184367894528
29	(59)=59	(536870911)=233*1103*2089	144115187807420416
31	(63)=3 ² * 7	(2147483647)=2147483647	2305843008139952128
37	(75)=3 * 5 ²	(137438953471)=223*616318177	9444732965670570950656
41	(83)=83	(2199023255551)=13367*164511353	2417851639228158837784576
43	(87)=3*29	(8796093022207)=431*9719*2099863	38685626227663735544086528
47	(95)=5*19	(140737488355327)=2351*4513*13264529	9903520314282971830448816128
53	(107)=107	(9007199254740991)=6361*69431*20394401	40564819207303336344294875201536

$$A = 166153499473114483824745506383331328$$

$$B = 2658455991569831744654692615953842176$$

$$C = 10889035741470030830754200461521744560128$$

$$D = (2361183241434822606847) = 228479 * 48544121 * 212885833$$

表 4.2: $P = 2$

p	$(2p+1)=$	$2^p - 1 =$ 分解	a
59	(119)=7*17	(576460752303423487)=179951*3203431780337	A
61	(123)=3*41	(2305843009213693951)=2305843009213693951	B
67	(135) = $3^3 * 5$	(147573952589676412927)=193707721*761838257287	C
71	(143)=11*13	D	E
73	(147)=3 * 7^2	F	G
79	(159)=3*53	I	J
83	(167)=167	K	L
89	(179)=179	M	N
97	(195)=3*5*13	O	P
101	(203)=7*29	Q	R
103	(207)= $3^2 * 23$	S	T
107	(215)=5*43	U	V
109	(219)=3*73	W	X
113	(227)=227	Y	Z
127	(255)=3*5*17	A1	B1
131	(263)=263	C1	D1

$$E = 2787593149816327892690784192460327776944128$$

$$F = (9444732965739290427391) = 439 * 2298041 * 9361973132609$$

$$G = 44601490397061246283066714178813853366747136$$

$$I = (604462909807314587353087) = 2687 * 202029703 * 1113491139767$$

$$J = 182687704666362864775460301858080473799697891328$$

$$K = (9671406556917033397649407) = 167 * 57912614113275649087721$$

$$L = 46768052394588893382517909811217778170473142550528$$

$$M = (618970019642690137449562111) = 618970019642690137449562111$$

$$N = 191561942608236107294793378084303638130997321548169216$$

$$O = (158456325028528675187087900671) = 11447 * 13842607235828485645766393$$

$$P = 12554203470773361527671578846336104669690446551334525075456$$

$$Q = (2535301200456458802993406410751) = 7432339208719 * 341117531003194129$$

$$R = 3213876088517980551083924184681057554444177758164088967397376$$

$$S = (10141204801825835211973625643007) = 2550183799 * 3976656429941438590393$$

$$T = 51422017416287688817342786954912132678309582883443383916822528$$

$$U = (162259276829213363391578010288127) = 162259276829213363391578010288127$$

$$V = 13164036458569648337239753460458722910223472318386943117783728128$$

$$W = (649037107316853453566312041152511) = 745988807 * 870035986098720987332873$$

$$X = 210624583337114373395836055367340540119236532374371439352601378816$$

$$Y = (10384593717069655257060992658440191) = 3391 * 23279 * 65993 * 1868569 * 1066818132868207$$

$$Z = 53919893334301279589334030174039256154977430310253516431710891278336$$

$$A1 = (170141183460469231731687303715884105727) = 170141183460469231731687303715884105727$$

$$B1 = 14474011154664524427946373126085988481573677491474835889066354349131199152128$$

$$C1 = (2722258935367507707706996859454145691647) = 263 * 10350794431055162386718619237468234569$$

$$D1 = 3705346855594118253554271520278013051303278379832814295408789189823493075632128$$

4.0.7 末尾の数

弱完全数でも末尾の数が 6, 8 は同様に成立する. $q = 2^p - 1$ は素数でなくても 末尾の数が 7, 1 は同様に成立する.

しかし, $q = 2^p - 1$ が合成数の解き, 各素因子の末尾の数はさまざまである. 素因子の数が 2 個の場合, Q_1, Q_2 とおく.

$q = Q_1 Q_2$ の末尾の数が 1, 7 なら可能性は絞られる.

- q の末尾の数 1 なら (3,7), (9,9)
- q の末尾の数 7 なら (1,7), (3,9)

$q = Q_1 Q_2 Q_3$ の末尾の数が 1, 7 ならどんな可能性があり例と対応させて調べるとよい.

表 4.3: mod10 での乗算表

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

4.0.8 $P = 3$

表 4.4: $P = 3$

p	$(2p+1)=$	$\frac{P^p-1}{P} =$ 分解	a
5	(11)=11	(121)=11 ²	9801
7	(15)=3*5	(1093)=1093	796797
11	(23)=23	(88573)=23*3851	5230147077
13	(27)=3 ³	(797161)=797161	423644039001
17	(35)=5*7	(64570081)=1871*34511	2779530261754401
19	(39)=3*13	(581130733)=1597*363889	225141952751788437
23	(47)=47	(47071589413)=47*1001523179	1477156353259726319517
29	(59)=59	(34315188682441)=59*28537*20381027	785021449541029367424039801
31	(63)=3 ² * 7	(308836698141973)=683*102673*4404047	63586737412824202325875602477
37	(75)=3 * 5 ²	(225141952945498681)=13097927*17189128703	A
41	(83)=83	(18236498188585393201)=83*2526913*86950696619	B
43	(87)=3*29	C	D
47	(95)=5*19	E	F

$$A = 33792599317408761542712904163659401$$

$$B = 221713244121518884968045982580046482001$$

$$C = (164128483697268538813) = 431 * 380808546861411923$$

$$D = 17958772773843029682849400545509814478917$$

$$E = (13294407179478751643893) = 1223 * 21997 * 5112661 * 96656723$$

$$F = 117827508169184117749529434503875992840011597$$

$$G = (9691622833840009948398361) = 107 * 24169 * 3747607031112307667$$

$$H = 62618368768939376720930024035982040019969414457001$$

$$I = (7065193045869367252382405533) = 14425532687 * 489769993189671059$$

$$J = 33277968516933911303947774618193177127885685499906811237$$

$$K = (63586737412824305271441649801) = 603901 * 105293313660391861035901$$

$$L = 2695515449871646815619769744243211980459605339549629443001$$

$$M = (46354731573948918542880962705293) = 221101 * 441019876741 * 475384700124973$$

$$N = 1432507426195237855339786052661605566302711392155333734434378997$$

$$O = (3754733257489862401973357979128773) = 3754733257489862401973357979128773$$

$$P = 9398681223266955568884336291512894246732289173595197254503404033277$$

$$Q = (33792599317408761617760221812158961) = 11243*20149*15768033143*9460375336977361$$

$$R = 761293179084623401079631239612544524098913602817908624975367225786001$$

表 4.5: $P = 3$

p	$(2p + 1)=$	$\frac{P^p-1}{P} =$ 分解	a
53	(107)=107	G	H
59	(119)=7*17	I	J
61	(123)=3*41	K	L
67	(135)=3 ³ * 5	M	N
71	(143)=11*13	O	P
73	(147)=3 * 7 ²	Q	R
79	(159)=3*53	S	T
83	(167)=167	U	V
89	(179)=179	W	X
97	(195)=3*5*13	Y	Z
101	(203)=7*29	$A1$	$B1$
103	(207)=3 ² * 23	$C1$	$D1$
107	(215)=5*43	$E1$	$F1$
109	(219)=3*73	$G1$	$H1$
113	(227)=227	$I1$	$J1$
127	(255)=3*5*17	$K1$	$L1$
131	(263)=263	$M1$	$N1$

$S = (24634804902390987219347201701063882933) = 432853009*392038110671*145171177264407947$
 $T = 404582408385911344893160305610930280409696733642031742793788413297107082637$
 $U = (1995419197093669964767123337786174517613) = 167*12119*1036745531*950996059627210897943351$
 $V = 2654465181419964333844024765113313569821231448014534796863835735316617556317717$
 $W = (1454660594681285404315232913246121223340241)$
 $= 179 * 1611479891519807 * 5042939439565996049162197$
 $X = 1410691630479007265542402365196584476859718059601935045571560890199346276163907738801$
 $Y = (9544028161703913537712243143807801346335324481)$
 $= 76631 * 2549755542947 * 48845962828028421155731228333$
 $Z = 60725649034264922116776708284357482128311260319954115892732202972361234658808964021817054401$
 $A1 = (773066281098016996554691694648431909053161283001)$
 $= 33034273 * 465092326319 * 50316775668019759306202964023$
 $B1 = 3984209833138121540081719830536694402438501789798340552014964369431205057870704638552259948050$
 $C1 = (6957596529882152968992225251835887181478451547013)$
 $= 6957596529882152968992225251835887181478451547013$
 $D1 = 3227209964841878447466193062734722465975186449738511206206756380031007356942426993809058144999$
 $E1 = (563565318920454390488370245398706861699754575308093) =$
 $50077 * 229837 * 48965028505045123993421250406516036571557$

$$\begin{aligned}
F1 &= 211737245793275644938256926846[42\text{digits}]895536600580124298348772633797 \\
G1 &= (5072087870284089514395332208588361755297791177772841) \\
&= 1091 * 521402591 * 3499901929 * 239789806103 * 10624346875389299603 \\
H1 &= 171507169092553272399988110745[44\text{digits}]424354215954748960360390731801 \\
I1 &= (410839117493011250666021908895657302179121085399600161) \\
&= 227 * 1583 * 2172539 * 526256453012063980796131127321354599535039 \\
J1 &= 112525853641624202021632199459[48\text{digits}]758561740499372153467580684001 \\
K1 &= (1965030762956430528586812143568753110946368598712640184849493) \\
&= 5843 * 681229 * 21520151 * 76082653 * 301515315752300874236564235591357673 \\
L1 &= 257423059957675431046184790351[61\text{digits}]973215046058831272463436521197 \\
M1 &= (159167491799470872815531783629069001986655856495723854972808973) \\
&= 263 * 605199588591144003100881306574406851660288427740394885828171 \\
N1 &= 168895269638230850309401840949[65\text{digits}]983561348165197935406290479477
\end{aligned}$$

4.0.9 末尾の数

3 を底とする完全数では次が成り立つ.

- $e \equiv 2 \pmod{4}$ のとき q の末尾の数は 3, a の末尾の数は 7.
- $e \equiv 0 \pmod{4}$ のとき q の末尾の数は 1, a の末尾の数は 1.

弱完全数でも a の末尾の数が 7, 1 は同様に成立する. $q = \frac{3^p-1}{2}$ は素数でなくても 末尾の数が 3, 1 は同様に成立する.

しかし, q が合成数の解き, 各素因子の末尾の数はさまざまである. 素因子の数が 2 個の場合, Q_1, Q_2 とおく.

$q = Q_1 Q_2$ の末尾の数が 1, 7 なら可能性は絞られる.

- q の末尾の数 1 なら (3,7), (9,9)
- q の末尾の数 7 なら (1,7), (3,9)

$q = Q_1 Q_2 Q_3$ の末尾の数が 1, 7 ならどんな可能性があり例と対応させて調べるとよい.

4.0.10 $P = 5$

表 4.6: $P = 5$

p	$(2p + 1) =$	$\frac{P^p - 1}{P} =$ 分解	a
5	(11)=11	(781)=11*71	488125
7	(15)=3*5	(19531)=19531	305171875
11	(23)=23	(12207031)=12207031	119209287109375
13	(27)=3 ³	(305175781)=305175781	74505805908203125
17	(35)=5*7	(190734863281)=409*466344409	29103830456695556640625
19	(39)=3*13	(4768371582031)=191*6271*3981071	A
23	(47)=47	B	C
29	(59)=59	D	E
31	(63)=3 ² * 7	F	G

表 4.7: $P = 5$

p	$(2p + 1) =$	$(P^p - 1) =$ 分解	a
37	(75)=3 * 5 ²	H	I
41	(83)=83	J	K
43	(87)=3*29	L	M
47	(95)=5*19	N	O
53	(107)=107	P	Q
59	(119)=7*17	R	S
61	(123)=3*41	T	U
67	(135)=3 ³ * 5	V	W
71	(143)=11*13	X	
73	(147)=3 * 7 ²	Z	$A1$
79	(159)=3*53	$B1$	$C1$

$$A = 18189894035457611083984375$$

$$B = (2980232238769531) = 8971 * 332207361361$$

$$C = 7105427357601001262664794921875$$

$$D = (46566128730773925781) = 59 * 35671 * 22125996444329$$

$$E = 1734723475976807094402611255645751953125$$

$$F = (1164153218269348144531) = 1861 * 625552508473588471$$

$$G = 1084202172485504434007219970226287841796875$$

$$H = (18189894035458564758300781) = 149 * 13971969971 * 8737481256739$$

$$\begin{aligned}
I &= 264697796016968855958850777824409306049346923828125 \\
J &= (11368683772161602973937988281) = 2238236249 * 5079304643216687969 \\
K &= 103397576569128459358926086506471619941294193267822265625 \\
L &= (284217094304040074348449707031) = 1644512641 * 172827552198815888791 \\
M &= 64623485355705287099328804067909004515968263149261474609375 \\
N &= (177635683940025046467781066894531) \\
&= 177635683940025046467781066894531 \\
O &= 25243548967072377773175314089049123822405817918479442596435546875 \\
P &= (2775557561562891351059079170227050781) \\
&= 5960555749 * 17154094481 * 27145365052629449 \\
Q &= 6162975822039154729779129416271767418766813761976663954555988311767578125 \\
R &= (43368086899420177360298112034797668457031) = 21180247636732981*2047572230657338751575051 \\
S &= 1504632769052528010199982767644474467607883239050892143495730124413967132568359375 \\
T &= (1084202172485504434007452800869941711425781) = 8419*918585913061*140194179307171898833699259 \\
U &= 94039548065783000637498922977796542254932228577235520106114563532173633575439453125 \\
V &= (16940658945086006781366450013592839241027832031) \\
&= 269 * 1609 * 26399 * 2454335007529 * 604088623657497125653141 \\
W &= 229588740394978028900143854926219858948958116553660212255660866276230080984532833099365234375 \\
X &= (10587911840678754238354031258495524525642395019531) \\
&= 569 * 18607929421228039083223253529869111644362732899 \\
Y &= 896831017167882925391186933305546324019367642800948918100842344180989584856433793902397155761718 \\
Z &= (264697796016968855958850781462388113141059875488281) \\
&= 4853479 * 5729041 * 9519524151770349914726200576714027279 \\
A1 &= 560519385729926828369491833315[41digits]537278131581842899322509765625 \\
B1 &= (4135903062765138374357043460349814267829060554504394531) \\
&= 205367807127911 * 58523123221688392679 * 344120456368919234899 \\
C1 &= 136845553156720417082395467118[50digits]744322988204658031463623046875
\end{aligned}$$

4.0.11 末尾の数

$a \equiv 25, 75 \pmod{100}$ は成り立つ.

4.0.12 $P = 7$ 表 4.8: $P = 7$

p	$(2p + 1) =$	$(P^p - 1) =$ 分解	a
3	(7)=7	(57)=3*19	2793
5	(11)=11	(2801)=2801	6725201
7	(15)=3*5	(137257)=29*4733	16148148793
11	(23)=23	(329554457)=1123*293459	93090977300134793
13	(27)=3 ³	(16148168401)=16148168401	223511436608353935601
17	(35)=5*7	(38771752331201)=14009*2767631689	1288498953284568548534420801
19	(39)=3*13	(1899815864228857)=419*4534166740403	3093685986836262112339927626793

表 4.9: $P = 7$

p	$(2p + 1) =$	$(P^p - 1) =$ 分解	a
23	$(47) = 47$	$(4561457890013486057) = 47 * 3083 * 31479823396757$	A
29	$(59) = 59$	$(536650959302196621139601) = 59 * 127540261 * 71316922984999$	B
31	$(63) = 3^2 * 7$	C	D
37	$(75) = 3 * 5^2$	E	F
41	$(83) = 83$	G	H
43	$(87) = 3 * 29$	I	J
47	$(95) = 5 * 19$	K	L
53	$(107) = 107$	M	N
59	$(119) = 7 * 17$	O	P
61	$(123) = 3 * 41$	Q	R
67	$(135) = 3^3 * 5$	S	T
71	$(143) = 11 * 13$	U	V
73	$(147) = 3 * 7^2$	W	X

$A = 17834484070599672225407746556059132793$
 $B = 246852216102829623577350845421202364881743396401$
 $C = (26295897005807634435840457) = 311 * 21143 * 3999088279399464409$
 $D = 592692170862893926209219560171029203619130597664793$
 $E = (3093685986836262383742193945201) = 223 * 2887 * 4805345109492315767981401$
 $F = 8203622558697478826660309198389254312666780494848270305646801$
 $G = (7427940054393865983365007662428001) = 83 * 20515909 * 4362139336229068656094783$
 $H = 47292251530001784637410177127186118373220132474676100080318673652001$
 $I = (363969062665299433184885375458972057) = 166003607842448777 * 2192537062271178641$
 $J = 113548695923534284914421835282373872709889396348036286703487710014262793$
 $K = (873889719459383939076909786476991909257)$
 $= 13722816749522711 * 63681511996418550459487$
 $L = 654585635808686369208943910457664184071462434342630427022350295255757960808793$
 $M = (102812251604677061048459359469231621132196401)$
 $= 8269 * 319591 * 38904276017035188056372051839841219$
 $N = 9060307782877217926754915842544557323346169012644208670628797275051$
 070279034171965187601
 $O = (12095758589038651555290195182195630994581774400857)$
 $= 459257 * 134927809 * 550413361 * 354639323684545612988577649$
 $P = 1254063221522591234440805721152441125518421478503867792800074932$
 $27585324645254553813463672815486793$
 $Q = (592692170862893926209219563927585918734506945642001)$
 $= 367 * 4759 * 177237331 * 1914662449813727660680530326064591907$
 $R = 301100579487574155389237453648[42digits]978837401438140457906182478001$
 $S = (69729641209848607524588472476516555753196007647835795257)$
 $= 228337 * 147300841 * 206244761 * 10052011757370829033540932021825161$
 $T = 416761959707504329552743754033[52digits]988654120686252470466511138793$
 $U = (167420868544846506666536922416116250363423614362453744412457)$
 $= 990643452963163 * 169002145064468556765676975247413756542145739$
 $V = 240254976208378066650998674599[59digits]692282259881493512306080724793$
 $W = (8203622558697478826660309198389696267807757103760233476210401)$
 $= 439 * 3675989 * 359390389 * 1958423494433591 * 7222605228105536202757606969$
 $X = 576852197876315738029047817714[62digits]229828085800348831357942813601$

4.1 フェルマーとオイラーの結果

底が奇素数 P で,

$q = \frac{P^p - 1}{P}$ の素数因子 (奇数) Q について $P - 1 \not\equiv 0 \pmod{Q}$ かつ

$$P^p \equiv 1 \pmod{Q}$$

ならば $\text{mod } Q$ で P の位数は素数 p である. $P \neq Q$ により, フェルマーの小定理によれば $P^{Q-1} \equiv 1 \pmod{Q}$ なので $Q-1$ は位数 p で割れるので

$Q-1 = kp$ と書けるが Q, p はともに奇数なので k は偶数.

$Q = 1 + 2k'p$ と書ける. オイラーの基準によって

$$P^{\frac{Q-1}{2}} = \left(\frac{P}{Q}\right)$$

$P^{\frac{Q-1}{2}} = P^{pk'} = 1$. ゆえに

$$\left(\frac{P}{Q}\right) = 1.$$

逆に素数 $Q = 2p + 1$ が素数 (p : Sophie Germain) とする. さらに $P - 1 \not\equiv 0 \pmod{Q}$ かつ $\left(\frac{P}{Q}\right) = 1$ を仮定すると, $P \equiv n^2 \pmod{Q}$ を満たす n がある.

$$P^p = P^{\frac{Q-1}{2}} \equiv n^{Q-1} \equiv 1 \pmod{Q}$$

これより, 素因子 Q は $P^p - 1$ の素因子になる. $P - 1 \not\equiv 0 \pmod{Q}$ を仮定しているので Q は $q = \frac{P^p - 1}{P - 1}$ の素数因子.

4.1.1 実例

$p = 73, W = 439 * 3675989 * 359390389 * 1958423494433591 * 7222605228105536202757606969$ について

```
1 ?- B=439, A is B-1, factorize(A,S),exps(S,SX).
SX = [2, 3, 73].
```

```
2 ?- B=3675989, A is B-1, factorize(A,S),exps(S,SX).
SX = [2^2, 73, 12589].
```

```
3 ?- B=3675989, A is B-1, factorize(A,S),exps(S,SX).
SX = [2^2, 73, 12589].
```

```
4 ?- B=359390389, A is B-1, factorize(A,S),exps(S,SX).
SX = [2^2, 3, 7, 29, 43, 47, 73].
```

```
5 ?- B=1958423494433591, A is B-1, factorize(A,S),exps(S,SX).
SX = [2, 5, 73, 2682771910183].
```

第5章 P を底とするフェルマーの完全数

P を奇素数とし $E > 0$ について $Q = P^E + 1$ とおく. これは偶数なので $L_E = \frac{Q}{2}$ 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, $L_E = \frac{Q}{2} = 2L'$ とすると $Q = 4L'$ なので

$$Q = P^E + 1 = 4L' \equiv 0 \pmod{4}.$$

ゆえに, $P^E \equiv -1$.

一方, $P = 2k + 1$ とおくと

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

これで前の式に矛盾した.

$E = 2^m$ 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ー数と理解する. ただし, $P = 2$ のとき $L_m = F_m = P^E + 1, E = 2^m$ とおく.

$a_m = P^{2^m - 1} L_m$ を P を底とするフェルマーの弱完全数と理解する.

L_m が素数の場合なら, a_m を P を底とするフェルマーの完全数と呼ぶ.

フェルマーの弱完全数はフェルマーの完全数に比べて豊富な例を持っている. しかも, フェルマー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.

5.1 オイラーの結果の一般化

L_E は奇数なのでその素因子を Q とおくと

$$P^E + 1 = 2L_E \equiv 0 \pmod{Q}.$$

$E = 2^m$ によって

$$P^E = P^{2^m} \equiv -1 \pmod{Q}.$$

ゆえに

$$(P^E)^2 = P^{2^{m+1}} \equiv 1 \pmod{Q}.$$

Q を法とすると P の位数は 2^{m+1} 以下であるが $P^E = P^{2^m} \equiv -1$ によって 2^m より大なので, P の位数は 2^{m+1} .

$P^E = P^{2^m} \equiv -1 \pmod{Q}$ により $Q \neq P$. フェルマーの小定理によって
 $P^{Q-1} \equiv 1 \pmod{Q}$. $Q-1$ は位数 2^{m+1} の倍数なので, $Q-1 = 2^{m+1}K$.
この結果は $P=2$ のときオイラーによる.
 $\frac{Q-1}{2} = 2^m K$ によれば

$$p^{\frac{Q-1}{2}} = p^{2^m K} \equiv (-1)^K \pmod{Q}.$$

オイラーの基準にしたがい

$$\left(\frac{p}{Q}\right) = p^{\frac{Q-1}{2}} \equiv (-1)^K \pmod{Q}.$$

5.2 例

5.2.1 $P = 2$

表 5.1: $P = 2$

m	2^m	$2^{2^m} + 1$	素因数分解
0	1	3	3
1	2	5	5
2	4	17	17
3	8	257	257
4	16	65537	65537
5	32	4294967297	$641 * 6700417$
6	64	18446744073709551617	$274177 * 67280421310721$
7	128	A	B
8	256	--	C

$$A = 340282366920938463463374607431768211457$$

$$B = 59649589127497217 * 5704689200685129054721$$

$$C = 1238926361552897 * 9346163971535797769163558199606896584051237541638188580280321$$

$m = 5, 6, 7, 8$ について, F_m の各素因子 Q について $Q - 1$ の素因数分解を行う.

表 5.2: 素因子 Q

m	Q	$Q - 1$	素因数分解
5	641	640	$[2^7, 5]$
5	6700417	6700416	$[2^7, 3, 17449]$
6	274177	274176	$[2^8, 3^2, 7, 17]$
6	67280421310721	67280421310720	$[2^8, 5, 47, 373, 2998279]$
7	59649589127497217	59649589127497216	A

$$A = [2^9, 116503103764643]$$

$m = 0, 1, 2, 3, 4$ のときのみ素数 (フェルマー素数)

5.2.2 $P = 3$ 表 5.3: $P = 3$

m	2^m	$2L_E$	素因数分解
1	2	10	$2 * 5$
2	4	82	$2 * 41$
3	8	6562	$2 * 17 * 193$
4	16	43046722	$2 * 21523361$
5	32	1853020188851842	$2 * 926510094425921$
6	64	3433683820292512484657849089282	$2 * 1716841910146256242328924544641$
7	128	A	B

$A = 11790184577738583171520872861412518665678211592275841109096962$

$B = 2 * 257 * 275201 * 138424618868737 * 3913786281514524929 * 153849834853910661121$

?- A is 17, B is A-1, factorize(B,C), exps(C,D).

A = 17,

D = [2^4].

?- A is 193, B is A-1, factorize(B,C), exps(C,D).

A = 193,

D = [2^6, 3].

?- A is 257-1, factorize(A,B), exps(B,C).

A = 256,

C = [2^8].

?- A is 275201-1, factorize(A,B), exps(B,C).

A = 275200,

C = [2^8, 5^2, 43].

?- A is 138424618868737-1, factorize(A,B), exps(B,C).

A = 138424618868736,

C = [2^13, 3, 2131, 2643131].

?- A is 3913786281514524929-1, factorize(A,B), exps(B,C).

A = 3913786281514524928,

C = [2^8, 31, 787, 3919, 159898891].

?- A is 153849834853910661121-1, factorize(A,B), exps(B,C).

A = 153849834853910661120,

C = [2^11, 3, 5, 433, 19801, 584118287].

これらは数値例とはいえ、実に見事な美しい結果である。

5.2.3 $P = 5$

表 5.4: $P = 5$

m	2^m	$2L_E$	素因数分解
1	2	26	$2 * 13$
2	4	626	$2 * 313$
3	8	390626	$2 * 17 * 11489$
4	16	152587890626	$2 * 2593 * 29423041$
5	32	23283064365386962890626	$2 * 641 * 75068993 * 241931001601$
6	64	A	$2 * B$

$A = 542101086242752217003726400434970855712890626$

$B = 769 * 3666499598977 * 96132956782643741951225664001$

$$m = 3, m + 1 = 4, 2^4 = 16.$$

```
13 ?- A is 17,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
17,16,[2^4]
A = 17,
B = 16,
D = [2^4].
```

```
8 ?- A is 11489,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
11489,11488,[2^5,359]
A = 11489,
B = 11488,
D = [2^5, 359].
```

```
9 ?- A is 2593,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
2593,2592,[2^5,3^4]
A = 2593,
B = 2592,
C = [2, 2, 2, 2, 2, 3, 3, 3, 3],
D = [2^5, 3^4].
```

```
10 ?- A is 641,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
641,640,[2^7,5]
A = 641,
B = 640,
C = [2, 2, 2, 2, 2, 2, 2, 5],
D = [2^7, 5].
```

```
11 ?- A is 75068993,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
75068993,75068992,[2^6,1172953]
A = 75068993,
B = 75068992,
C = [2, 2, 2, 2, 2, 2, 1172953],
D = [2^6, 1172953].
```

```
12 ?- A is 241931001601,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
241931001601,241931001600,[2^8,3^2,5^2,23,182617]
A = 241931001601,
B = 241931001600,
C = [2, 2, 2, 2, 2, 2, 2, 2, 3|...],
D = [2^8, 3^2, 5^2, 23, 182617].
```

5.2.4 $P = 7$

表 5.5: $P = 7$

m	2^m	$2L_E$	素因数分解
1	2	50	$2 * 5^2$
2	4	2402	$2 * 1201$
3	8	5764802	$2 * 17 * 169553$
4	16	33232930569602	$2 * 353 * 47072139617$
5	32	1104427674243920646305299202	$2 * 7699649 * 134818753 * 531968664833$
6	64	A	$2 * B$

$$A = 1219760487635835700138573862562971820755615294131238402$$

$$B = 35969 * 1110623386241 * 15266848196793556098085000332888634369$$

```
14 ?- A is 353,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
353,352,[2^5,11]
A = 353,
B = 352,
D = [2^5, 11].
```

```
15 ?- A is 47072139617,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
47072139617,47072139616,[2^5,67,1847,11887]
A = 47072139617,
B = 47072139616,
D = [2^5, 67, 1847, 11887].
```

```
16 ?- A is 7699649,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
7699649,7699648,[2^6,11,10937]
A = 7699649,
B = 7699648,
D = [2^6, 11, 10937].
```

5.2.5 $P = 11$

$$A = 2 * 193 * 257 * 21283620033217629539178799361$$

$$B = 4457915684525902395869512133369841539490161434991526715513934826242$$

$$C = 2 * 316955440822738177 * 7032401262704707649518767703756385761576062060673$$

```
17 ?- A is 6304673,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

表 5.6: $P = 11$

m	2^m	$2L_E$	素因数分解
1	2	122	$2 * 61$
2	4	14642	$2 * 7321$
3	8	214358882	$2 * 17 * 6304673$
4	16	45949729863572162	$2 * 51329 * 447600088289$
5	32	2111377674535255285545615254209922	A
6	64	B	C

6304673,6304672,[2^5,11,17911]

A = 6304673,

B = 6304672,

D = [2^5, 11, 17911].

18 ?- A is 51329,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

51329,51328,[2^7,401]

A = 51329,

B = 51328,

D = [2^7, 401].

19 ?- A is 447600088289,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

447600088289,447600088288,[2^5,127,110137817]

A = 447600088289,

B = 447600088288,

D = [2^5, 127, 110137817].

?- A=17,B is A-1,factorize(B,C),exps(C,D).

A = 17,

B = 16,

D = [2⁴].

?- A=11489,B is A-1,factorize(B,C),exps(C,D).

A = 11489,

B = 11488,

D = [2⁵, 359].

?- A=2593,B is A-1,factorize(B,C),exps(C,D).

A = 2593,

B = 2592,

D = [2⁵, 3⁴].

?- A=29423041,B is A-1,factorize(B,C),exps(C,D).

A = 29423041,

B = 29423040,

D = [2⁶, 3, 5, 30649].

?- A=641,B is A-1,factorize(B,C),exps(C,D).

A = 641,

B = 640,

D = [2⁷, 5].

?- A=75068993,B is A-1,factorize(B,C),exps(C,D).

A = 75068993,

B = 75068992,

D = [2⁶, 1172953].

?- A=241931001601,B is A-1,factorize(B,C),exps(C,D).

A = 241931001601,

B = 241931001600,

D = [2⁸, 3², 5², 23, 182617].

5.3 フェルマーの完全数の方程式

$e = 2^m - 1$ とおき, $q = \frac{P^{e+1}-1}{2}$ は素数とする. $a = P^e q$ は P を底とするフェルマーの完全数である.

これの満たす方程式を求める.

$e = 2^m - 1$ とおき, $q = \frac{P^{e+1}-1}{2}$ は素数とする. $a = P^e q$ は P を底とするフェルマーの完全数である.

これの満たす方程式を求める.

$P^{e+1} + 1 = 2q$ により, $2q + 2 = P^{e+1} + 3$. さらに $\sigma(a) = \frac{P^{e+1}-1}{P}(q+1)$ によって

$$\begin{aligned}\bar{P}\sigma(a) &= (P^{e+1} - 1)(q + 1) \\ &= (2q - 2)(q + 1) \\ &= 2q(q + 1) - 2(q + 1) \\ &= q(P^{e+1} + 3) - 2(q + 1) \\ &= qP^{e+1} + q - 2 \\ &= aP + q - 2.\end{aligned}$$

よって,

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

$\bar{P}\sigma(a) - aP = \text{Maxp}(a) - 2$ が P を底とするフェルマーの完全数の方程式である.

5.4 例

5.4.1 $P = 3$ のとき

$P = 3$ のとき $2\sigma(a) - 3P = \text{Maxp}(a) - 2$ が 3 を底とするフェルマーの完全数の方程式である.

この方程式の完全な解を得たい. これは無理であろう.

さらに多くの解を得るため

$a = 3^e q r$ の解を探すことが策のひとつ.

$s(a) = 2$ に限ると, $a = 15 = 3 * 5, a = 1107 = 3^3 * 41$ の 2 例のみ.

さらに多くの解を得るため

$a = 3^e q r$ の解を探すことが策のひとつだが $a = 14883 = 3 * 11^2 * 41$ 解がすでにある. 事態は複雑怪奇なのだ.

5.4.2 $P = 5$ のとき

$P = 5$ のとき $4\sigma(a) - 5P = \text{Maxp}(a) - 2$ が 5 を底とするフェルマーの完全数の方程式である.

$s(a) = 2$ に限ると, $a = 65 = 5 * 13, a = 39125 = 5^3 * 313$ の 2 例のみ.

表 5.7: $P = 3$

a	素因数分解
15	$3 * 5$
741	$3 * 13 * 19$
1107	$3^3 * 41$
14883	$3 * 11^2 * 41$
38781	$3^2 * 31 * 139$

表 5.8: $p = 5$

a	素因数分解
65	$5 * 13$
14861	$7 * 11 * 193$
39125	$5^3 * 313$

表 5.9: $p = 7$

a	素因数分解
411943	$7^3 * 1201$

表 5.10: $P = 11$

a	素因数分解
671	$11 * 61$
861773	$11 * 157 * 499$

表 5.11: $p = 19$

a	素因数分解
3439	$19 * 181$

5.5 $a = P^e qr$ の解

$\bar{P}\sigma(a) - aP = \text{Maxp}(a) - 2$ の解 $a = P^e qr$ があるとする.

$$(P^{e+1} - 1)\tilde{q}\tilde{r} - P^{e+1}qr = r - 2$$

を得るので $\Gamma = P^{e+1} - 1, \Delta = q + r$ を用いると

$$\Gamma(qr + \Delta + 1) - (\Gamma + 1)qr = r - 2.$$

これより, $\Delta' = \tilde{q} + r = \Delta + 1$ によって

$$\Gamma\Delta' = \tilde{q}r - 2.$$

$\tilde{q}_0 = \tilde{q} - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + 2$ によれば

$$\tilde{q}_0 r_0 = D.$$

これによって, 与えられた $\Gamma = P^{e+1} - 1$ について, D の因子分解 $\tilde{q}_0 r_0$ を求め $q = \tilde{q}_0 - 1 + \Gamma, r = r_0 + \Gamma$ がともに素数なら $a = P^e qr$ が解である.

その結果, 得られた解は $P = 3$ のときの と $P = 11$ のときの だけだった. 少し残念である.

表 5.12: $P = 3$

a	素因数分解
741	$3^1 * 13 * 19$
38781	$3^2 * 31 * 139$
4954286665155815901	$3^1 * 536917 * 52088299$

表 5.13: $P = 11$

a	素因数分解
861773	$11^1 * 157 * 499$
18850718310561181	$11^4 * 164431 * 7830211$

第6章 P を底とする概完全数

6.1 $P = 5$ の場合

P を素数とし $E > 0$ について $a = P^E$ とおくと $\sigma(a) = \sigma(P^E) = \frac{aP-1}{P}$ によって

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

これが $a = P^E$ に関する方程式である.

この解 P を 3 を底とする概完全数という.

$P = 5$ については $4\sigma(a) - 5a = -1$ となる.

$a \leq 20000$ についてパソコンで計算して表を作る.

表 6.1: $4\sigma(a) - 5a = -1$

a	$\sigma(a)$	素因数分解
5	6	[5]
25	31	[5 ²]
77	96	[7, 11]
125	156	[5 ³]
625	781	[5 ⁴]
3125	3906	[5 ⁵]
15625	19531	[5 ⁶]
390625	488281	[5 ⁷]

$s(a) = 1$ を期待していたところに $s(a) = 2$ の例が出てきた.

6.1.1 $s(a) = 2$ のときの証明

方程式 $4\sigma(a) - 5a = -1$ の解を $s(a) = 2$ のときに求めよう.

a を素因数分解し $a = p^e q^f$ ($2 < p < q$) とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\bar{p}\bar{q}}$$

であり, $A = pX - 1, B = qY - 1, \rho' = \bar{p}\bar{q}$ とおけば

$$\frac{4AB}{\rho'} = 5XY - 1.$$

書き直して

$$4AB = 5\rho'XY - \rho'.$$

$4AB - 5\rho'XY$ の XY の係数を R とおけば

$$R = 4pq - 5\rho' = 20 - (p-5)(q-5).$$

$-\rho' + 4(pX + qY - 1) = RXY$ によって $R > 0$. $0 < R = 20 - (p-5)(q-5)$ により 次の場合がある.

$$(1) p = 5, R = 20. \rho' = 4\bar{q},$$

$$(2) p = 3, R = 30 + 2q. \rho' = 2\bar{q},$$

$$(3) p = 7, R = 30 - 2q; q = 11, 13. \rho' = 6\bar{q}.$$

次の基本等式

$$RXY - 4(pX + qY - 1) = -\rho'$$

を各場合ごとに調べる.

1. $p = 5, R = 20. \rho' = 4\bar{q}$ の場合.

基本等式を 4 で割って

$$5XY - (5X + qY - 1) = -\bar{q}.$$

$(5X - q)Y - 5X = -\bar{q} - 1 = q$ により

$$(5X - q)(Y - 1) = 0.$$

よって $5X = 5^{f+1} = q$ となり矛盾.

2. $p = 3, R = 30 + 2q. \rho' = 2\bar{q}.$

$R_1 = R/2 = 5 + q$ とおくと

$$R_1XY - 2(3X + qY - 1) = -\bar{q}.$$

変形して

$$(R_1X - 2q)Y = 6X - q - 1.$$

$Y = q$ のとき,

$(R_1X - 2q)q = 6X - q - 1$ によって $X \geq 3$ により

$$(R_1q - 6)X = 2q^2 - q - 1 \geq 3(5 + q)q - 6q = 3q^2 + 15q - 6q = 3q^2 + 9q.$$

これから矛盾が出る.

$Y \geq q^2$ のとき,

$$(R_1X - 2q)Y = 6X - q - 1 \geq (R_1X - 2q)q^2 = ((5+q)X - 2q)q^2 = (5+q)Xq^2 - 2q^3.$$

$$2q^3 - q - 1 \geq 3((5+q)q^2 - 6) = 3q^3 + 15q^2 - 18.$$

これから矛盾が出る.

3. $p = 7, R = 30 - 2q; q = 11, 13; \rho' = 6\bar{q}$.

$$R_1XY - 2(7X + qY - 1) = -3\bar{q}.$$

$q = 11$ のとき, $R_1 = 4$.

$$4XY - 2(7X + 11Y - 1) = -30.$$

$4XY - 2(7X + 11Y) = -32$ を変形して

$$2(2X - 11)Y = 14X - 32 = 7(2X - 11) - 32 = 7(2X - 11) + 45.$$

$(2X - 11)(2Y - 7) = 45$ の解として $2X - 11 = 3, 2Y - 7 = 15$ があり, $X = 7, Y = 11$. ここで $a = 77$. かくして 5 のべきでない解が発見された.

$q = 13$ のとき, $R_1 = 2$.

$$XY - (7X + 13Y) = -25.$$

$(X - 7)(Y - 13) = 91 - 25 = 65$. しかし, X, Y は奇数なので $X - 7, Y - 13$ はともに偶数で矛盾. したがって $s(a) = 2$ のとき $a = 77$.

しかしながら $s(a) = 3$ の解がまだある可能性が残る.

6.2 $p = 7$ の場合

$6\sigma(a) - 7a = -1$ が方程式である.

$a = 5^e$ のときあったような $a = pq$ 型の解がなく $s(a) = 3$ の解 [7, 61, 229] が出ている. これは不思議なことではないか.

表 6.2: $6\sigma(a) - 7a = -1$

a	$\sigma(a)$	素因数分解
7	8	[7]
49	57	[7 ²]
343	400	[7 ³]
2401	2801	[7 ⁴]
16807	19608	[7 ⁵]
97783	114080	[7, 61, 229]
117649	137257	[7 ⁶]

表 6.3: $10\sigma(a) - 11a = -1$

a	$\sigma(a)$	素因数分解
11	12	[11]
121	133	[11 ²]
611	672	[13, 47]
1331	1464	[11 ³]
14641	16105	[11 ⁴]
161051	177156	[11 ⁵]

表 6.4: $16\sigma(a) - 17a = -1$

a	$\sigma(a)$	素因数分解
17	18	[17]
289	307	[17 ²]
1073	1140	[29, 37]
2033	2160	[19, 107]
4913	5220	[17 ³]

6.3 pq 形の概完全数

$a = pq (p < q)$ の形の非べきの概完全数があるとしてみよう.

$$\overline{P}\sigma(a) = \overline{P}\widetilde{pq}, Pa = Ppq$$

により, $\Delta = p + q$ とおけば $pq = \overline{P}\Delta + P$ となるのでこれより

$$(p - \overline{P})(q - \overline{P}) = P(P - 1) + 1.$$

$D = P(P-1) + 1$, $p_0 = p - \bar{P}$, $q_0 = p - \bar{P}$ とおく. すると $D = p_0 q_0$ を満たす.

さて与えられた P に対して $D = P(P-1) + 1$ を分解して $D = p_0 q_0$ として $p_0 + \bar{P}$, $q_0 + \bar{P}$ がともに素数となるときの

$p = p_0 + \bar{P}$, $q = q_0 + \bar{P}$ とおけば, $a = pq (p < q)$ の形の概完全数が得られる.

例えば, $P = 3$ のとき $\bar{P} = 2$, $D = P(P-1) + 1 = 13$, $p_0 = 1$, $q_0 = 13$; $p = 3$, $q = 15$. ここで 15 は素数では無い.

6.3.1 非べき概完全数の数表

表 6.5: 非べきの概完全数

a	素因数分解	$\sigma(a)$
$P = 5$		
77	$7 * 11$	96
$P = 11$		
611	$13 * 47$	672
$P = 17$		
2033	$19 * 107$	2160
1073	$29 * 37$	1140
$P = 31$		
6031	$37 * 163$	6232
$P = 37$		
5293	$67 * 79$	5440
$P = 41$		
25241	$43 * 587$	25872
$P = 47$		
9983	$67 * 149$	10200

6.4 $s(a) = 3, a = p^e qr$ の場合

素数 P に対して $\bar{P}\sigma(a) - Pa = -1$ を満たす自然数 (概完全数) を決定しよう.

$s(a) = 3$ を仮定すると相異なる素数 p, q, r によって $a = XYZ, X = p^e, Y = q^f, Z = r^g$ とかける.

計算を楽にするため, $p = P, f = g = 1$ とする. こうしても重要な例は出てくるはずである.

$a = Xqr$ のとき

$$\bar{p}\sigma(a) = (pX - 1)\tilde{q}\tilde{r} = \bar{p}(pa - 1) = \bar{p}(Xqr - 1).$$

これより

$$(pX - 1)\tilde{q}\tilde{r} = \bar{p}(Xqr - 1).$$

移項して

$$pX(\tilde{q}\tilde{r} - qr) = \tilde{q}\tilde{r} - 1.$$

$\tilde{q}\tilde{r} - qr = q + r + 1$ なのでこれを Δ とおく. $\tilde{q}\tilde{r} - 1 = qr + \Delta - 1$ によって $pX\Delta = qr - 1 + \Delta$ を $u = pX - 1$ とおいて変形して

$$qr - 1 = u \times \Delta = u(q + r) + u.$$

$$(q - u)(r - u) = qr - u(q + r) + u^2 = u^2 + u + 1.$$

このようにして次のアルゴリズムができた.

$X = p^e$ を与える. $u = pX - 1$ として $v = u^2 + u + 1$ を異なる2つの約数の積 $q_0 r_0$ に分解し $q = q_0 + u, r = r_0 + u$ がともに素因数になるとき $a = p^e qr$ が求まる.

6.4.1 $p = 2$ のとき

$p = 2$ のときの計算では Xqr の解は出てこなかった. それを確認しよう.

$p = 2$ なら $u \equiv 1 \pmod{2}$ なので $v \equiv 1 \pmod{2}$.

q, r は奇素数なので $q_0 = q + u \equiv 0, r_0 = r + u \equiv 0, \pmod{2} v = q_0 r_0 \equiv 0, \pmod{2}$ となって矛盾.

$p = 3$ のときも Xqr の解は出てこないようだが証明はできていない.

6.4.2 $a = p^e qr$ のときの計算例

注意

$p = 7, e = 1$ のときの $7 * 61 * 229 = 97783$ は10万以下で例外的に小さい. それが理由で見つけられたのである.

表 6.6: $a = p^e qr$ のとき

$p^e * q * r$	a	$\sigma(a)$
$5^5 * 15661 * 6613597$	323673570678125	404591963347656
$5^8 * 1953613 * 7802966033$	5954678078370011328125	7443347597962514160156
$7 * 61 * 229$	97783	114080
$7^3 * 2593 * 32257$	28689343543	33470900800
$11^4 * 161053 * 8645915567$	20386869817488238691	22425556799237062560
$11^4 * 161087 * 701168173$	1653687443443990691	1819056187788389760
$19 * 373 * 10357$	73400059	77477840

第7章 亜完全数

7.1 p を底とする亜完全数

$e > 0, p, q$ (素数) に対して $a = p^e q$ を p を底とする亜完全数という.

$X = p^e$ とおくと、 $-m = \bar{p}\sigma(a) - pa$ と m を定めるとき $\sigma(a) = \frac{(pX-1)(q+1)}{\bar{p}}$ により

$$\begin{aligned} -m &= \bar{p}\sigma(a) - pa \\ &= (pX-1)(q+1) - pqX \\ &= pXq - q + pX - 1 - pqX \\ &= -q + pX - 1. \end{aligned}$$

よって、 $q = pX - 1 + m = p^{e+1} - 1 + m$.

とくに a を m だけ平行移動した亜完全数、という.

実際には、与えられた p, m に対して $(pX - 1 + m) = p^{e+1} - 1 + m$ が素数となる e を探してこれを q とおき $a = p^e q$ を平行移動 m 、底 p の亜完全数と言う.

7.1.1 $p = 3, m = 3$ の例

例を与える.

表 7.1: $p = m = 3$

e	素因数分解	a
2	$3^2 * 29$	261
3	$3^3 * 83$	2241
7	$3^7 * 6563$	14353281
9	$3^9 * 59051$	1162300833
13	$3^{13} * 4782971$	7625600673633
14	$3^{14} * 14348909$	68630386930821

- $e \equiv 2 \pmod{4}$ ならば、 $q \equiv 9, a \equiv 1 \pmod{10}$,

- $e \equiv 3 \pmod{4}$ ならば, $q \equiv 3, a \equiv 1 \pmod{10}$,
- $e \equiv 1 \pmod{4}$ ならば, $q \equiv 1, a \equiv 3 \pmod{10}$.

7.1.2 $p = 3, m = 5$ の例

表 7.2: $p = 3, m = 5$

$e \pmod{4}$	e	素因数分解	a
2	2	$3^2 * 31$	279
1	5	$3^5 * 733$	178119
0	8	$3^8 * 19687$	129166407
1	9	$3^9 * 59053$	1162340199

- $e \equiv 2 \pmod{4}$ ならば, $q \equiv 1, a \equiv 9 \pmod{10}$,
- $e \equiv 1 \pmod{4}$ ならば, $q \equiv 3, a \equiv 9 \pmod{10}$,
- $e \equiv 0 \pmod{4}$ ならば, $q \equiv 7, a \equiv 7 \pmod{10}$.

7.1.3 $p = 3, m = -3$ の例

表 7.3: $m = -3$

e	素因数分解	a
2	$3^2 * 23$	207
4	$3^4 * 239$	19359
20	$3^{20} * 10460353199$	36472996363223648799

- $e \equiv 2 \pmod{4}$ ならば, $q \equiv 3, a \equiv 7 \pmod{10}$,
- $e \equiv 0 \pmod{4}$ ならば, $q \equiv 9, a \equiv 9 \pmod{10}$.

証明はまだ

7.1.4 $p = 5, m = 3$ の例

例を与える.

表 7.4: $p = 5, m = 3$

e	素因数分解	a
2	$5^2 * 127$	3175
16	$5^{16} * 762939453127$	116415321827239990234375

- $e \equiv 2 \pmod{4}$ ならば, $q \equiv 127, a \equiv 175 \pmod{1000}$,
- $e \equiv 0 \pmod{4}$ ならば, $q \equiv 127, a \equiv 375 \pmod{1000}$.

証明はまだ

7.1.5 $p = 5, m = -3$ の例表 7.5: $p = 5, m = -3$

e	素因数分解	a
4	$5^4 * 3121$	1950625
6	$5^6 * 78121$	1220640625
14	$5^{14} * 30517578121$	186264514898681640625

- $e \equiv 2 \pmod{4}$ ならば, $q \equiv 121, a \equiv 625 \pmod{1000}$,
- $e \equiv 0 \pmod{4}$ ならば, $q \equiv 121, a \equiv 625 \pmod{1000}$.

証明はまだ

7.2 $m = -1$ の例

このとき $q = p^{e+1} - 2$ が素数になる.

7.2.1 $p = 3, m = -1$ の例

これは亜完全度 1 なので以前出てきた 3 を底とした亜完全数である.

表 7.6: $p = 3, m = -1$

a	$\sigma(a)$	素因数分解
21	32	$[3, 7]$
2133	3200	$[3^3, 79]$
19521	29282	$[3^4, 241]$
176661	264992	$[3^5, 727]$
129127041	193690562	$[3^8, 19681]$

表 7.7: $m = -1$

e	素因数分解	a
13	$5^{13} * 6103515623$	7450580594482421875
25	$5^{25} * 1490116119384765623$	444089209850062615573406219482421875

7.2.2 $p = 5, m = -1$ の例

?- A is $5^{14}-2$, factorize(A,B).
A = 6103515623,
B = [6103515623].

7.2.3 $p = 7, m = -1$ の例

表 7.8: $p = 7, W = 1$

e	素因数分解	a
3	$7^3 * 2399$	822857
6	$7^6 * 823541$	96888775109
7	$7^7 * 5764799$	4747559862857
11	$7^{11} * 13841287199$	27368747336126262857
14	$7^{14} * 4747561509941$	3219905755811823280691909
27	$7^{27} * 34522673169589$	2268566409077894898417252393023957827
30	$7^{30} * 157775382034845806615042741$	3556153025177363557255317338486834931022525498125509

?- A is 7^7-2 , factorize(A,B).
A = 823541,

$B = [823541]$.

7.2.4 $p = 11, m = -1$ の例

表 7.9: $p = 11, m = -1$

e	素因数分解	a
3	$11^3 * 14639$	19484509
5	$11^5 * 1771559$	285311348509

たとえば

```
?- A is 11^4-2, factorize(A,B).
A = 14639,
B = [14639].
```

7.2.5 $p = 13, m = -1$ の例

表 7.10: $p = 13, m = -1$

e	素因数分解	a
3	$13^3 * 28559$	62744123
4	$13^4 * 371291$	10604442251
11	$13^{11} * 23298085122479$	41753905413409532046257723

```
?- A is 13^4-2, factorize(A,B).
A = 28559,
B = [28559].
```

7.2.6 $p = 17, m = -1$ の例

表 7.11: $p = 17, m = -1$

e	素因数分解	a
5	$17^5 * 24137567$	34271893467919

?- A is 17^6-2, factorize(A,B).
 A = 24137567,
 B = [24137567].

7.3 亜完全度

$W = \bar{p}\sigma(a) - pa$ とおきこれを亜完全度と呼ぶ.

亜完全度 1 のときとくに真性亜完全数という. このとき $q = p^{e+1} - 2$ を満たす.

$W = 1$ のときは $a = p^E$ を解としてもつ.

意外にも $W = -m$ が成り立つ.

W, p に対して $W = \bar{p}\sigma(a) - pa$ を亜完全数の方程式と呼びこれを満たす a を求めよう.

究極の完全数と違い, $\text{Maxp}(a)$ がでてこない.

亜完全度 1 のとき次の公式を満たす.

$$\bar{p}\sigma(a) - pa = 1$$

そこで a でこの公式を満たす数をすべて拾い出してみよう. ただし $a \leq 20000$ 程度に限って探索する.

7.3.1 $p = 3, W = 1$ の例

表 7.12: $p = 3, W = 1$

a	$\sigma(a)$	a の素因数分解
21	32	[3, 7]
2133	3200	[3 ³ , 79]
19521	29282	[3 ⁴ , 241]
176661	264992	[3 ⁵ , 727]

(

7.3.2 $p = 5, W = 1$ の例

$a = 3$ が微小解. (3,5) は双子素数.

$a = 29491$ は素因数分解 [7, 11, 383] を持つ非通常解 (エイリアン解)

7.3.3 $p = 7, W = 1$ の例

$a = 5$ が微小解. (5,7) は双子素数.

表 7.13: $p = 5, W = 1$

a	$\sigma(a)$	a の素因数分解
3	4	[3]
115	144	[5, 23]
29491	36864	[7, 11, 383]

表 7.14: $p = 7, W = 1$

a	$\sigma(a)$	a の素因数分解
5	6	[5]
329	384	[7, 47]
822857	960000	[7 ³ , 2399]

7.3.4 $p = 11, W = 1$ の例表 7.15: $p = 11, W = 1$

a	$\sigma(a)$	a の素因数分解
174109	191520	[13, 59, 227]

7.3.5 $p = 13, W = 1$ の例表 7.16: $p = 13, W = 1$

a	$\sigma(a)$	a の素因数分解
11	12	[11]
731	792	[17, 43]
2171	2352	[13, 167]

$a = 11$ が微小解.

(11, 13) は双子素数.

7.4 亜完全度1の微小解

$W = 1$ を満たすとき

$$\bar{p}\sigma(a) - pa = 1$$

の微小解とは $s(a) = 1$ を満たす解のことである.

$a = q^f$ とおくと,

$$\bar{p}\sigma(a) - pa = \frac{\bar{p}(qa - 1)}{\bar{q}} - pa$$

によって,

$$\bar{p}(qa - 1) - \bar{q}(pa - 1) = \bar{q}.$$

これより

$$a(p - q) = p + q - 2.$$

$p > q$ なので $f \geq 2$ とすると,

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

$p(1 - q^2) \geq -q^3 - q + 2$ より,

$$p \leq q + \frac{2}{q-1}.$$

$q - 1 \geq 3$ のとき $\frac{2}{q-1} < 1$ なので $p \leq q$. $p > q$ に矛盾.

$q = 3$ なら $p \leq q + \frac{2}{q-1} = 4$. これも矛盾.

$f = 1$ になり,

$$\bar{p}\sigma(a) - pa = \bar{p}(q + 1) - pq = p - q - 1 = 1.$$

$p = q + 2$ なので (q, p) はいわゆる双子素数である.

底が p の $W = 1$ の亜完全数の方程式 $\bar{p}\sigma(a) - pa = 1$ に微小解のある条件は (q, p) が双子素数になることで, このとき q が微小解なのである.

双子素数が無限にあるか, という問いは古くから問題にされてきたが現代でも未解決の難問である.

微小解が無限にあるかは双子素数の問題であった. これも不思議なことではないだろうか.

7.5 $a = p^e qr$ 型の亜完全数

$a = p^e qr, p < q, r: (\text{素数})$ を底が p の $p^e qr$ 型の亜完全数という.
 $p\sigma(a) - ap = W$ とおくと、 $\Gamma = p^{e+1} - 1, \Delta = q + r$ を用いると

$$\Gamma(qr + \Delta + 1) = (\Gamma + 1)qr + W.$$

これより

$$qr = \Gamma\Delta + \Gamma - W.$$

$q_0 = q - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + \Gamma - W$ とおくと

$$q_0 r_0 = D.$$

こうして、亜完全度 W の亜完全数 $a = p^e qr$ が得られる.

表 7.17: $p = 7, W = 1; a = 7^e qr$

a	$\sigma(a)$	a の素因数分解
27466313	32044032	$[7^2, 487, 1151]$

表 7.18: $p = 19, W = -1; a = 19^e qr$

a	$\sigma(a)$	a の素因数分解
73400059	77477840	$19 * 373 * 10357$

表 7.19: $p = 3, W = 3; a = 3^e qr$

a	$\sigma(a)$	a の素因数分解
1023	1536	$3^1 * 11 * 31$
5017599	7526400	$3^3 * 83 * 2239$
1207359	1811040	$3^3 * 97 * 461$

表 7.20: $p = 3, W = -3; a = 3^e qr$

a	$\sigma(a)$	a の素因数分解
897	1344	$3^1 * 13 * 23$
46593	69888	$3^2 * 31 * 167$
26937	40404	$3^2 * 41 * 73$
19035755649	28553633472	$3^5 * 733 * 106871$
6519443841	9779165760	$3^5 * 743 * 36109$
43076441601	64614662400	$3^6 * 2399 * 24631$

第8章 素数べきの方程式変位

一般に P を素数とし素数べき $a = P^E$ は次の方程式を満たす:

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

これを整数 m だけ変位させる. その意味は $g_m = P - 1 - m$ を $\sigma(a)$ の係数と定め, さらに $\widetilde{g}_m = P - m$ を a の係数にし, かつ P を解に持つように定数項 α を調整する. すなわち方程式

$$g_m\sigma(a) = \widetilde{g}_m a + \alpha$$

が $a = P$ を解に持つようにする.

$$g_m(P+1) = \widetilde{g}_m P + \alpha \text{ を解けば } \alpha = -(m+1).$$

$$g_m\sigma(a) = \widetilde{g}_m a - m - 1. \tag{8.1}$$

これを 変位 m の素数べき方程式という.

これは解として必ず P を持ちこれが通常解である.

$m = -1$ のとき通常解しかない. 実際, $g_{-1} = P$ なので素数べき方程式は

$$P\sigma(a) = \widetilde{P}a$$

となり a は P の倍数なので $a = P^e L$ とかけ, L は P の倍数ではない, としてよい.

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

によれば

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

$\sigma(L) \geq L$ によれば

$$(P^2 - 1)P^e \geq P(P^{e+1} - 1).$$

これから

$$(P^2 - 1)P^{e-1} = P^{e+1} - P^{e-1} \geq P^{e+1} - 1.$$

$1 \geq P^{e-1}$ がえられるので $e = 1$. かつ $L = 1$. ゆえに $a = P$.

$m = 0$ なら素数べきの方程式になる.

そこで $m = -2, 1, 2$ を $P = 5, 7, 11$ について試してみよう.

8.0.1 $m = -2$ の例

$g_m = P - 1 - m$ なので $m = -2$ のとき $(P + 1)\sigma(a) = (P + 2)a + 1$.
 $s(a) = 1$ の解は $a = P$ のみである.

8.0.2 $s(a) = 2$ の解

$s(a) = 2$ の解を $a = qr$ として探す.
 $\tilde{P} = P + 1$ を用いると $\sigma(a) = \tilde{q}\tilde{r}$ によって
 $\tilde{P}\tilde{q}\tilde{r} = (\tilde{P} + 1)qr + 1$, $\tilde{q}\tilde{r} = qr + \Delta + 1$ となる. そこで

$$\tilde{P}(\Delta + 1) = qr + 1.$$

$q_0 = q - \tilde{P}, r_0 = r - \tilde{P}$ とおけば

$$q_0 r_0 = \tilde{P}^2 + \tilde{P} - 1.$$

これをアルゴリズムとみて解を探す.

素数 P に対して $D = \tilde{P}^2 + \tilde{P} - 1$ とおきこれを異なる因数 q_0, r_0 の積に分解し $q = q_0 + \tilde{P}, r = r_0 + \tilde{P}$ がともに素数の場合に $a = qr$ として解がえられる.

8.0.3 $m = -2$ 表 8.1: $m = -2$ の例

P=3		
a	素因数分解	$\sigma(a)$
3	[3]	4
115	[5, 23]	144
29491	[7, 11, 383]	36864
P=5		
5	[5]	6
329	[7, 47]	384
P=11		
11	[11]	12
731	[17, 43]	792
2171	[13, 167]	2352
P=17		
17	[17]	18
6821	[19, 359]	7200
P=41		
41	[41]	42
8357	[61, 137]	8556

8.0.4 $m = 1$ の例表 8.2: $m = 1$

P=3		
a	素因数分解	$\sigma(a)$
3	[3]	4
10	[2, 5]	18
136	$[2^3, 17]$	270
32896	$[2^7, 257]$	65790
P=23		
23	[23]	24
2291	[29, 79]	2400
P=83		
83	[83]	84
39449	[103, 383]	39936

$P = 3$ なら $\sigma(a) - 2a = -2$ になるので 完全数を 2 だけ平行移動したもの. フェルマー素数とフェルマー完全数がでてくる.

8.0.5 $m = 2$ の例表 8.3: $m = 2$ の例

P=5		
a	素因数分解	$\sigma(a)$
5	[5]	6
33	[3, 11]	48
261	[3 ² , 29]	390
385	[5, 7, 11]	576
897	[3, 13, 23]	1344
2241	[3 ³ , 83]	3360
26937	[3 ² , 41, 73]	40404
46593	[3 ² , 31, 167]	69888
P=7		
7	[7]	8
3175	[5 ² , 127]	3968
P=11		
11	[11]	12
299	[13, 23]	336
P=23		
23	[23]	24
1943	[29, 67]	2040

表 8.4: $m = 2$ の例; 続き

P=29		
a	素因数分解	$\sigma(a)$
29	[29]	30
2993	[41, 73]	3108
5177	[31, 167]	5376
P=41		
41	[41]	42
5893	[71, 83]	6048
7261	[53, 137]	7452
P=59		
59	[59]	60
12827	[101, 127]	13056
19099	[71, 269]	19440

8.0.6 $P = 5, m = 2$ は解が多い

解が多い場合は $P = 5$ のときで, この場合の方程式は $2\sigma(a) = 3a - 3$.

$a = 3^e q$ の形の解があるとすると $q = 3^{e+1} + 2$.

これは, 亜完全数に似た形でたぶん解は無限にある.

さらに $s(a) = 3$ の解もある.

$a = 3^e qr$ の形の解があるとすると. $\Gamma = 3^{e+1} - 1, \Delta = q + r$ おくとき

$2\sigma(a) = \Gamma(qr + \Delta + 1), 3a - 3 = (\Gamma + 1)qr - 3$ を使うと

$$qr = \Gamma\Delta + \Gamma + 3.$$

$q_0 = q - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + \Gamma + 3$. とおくと

$$q_0 r_0 = D. \tag{8.2}$$

表 8.5: $m = 2, P = 5; 3^e qr$ の例

a	素因数分解	$\sigma(a)$
897	$3^1 * 13 * 23$	1344
46593	$3^2 * 31 * 167$	69888
26937	$3^2 * 41 * 73$	40404
19035755649	$3^5 * 733 * 106871$	28553633472
6519443841	$3^5 * 743 * 36109$	9779165760
43076441601	$3^6 * 2399 * 24631$	64614662400

8.0.7 $m = -3$

表 8.6: $m = -3$ の例

P=3		
a	素因数分解	$\sigma(a)$
3	[3]	4
133	[7, 19]	160
P=7		
7	[7]	8
403	[13, 31]	448
583	[11, 53]	648
P=11		
11	[11]	12
713	[23, 31]	768
817	[19, 43]	880
P=19		
19	[19]	20
2077	[31, 67]	2176
5773	[23, 251]	6048

表 8.7: $m = -3$ の例

P=23		
a	素因数分解	$\sigma(a)$
23	[23]	24
2623	[43, 61]	2728
2923	[37, 79]	3040
P=31		
31	[31]	32
4453	[61, 73]	4588
4717	[53, 89]	4860
5311	[47, 113]	5472
7093	[41, 173]	7308
11581	[37, 313]	11932
P=43		
43	[43]	44
9313	[67, 139]	9520
P=47		
47	[47]	48
11023	[73, 151]	11248
35033	[53, 661]	35748
P=59		
59	[59]	60
15553	[103, 151]	15808
21409	[79, 271]	21760
31169	[71, 439]	31680
46297	[67, 691]	47056

8.0.8 $m = 3$

表 8.8: $m = -3$ の例

P=67		
a	素因数分解	$\sigma(a)$
67	[67]	68
21733	[103, 211]	22048
P=71		
71	[71]	72
21971	[127, 173]	22272
24307	[109, 223]	24640
50879	[83, 613]	51576
P=83		
83	[83]	84
50573	[103, 491]	51168

8.0.9 $m = qr$ の解

素数 P について $(P - 1 - m)\sigma(a) - (P - m)a = -m - 1$ の解を $a = qr$ の形に限定して探す.

$v = P - m$ とおくと $(v - 1)\sigma(a) - va = -m - 1$ になり

$(v - 1)\sigma(a) = (v - 1)\tilde{q}r = (v - 1)(qr + \Delta + 1), va = vqr$ により

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

$$(v - 1)qr + (v - 1)(\Delta + 1) - vqr = -qr + (v - 1)\Delta + v - 1$$

により

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

$u = v - 1 = P - m - 1$ とおくと

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

$u = v - 1, D = u^2 + p, q_0 = q - u, r_0 = r - u$ とおけば

$$q_0 r_0 = D. \tag{8.3}$$

表 8.9: $m = -3$

a	素因数分解	$\sigma(a)$
p=3		
133	$7 * 19$	160
p=7		
583	$11 * 53$	648
403	$13 * 31$	448
p=11		
817	$19 * 43$	880
713	$23 * 31$	768
p=19		
5773	$23 * 251$	6048
2077	$31 * 67$	2176
p=23		
2923	$37 * 79$	3040
2623	$43 * 61$	2728
p=31		
11581	$37 * 313$	11932
7093	$41 * 173$	7308
5311	$47 * 113$	5472
4717	$53 * 89$	4860
4453	$61 * 73$	4588

8.0.10 例

表 8.10: $m = -3$; 続き

a	素因数分解	$\sigma(a)$
p=43		
9313	$67 * 139$	9520
p=47		
35033	$53 * 661$	35748
11023	$73 * 151$	11248
p=59		
46297	$67 * 691$	47056
31169	$71 * 439$	31680
21409	$79 * 271$	21760
15553	$103 * 151$	15808
p=67		
21733	$103 * 211$	22048
p=71		
50879	$83 * 613$	51576
24307	$109 * 223$	24640
21971	$127 * 173$	22272
p=79		
81079	$89 * 911$	82080
p=83		
50573	$103 * 491$	51168

表 8.11: $m = 3$ の例

$p = 3$		
a	素因数分解	$\sigma(a)$
3	[3]	4
$p = 5$		
5	[5]	6
14	[2, 7]	24
44	[2 ² , 11]	84
110	[2, 5, 11]	216
152	[2 ³ , 19]	300
884	[2 ² , 13, 17]	1764
2144	[2 ⁵ , 67]	4284
8384	[2 ⁶ , 131]	16764
18632	[2 ³ , 17, 137]	37260
$p = 7$		
7	[7]	8
55	[5, 11]	72
$p = 11$		
11	[11]	12
221	[13, 17]	252
$p = 19$		
19	[19]	20
2329	[17, 137]	2484

表 8.12: $m = 3$ の例; 続き

$p = 31$		
a	素因数分解	$\sigma(a)$
31	[31]	32
3811	[37, 103]	3952
$p = 43$		
43	[43]	44
33661	[41, 821]	34524
$p = 59$		
59	[59]	60
34709	[61, 569]	35340
$p = 71$		
71	[71]	72
19367	[107, 181]	19656
$p = 79$		
79	[79]	80
22879	[137, 167]	23184

表 8.13: $m = -6$

a	素因数分解	$\sigma(a)$
$p = 7$	$D = 151, U = 12$	
2119	$13 * 163$	2296
$p = 11$	$D = 267, U = 16$	
4811	$17 * 283$	5112
$p = 17$	$D = 501, U = 22$	
12029	$23 * 523$	12576
$p = 19$	$D = 595, U = 24$	
3379	$31 * 109$	3520
2419	$41 * 59$	2520
$p = 41$	$D = 2157, U = 46$	
103541	$47 * 2203$	105792
$p = 47$	$D = 2751, U = 52$	
148559	$53 * 2803$	151416
$p = 61$	$D = 4417, U = 66$	
300361	$67 * 4483$	304912
$p = 67$	$D = 5251, U = 72$	
388579	$73 * 5323$	393976
$p = 79$	$D = 7135, U = 84$	
134479	$89 * 1511$	136080

表 8.14: $m = -3$; 続き

a	素因数分解	$\sigma(a)$
$p = 43$	$D = 2068, U = 45$	
9313	$67 * 139$	9520
$p = 47$	$D = 2448, U = 49$	
35033	$53 * 661$	35748
11023	$73 * 151$	11248
$p = 59$	$D = 3780, U = 61$	
46297	$67 * 691$	47056
31169	$71 * 439$	31680
21409	$79 * 271$	21760
15553	$103 * 151$	15808
$p = 67$	$D = 4828, U = 69$	
21733	$103 * 211$	22048
$p = 71$	$D = 5400, U = 73$	
50879	$83 * 613$	51576
24307	$109 * 223$	24640
21971	$127 * 173$	22272
$p = 79$	$D = 6640, U = 81$	
81079	$89 * 911$	82080
$p = 83$	$D = 7308, U = 85$	
50573	$103 * 491$	51168

第9章 疑似完全数

9.1 疑似完全数の定義

$\sigma(a) = 2a + 1$ を満たす数には名前があって疑似完全数 (pseudoperfect number) と呼ぶ. 疑似完全数は一つも発見されていない.

これの一般化を考えよう. ヒントは $a = P^E$ の満たす方程式 $\bar{P}\sigma(a) = Pa - 1$ である. これの定数を X だけ変化させて

$\bar{P}\sigma(a) = Pa - 1 + X$ とおきその解 a がなさそうなら a こそ P を底とする疑似完全数と言えそうである.

$P \geq 3$ で考える.

9.1.1 $X = 0$

$\bar{P}\sigma(a) = Pa - 1$ なので $a = P^e$ などの解がある. P^e 以外の解に興味がある.

9.1.2 $X = 1$

$X = 1$ のとき $\bar{P}\sigma(a) = Pa$ になりパソコンによる解は

表 9.1: $X = 1$

$p = 3$		
a	$\sigma(a)$	素因数分解
2	3	[2]

これが唯一解らしいので以下証明する.

$\bar{P}\sigma(a) = Pa$ なので \bar{P} は偶数に注意して $a = 2^e L$, (L : 奇数), と書ける.

$$\bar{P}(2^{e+1} - 1)\sigma(L) = P2^e L.$$

$\sigma(L) \geq L$ によって

$$P2^e L \geq \bar{P}(2^{e+1} - 1)L.$$

$$P2^e \geq \bar{P}(2^{e+1} - 1) = (2 \times 2^e - 1)P - 2^{e+1} + 1,$$

によって,

$$P + 2^{e+1} - 1 \geq P2^e. \quad (9.1)$$

$$2^{e+1} - 1 \geq P(2^e - 1) \geq 3(2^e - 1)$$

によれば

$$3 \geq 2^e + 1.$$

よって, $e = 1$. (9.1) によれば, $P + 4 - 1 \geq 2P$. $3 \geq P$ なので $p = 3$. $a = 2$.

この結果は $\bar{P}\sigma(a) = Pa$ の解を疑似完全数と呼ぶと, この場合の疑似完全数は $p = 3$ で $a = 2$, と言い換えられる.

9.1.3 $X = 2$

$X = 2$ のとき $\overline{P}\sigma(a) = Pa + 1$ になりパソコンによる解は

表 9.2:

a	$\sigma(a)$	素因数分解
$p = 3$		
21	32	[3, 7]
2133	3200	[3 ³ , 79]
$p = 5$		
3	4	[3]
115	144	[5, 23]
$p = 7$		
5	6	[5]
329	384	[7, 47]
$p = 13$		
11	12	[11]
731	792	[17, 43]
2171 2352		[13, 167]

急に解が増えた。

9.1.4 $X = -1$

$X = -1$ のとき $\overline{P}\sigma(a) = Pa - 2$ になりパソコンによる解は無い。

P は奇素数なので \overline{P} は偶数になり a も偶数. $a = 2^e L$, (L : 奇数), と書ける

$$\overline{P}(2^{e+1} - 1)\sigma(L) = P2^e L - 2.$$

i. $L > 1$, L : 非素数と仮定する. $\sigma(L) \geq L + 2$ によって

$$p2^e L - 2 = \overline{P}(2^{e+1} - 1)\sigma(L) \geq \overline{P}(2^{e+1} - 1)(L + 2).$$

$N = 2^{e+1} - 1$ とおくと $2^e = \frac{N+1}{2}$.

$$P2^e L - 2 = PL \frac{N+1}{2} - 2 \geq \overline{P}N(L + 2).$$

2倍して

$$PL(N + 1) - 4 \geq 2\overline{P}N(L + 2) = 2PN(L + 2) - 2N(L + 2).$$

L で整理して

$$L(P(N+1) - 2NP + 2N) \geq 4(N\bar{P} + 1) > 0.$$

よって $P(N+1) - 2NP + 2N = 2N + P - NP > 0$.

$2N + P - NP \geq 2$ の場合.

$N(2-P) \geq 2-P$ によって $P \geq 3$ なので $N = 2^{e+1} - 1 \leq 1$ となり矛盾.

$2N + P - NP = 1$ の場合. $p = \frac{2N-1}{N-1} = 2 + \frac{1}{N-1}$ によって, $N-1 = 1$. 矛盾.

ii. $L > 1, L$: 素数と仮定する. $\sigma(L) = L+1$ によって

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

変形して

$$PL(N+1) - 4 = 2\bar{P}N(L+1).$$

$P \geq 3$ を用いて

$$P((N-1)L + 2N) = 4 + 2N(L+1) \geq 3((N-1)L + 2N) = 3(N-1)L + 6N.$$

$$L(2N - 3N + 3) = L(3 - N) \geq 6N - 2N - 4 = 4(N - 1).$$

$N \geq 3$ に矛盾.

iii. $L = 1$ と仮定する.

$$\bar{P}(2^{e+1} - 1)\sigma(L) = P2^e L - 2$$

に $L = 1$ を代入して

$$\bar{P}(2^{e+1} - 1) = P2^e - 2.$$

$2^{e+1} - 1 = N$ を用いて,

$$2N\bar{P} = P(N+1) - 4.$$

$N = \frac{P-4}{P-2}$ が出て矛盾.

9.1.5 $X = -2$

$X = -2$

$p = 3$ のとき $2\sigma(a) = 3a - 3$ となる. $a = 3^e q$ が解とすると $q = 3^{e+1} + 2$ が素数なら良い.

表 9.3: $\overline{P}\sigma(a) = Pa - 3$

a	$\sigma(a)$	素因数分解
$p = 3$		
5	6	[5]
33	48	[3, 11]
261	390	[3 ² , 29]
385	576	[5, 7, 11]
897	1344	[3, 13, 23]
2241	3360	[3 ³ , 83]
$p = 5$		
7	8	[7]
3175	3968	[5 ² , 127]
$p = 11$		
13	14	[13]
$p = 17$		
19	20	[19]

第10章 オイラー関数と素数兄弟

10.1 オイラー関数

a を分母とする真分数 $\frac{a}{b}$ の個数を $\varphi(a)$ と書きこれを関数と見るときオイラー関数という.

a, b が互いに素なら $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これを オイラー関数の乗法性という.

a が素数べき p^e のとき $\varphi(a) = \varphi(p^e) = \frac{a(p-1)}{p}$ と書けるから $p\varphi(a) = (p-1)a$ を満たす. $p = 2$ なら $2\varphi(a) = a$ となって, $\sigma(a) = 2a - 1$ と見かけが似ている.

10.2 オイラー関数の基本性質

ただし $\varphi(1) = 1$ とする. オイラー関数 $\varphi(a)$ の性質 ($a > 1$) を列挙しよう.

- (1) $a - 1 \geq \varphi(a)$,
- (2) a が素数なら $\varphi(a) = a - 1$. さらに $\varphi(a) = a - 1$ なら a は素数,
- (3) a が素数でないなら $a \geq \varphi(a) + \sqrt{a}$,
- (4) a, b が互いに素なら $\varphi(ab) = \varphi(a)\varphi(b)$ (乗法性).

10.2.1 オイラー関数数表

表 10.1:

a	素因数分解	$s(a)$	$\varphi(a)$	a	素因数分解	$s(a)$	$\varphi(a)$
2	[2]	1	1	27	[3 ³]	1	18
3	[3]	1	2	28	[2 ² , 7]	2	12
4	[2 ²]	1	2	29	[29]	1	28
5	[5]	1	4	30	[2, 3, 5]	3	8
6	[2, 3]	2	2	31	[31]	1	30
7	[7]	1	6	32	[2 ⁵]	1	16
8	[2 ³]	1	4	33	[3, 11]	2	20
9	[3 ²]	1	6	34	[2, 17]	2	16
10	[2, 5]	2	4	35	[5, 7]	2	24
11	[11]	1	10	36	[2 ² , 3 ²]	2	12
12	[2 ² , 3]	2	4	37	[37]	1	36
13	[13]	1	12	38	[2, 19]	2	18
14	[2, 7]	2	6	39	[3, 13]	2	24
15	[3, 5]	2	8	40	[2 ³ , 5]	2	16
16	[2 ⁴]	1	8	41	[41]	1	40
17	[17]	1	16	42	[2, 3, 7]	3	12
18	[2, 3 ²]	2	6	43	[43]	1	42
19	[19]	1	18	44	[2 ² , 11]	2	20
20	[2 ² , 5]	2	8	45	[3 ² , 5]	2	24
21	[3, 7]	2	12	46	[2, 23]	2	22
22	[2, 11]	2	10	47	[47]	1	46
23	[23]	1	22	48	[2 ⁴ , 3]	2	16
24	[2 ³ , 3]	2	8	49	[7 ²]	1	42
25	[5 ²]	1	20	50	[2, 5 ²]	2	20
26	[2, 13]	2	12	51	[3, 17]	2	32

表 10.2:

a	素因数分解	$s(a)$	$\varphi(a)$	a	素因数分解	$s(a)$	$\varphi(a)$
2	[2]	1	1	32	[2 ⁵]	1	16
3	[3]	1	2	34	[2, 17]	2	16
4	[2 ²]	1	2	40	[2 ³ , 5]	2	16
6	[2, 3]	2	2	48	[2 ⁴ , 3]	2	16
5	[5]	1	4	60	[2 ² , 3, 5]	3	16
8	[2 ³]	1	4	19	[19]	1	18
10	[2, 5]	2	4	27	[3 ³]	1	18
12	[2 ² , 3]	2	4	38	[2, 19]	2	18
7	[7]	1	6	54	[2, 3 ³]	2	18
9	[3 ²]	1	6	25	[5 ²]	1	20
14	[2, 7]	2	6	33	[3, 11]	2	20
18	[2, 3 ²]	2	6	44	[2 ² , 11]	2	20
15	[3, 5]	2	8	50	[2, 5 ²]	2	20
16	[2 ⁴]	1	8	66	[2, 3, 11]	3	20
20	[2 ² , 5]	2	8	23	[23]	1	22
24	[2 ³ , 3]	2	8	46	[2, 23]	2	22
30	[2, 3, 5]	3	8	35	[5, 7]	2	24
11	[11]	1	10	39	[3, 13]	2	24
22	[2, 11]	2	10	45	[3 ² , 5]	2	24
13	[13]	1	12	52	[2 ² , 13]	2	24
21	[3, 7]	2	12	56	[2 ³ , 7]	2	24
26	[2, 13]	2	12	70	[2, 5, 7]	3	24
28	[2 ² , 7]	2	12	72	[2 ³ , 3 ²]	2	24
36	[2 ² , 3 ²]	2	12	78	[2, 3, 13]	3	24
42	[2, 3, 7]	3	12	84	[2 ² , 3, 7]	3	24
17	[17]	1	16	90	[2, 3 ² , 5]	3	24

10.2.2 オイラーの公式

オイラー関数に関する次の公式は定義からすぐ導かれる。

$$a = \sum_{a'|a} \varphi(a') \tag{10.1}$$

ここに $a'|a$ は a' が a の約数を意味する。これをオイラーの公式という。

たとえば $a = 12$ とおくと, $a' = 12, 6, 4, 3, 2, 1$ であり,

$$\varphi(12) = 4, \varphi(6) = 2, \varphi(4) = 2, \varphi(3) = 2, \varphi(2) = 1, \varphi(1) = 1.$$

これらを加えると $4 + 2 + 2 + 2 + 1 + 1 = 12$ となって分母 12 が出て来る.

この公式を使うと, オイラー関数 $\varphi(a)$ の値が機械的に計算できる.

a が素数の平方 p^2 なら約数は $p^2, p, 1$ なので $p^2 = \varphi(p^2) + \varphi(p) + 1 = \varphi(p^2) + (p-1) + 1$ により $\varphi(p^2) = p^2 - p = p(p-1)$.

同様にして $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ が示される.

p, q を相異なる素数とすると pq の約数は $pq, q, p, 1$ なので $pq = \varphi(pq) + \varphi(q) + \varphi(p) + 1 = \varphi(pq) + (q-1) + (p-1) + 1$ により $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

10.2.3 乗法性

a, b を互いに素な自然数とすると, $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これがオイラー関数の乗法性である. ここでは高校の数学 I にある集合の数え方を用いた簡単な証明方法を述べよう.

10.2.4 乗法性の証明

$a > 1$ に対して a 以下の自然数の集合を $S(a)$ と書く. a の素因子 p について, $S(a)$ 内の p の倍数全体は $pS(a/p)$ と書くことができる. ここで自然数の集合 T についてその元の p 倍数全体を pT で示した. たとえば $2\{1, 2, 3\} = \{2, 4, 6\}$.

a の相異なるすべての素因子を p_1, \dots, p_s とする. $A_j = p_j S(a/p_j)$ とおくと和集合 $A_1 \cup \dots \cup A_s$ に属さない $S(a)$ の元 b は a 未満で a と互いに素な自然数である. したがって $A_1 \cup \dots \cup A_s$ の $S(a)$ についての補集合の元の個数が オイラー関数の値 $\varphi(a)$ である.

有限集合 T の元の個数を絶対値記号を流用して $|T|$ で示すとき $\varphi(a) = a - |A_1 \cup \dots \cup A_s|$ と書ける.

$p = p_j$ とおくと $|A_j| = \frac{a}{p}$ になる.

簡単のため, $s = 2, p = p_1, q = p_2$ とすると $A_1 \cap A_2 = pqS(a/pq)$ によって $|A_1 \cap A_2| = \frac{a}{pq}$.

ゆえに

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

を用いると

$$\begin{aligned} \varphi(a) &= a - |A_1 \cup A_2| = a - |A_1| - |A_2| + |A_1 \cap A_2| \\ &= a - \frac{a}{p} - \frac{a}{q} + \frac{a}{pq} \\ &= a\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \end{aligned}$$

書き直すと

$$\varphi(a) = a\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$$

一般に $\bar{a} = a - 1$ と書く.

さて, $a = p^e q^f$ と書くとき

$$\varphi(a) = a\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = p^e\left(1 - \frac{1}{p}\right)q^f\left(1 - \frac{1}{q}\right) = p^{e-1}\bar{p}q^{f-1}\bar{q}$$

となる. ここで $\bar{p} = p - 1, \bar{q} = q - 1$.

一般には素因数分解して $a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ のように相異なる素数 p_1, p_2, \dots, p_s のべきの積で書くと次のようになる:

$$\varphi(a) = p_1^{e_1-1}\bar{p}_1 p_1^{e_2-1}\bar{p}_2 \cdots p_s^{e_s-1}\bar{p}_s.$$

これからオイラー関数の乗法性は直ちに導かれる.

10.3 オイラー関数について3点セット

オイラー関数について3点セットを考える.

(1) $2\varphi(a) - a = 0$ を満たす自然数 a は何か.

(2) $2\varphi(a) - a = 1$ を満たす自然数 a は何か.

(3) $2\varphi(a) - a = -1$ を満たす自然数 a は何か.

1番目の a は 2^e になることが示される.

実際, $2\varphi(a) = a$ とすると a は偶数なので $a = 2^e L$ (L : 奇数) と書ける.

$$\varphi(a) = \varphi(2^e)\varphi(L) = 2^{e-1}\varphi(L)$$

なので, $2\varphi(a) = 2^e\varphi(L)$. 条件式 $2\varphi(a) = a = 2^e L$ によれば

$$2^e\varphi(L) = 2^e L$$

$\varphi(L) = L$ になり, $L = 1$. すなわち $a = 2^e$.

10.4 フェルマー数

$m = 2^e$ について $f = 2^m$ を f_e とし さらに $F_e = f_e + 1$ と書いてこれをフェルマー数という.

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ はみな素数でこれらをフェルマー素数という.

これら5つの素数をまとめてフェルマー素数5兄弟, と呼ぼう.

$j \leq 4$ に関して $a_j = F_0 F_1 \cdots F_j$ とおくと

$$\varphi(a_j) = f_0 f_1 \cdots f_j = 2^{1+2+\cdots+2^j} = 2^{2^{j+1}-1}$$

$$2\varphi(a_j) = f_{j+1}.$$

一方, $(f_j)^2 = f_{j+1}$ により

$$f_{j+1} - 1 = (f_j)^2 - 1 = (f_j - 1)F_j$$

これより $f_{j+1} - 1 = F_0 F_1 \cdots F_j = a_j$. ゆえに $2\varphi(a_j) = f_{j+1} = a_j + 1$. すなわち $2\varphi(a_j) - a_j = 1$ を満たす. $2\varphi(a) - a = 1$ を満たす自然数 a としてはこれらの a_0, a_1, \dots, a_4 が知られている.

手計算で確認しよう.

- (1) $a_0 = 3, \varphi(3) = 2$. このとき $2\varphi(3) - 3 = 1$.
- (2) $a_1 = 3 * 5 = 15, \varphi(15) = 8$. このとき $2\varphi(15) - 15 = 1$.
- (3) $a_2 = 3 * 5 * 17 = 255, \varphi(255) = 128$. このとき $2\varphi(255) - 255 = 1$.

表 10.3: $a - 2\varphi(a) = -1$ の表

a	$\varphi(a)$	素因数分解
3	2	[3]
15	8	[3, 5]
255	128	[3, 5, 17]
65535	32768	[3, 5, 17, 257]
4294967295	7304603328	[3, 5, 17, 257, 65537]

$a - 2\varphi(a) = -1$ の解にフェルマー素数の 5 兄弟が順に出てくる. これはきわめて美しい結果といわざるを得ない.

問題にすべきことはこの逆である. すなわち, $2\varphi(a) - a = 1$ を満たす a はこれらの 5 個の数しかないか?.

これを示すため最初に $2\varphi(a) - a = 1$ を満たす a に平方因子がないことを示す.

実際, $a = p^e b, e > 1, b$ は p で割れないとする. $\varphi(a) - a$ は p^{e-1} を因子としてもつが, 右辺は 1 なので矛盾.

$a = p_1 p_2 \cdots p_s$ とおくと $\overline{p_1} = p_1 - 1$ を使うと

$\varphi(a) = \overline{p_1} \overline{p_2} \cdots \overline{p_s}$ により

$$2\overline{p_1} \overline{p_2} \cdots \overline{p_s} - p_1 p_2 \cdots p_s = 1$$

を解けばよい.

10.4.1 部分的証明

$s(a) = 1, 2, 3$ については何とか解ける.

$s(a) = 2$ のとき. $p = p_1, q = p_2$ とおくと,

$$2\overline{p} \overline{q} = pq + 1.$$

これより $1 + pq = 2\bar{p}\bar{q}$ は偶数なので, p, q はともに奇数.

$3 \leq p < q$ とする.

$\bar{p} = p - 1$, によって

$$2\bar{p}\bar{q} - pq - 1 = p(2\bar{q} - q) - 2\bar{q} - 1.$$

これより

$$2q - 1 = 2\bar{q} + 1 = p(2\bar{q} - q) \geq 3(q - 2) = 3q - 6.$$

$q \leq 5$ をえるが $3 \leq p < q$ によれば $q \geq 5$. ゆえに $p = 3, q = 5$ が導かれる.

$s(a) = 3$ のとき. $p = p_1, q = p_2, r = p_3$ とする.

$$2\bar{p}\bar{q}\bar{r} = pqr + 1.$$

これより p, q, r はともに奇数.

$p = 3$ を仮定するとき

$$4\bar{q}\bar{r} = 3qr + 1.$$

$q(4\bar{r} - 3r) = 4\bar{r} + 1$ により

$$q = \frac{4\bar{r} + 1}{r - 4} = \frac{4r - 3}{r - 4} = 4 + \frac{13}{r - 4}.$$

$r \geq q + 2 \geq 7$ なので $r - 4 = 13$. よって $r = 17, q = 5$. 解は $p = 3, q = 5, r = 17$.

これしか解が無いことを示すため $p \geq 5$ を仮定して矛盾を導く.

このとき $q \geq 7, r \geq 11$. $A = \bar{q}\bar{r}, B = pq$ とおくと $2\bar{p}A = pB + 1$ から

$$5(2A - B) \leq p(2A - B) = 2A + 1.$$

$8A \leq 5B + 1$ を変形して

$$q(3r - 8) \leq 8r - 7 < 9r - 7.$$

ゆえに $r \geq 11$ なので

$$q < 3 + \frac{17}{3r - 8} < 3 + \frac{17}{33 - 8} < 4.$$

$q \geq 7$ に矛盾.

$s > 5$ なら解が無いことを示したい.

10.4.2 不existence

$2\varphi(a) - a = -1$ を満たす自然数 a はないことを示したい.

$$2\bar{p}_1\bar{p}_2 \cdots \bar{p}_s - p_1p_2 \cdots p_s = -1$$

を解けばよい.

$s = 1, 2, 3, 4$ までは何とかがんばれば解けると思う. しかし解が無いことを示すだけなので張り合いがない.

10.5 見事な解

2014年9月24日 私は広島県西条市のホテルで私のホームページにある掲示板「数の不思議世界」に驚くべき結果が報じられた.

$2\varphi(a) - a = 1$ の解には別の1系統がある. その解は

$$a = 83623935 (= [3, 5, 17, 353, 929])$$

$$a = 6992962672132095 (= [3, 5, 17, 353, 929, 83623937])$$

私はにわかには信じれなかったが, 丹念に計算するとすべて正しかった.

10.6 $a = P^e$

素数 P に対して $a = P^e$ とおけば $P\varphi(a) = a\bar{P}$ を満たす.

$$P\varphi(a) = a\bar{P}$$

をオイラー関数での素数べき方程式という. この逆を考える.

一般に $P\varphi(a) = \bar{P}a$ を満たす a は P で割れるから $a = P^e L$ (L は P でわれない) と書ける.

$$P\varphi(a) = P\varphi(P^e L) = P^e \bar{P}\varphi(L) = \bar{P}a = \bar{P}P^e L$$

によれば $\varphi(L) = L$. よって $L = 1; a = P^e$.

10.6.1 $a = P^e$ の3点セット

3点セットにして

(1) $P\varphi(a) - \bar{P}a = -1$ を満たす自然数 a は何か,

(2) $P\varphi(a) - \bar{P}a = 1$ を満たす自然数 a は何か,

(3) $P\varphi(a) - \bar{P}a = 0$ を満たす自然数 a は何か

を問題にする. 3番は解けている.

10.6.2 $P = 3$ のときの3点セット

$P = 3$ のとき $W = 3\varphi(a) - 2a$ として, $W = 0, -1, 1$ の場合をパソコンに計算してもらった結果は次の通り.

$W = 0$ のとき.

ここでは 3^e が並ぶ. これはすでに証明された結果である.

表 10.4: $3\varphi(a) - 2a = 0$

a	$\varphi(a)$	素因数分解
3	2	[3]
9	6	[3 ²]
27	18	[3 ³]
81	54	[3 ⁴]
243	162	[3 ⁵]
729	486	[3 ⁶]
2187	1458	[3 ⁷]
6561	4374	[3 ⁸]

$W = 1$ のとき.

表 10.5: $3\varphi(a) - 2a = -1$

a	$\varphi(a)$	素因数分解
2	1	[2]

パソコンでの計算結果を基にして次の結果を証明する.

定理 2 (1) $3\varphi(a) = 2a + 1$ のとき解はない.

(2) $3\varphi(a) = 2a - 1$ のとき $a = 2$.

Proof. $a = 2$ のとき $3\varphi(a) - 2a = 1$.

$a \geq 3$ なら $\varphi(a)$ は偶数なので $3\varphi(a) - 2a$ も偶数. $3\varphi(a) - 2a = 1$ に矛盾.

10.6.3 5点セット

少し広げて $W = -2$ と 2 の場合を調べよう.

$W = -2$.

表 10.6: $3\varphi(a) - 2a = -2$

a	$\varphi(a)$	素因数分解
4	2	[2 ²]

$3\varphi(a) - 2a = -2$ を解く.

$a = 2$ は解ではないことに最初に注意する.

1. a は偶数の場合.

$a = 2^e L$ と書くとき

$$0 = 3\varphi(a) - 2a - 2 = 3\varphi(2^e L) - 2^{e+1}L - 2 = 3 * 2^{e-1}\varphi(L) - 2^{e+1}L - 2.$$

$e - 1 = 1, 0$ を満たす.

$e = 2$ のとき. $3 * 2\varphi(L) - 2^3L - 2$ によると $\varphi(L)$ は奇数なので $L = 1$. ゆえに $a = 4$.

$e = 1$ のとき. $3\varphi(L) - 2^2L - 2$ によると $3(L - 1) \geq 3\varphi(L) = 4L + 2$. ゆえに $L < 1$ が出て矛盾.

2. a は奇数の場合: 解の不存在の証明ができなかった.

10.7 $P = 3$ のときのフェルマー素数

5点セットの最後の場合は $3\varphi(a) - 2a = 2$ を満たすときである.

表 10.7: $3\varphi(a) - 2a = 2$ を満たす a

a	$\varphi(a)$	素因数分解
5	4	[5]
35	24	[5, 7]
1295	864	[5, 7, 37]

これらは $3\varphi(a) - 2a = 2$ の解で, $2\varphi(a) - a = 1$ の解の場合と同じく a には平方因子はなく異なる素数の積になっている.

実際 $a = p(p \neq 5, 7, 37: \text{素数})$ が $3\varphi(a) - 2a = 2$ の解とすると,

$$3\varphi(p) - 2p - 2 = 3\bar{P} - 2 = p - 5 = 0$$

により $p = 5$.

$a = 5q(q: \text{素数})$ が $3\varphi(a) - 2a = 2$ の解のとき,

$$3\varphi(5q) - 10q - 2 = 12\bar{q} - 10q - 2 = 2q - 14 = 0$$

より $q = 7$.

$a = 5 \times 7q(q: \text{素数})$ が $3\varphi(a) - 2a = 2$ の解のとき,

$$0 = 3\varphi(35q) - 70q - 2 = 72\bar{q} - 70q - 2 = 2(q - 37) = 0$$

より $q = 37$.

以上はパソコン計算の追試のようなものだが、次に未知の世界に挑む。

$a = 5 \times 7 \times 37q$ (q : 素数) が $3\varphi(a) - 2a = 2$ の解としてみると、

$$3\varphi(5 \times 7 \times 37q) - 2 \times 5 \times 7 \times 37q - 2 = 36^2 \bar{q} - 35 \times 37q - 2 = 2(q - 36^2 - 1) = 0.$$

よって $q = 36^2 + 1$. さて $36^2 + 1$ は本当に素数だろうか. Prolog の実行によってそれを確認しよう.

?- A is 36^2+1, factorize(A,B).

の結果は

A = 1297,

B = [1297].

したがって $36^2 + 1$ が素数であることが確認されて、 $a = 5 \times 7 \times 37 \times 1297$ が新しい $3\varphi(a) - 2a = 2$ の解になることが確定した.

表 10.8: $3\varphi(a) - 2a = 2$ を満たす a の追加

a	$\varphi(a)$	素因数分解
5	4	[5]
35	24	[5, 7]
1295	864	[5, 7, 37]
1679615	1119744	[5, 7, 37, 1297]

あえて次の場合を試みた. たぶん駄目であろうと思いつつ進む.

Q を素数として $a = 5 \times 7 \times 37 \times 1297Q$ (Q : 素数) が $3\varphi(a) - 2a = 2$ の解とすると、

$$\begin{aligned} 3\varphi(5 \times 7 \times 37 \times 1297Q) - 5 \times 7 \times 37 \times 1297Q - 2 &= 36^2 \times 1296\bar{Q} - 70 \times 37 \times 1297Q - 2 \\ &= 2(Q - 36^2 \times 1296 - 1) = 0. \end{aligned}$$

しかし、かくして得られた $Q = 36^2 \times 1296 + 1 = 6^8 + 1$ は素数ではなかった.

実際に Prolog によると $36^2 \times 1296 + 1 = 36^4 + 1 = 6^8 + 1 = 1679617$ の素因数分解は [17, 98801] であった.

もうひとつ先も $36^8 + 1 = 6^{16} + 1 = 2821109907457 = 353 \times 1697 \times 409377$ となり合成数.


```
?- A=17, B is A-1, factorize(B, BB), exps(BB, BS).
```

```
A = 17,
B = 16,
BS = [2^4].
```

```
?- A=98801, B is A-1, factorize(B, BB), exps(BB, BS).
```

```
A = 98801,
B = 98800,
BS = [2^4, 5^2, 13, 19].
```

```
?- A=353, B is A-1, factorize(B, BB), exps(BB, BS).
```

```
A = 353,
B = 352,
BS = [2^5, 11].
```

```
?- A=1697, B is A-1, factorize(B, BB), exps(BB, BS).
```

```
A = 1697,
B = 1696,
BS = [2^5, 53].
```

```
?- A=409377, B is A-1, factorize(B, BB), exps(BB, BS).
```

```
A = 409377,
B = 409376,
BS = [2^5, 11, 1163].
```

その昔オイラーは $F_6 = 4294967297$ を素因数分解して $[641, 6700417]$ を得てセンセーションを巻き起こした。さて今回、 $6^8 + 1$ の因数分解はそれと類似の現象であると言えよう。

今回得られた素数の4つ組 $5, 7, 37, 1297$ は $6 - 1, 6 + 1, 6^2 + 1, 6^4 + 1$ と表される。

$m = 2^e$ とおけば $6^m + 1$ を G_e とすると $G_0 = 7, G_1 = 37, G_2 = 1297$ らは素数。

$G_4 = 6^8 + 1 = 1679617 = 17 \times 98801$ となり合成数。

素数 $5, 7, 37, 1297$ は $P = 3$ のときのフェルマー素数と呼ばれてもいいのではないか。

フェルマー素数5兄弟に対抗して、これらの素数 $5, 7, 37, 1297$ を ($P = 3$ の場合の) 素数4姉妹と呼びたい。しかし最初の5は例外的である。

$P = 3$ のときの成功につられて一般の素数 P に対して $P\varphi(a) = \overline{P}a$ の場合を調べて素数 P に対するフェルマー素数を探すことにしよう。その前にフェルマー素数の仕組みを考えてみる。

10.7.1 フェルマー素数の仕組み

フェルマー素数は2のべきプラス1の形である。

2を偶数 g に一般化して $g^m + 1$ を考える. これが素数になるには m 自身が2のべき 2^e でないといけない.

実際, m を素因数分解したとき $m = 2^e L (L: 3$ 以上の奇数) とおくと

$g^m = (g^{2^e})^L$ において $x = g^{2^e}, y = -x$ とすれば等比級数の和の公式によって, $L > 1$ に注意して

$$g^m + 1 = x^L + 1 = 1 - (-x)^L = 1 - y^L = (1 - y)(1 + y + \cdots + y^{L-1})$$

になり $L > 1$ なら $g^m + 1$ が素数にならない.

したがって $m = 2^e$ について $h_e = g^m$ とおく. さらに $H_e = h_e + 1$ とする.

$$h_{t+1} = (h_t)^2 = (h_t)^2 - 1 + 1 = (h_t - 1)(h_t + 1) + 1$$

によると,

$$h_{t+1} - 1 = (h_t - 1)(h_t + 1) = (h_t - 1)H_t.$$

これを繰り返すと

$$h_{t+1} - 1 = (h_t - 1)H_t = (h_{t-1} - 1)H_{t-1}H_t = (h_0 - 1)H_0H_1 \cdots H_t.$$

$h_0 - 1 = g - 1$ になる. $B_t = H_0H_1 \cdots H_t$ とおけば

$$h_{t+1} - 1 = (g - 1)B_t.$$

さて H_0, H_1, \dots, H_t が全て素数とすると $\varphi(H_i) = H_i - 1 = h_i$ なので B_t についてそのオイラー関数を考える.

$$\varphi(B_t) = h_0h_1 \cdots h_t = g^{1+2+\cdots+2^t} = g^{2^{t+1}-1}.$$

その結果

$$g\varphi(B_t) = g^{2^{t+1}} = h_{t+1} = (g - 1)B_t + 1.$$

$a = B_t$ は $g\varphi(a) = (g - 1)a + 1$ の解であるがこれのみならず B_0, B_1, \dots, B_t がすべて解になる.

10.8 再び, オイラー

$H_e = h_e + 1, h_e = g^{2^e}$ に注意して H_e が合成数とし, その素因子を Q とおく. すると

$$h_e + 1 \equiv 0 \pmod{Q}.$$

$g^{2^{e+1}} = h_e^2 \equiv 1 \pmod{Q}$ によって \pmod{Q} での g の位数は 2^{e+1} .

したがって Q が g の約数でない限り, $Q - 1 = 2^{e+1}k$ と書ける.

10.8.1 2素数の追加

H_0, H_1, \dots, H_t が全て素数の時これらと異なる2素数 p, q を追加し $a = B_t pq$ も $g\varphi(a) = (g-1)a + 1$ の解であると仮定する.

$$g\varphi(a) = g\varphi(B_t pq) = g\varphi(B_t)\varphi(pq), \Delta = p + q \text{ と定めると } \varphi(pq) = \overline{pq} = pq - \Delta + 1.$$

$$g\varphi(B_t) = h_{t+1}, \overline{g}B_t = h_{t+1} - 1$$

よって, $L = h_{t+1}$ を用いて $g\varphi(a) = \overline{g}a + 1$ を書き直すと

$$g\varphi(a) = L(pq - \Delta + 1), \overline{g}a = \overline{g}B_t pq = (L-1)pq$$

よって

$$L(pq - \Delta + 1) = (L-1)pq + 1.$$

整理すると

$$L(pq - \Delta + 1) = (L-1)pq.$$

$pq = L(\Delta - 1) + 1$ になり

$$(p-L)(q-L) = L^2 - L + 1.$$

さて $L^2 - L + 1 = \alpha\beta$ と2因子の積に表すとき $p = \alpha + L, q = \beta + L$ ともに素数なら $a = B_t pq$ も $g\varphi(a) = (g-1)a + 1$ の解になる.

10.8.2 例題

$g = 2, t = 2, B_2 = 3 * 5 * 17$ として, $\varphi(B_2) = 2 * 2 * 4 * 8$ なので $g\varphi(B_t) = h_{t+1} = L$ によれば $L = 16^2 = 256$.

$L^2 - L + 1 = 65281$. $65281 = 97 * 673$ は素因数分解.

$\alpha = 1, \beta = 65281$ のとき $p = 257, q = 65281 + 256 = 65537$; これらは素数なので解になった.

$\alpha = 97, \beta = 673$ のとき $p = 256 + 97 = 353, q = 673 + 256 = 929$; これらは幸いにして素数なので解になった.

65281 は2つの素因子を持ち2通りの分解を持つがそれは不思議ではない. ここから素因子の組が2つできた. 偶然の結果かもしれないが, 神秘的ですらある.

10.8.3 素数の追加

新しく得られた $a = 3 * 5 * 17 * 353 * 929$ は $a - 2\varphi(a) = -1$ を満たす. a にこれと異なる素数 P を追加して $a_1 = aP$ が $a_1 - 2\varphi(a_1) = -1$ を満たすようにできるか考えてみよう.

$$2\varphi(a_1) = 2\varphi(a)\overline{P} = a_1 + 1 = aP + 1$$

とする. $2\varphi(a) = a + 1$ を使うと

$$(a + 1)\overline{P} = a_1 + 1 = aP + 1.$$

これより, $P = a + 2$. こうして得られた結果は発見的手法によるもので, ここからが大切である. $a + 2 = 3 * 5 * 17 * 353 * 929 + 2 = 83623937$ は次のようにして素数であることを確認できる.

表 10.9: $a - 2\varphi(a) = -1$ の表

a	$\varphi(a)$	素因数分解
83623935	41811968	[3, 5, 17, 257, 353, 929]
6992962672132095	3496481336066048	[3, 5, 17, 257, 353, 929, 83623937]

$a - 2\varphi(a) = -1$ の解が 1 系統, 2 つの解がえられた. これはきわめて不思議で美しい結果といわざるを得ない.

もっと別の解があるかもしれない.

10.8.4 1 素数の追加の追加

偶数 g があり a が $g\varphi(a) = \overline{g}a + 1$ を満たすとする.

さらに a と互いに素な素数 p があり $a_1 = ap$ は同じく $g\varphi(a_1) = \overline{g}a_1 + 1$ を満たすと仮定する. すると $p = \overline{g}a + 2$.

例

$g = 10, a = 11$ とすると $g\varphi(a) = \overline{g}a + 1$ を満たす. $\overline{g}a + 2 = 9 * 11 + 2 = 101$. これは素数.

$g = 6, a = 7$ とすると $g\varphi(a) = \overline{g}a + 1$ を満たす. $\overline{g}a + 2 = 37$. これは素数.

10.8.5 2 素数の追加の追加

偶数 g があり a が $g\varphi(a) = \overline{g}a + 1$ を満たすとする.

さらに a と互いに素な素数 p, q があり $a_1 = apq$ は同じく $g\varphi(a_1) = \overline{g}a_1 + 1$ を満たすと仮定する.

$$g\varphi(a_1) = g\varphi(apq) = g\varphi(a)\overline{p}q, \overline{g}a_1 + 1 = \overline{g}apq + 1 \text{ なので}$$

$$g\varphi(a)\overline{p}q = \overline{g}apq + 1.$$

$g\varphi(a) = \overline{g}a + 1$ によって

$$(\overline{g}a + 1)\overline{p}q = \overline{g}apq + 1.$$

$\overline{p}q = pq - \Delta + 1, (\Delta = p + q)$ を代入すると

$$(\bar{g}a + 1)(pq - \Delta + 1) = \bar{g}apq + 1.$$

これより

$$\begin{aligned} (\bar{g}a + 1)(pq - \Delta + 1) &= \bar{g}(pq - \Delta + 1) + pq - \Delta + 1 = \bar{g}apq + 1 \\ pq &= ((\bar{g}a + 1)\Delta - \bar{g}a. \end{aligned}$$

$\Gamma = \bar{g}a + 1$ とおけば

$$(p - \Gamma)(q - \Gamma) = \Gamma^2 - \Gamma + 1.$$

$D = \Gamma^2 - \Gamma + 1, p_0 = p - \Gamma, q_0 = -\Gamma$ とおくと $p_0q_0 = D$ を満たす.

10.8.6 計算例

表 10.10:

g	a	$\bar{g}a + 1$	D	pq	$\sigma(pq)$
2	3	4	85	$5 * 17$	108
2	$5 * 3$	16	4369	$17 * 257$	4644
2	$17 * 5 * 3$	256	16843009	$257 * 65537$	16908804
2	$17 * 5 * 3$	256	327937	$353 * 929$	329220
6	7	36	47989	$37 * 1297$	49324

10.9 $P = 5$ のときのフェルマー素数

$P = 5$ のときのフェルマー素数を探す.

表 10.11: $5\varphi(a) - 4a = 4$

a	$\varphi(a)$	素因数分解
119	96	$[7, 17]$

この場合は解として $7 * 17$ しか出てこない.

$s(a) = 1. a = q$ 素数とすると $5(q - 1) = 4q + 4. q = 9$ となり素数ではない.

$s(a) = 2. a = pq$ と素数の積とすると,

$$5\bar{P}(q - 1) = 4pq + 4$$

$pq - 5(p + q - 1) = 4$ により

$$(p - 5)(q - 5) = 24 = 2 \times 12.$$

これより $p-5=2, q-5=12$. よって $p=7, q=17$.

次に $7, 17$ と異なる素数 Q に対し $a=7*17*Q$ が $5\varphi(a)-4a=4$ を満たすとするとうまく解けるが $Q=121$ となって素数に反する.

これ以外の解が見つからないので, $P=5$ のときのフェルマー素数を探すことは断念.

10.10 $P=7$ のときのフェルマー素数

$P=7$ とする. $7\varphi(a)-6a=6$ を満たす a をパソコンで求める.

表 10.12: $7\varphi(a)-6a=6$ を満たす a

a	$\varphi(a)$	素因数分解
13	12	[13]
209	180	[11, 19]
44099	37800	[11, 19, 211]

$a=11 \times 19=209$ のとき $\varphi(a)=180, 7 \times 180=1260, 6 \times 209=1254=1260-6$.

これを基にして次の解を探す. そのために $11, 19$ と異なる素数 q があり $a=11 \times 19q$ が解であると仮定する.

$7\varphi(a)=7 \times 180q, 6a=6 \times 11 \times 19q$ により

$$7\varphi(a)-6a=7 \times 180q-6 \times 11 \times 19q=6(7 \times 30q-11 \times 19q)=6(q-211).$$

により $q=211$. これは素数.

これを基にしてさらに次の解を探す. $a=11 \times 19 \times 211q$ が解であるとする.

$$7\varphi(a)-6a=7 \times 180 \times 210q-6 \times 11 \times 19 \times 211q$$

$g=210$ とおくと

$$\begin{aligned} 7 \times 180 \times 210-6 \times 11 \times 19 \times 211 &= 6(7 \times 30 \times 210-11 \times 19 \times 211) \\ &= 6(g^2-(g-1)(g+1)) \\ &= 6. \end{aligned}$$

よって

$$7\varphi(a)-6a=6(q-210^2)=6.$$

これより, $q-210^2=1$.

そこで $q=210^2+1$ は素数であることを確認する.

```
?- A is 210^2,factorize(A,B).
A = 44100,
B = [2, 2, 3, 3, 5, 5, 7, 7].
```

```
?- A is 210^2+1,factorize(A,B).
A = 44101,
B = [44101].
```

これらが解であることを Prolog で確認する.

```
?- G is 210,A is 11*19*(G+1)*(G^2+1), euler(A,H), HH is 7*H-6*A.
G = 210,
A = 1944809999,
H = 1666980000,
HH = 6.
```

驚いたことに $210^4 + 1$ も素数となってつながった. 私はこのことに遭遇し, 美しい数理の世界を発見したことを確信した. そして, 素数 4 姉妹を組織的に探索することにしたのである.

```
?- A is 210^4+1,factorize(A,B).
A = 1944810001,
B = [1944810001].
```

しかしその先は $210^8 + 1 = 17 \times 222487408005882353$ となり合成数なのである. 正直のところほっとした.

さらに $210^{16} + 1 = 4289 * 3375137 * 988237349365458759113415457$ となる.

```
1 ?- B=17,A is B-1,factorize(A,AA),exps(AA,AS).
B = 17,
A = 16,
AA = [2, 2, 2, 2],
AS = [2^4].
```

```
2 ?- B=222487408005882353,A is B-1,factorize(A,AA),exps(AA,AS).
B = 222487408005882353,
A = 222487408005882352,
AA = [2, 2, 2, 2, 113, 197, 1297, 21841, 22051],
AS = [2^4, 113, 197, 1297, 21841, 22051].
```

$m = 3, m + 1 = 4$ なので 2^4 が出た.

```
A = 17,
B = 16,
```

BS = [2^4].

2 ?- A=4289, B is A-1, factorize(B, BB), exps(BB, BS).

A = 4289,

B = 4288,

BS = [2^6, 67].

3 ?- A=3375137, B is A-1, factorize(B, BB), exps(BB, BS).

A = 3375137,

B = 3375136,

BS = [2^5, 29, 3637].

$7\varphi(a) - 6a = 6$ を満たす a は 210. これを α とおくと,

$$13, \alpha - 1, (\alpha - 1) * (\alpha + 1), (\alpha - 1) * (\alpha + 1) * (\alpha^2 + 1), (\alpha - 1) * (\alpha + 1) * (\alpha^2 + 1)(\alpha^4 + 1)$$

が解であり, たぶんこれしかない.

$\alpha + 1, \alpha^2 + 1, \alpha^4 + 1$ は $P = 7$ のときのフェルマー素数と呼ばれる権利がある. $g = \alpha = 210$ のときは $210\varphi(a) = 209a + 1$ の解になっている.

$\alpha - 1 = 11 * 19$ なので素数ではない.

$7\varphi(a) - 6a = 6$ を満たす a は $\gamma = 11 * 19$ とおくと

$$\gamma, \gamma * (\alpha + 1), \gamma * (\alpha + 1)(\alpha^2 + 1), \gamma * (\alpha + 1)(\alpha^2 + 1)(\alpha^4 + 1).$$

10.11 $a = pqr$ のときの証明

$s(a) = 3$ とする. この場合も a は平方因子がないことがわかり, $a = pqr, p < q < r$ と書けるので次の方程式を解く:

$$7\overline{pqr} = 6pqr + 6.$$

これから $p = 11, q = 19, r = 211$ を導くのは簡単ではない. しかし, 実行してみたら意外におもしろかった.

$A = \overline{qr}, B = qr$ で置き換えると $7\overline{pA} = 6pB + 6$ となるので $7\overline{pA} = 7pA - 7A$ より

$$p(7A - 6B) = 7A + 6$$

$$C = 7A - 6B = qr - 7(q + r - 1) = (q - 7)(r - 7) - 42$$

となり, $q_1 = q - 7, r_1 = r - 7$ とおけば $C = q_1 r_1 - 42$.

一方, $7A + 6 = 7\overline{pqr} + 6 > 7q_1 r_1 + 6$ によって

$$p(7A - 6B) = pC = p(q_1 r_1 - 42) = 7A + 6 > 7q_1 r_1 + 6$$

と変形して

$(p-7)q_1r_1 > 6 + 42p$. $p > 7$ になるが p は素数なので $p \geq 11$.
 $p = 11$ と $p \geq 13$ について場合に分ける.

10.12 $p = 11$

$p = 11$.

$r > q > p = 11$ により $q \geq 13, r \geq 17$.

$\bar{q} = q - 1 = q_1 + 6, \bar{r} = r - 1 = r_1 + 6$ を代入して

$$\begin{aligned} pC &= 11(q_1r_1 - 42) = 7A + 6 = 7\bar{q}\bar{r} + 6 \\ &= 7(q_1 + 6)(r_1 + 6) + 6 \\ &= 7q_1r_1 + 42(q_1 + r_1) + 7 * 36 + 6 \end{aligned}$$

これより

$$4q_1r_1 = 42(q_1 + r_1) + 7 * 36 + 6 + 11 * 42.$$

2で割って

$$2q_1r_1 = 21(q_1 + r_1) + 7 * 18 + 3 + 11 * 21.$$

$7 * 18 + 3 + 11 * 21 = 360$ に注意して

$$q_1(2r_1 - 21) = 21r_1 + 360.$$

2倍して

$$2q_1(2r_1 - 21) = 21(2r_1 - 21) + 2 * 360 + 21^2.$$

$$2q_1(2r_1 - 21) - 21(2r_1 - 21) = (2q_1 - 21)(2r_1 - 21) = 2 * 360 + 21^2.$$

$2 * 360 + 21^2 = 1161 = 3^3 * 43$ によって $\alpha = 2q_1 - 21, \beta = 2r_1 - 21$ とおくと

$$\alpha\beta = 3^3 * 43.$$

$q \geq 13, r \geq 17$ なので $q_1 \geq 6, r_1 \geq 10$.

数値の比較によって, $\alpha > 0, \beta > 0$ なので

q, r がともに素数になるのは $q = 19, r = 211$.

表 10.13:

α	$\beta > 0$	q_1	r_1	q	r
3	387	12	204	19	211
9	129	15	75	22	82
27	43	24	32	31	39

10.12.1 $p \geq 13$.

$$p(q_1 r_1 - 42) = 7A + 6 = 7q\bar{r} + 6 \geq 13(q_1 r_1 - 42)$$

によって

$$p = \frac{7(q_1 + 6)(r_1 + 6) + 6}{q_1 r_1 - 42}.$$

かつ

$$7(q_1 + 6)(r_1 + 6) + 6 \geq 13q_1 r_1 - 13 * 42.$$

$$7(6(q_1 + r_1) + 6^2) + 6 \geq 6q_1 r_1 - 13 * 42$$

を 6 で割ると

$$7(q_1 + r_1) + 6 \geq q_1 r_1 - 13 * 7 - 1.$$

$$134 \geq (q_1 - 7)(r_1 - 7) - 49.$$

$q_2 = q_1 - 7, r_2 = r_1 - 7$ とおくとき

$$183 \geq q_2 * r_2$$

$p \geq 13$ によって $q \geq 17$. これより $q_2 \geq 3$.

したがって $r_2 \leq \frac{183}{3} = 61$. ゆえに $r \leq 14 + 61 = 75$.

$$p = \frac{7(q_1 + 6)(r_1 + 6) + 6}{q_1 r_1 - 42} = p_0. \tag{10.2}$$

の右辺 p_0 を計算した結果 13 以上で素数になればそこから解がでる.

以上の計算にあるように p_0 を計算した結果整数になる場合があるがそれは 15 で素数ではない. これから解はもうないことが分かる.

以上の計算は $s(a) = 3$ の場合であり $s(a) \geq 4$ の場合にも矛盾を導いて解がこれ以上ないことを確定したいが困難が大きいと想定される.

今はひたすらため息をはくだけ.

表 10.14: $q = 17$

q	19	23	29	31	37	41	43	47	53	59	61	67	71	73
q_1	12	16	22	24	30	34	36	40	46	52	54	60	64	66
$p_0 =$	25.9	20.9	17.6	17	15.6	15	14.8	14.4	13.9	13.6	13.5	13.2	13.1	13.1

表 10.15: $q = 19$

q	23	29	31	37	41	43	47
q_1	16	22	24	30	34	36	40
$p_0 =$	18.5	15.9	15.3	14.2	13.7	13.5	13.2

表 10.16: $q = 23$

q	29	31
q_1	22	24
$p_0 =$	13.9	13.5

10.13 素数 3 姉妹の一般形

一般に偶数 g に対して $g+1, g^2+1, g^4+1$ が素数になる場合これを素数 **3** 姉妹という. ここで $B_1 = g+1, B_2 = B_1(g^2+1), B_3 = B_2(g^4+1) = (g+1)(g^2+1)(g^4+1)$ とおくと

$$(g-1)B_1 = g^2 - 1, (g-1)B_2 = g^4 - 1, (g-1)B_3 = g^8 - 1.$$

$B_3 = (g+1)(g^2+1)(g^4+1)$ により

$$\varphi(B_3) = g * g^2 * g^4 = g^7.$$

$$g\varphi(B_3) = g^8 = g^8 - 1 + 1 = (g-1)B_3 + 1.$$

ゆえに B_3 は $g\varphi(a) = (g-1)a + 1$ の解になる.

また B_1 と B_2 もこの解である. 実際

$$g\varphi(B_1) - (g-1)B_1 = g^2 - (g-1)(g+1) = 1,$$

$$g\varphi(B_2) - (g-1)B_2 = g^4 - (g-1)(g+1)(g^2+1) = 1.$$

10.13.1 素数 3 姉妹の探索

偶数 g に対して $a_1 = g + 1, a_2 = g^2 + 1, a_4 = g^4 + 1$ が素数になる場合を求め, $g - 1$ と $a_8 = g^8 + 1$ を素因数分解した結果次の表が得られた. $a_8 = g^8 + 1$ は 17 で割れる場合が多い. すべて合成数であった. 素因数分解も表示するため, 次行に表示させた.

表 10.17: $g < 1000$ での素数 3 姉妹

g	$g - 1$ の素因数分解	a_1	a_2	a_4	a_8
2	1=[1]	3	5	17	257
4	3=[3]	5	17	257	65537
6	5=[5]	7	37	1297	1679617= 17 * 98801
16	15=[3,5]	17	257	65537	4294967297 = 641 * 6700417
180	179=[179]	181	32401	1049760001	1101996057600000001
180	--	--	--	--	= 17 * 14561 * 4451843795473
210	209=[11,19]	211	44101	1944810001	3782285936100000001
210	--	--	--	--	= 17 * 222487408005882353
430	429=[3,11,13]	431	184901	34188010001	1168820027760100000001
430	--	--	--	--	= 17 * 68754119280005882353
466	465=[3,5,31]	467	217157	47156728337	2223757027355305328897
466	--	--	--	--	= 17 * 2689 * 48646053143641969
556	555=[3,5,37]	557	309137	95565066497	9132681934384901718017
556	--	--	--	--	= 17 * 537216584375582454001
690	689=[13,53]	691	476101	226671210001	51379837442864100000001
690	--	--	--	--	= 17 * 3022343378992005882353
760	759=[3,11,23]	761	577601	333621760001	111303478745497600000001
760	--	--	--	--	= 17 * 4550737 * 18610577 * 77306897
936	935=[5,11,17]	937	876097	767544201217	589124100820307495878657
936	--	--	--	--	= 271897777 * 2166711722767441
966	965=[5,193]	967	933157	870780120337	758258017972378640752897
966	--	--	--	--	= 17 * 881 * 2081 * 18032177 * 1349186353

たとえば $g = 2$ なら $g + 1 = 3, g^2 + 1 = 5, g^4 + 1 = 17$
 $g = 16$ なら $g + 1 = 17, g^2 + 1 = 257, g^4 + 1 = 65537$ となりフェルマー素数の 5 兄弟の年長 3 人組が出ている.
 これらを除くと, $g = 6, 180, 210, 430$ について調べるのがおもしろそうである.

10.13.2 $g = 180$

$g = 180$ のときの素数 3 姉妹の場合を計算しよう.

$g + 1, g^2 + 1, g^4 + 1$ が素数になる場合これを素数 3 姉妹という.

$g - 1 = 179$ も素数なので $g - 1 = 179, g + 1 = 181, g^2 + 1 = 32401, g^4 + 1 = 1049760001$ が素数 4 姉妹になる.

$B_1 = g + 1, B_2 = B_1(g^2 + 1), B_3 = B_2(g^4 + 1) = (g + 1)(g^2 + 1)(g^4 + 1)$ とおくとき

$B_1 = 181, B_2 = B_1 * 32401, B_3 = B_2 * 1049760001$ は $180\varphi(a) = 179a + 1$ の解になる.

$g - 1 = 179$ も素数であって $C_j = 179B_j (j > 0)$ とおく. すると,

$$180\varphi(C_j) = 178(C_j + 1).$$

よって C_j は $90\varphi(a) = 89(a + 1)$ の解 a になる. さらに $C_0 = g - 1 = 179$ も解.

表 10.18: $90\varphi(a) = 89(a + 1)$

a	$\varphi(a)$	素因数分解
179	178	[179]
32399	32040	[179, 181]
1049759999	1038096000	[179, 181, 32401]
1101996057599999999	1089751656960000000	[179, 181, 32401, 1049760001]

計算機の性能がもっとよければその先も見えるはずなのである.

10.13.3 $g = 430$

$g = 430$ のときの素数 3 姉妹の場合を計算しよう.

429 は [3, 11, 13] という素因数分解をもつ. $431 = g + 1, 184901 = g^2 + 1, 34188010001 = g^4 + 1$ は素数 3 姉妹なのだがこれに合成数 429 もいれて 4 姉妹

$429, 429 * B_1, 429 * B_2, 429 * B_4$ は $43\varphi(a) = 24(a + 1)$ の解になる. パソコンでチェックすると次の通り.

表 10.19: $43\varphi(a) = 24(a + 1)$

a	$\varphi(a)$	素因数分解
429	240	[3, 11, 13]
184899	103200	[3, 11, 13, 431]

10.13.4 $g = 936$

$g = 936$ のときの素数 3 姉妹の場合を計算しよう.

935 は $[5, 11, 17]$ という素因数分解をもつ.

$935, 935 * B1, 935 * B2, 935 * B4$ は $117\varphi(a) = 80(a + 1)$ の解になる. パソコンでチェックすると次の通り.

表 10.20: $117\varphi(a) = 80(a + 1)$

a	$\varphi(a)$	素因数分解
935	640	$[5, 11, 17]$
61775	42240	$[5^2, 7, 353]$
876095	599040	$[5, 11, 17, 937]$

素因数分解 $[5, 11, 17], [5, 11, 17, 937]$ を持つ解は期待通りであるが素因数分解 $[5^2, 7, 353]$ を持つ 2 番目の解が不思議である.

10.14 素数4姉妹の場合

素数3姉妹に対して $g-1$ も素数の場合 $g-1, g+1, g^2+1, g^4+1$ を素数4姉妹と呼ぶ。
 $g-1$ も素数であって $C_j = (g-1)B_j$ ($j > 0$) とおくと、

$$g\varphi(C_j) = g\varphi((g-1)B_j) = (g-2)g\varphi(B_j) = (g-2)((g-1)B_j + 1) = (g-2)(C_j + 1).$$

さらに $C_0 = g-1$ が素数のとき

$$g\varphi(C_0) = g(g-2) = (g-2)g = (g-2)(C_0 + 1).$$

とくに $g=6$ なら

$$3\varphi(C_j) = 2(C_j + 1) = 2C_j + 2.$$

$3\varphi(a) = 2a + 2$ の解として C_0, C_1, C_2, C_3 ($C_0 = g-1$ とおいた) が得られた。
 しかし、4姉妹以外の解があるかもしれない。

10.14.1 養女登場

$\alpha - 1 = 11 * 19 = \gamma$ は素数ではないが養女とみてこれも加え4姉妹とみなす。
 さて $C_j = (\alpha - 1)B_j$ ($j = 1, 2, 3$) とおきそのオイラー関数を考える。

$$\begin{aligned} \alpha\varphi(C_j) &= \varphi(11 * 19)\alpha\varphi(B_j) \\ &= 180((\alpha - 1)B_j + 1) \\ &= 180(C_j + 1). \end{aligned}$$

$\alpha = 210$ なので

$$\alpha\varphi(C_j) = 210\varphi(C_j) = 180(C_j + 1).$$

ゆえに $7\varphi(C_j) = 6(C_j + 1)$ 。よって C_1, C_2, C_3 は $7\varphi(a) = 6(a + 1)$ の解になっている。

$11 * 19$ も解である。これを C_0 とする。 $\alpha - 1, \alpha + 1, \alpha^2 + 1, \alpha^4 + 1$ を4姉妹とするとこれらの順の積から $7\varphi(a) = 6(a + 1)$ の解 C_0, C_1, C_2, C_3 が得られた。

しかし $C_{-1} = 13$ という素数解もあった。このような解のあることに理屈がつかない。

13の声を聴いてほしい。

13の声: お父さん、4姉妹以外に僕もいることを忘れないで下さい。

10.14.2 $3\varphi(a) = 2a + 2$ の解

$g = 6$ についての素数 4 姉妹の式は $3\varphi(a) = 2a + 2$ である.

パソコンによる結果は次の通りで明らかに解の一部しかでていない. これを元に考えるのはやや危険である. この表によると解は 5 の倍数らしい.

表 10.21: $3\varphi(a) = 2(a + 1)$ を満たす a

a	$\varphi(a)$	素因数分解
5	4	[5]
35	24	[5, 7]
1295	864	[5, 7, 37]

そこで $a = 5L$ (L は 5 で割れないとする) とおくと

$$12\varphi(a) = 6\varphi(5L) = 4\varphi(L), 2a + 2 = 10L + 2$$

により

$$6\varphi(L) = 5L + 1.$$

この解には 平方因子はない.

$s(L) = 1$ のとき.

$L = p$ とおいて簡単な計算によって $p = 7$.

$s(L) = 2$ のとき.

$L = pq, p < q$ とおく.

$6\bar{p}\bar{q} = 5pq + 1$ により

$$p(q - 6) = 6q - 5.$$

$p_6 = p - 6, q_6 = q - 6$ を使うと簡単な計算によって

$$pq_6 = 6q_6 + 31.$$

これより

$$p_6q_6 = 31.$$

よって $p_6 = 1, q_6 = 31$. すなわち $p = 7, q = 37$.

$s(L) = 3$ のとき.

$L = pqr, p < q < r$ とおく.

$\varphi(L) = \bar{p}\bar{q}\bar{r}$ により $A = \bar{q}\bar{r}, B = qr$ とおけば $6\varphi(L) = 5L + 1$ は次の形になる.

$$6\bar{p}A = 5pB + 1.$$

これより

$$p(6A - 5B) = 6A + 1$$

をえて,

$$6A - 5B = q(6\bar{r} - 5r) - 6\bar{r} = q_6 r_6 - 30$$

により

$$p(q_6 r_6 - 30) = 6A + 1 = 6\bar{q}'\bar{r} + 1.$$

$\bar{q} = q_6 + 5, \bar{r} = r_6 + 5, \Delta_6 = q_6 + r_6, \beta = q_6 r_6 - 30$ を用いて

$$6\bar{q}'\bar{r} + 1 = 6(q_6 + 5)(r_6 + 5) + 1 = 6q_6 r_6 + 5\Delta_6 + 25 + 1$$

と

$$p = 6 + \frac{6(55 + \Delta_6) + 1}{\beta} > 6$$

をえる.

$p = 7$ のとき,

$$6(55 + \Delta_6) + 1 = \beta = q_6 r_6 - 30.$$

$x = q_6, y = r_6$ とおけば

$$xy = 30 + 6 \times 5(11 + x + y) + 1 = 30(x + y) + 30 \times 12 + 1.$$

$x' = x - 30, y' = y - 30$ とすると

$$x'y' = 900 + 361 = 1261 = 13 \times 97. \quad (10.3)$$

$x' = 13, y' = 97$ とおくとき $q = 13 + 30 + 6 = 49$ は素数ではない.

$x' = 1, y' = 1261$ としてみると $q = 1 + 30 + 6 = 37, r = 1261 + 30 + 6 = 1297$ となりこれらは素数.

$37 = 6^2 + 1, 1297 = 6^4 + 1$ となることに注意.

このときの解は

$$p = 6 + 1 = 7, q = 6^2 + 1 = 37, r = 6^4 + 1 = 1297.$$

$p > 7$ のとき $p \geq 11$.

$$6(55 + \Delta_6) + 1 \geq 5\beta.$$

これから前と同様に式変形すると $x' < y', 132 \geq x'y' > x'^2$. よって $11 \geq x'$. これより可能性が絞られて, パソコン計算で矛盾が出る.

10.14.3 $7\varphi(a) - 6a = 6$ を満たす a

$7\varphi(a) - 6a = 6$ を満たす a を証明で求める.

$s(a) = 1$ とする.

$a = p^e$ に対して, $e > 1$ とすると, $e = 2, p = 2, 3$. これより直ちに矛盾.

$a = p$ なら $7\varphi(a) - 6a = 7\overline{P} = 6p + 6$. これより $p = 13$.

$s(a) = 2$ とする. この場合も a は平方因子がないことがわかり, $a = pq, p < q$ と書ける.

$7\overline{P}(q-1) = 6pq + 6$ によって,

$$p(q-7) = 7q - 1 = 7(q-7) + 48.$$

$p = 7 + \frac{48}{q-7}$ によって $q-7 = 48, 24, 16, 12, 8, 6$. $q-7 = 12, p = 7+4$.

よって $p = 11, q = 19$.

10.15 素数親子の探索

偶数 g に対して $a_1 = g+1, a_2 = g^2+1$ が素数になる場合 (a_1, a_2) が素数親子である. 素数親子 (a_2 が大五郎) を求めた.

$a_0 = g-1$ を素因数分解し, そのオイラー関数 e_0, g と e_0 の最大公約数 D でそれらを割ってできた対 $([\alpha, \beta])$ を求めた結果次の表が得られた.

素数親子だと条件が緩和されるから扱いやすい例も増える. 念のため, この場合も詳しく述べる.

$B_2 = a_1 a_2$ とおくと a_1, a_2 が素数なので

$$\varphi(B_2) = \varphi(a_1)\varphi(a_2) = g^3.$$

$$\bar{g} = g-1 = a_0, \bar{g}B_2 = \bar{g}(g+1)(g^2+1) = g^4-1$$

$$g\varphi(B_2) = g^4-1+1 = \bar{g}B_2+1.$$

したがって B_2 (そして $B_1 = a_1$ も) も次の方程式の解である.

$$g\varphi(a) = \bar{g}a+1$$

10.15.1 数値例**10.15.2** $a_0 = g-1$

$a_0 = g-1$ も入れて $C_2 = a_0 B_2$ とおけば $g\varphi(B_2) = \bar{g}(B_2) + 1$ によって,

$$g\varphi(C_2) = \varphi(a_0)g\varphi(B_2) = \varphi(g-1)(\bar{g}(B_2) + 1) = \varphi(g-1)(C_2 + 1)$$

表 10.22: 素数親子の表

g	$a_0 = g - 1$	$\varphi(a_0)$	$[\alpha, \beta]$	a_1	a_2	a_4 素因数分解
4	3=[3]	2	[2,1]	5	17	257=[257]
6	5=[5]	4	[3,2]	7	37	1297=[1297]
10	9=[3,3]	6	[5,3]	11	101	10001=[73,137]
16	15=[3,5]	8	[2,1]	17	257	65537=[65537]
36	35=[5,7]	24	[3,2]	37	1297	1679617=[17,98801]
40	39=[3,13]	24	[5,3]	41	1601	2560001=[769,3329]
66	65=[5,13]	48	[11,8]	67	4357	18974737=[17,409,2729]
126	125=[5,5,5]	100	[63,50]	127	15877	252047377=[41,89,69073]
130	129=[3,43]	84	[65,42]	131	16901	285610001=[97,2944433]
150	149=[149]	148	[75,74]	151	22501	506250001=[41,193,63977]
156	155=[5,31]	120	[13,10]	157	24337	592240897=[73,953,8513]
180	179=[179]	178	[90,89]	181	32401	1049760001=[1049760001]
210	209=[11,19]	180	[7,6]	211	44101	1944810001=[1944810001]
240	239=[239]	238	[120,119]	241	57601	3317760001=[17,6481,30113]
250	249=[3,83]	164	[125,82]	251	62501	3906250001=[457,8547593]
256	255=[3,5,17]	128	[2,1]	257	65537	4294967297=[641,6700417]
270	269=[269]	268	[135,134]	271	72901	5314410001=[17,73,113,37897]
280	279=[3,3,31]	180	[14,9]	281	78401	6146560001=[17,361562353]
306	305=[5,61]	240	[51,40]	307	93637	8767700497=[67777,129361]
396	395=[5,79]	312	[33,26]	397	156817	24591257857=[41,599786777]
400	399=[3,7,19]	216	[50,27]	401	160001	25600000001=[17,1505882353]

表 10.23: $g = 6; 6\varphi(a) - 5a = 1$

a	$\varphi(a)$	素因数分解
7	6	[7]
259	216	[7, 37]

によって

$$g\varphi(C_2) = \varphi(g - 1)(C_2 + 1).$$

したがって

$$g\varphi(a) = \varphi(g - 1)(a + 1) \tag{10.4}$$

の解として

$$C_2, C_1, C_0 = g - 1$$

が得られた.

表 10.24: $g = 40; 40\varphi(a) - 39a = 1$

a	$\varphi(a)$	素因数分解
41	40	[41]
12361	12052	[47, 263]
65641	64000	[41, 1601]

表 10.25: $g = 10; 10\varphi(a) - 9a = 1$

a	$\varphi(a)$	素因数分解
11	10	[11]
391	352	[17, 23]
1111	1000	[11, 101]

さらに $(g, \varphi(g-1))$ の最大公約数で各項を割ってできた数のペアを $[\alpha, \beta]$ と書くとき方程式は次のように書けて, 解として最初から 3 個ある.

$$\alpha\varphi(a) = \beta(a+1).$$

10.16 $5\varphi(a) = 3(a+1)$ の解

($\alpha = 5, \beta = 3$) に対応して方程式 $5\varphi(a) = 3(a+1)$ ができる.

表 10.26: $5\varphi(a) = 3(a+1)$ を満たす a

a	$\varphi(a)$	素因数分解
9	6	$[3^2]$
39	24	$[3, 13]$
99	60	$[3^2, 11]$
1599	960	$[3, 13, 41]$
3399	2040	$[3, 11, 103]$
3519	2112	$[3^2, 17, 23]$
9999	6000	$[3^2, 11, 101]$
2559999	1536000	$[3, 13, 41, 1601]$

意外にも解が多い. 解は 3 を因子にもつか 3^2 を因子に持つかで 2 つに分かれる.
 3^2 を因子に持つときの素因数分解は

$$[3^2], [3^2, 11], [3^2, 17, 23], [3^2, 11, 101]$$

である.

$g = 10$ とおくと, $g-1 = 3^2, g+1 = 11, g^2+1 = 101$ なのでこれは子連れ狼の家族である.
 $[3^2, 17, 23]$ は偶然拾われた子どものようだ.

3 を因子に持つときの素因数分解は

$$[3, 13], [3, 13, 41], [3, 11, 103], [3, 13, 41, 1601]$$

であり, $g = 40$ とすると, $g-1 = 39 = 3 \times 13, g+1 = 41, g^2+1 = 1601$ は素数なのでこれら
 で子連れ狼の別家族でやはり $[3, 11, 103]$ 偶然拾われた子どものようだ.

次の予想を立てる:

- (1) 解は 3 で割れる.
- (2) 解は以上の 2 家族 6 名に拾われた子ども 2 を加えて 8 名.

この証明は難しそうである.

(1) 解は 3 で割れる.

を証明無しで受け入れる.

$5\varphi(a) = 3(a+1)$ を満たす a の平方因子はあったとすれば 3^2 だけなので

i. $a = 3L, (L:3 \text{ で割れない})$. と ii. $a = 3^2L, (L:3 \text{ で割れない})$ の 2 つの場合がある.

10.16.1 $a = 3L$ の場合

i. $a = 3L$, ($L:3$ で割れない).

$a = 3$ によって

$5\varphi(a) = 5\varphi(3L) = 10\varphi(L)$, $3(a+1) = 9L+3$ によって

$$10\varphi(L) = 9L + 3.$$

$s(L) = 1$. $L = p$ とおくとき, $10\bar{p} = 9p + 3$ によって $p = 13$.

$s(L) = 2$. $L = pq$ とおくとき, $10\bar{p}\bar{q} = 9pq + 3$ によって $p(q-10) = 10q - 7$.

$q_{10} = q - 10$, $p_{10} = p - 10$ を使うと $pq_{10} = 10q_{10} + 93$ により

$$p_{10}q_{10} = 93 = 3 \times 31.$$

$p_{10} = 1$, $q_{10} = 93$; $p = 11$, $q = 103$ および $p_{10} = 3$, $q_{10} = 31$; $p = 13$, $q = 41$.

$s(L) = 3$. $L = pqr$ とおくとき, $A = \bar{q}\bar{r}$, $B = qr$ とおけば

$$10\bar{q}A = 9pB + 3.$$

$$p(10A - 9B) = 10A + 3$$

となり $10A - 9B = q_{10}r_{10} - 90$. ここで $q_{10} = q - 10$, $r_{10} = r - 10$.

$\gamma = q_{10}r_{10} - 90$ とおくとき $p\gamma = 10A + 3$. $\Delta_{10} = q_{10} + r_{10}$ を使うと

$$10A + 3 = 10(q_{10}r_{10} - 90 + 9\Delta_{10} + 171) + 3$$

$$p = 10 + \frac{90\Delta_{10} + 1713}{\gamma} > 10.$$

$x = q_{10}$, $y = r_{10}$ とおけば $\gamma = xy - 90$.

$p \geq 11$ なので $p = 11$ とする.

$$p\gamma = 11(xy - 90) = 10(xy + 9(x + y)) + 813.$$

よって $xy = 90(x + y) + 990 + 813$.

$\alpha = x - 90$, $\beta = y - 90$ とおけば

$$\alpha\beta = 990 + 813 + 8100 = 9903 = 3 \times 3301.$$

1). $\alpha = 1$, $\beta = 9903$; $q = 101$, $r = 10003 = 7 \times 1429$. 素数ではない.

2). $\alpha = 3$, $\beta = 3301$; $q = 103$, $r = 3401 = 19 \times 179$. 素数ではない. したがって解は無い.

次に $p = 13$ とする.

$$p\gamma = 13(xy - 90) = 10(xy + 9(x + y)) + 813.$$

よって

$$3xy = 90(x + y) + 990 + 813 = 3 \times 30(x + y) + 3 \times 661.$$

すなわち

$$xy = 30(x + y) + 661.$$

$\alpha = x - 30 = q - 40, \beta = y - 30 = r - 40$ とおけば

$$\alpha\beta = 900 + 661 = 1561 = 7 \times 223.$$

1). $\alpha = 1, \beta = 1561; q = 101, r = 1601$. 素数.

$$a = 3 \times 13 \times 101 \times 1601.$$

1). $\alpha = x - 30 = 1, \beta = y - 30 = 1561; q = 41, r = 1601$. ここから $a = 3 \times 13 \times 41 \times 1601$. これは予測された解.

2). $\alpha = x - 30 = 7, \beta = y - 30 = 223; q = 47, r = 263; a = 3 \times 13 \times 47 \times 263$. これは意外な解.

私は非常に感動した. 大五郎の友達が見つかったような気がした.

表 10.27: $5\varphi(a) = 3(a + 1)$ を満たす a

a	$\varphi(a)$	素因数分解
9	6	$[3^2]$
39	24	$[3, 13]$
99	60	$[3^2, 11]$
1599	960	$[3, 13, 41]$
3399	2040	$[3, 11, 103]$
3519	2112	$[3^2, 17, 23]$
9999	6000	$[3^2, 11, 101]$
2559999	1536000	$[3, 13, 41, 1601]$
482079	289248	$[3, 13, 47, 263]$

$p \geq 17$ のとき解はないことをいいたい.

研究課題にさせて下さい.

10.16.2 $a = 3^2L$ の場合

ii. $a = 3^2L, (L : 3 \text{ で割れない})$.

$a = 3^2L$ によって $5\varphi(a) = 5\varphi(9L) = 30\varphi(L)$, $3(a+1) = 27L+3$ となり

$$10\varphi(L) = 9L + 1.$$

$s(L) = 1$ のとき $L = 11$.

$s(L) = 2$ のとき $L = 11 \times 101$.

$s(L) = 3$ のとき $L = pqr$.

$A = \bar{q}'\bar{r}$, $B = qr$ とおけば

$$10\bar{q}'A = 9pB + 1.$$

$$p(10A - 9B) = 10A + 1$$

となり $10A - 9B = xy - 90$. ここで $x = q - 10$, $y = r - 10$.

$$10A + 1 = 10\bar{q}'\bar{r} + 1 = 10(x+9)(y+9) + 1 = 10xy + 90(x+y) + 811.$$

により

$$p(xy - 90) = 10xy + 90(x+y) + 811$$

これから $p \geq 11$.

$p = 11$ とする.

$$xy = 90(x+y) + 811 + 990 = 90(x+y) + 1801.$$

2). $\alpha = x - 90 = q - 100$, $\beta = y - 90 = r - 100$ によって

9901 は素数なので $\alpha = 1$; $\beta = 9901$. $q = 101$ は素数. しかしながら $r = 9901 + 100 = 10^4$. これは素数ではない.

10.17 素数おひとりの世界

$a = p$ が素数のとき $\varphi(a) = a - 1$ を満たす. 逆に $\varphi(a) = a - 1$ を満たす自然数 a は素数になる. 素数についてこのような取り扱いはごく自然である.

$\bar{p} = p - 1 = g$ とおき $a = p$ が素数のとき $g\varphi(a) = \bar{P}^2 = (p - 2)p + 1 = \bar{g}a + 1$ と表される. 素数 p が与えられたとき $g = p - 1$ とおく.

$$g\varphi(a) = \bar{g}a + 1 \quad (10.5)$$

を満たす a を求めよ.

$a = p$ はこの方程式の解であり, 通常解とする. この他の解があれば p の親族解と考える.

親族解のみつからない素数 p は素数ひとりと呼んでもよいだろう.

素数ひとりとはたしているか, ひとりと思っけていても探索すると親戚筋がでてくるかもしれない.

10.17.1 数値解の例

$P = 3$ のとき $2\varphi(a) = a + 1$.

表 10.28: $P = 3$

a	$\varphi(a)$	素因数分解
3	2	[3]
15	8	[3, 5]
255	128	[3, 5, 17]
65535	32768	[3, 5, 17, 257]

この場合 $g = 2$ で式は $2\varphi(a) = a + 1$ なのですでに扱ってきた.

これらはフェルマー素数の積の解であるが他の解もでてきた.

$P = 5$ のとき $4\varphi(a) = 3a + 1$.

表 10.29: $P = 5$

a	$\varphi(a)$	素因数分解
5	4	[5]
85	64	[5, 17]
21845	16384	[5, 17, 257]

$g = 4$ になり $4\varphi(a) = 3a + 1$ が式である. これらは 5 から始まるフェルマー素数の積である.

これ以外の解があるだろうか.

$5\varphi(a) = 6a + 1$ が式であり素数 3 姉妹としてすでに扱った. これ以外の解があるだろうか.

表 10.30: $P = 7$

a	$\varphi(a)$	素因数分解
7	6	[7]
259	216	[7, 37]
335923	279936	[7, 37, 1297]

表 10.31: $P = 11$

a	$\varphi(a)$	素因数分解
11	10	[11]
391*	352	[17, 23]
1111	1000	[11, 101]

表 10.32: $P = 13$

a	$\varphi(a)$	素因数分解
13	12	[13]
589*	540	[19, 31]

$g = 10$ であって (11,1111) は素数親子であり, 391* ([17, 23]) は例外的解.

$g = 12$. 素数親子ですらないが, 589 ([19, 31]) は例外的解.

以下では 例外的解が引き続きあり素数ひとは認めることができない.

表 10.33: $P = 17$

a	$\varphi(a)$	素因数分解
17	16	[17]
4369	4096	[17, 257]

$g = 16$ のとき $g^2 + 1 = 257$ になるのでこれはフェルマー素数による 5 兄弟の一部.

表 10.34: $P = 19$

a	$\varphi(a)$	素因数分解
19	18	[19]
167743*	158424	[43, 47, 83]

$g = 18$ で $s(a) = 3$ という扱づらい例がでている.

表 10.35: $P = 23$

a	$\varphi(a)$	素因数分解
23	22	[23]
2279*	2184	[43, 53]

表 10.36: $P = 29$

a	$\varphi(a)$	素因数分解
29	28	[29]
4469*	4320	[41, 109]

10.17.2 $s(a) = 2$ の解

$g\varphi(a) = \bar{p}a + 1$ に $s(a) = 2$ の解 $a = qr$, ($q < r$) があるとしよう.

$\varphi(a) = \bar{q}\bar{r} = qr - \Delta + 1$ によって

$$qr = g(\Delta - 1) + 1.$$

これより

$$(q - g)(r - g) = g^2 - g + 1.$$

$g^2 - g + 1 = p^2 - 3p + 3$ なので $D = p^2 - 3p + 3$ とおく.

$p = 11$ のとき $D = 91 = 7 * 13$.

$q = 10 + 7, r = 10 + 13 = 23$.

$p = 13$ のとき $D = 133 = 7 * 19$.

$q = 12 + 7 = 19, r = 12 + 19 = 31$.

$p = 23$ のとき $D = 463$.

$q = 22 + 2 = 23, r = 22 + 463 = 485$; 素数ではない.

$p = 29$ のとき $D = 757$.

$q = 28 + 2 = 31, r = 28 + 757 = 785$; 素数ではない.

$p = 31$ のとき $871 = 13 * 67$.

$q = 30 + 13 = 43, r = 31 + 67 = 97$; 素数.

$p = 37$ のとき $D = 1261 = 13 * 97$.

$q = 36 + 13 = 7^2$; 素数ではない.

$q = 36 + 1 = 37, r = 36 + 1261 = 1297$; 素数.

$p = 41, D = 1561 = 7 * 223. q = 47, r = 263$.

$q = 41, r = 1601$.

$p = 43, D = 1723$.

$q = 43, r = 1765$; 素数ではない.

$p = 47, D = 2071 = 19 * 109$.

$q = 65 = 5 * 13, r = 155 = 5 * 31$; 素数ではない.

表 10.37:

$P = 3$			
g	qr	素因数分解	$\sigma(qr)$
2	15	$a = 3 * 5$	24
$P = 5$			
4	85	$a = 5 * 17$	108
$P = 7$			
6	259	$a = 7 * 37$	304
$P = 11$			
10	1111	$a = 11 * 101$	1224
	391	$a = 17 * 23$	432

表 10.38:

$P = 13$			
12	589	$a = 19 * 31$	640
$P = 17$			
16	4369	$a = 17 * 257$	4644
$P = 31$			
30	4171	$a = 43 * 97$	4312
$P = 37$			
36	47989	$a = 37 * 1297$	49324
$P = 41$			
40	65641	$a = 41 * 1601$	67284
	12361	$a = 47 * 263$	12672
$P = 67$			
66	291919	$a = 67 * 4357$	296344
$P = 83$			
82	91759	$a = 89 * 1031$	92880

10.18 素数ひとりの別の世界

素数 p の判定をする方程式はいろいろありうるがなるべく簡単なものを取る。

$a = p$ が素数のとき $\varphi(a) = p - 1$ なのでこの係数として \tilde{p}, p, \bar{p} のどれかを考える。

1. $\tilde{p}\varphi(a) = p^2 - 1 = pa - 1$ と変形すると中抜きして

$$\tilde{p}\varphi(a) = pa - 1. \tag{10.6}$$

2. $p\varphi(a) = p^2 - p = \bar{p}a$ と変形すると

$$p\varphi(a) = \bar{p}a.$$

この解は $a = p^e$ であることは既知の事実である。

3. $\bar{p}\varphi(a) = p^2 - 2p + 1 = (\bar{p} - 1)a + 1$ と変形できる。

$g = p - 1$ とおけば

$$g\varphi(a) = \bar{g}a + 1$$

となってこれはすでに扱われたものである。

結局 方程式 (10.6) のみが新しい。これをパソコン君の計算で求めよう。

表 10.39:

P=3		
3	2	[3]
P=5		
5	4	[5]
P=7		
7	6	[7]
247	216	[13, 19]
P=11		
11	10	[11]
P=13		
13	12	[13]
P=17		
17	16	[17]
1817	1716	[23, 79]
P=19		
19	18	[19]
P=23		
23	22	[23]
2279	2184	[43, 53]

表 10.40:

<hr/>		
$P = 29$		
29	28	[29]
4469	4320	[41, 109]
<hr/>		
$P = 31$		
31	30	[31]
<hr/>		
$P = 37$		
37	36	[37]
<hr/>		
$P = 41$		
41	40	[41]
<hr/>		
$P = 43$		
43	42	[43]
<hr/>		
$P = 47$		
47	46	[47]
9167	8976	[89, 103]
26447	25896	[53, 499]
<hr/>		

10.19 P が 11 を超えた世界

表 10.41: $11\varphi(a) = 10(a + 1)$ を満たす a

a	$\varphi(a)$	素因数分解
527	480	[17, 31]
923	840	[13, 71]
33263	30240	[29, 31, 37]
47519	43200	[19, 41, 61]

理屈が見つからない解が並んでいる。

このまま負けたくないのだから $s(a) = 2$ のとき $a = pq$ として解を探す。

$$11\varphi(a) = 11(p - 1)(q - 1) = 10pq + 1$$

から $(p - 11)(q - 11) = 120$. 120 を偶数の積 α, β にして $\alpha + 11, \beta + 11$ が素数の場合を探せばよい。

120 = 8 * 15 なので 奇数の積 $1 * 15, 3 * 5, 5 * 3, 15 * 1$ をつくりこれに (2, 4) または (4, 2) を掛ければよい。

表 10.42:

奇数	奇数	α	β	α_1	β_1	p	q	p	q
1	15	2	60	4	30	13	71	e	41
3	5	6	20	12	10	17	31	23	e
5	3	10	12	20	6	e	23	31	e
15	1	30	4	60	2	41	e	71	13

e と表示したのは 15, 21 など合成数の場合で、これを除くペア (p, q) を探すと (13, 71) と (17, 31) との 2 組がある。

表 10.43: $13\varphi(a) = 12a + 12$ を満たす a

a	$\varphi(a)$	素因数分解
779	720	[19, 41]
74359	68640	[23, 53, 61]

本当に理屈が見つからない解が並んでいる。

表 10.44: $17\varphi(a) = 16a + 16$ を満たす a

a	$\varphi(a)$	素因数分解
1189	1120	[29, 41]
168299	158400	[31, 61, 89]

正直言ってわけの分からない解が並んでいる。

10.20 6^e の場合

これまでは素数べきに限っていたが、合成数のべきの場合も考えてみた。その結果得られたモノは想像を絶する美しい数理の世界であった。

$e > 1$ に対して $a = 6^e$ とおく。

$$3\varphi(a) = 3\varphi(6^e) = 3\varphi(3^e)\varphi(2^e) = 6^e = a.$$

$W = 3\varphi(a) - a$ においてパソコン君に計算してもらう。

表 10.45: $3\varphi(a) - a = 0$

a	$\varphi(a)$	素因数分解
6	2	$[2, 3]$
12	4	$[2^2, 3]$
18	6	$[2, 3^2]$
24	8	$[2^3, 3]$
36	12	$[2^2, 3^2]$
48	16	$[2^4, 3]$
54	18	$[2, 3^3]$
72	24	$[2^3, 3^2]$
96	32	$[2^5, 3]$
108	36	$[2^2, 3^3]$
144	48	$[2^4, 3^2]$
162	54	$[2, 3^4]$
192	64	$[2^6, 3]$

$3\varphi(a) - a = 0$ の解は $a = 2^e 3^f$, $e, f > 0$ らしい.

実際, $a = 3\varphi(a)$ によって a は 3 の倍数だから $a = 3^f L$ とかける. ここで L は 3 で割れない.

$3\varphi(a) = 3\varphi(3^f L) = 2 \times 3^f \varphi(L)$, $a = 3^f L$ によれば $2\varphi(L) = L$. このとき $L = 2^e$ となる. その結果, $a = 2^e 3^f$.

10.20.1 $3\varphi(a) - a = 1$ の場合

表 10.46: $3\varphi(a) - a = 1$

a	$\varphi(a)$	素因数分解
2	1	[2]

表 10.47: $3\varphi(a) - a = 2$

a	$\varphi(a)$	素因数分解
4	2	[2 ²]
10	4	[2, 5]
70	24	[2, 5, 7]
2590	864	[2, 5, 7, 37]

$3\varphi(a) - a = 2$ を満たすとき, $\varphi(a)$ は偶数だから a も偶数. そこで $a = 2^e L$ とおけば

$$2 = 3\varphi(a) - a = 3\varphi(2^e L) - 2^e L = 3 \times 2^{e-1} \varphi(L) - 2^e L = 2^e \left(\frac{3}{2} \varphi(L) - L \right).$$

よって

$$4 = 2^e (3\varphi(L) - 2L)$$

これより $L = 1$ なら $a = 4$.

$L > 1$ のとき $e = 1; 3\varphi(L) - 2L = 2$. これはすでに扱った.

3 を底とする完全数になるので L は分かっている.

10.20.2 $3\varphi(a) - a = 4$ の場合

表 10.48: $3\varphi(a) - a = 4$

a	$\varphi(a)$	素因数分解
8	4	[2 ³]
14	6	[2, 7]
20	8	[2 ² , 5]
140	48	[2 ² , 5, 7]
5180	1728	[2 ² , 5, 7, 37]

$s(a) = 1$. $a = p^e$ とおくと, $p = 2$. $0 = 3\varphi(a) - a - 4 = 3 \cdot 2^{e-1} - 2^e - 4$. よって $e - 1 = 2; a = 8$.

a は偶数なので $a = 2^e L$ と奇数 L で書ける.

$$3 * 2^{e-1} \varphi(L) = 2^e L + 4$$

により $e - 1 = 0, 1$.

$e = 2$ なら $3\varphi(L) = 2L + 2$. この L はすでに扱った.

$e = 1$ なら

$$3\varphi(L) = 2L + 4.$$

$2L = 3\varphi(L) - 4$ により L は相異なる素因子を持たない.

$L = q$ とすれば $3(q - 1) = 2q + 4$. ゆえに $q = 7; a = 14$.

10.20.3 $3\varphi(a) - a = 8, 16$ 表 10.49: $3\varphi(a) - a = 8$

a	$\varphi(a)$	素因数分解
16	8	$[2^4]$
22	10	$[2, 11]$
28	12	$[2^2, 7]$
40	16	$[2^3, 5]$
280	96	$[2^3, 5, 7]$
10360	3456	$[2^3, 5, 7, 37]$

表 10.50: $3\varphi(a) - a = 16$

a	$\varphi(a)$	素因数分解
32	16	$[2^5]$
38	18	$[2, 19]$
44	20	$[2^2, 11]$
56	24	$[2^3, 7]$
80	32	$[2^4, 5]$
560	192	$[2^4, 5, 7]$

10.21 変位のある素数べき方程式

オイラー関数についての素数べき方程式を整数 m だけ変位させる. その意味は $g_m = P - 1 - m$ を $\varphi(a)$ の係数と定め, さらに \overline{g}_m を a の係数にし, かつ P を解に持つように定数項 α を調整する. すなわち方程式

$$g_m \varphi(a) = \overline{g}_m a + \alpha$$

が $a = P$ を解に持つとする.

$$g_m \overline{P} = \overline{g}_m P + \alpha \text{ により } \alpha = P - g_m = m + 1. \text{ かくて}$$

$$g_m \varphi(a) = \overline{g}_m a + m + 1. \tag{10.7}$$

10.21.1 例

$m = 1$

$$(P - 2)\varphi(a) = (P - 3)a + 2$$

になるので $P = 5$ なら $3\varphi(a) = 2a + 2$

$P = 7$ なら $5\varphi(a) = 4a + 2$

表 10.51: $(P - 2)\varphi(a) = (P - 3)a + 2$

a	$\varphi(a)$	素因数分解
$P = 5$		
5	4	[5]
35	24	[5, 7]
1295	864	[5, 7, 37]
$P = 7$		
7	6	[7]
$P = 11$		
11	10	[11]

$P = 5$ のときは $g = 4$ に対応する素数 3 姉妹, 5, 7, 37.

$m = 2$

$$(P - 3)\varphi(a) = (P - 4)a + 3$$

になるので $P = 5$ なら $2\varphi(a) = a + 3$

$P = 7$ なら $4\varphi(a) = 3a + 3$

表 10.52: $(P - 3)\varphi(a) = (P - 4)a + 3$

a	$\varphi(a)$	素因数分解
$P = 5$		
5	4	[5]
9	6	[3 ²]
21	12	[3, 7]
45	24	[3 ² , 5]
285	144	[3, 5, 19]
765	384	[3 ² , 5, 17]
27645	13824	[3, 5, 19, 97]
$P = 7$		
7	6	[7]
95	72	[5, 19]
9215	6912	[5, 19, 97]
$P = 11$		
11	10	[11]

$P = 5$ のとき

$2\varphi(a) = a + 3$ なので $a - 2\varphi(a) = -3$ であり興味ある例を提供した $a - 2\varphi(a) = -1$ と類似している。

$s(a) = 1$ の解は $a = 5, 3^2$.

問題 $a = 9qr, 3 < q, r : \text{素数}$, となる解を求めよ.

問題 $a = 15qr, 7 < q, r : \text{素数}$, となる解を求めよ.

第11章 φ 完全数

究極の完全数の定義を参考にユークリッド関数の代わりにオイラー関数を使って究極の完全数に類似の概念を定義しよう.

素数 $p, e \geq 2$ に対して $\varphi(p^e)$ は合成数なので完全数の定義をそのままは使えない.

そこで, 1 を加えて $\varphi(p^e) + 1$ が素数 q になるとき $a = p^e q$ をもって p を底とする φ 完全数と定義する.

φ 完全数は次の方程式を持つ:

$$p\varphi(a) = \overline{pa} - p\overline{\text{Maxp}(a)}.$$

これはとくに微小解をもち φ 完全数ではない.

$p = 2$ の場合は微小解がない. したがって, φ 完全数の方程式を満たす解は φ 完全数に限ることは正しいかもしれない.

11.1 p を底とする φ 完全数の例

$p = 2$ なら $q = 2^{e-1} + 1$ が素数の場合なので, これらはフェルマー素数である.

11.1.1 2 を底とするとき

表 11.1: 2 を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	12	$2^2 * 3$	4
3	40	$2^3 * 5$	16
5	544	$2^5 * 17$	256
9	131584	$2^9 * 257$	65536
17	8590065664	$2^{17} * 65537$	4294967296

$e > 4$ なら $q \equiv 7; a \equiv 6 \pmod{10}$ が成り立つ.

5つのフェルマー素数に応じて5つの φ 完全数ができた. これらはフェルマー φ 完全数と呼ぶ方がよい. 後で本物の φ 完全数がでてくる.

11.1.2 3 を底とするとき

$$q = 2 * 3^{e-1} + 1, a = 3^e q.$$

表 11.2: 3 を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	63	$3^2 * 7$	36
3	513	$3^3 * 19$	324
5	39609	$3^5 * 163$	26244
6	355023	$3^6 * 487$	236196
7	3190833	$3^7 * 1459$	2125764
10	2324581983	$3^{10} * 39367$	1549681956
17	11118121262251209	$3^{17} * 86093443$	7412080755407364
18	100063090585419903	$3^{18} * 258280327$	66708726798666276
31	A	$3^{31} * 411782264189299$	--
55	B	$3^{55} * 116299474006080119380780339$	--
58	C	$3^{58} * 3140085798164163223281069127$	--
61	D	$3^{61} * 84782316550432407028588866403$	--
66	E	$3^{66} * 20602102921755074907947094535687$	--

$$A = 254346949651297838759162883153,$$

$$B = 20288351481136358057581329008802658030311343782261873,$$

$$C = 14790208229748405023976788724953791575694603909307209503,$$

$$D = 10782061799486587262479078977184803713214502375769989938009.$$

$$E = 636669967197883491262127134516306911101006058595257340533039423$$

- $e \equiv 2 \pmod{4}$ のとき $q \equiv 7, a \equiv 3 \pmod{10}$.
- $e \equiv 1 \pmod{4}$ のとき $q \equiv 3, a \equiv 9 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ のとき $q \equiv 9, a \equiv 3 \pmod{10}$.

Proof.

$$e \equiv 2 \pmod{4}.$$

$$e = 4k + 2 \text{ となるので, } q = 2(3^{e-1}) + 1 \equiv 1 + 1 = 2 \pmod{5}. \text{ よって } q \equiv 2 + 5 = 7 \pmod{10}.$$

$$a = 3^e q \equiv -4 \times 7 \equiv 3 \pmod{5}. a \text{ は奇数なので } a \equiv 3 \pmod{10}.$$

$$e \equiv 1 \pmod{4}.$$

$$e = 4k + 1 \text{ となるので, } q = 2(3^{e-1}) + 1 \equiv 2 + 1 = 3 \pmod{5}. \text{ よって } q \equiv 3 \pmod{10}.$$

$$a = 3^e q \equiv 3 \times 3 \equiv -1 \pmod{5}. a \text{ は奇数なので } a \equiv 9 \pmod{10}.$$

$$e \equiv 3 \pmod{4}.$$

$$e = 4k + 3 \text{ となるので, } q = 2(3^{e-1}) + 1 \equiv -2 + 1 = -1 \pmod{5}. \text{ よって } q \equiv 4 \pmod{5}.$$

$$a = 3^e q \equiv 3 \times 4 \equiv 12 \equiv 2 \pmod{5}. \text{ } a \text{ は奇数なので } a \equiv 3 \pmod{10}.$$

11.1.3 5 を底とするとき

$$q = 4 * 5^{e-1} + 1, a = 5^e q.$$

表 11.3: 5 を底とする φ 完全数

$e \bmod 4$	e	a	素因数分解	$\varphi(a)$
3	3	12625	$5^3 * 101$	10000
3	7	4882890625	$5^7 * 62501$	3906250000
3	19	A	$5^{19} * 15258789062501$	B
3	51	C	$5^{51} * 355271367880050092935562133789062501$	--

$$A = 291038304567356109619140625,$$

$$B = 232830643653869628906250000$$

$$C = 157772181044202361082345713056557246378730496871867217123508453369140625$$

次は表の観察結果 (証明は不明)

$$a \equiv 625 \pmod{1000}$$

$$e > 3 \text{ なら } q \equiv 501 \pmod{1000}$$

11.1.4 7 を底とするとき

表 11.4: $[p = 7, m = 0]$

$e \bmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	2107	$7^2 * 43$	1764
1	5	242138449	$7^5 * 14407$	207532836
2	10	A	$7^{10} * 242121643$	B
0	100	C	$7^{100} * C$	--

$$A = 68393371394714107,$$

$$B = 58622889524776164$$

$$C = 2772408436821221135438269516371614409306174170489678915086195998335735536831652622859$$

- $e \equiv 2 \pmod{4}$ のとき $q \equiv 3, a \equiv 7 \pmod{10}$.
- $e \equiv 1 \pmod{4}$ のとき $q \equiv 7, a \equiv 9 \pmod{10}$.

11.1.5 11 を底とするとき

表 11.5: $[p = 11, m = 0]$

$e \bmod 4$	e	a	素因数分解	$\varphi(a)$
3	11	A	$11^{11} * 259374246011$	B
3	25	C	$11^{25} * D$	--

$$A = 74002499442866912682721,$$

$$B = 67274999493256000920100,$$

$$C = 10671895716335937864242408834743270337427552858851161$$

$$D = 98497326758076110947118411.$$

- $e \equiv 3 \pmod{4}$ のとき $q \equiv 1, a \equiv 1 \pmod{10}$.
- $e \equiv 1 \pmod{4}$ のとき $q \equiv 1, a \equiv 1 \pmod{10}$.

11.1.6 13 を底とするとき

表 11.6: $[p = 13, m = 0]$

$e \bmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	26533	$13^2 * 157$	24336
3	3	4457713	$13^3 * 2029$	4112784
1	5	127254363769	$13^5 * 342733$	117465223824
3	35	A	$13^{35} * B$	--
1	49	C	$13^{49} * D$	--
2	54	E	$13^{54} * F$	--

$A = 873519401092878854401927853123365158780648390553335676472198548937712602981233$

$B = 897956346939432936161147153677736549869$

$C = 135421125769648021857682633667[50digits]522259722098657982526674878569$

$D = 3535592115828121264027042475895878223649788781400643853$

$E = 186689521630974256728663151915[61digits]717821636496271357368762043893$

$F = 1312740603462170628484392682002808313293601026012589257740637$

- $e \equiv 2 \pmod{4}$ のとき $q \equiv 7, a \equiv 3 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ のとき $q \equiv 9, a \equiv 3 \pmod{10}$.
- $e \equiv 1 \pmod{4}$ のとき $q \equiv 3, a \equiv 9 \pmod{10}$.

$e = 4k + 2. q = 12 * 13^{4k+1} + 1 \equiv 12 * 13 + 1 \equiv 7 \pmod{5}. q \equiv 7 \pmod{10}.$

$a = 13^{4k+2} * q \equiv 3 \pmod{5}; a \equiv 3 \pmod{10}.$

$e = 4k + 3. q = 12 * 13^{4k+2} + 1 \equiv 2 * 9 + 1 \equiv 9 \pmod{5}. q \equiv 9 \pmod{10}.$

$a = 13^{4k+3} * q \equiv 3 \pmod{5}; a \equiv 3 \pmod{10}.$

$e = 4k + 1. q = 12 * 13^{4k} + 1 \equiv 2 + 1 \equiv 3 \pmod{5}. q \equiv 3 \pmod{10}.$

$a = 13^{4k+1} * q \equiv 3 * 3 \pmod{5}; a \equiv 9 \pmod{10}.$

11.1.7 17 を底とするとき

表 11.7: $[p = 17, m = 0]$

$e \bmod 4$	e	a	素因数分解	$\varphi(a)$
5	1897407443809	$17^5 * 1336337$	1785793904896	
21	A	$17^{21} * B$	--	

$$A = 4492889724084297632770793894724524768890402723617889,$$

$$B = 65027702506361160358425617.$$

11.2 φ 完全数の平行移動

m だけ平行移動した φ 完全数の定義は次の通り.

$\varphi(p^e) + 1 + m$ が素数 q になるとき $a = p^e q$ を (p を底とする) m だけ平行移動した φ 完全数の定義とする.

11.2.1 $[p = 2, m = 2]$

表 11.8: $p = 2, m = 2$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	20	$2^2 * 5$	8
3	3	56	$2^3 * 7$	24
0	4	176	$2^4 * 11$	80
1	5	608	$2^5 * 19$	288
3	7	8576	$2^7 * 67$	4224
0	8	33536	$2^8 * 131$	16640
1	13	33579008	$2^{13} * 4099$	16785408
0	16	2147680256	$2^{16} * 32771$	1073807360
1	17	8590327808	$2^{17} * 65539$	--
3	19	137440526336	$2^{19} * 262147$	--
1	29	144115189686468608	$2^{29} * 268435459$	--

11.2.2 $[p = 2, m = 4]$

表 11.9: $p = 2, m = 4$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	28	$2^2 * 7$	12
0	4	208	$2^4 * 13$	96
2	6	2368	$2^6 * 37$	1152
0	12	8409088	$2^{12} * 2053$	4202496
0	48	39614081257133576171655528448	$2^{48} * 140737488355333$	--

11.2.3 $[p = 2, m = -2]$

表 11.10: $p = 2, m = -2$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
3	3	24	$2^3 * 3$	8
0	4	112	$2^4 * 7$	48
2	6	1984	$2^6 * 31$	960
0	8	32512	$2^8 * 127$	16128
2	14	134201344	$2^{14} * 8191$	67092480
2	18	34359476224	$2^{18} * 131071$	—
0	20	549754765312	$2^{20} * 524287$	—

$q = 2^{e-1} - 1$ が素数なのでこれらはメルセンヌ素数である. -2 だけ平行移動しているとはいえ, これらの $a = 24, 112, 1984, \dots$ は φ 完全数と呼んでもよいものである. これらの末尾の数は $2, 4$ になっている.

$e > 3$ のとき

- $e \equiv 0 \pmod 4$ なら $q \equiv 7 \pmod{10}$. $a \equiv 2 \pmod{10}$.
- $e \equiv 2 \pmod 4$ なら $q \equiv 1 \pmod{10}$. $a \equiv 4 \pmod{10}$.

$e = 4k + 4, (k \geq 0)$ のとき, $q = 2^{4k+3} - 1 \equiv 8 - 1 = 7 \pmod 5$. q は奇数なので $q \equiv 7 \pmod{10}$.
 $a = 2^e q = 2^{4k+4} q \equiv q \equiv 7 \pmod 5$.

a は奇数なので $a \equiv 2 \pmod{10}$.

11.2.4 $[p = 2, m = -4]$

11.2.5 $[p = 3, m = 4]$

$$A = 53177628719327154257979$$

$$B = 3140085798164506375167893541$$

$$q = p^{e-1} p + 1 + m = 3^{e-1} \times 2 + 5 : \text{素数}$$

表 11.11: $[p = 2, m = -4]$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
3	3	8	$2^3 * 1$	4
0	4	80	$2^4 * 5$	32
1	5	416	$2^5 * 13$	192
2	6	1856	$2^6 * 29$	896
3	7	7808	$2^7 * 61$	3840
2	10	521216	$2^{10} * 509$	260096
3	11	2091008	$2^{11} * 1021$	1044480
1	13	33529856	$2^{13} * 4093$	16760832
3	15	536772608	$2^{15} * 16381$	268369920

表 11.12: $p = 3, m = 4$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	99	$3^2 * 11$	60
3	3	621	$3^3 * 23$	396
0	4	4779	$3^4 * 59$	3132
1	5	40581	$3^5 * 167$	26892
2	6	357939	$3^6 * 491$	238140
1	9	258378741	$3^9 * 13127$	172239372
2	10	2324818179	$3^{10} * 39371$	1549839420
3	23	5908625413572383291421	$3^{23} * 62762119223$	3939083608985493408396
0	24	A	$3^{24} * 188286357659$	—
1	29	B	$3^{29} * 45753584909927$	—

11.2.6 $[p = 3, m = 6]$

$$A = 478598658467166079446267$$

表 11.13: $p = 3, m = 6$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	117	$3^2 * 13$	72
0	4	4941	$3^4 * 61$	3240
2	10	2324936277	$3^{10} * 39373$	1549918152
0	12	188290077741	$3^{12} * 354301$	125526364200
0	16	1235347093894941	$3^{16} * 28697821$	823564700565480
2	18	100063092909942837	$3^{18} * 258280333$	66708728348348232
1	25	A	$3^{25} * 564859072969$	—

11.2.7 $[p = 3, m = -2]$ 表 11.14: $p = 3, m = -2$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	45	$3^2 * 5$	24
3	3	459	$3^3 * 17$	288
0	4	4293	$3^4 * 53$	2808
0	8	28691253	$3^8 * 4373$	19123128
1	9	258260643	$3^9 * 13121$	172160640
1	13	1694575624563	$3^{13} * 1062881$	1129716020160
1	21	72945992743881219603	$3^{21} * 6973568801$	48630661822280577600
0	24	A	$3^{24} * 188286357653$	—
0	28	B	$3^{28} * 15251194969973$	—
0	36	C	$3^{36} * 100063090197999413$	—

$$A = 53177628717632577039093$$

$$B = 348898422018217481349886053$$

$$C = 15018933029959449457798796619515973$$

$$q = p^{e-1}\bar{p} + 1 + m = 3^{e-1} \times 2 - 1 : \text{素数}$$

11.2.8 $[p = 3, m = -8]$ 表 11.15: $[p = 3, m = -8]$

a	素因数分解	$\varphi(a)$
30	$[2, 3, 5]$	8
147	$[3, 7^2]$	84
297	$[3^3, 11]$	180
3807	$[3^4, 47]$	2484

$30([2, 3, 5])$ が非通常解.

11.2.9 $[p = 5, m = 2]$ 表 11.16: $p = 5, m = 2$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
2	2	575	$5^2 * 23$	440
3	3	12875	$5^3 * 103$	10200
0	4	314375	$5^4 * 503$	251000
1	5	7821875	$5^5 * 2503$	6255000
2	6	195359375	$5^6 * 12503$	156275000
3	11	1907348779296875	$5^{11} * 39062503$	1525878984375000
0	12	47683716552734375	$5^{12} * 195312503$	38146973046875000
3	15	A	$5^{15} * 24414062503$	B
0	16	C	$5^{16} * 122070312503$	D
1	17	E	$5^{17} * 610351562503$	F
1	21	G	$5^{21} * 381469726562503$	--
0	28	H	$5^{28} * 29802322387695312503$	--

$$A = 745058059783935546875$$

$$B = 596046447802734375000$$

$$C = 18626451492767333984375$$

$$D = 14901161194091796875000$$

$$E = 465661287310028076171875$$

$$F = 372529029847412109375000$$

$$G = 181898940354587078094482421875$$

$$H = 1110223024625156540535390377044677734375$$

11.2.10 $[p = 5, m = 6]$ 表 11.17: $p = 5, m = 6$

$e \pmod 4$	e	a	素因数分解	$\varphi(a)$
3	3	13375	$5^3 * 107$	10600
3	23	A	$5^{23} * 9536743164062507$	--
3	43	B	$5^{43} * 909494701772928237915039062507$	--

$$A = 113686837721616113185882568359375$$

$$B = 1033975765691284593589260865095411645597778260707855224609375$$

表 11.18: $p = 5, m = -2$

$e \pmod 4$	e	a	素因数分解
2	2	475	$5^2 * 19$
0	4	311875	$5^4 * 499$
2	10	76293935546875	$5^{10} * 7812499$
2	14	29802322381591796875	$5^{14} * 4882812499$
0	16	18626451492156982421875	$5^{16} * 122070312499$
0	40	166174449004242213989712695356502081267535686492919921875	$5^{40} * 7275957614183425903320$

11.3 φ 完全数の平行移動の方程式

$q = \varphi(p^e) + 1 + m$ が素数になるとき $a = p^e q$ とすると,

$$\begin{aligned}\varphi(a) &= \varphi(p^e q) = p^{e-1} \bar{p} \bar{q} \\ &= p^e \bar{p} (q-1)/p \\ &= \bar{p} a / p - (q-1-m).\end{aligned}$$

かくして $\text{Maxp}(a) = q$ に注意し

$$\varphi(a) = \frac{\bar{p}}{p} a - \overline{\text{Maxp}(a)} + m. \quad (11.1)$$

が得られた. 分母を払った次の式もよく使われる.

$$p\varphi(a) = \bar{p} a - p\overline{\text{Maxp}(a)} + pm. \quad (11.2)$$

が得られた.

これが m だけ平行移動した φ 完全数の方程式 (*) である.

φ 完全数の方程式 (*) で定義された数は素数により定義された φ 完全数になるわけではない.

$q = \varphi(p^e) + 1 + m$ が素数になると仮定されているので $1 + m$ は p で割れない.

φ 完全数の方程式 (*) 自身を扱うとき $1 + m$ は p で割れない, などのことにこだわらないでも良い. 実際に $m = p - 1$ の場合が重要な結果を与えるのである.

11.3.1 φ 完全数の方程式 (*) の解

$m = 0$ の場合に φ 完全数の方程式 (*)

$$\varphi(a) = \frac{\bar{p}}{p}a - \overline{\text{Maxp}(a)}$$

を満たす例の計算結果を与える.

11.3.2 2 を底とするとき

表 11.19: $\varphi(a) = \frac{1}{2}a - \overline{\text{Maxp}(a)}$

a	素因数分解	$\varphi(a)$
12	$[2^2, 3]$	4
40	$[2^3, 5]$	16
544	$[2^5, 17]$	256
131584	$[2^9, 257]$	65536

11.3.3 3 を底とするとき

表 11.20:

a	素因数分解	$\varphi(a)$
6	$[2, 3]$	2
63	$[3^2, 7]$	36
513	$[3^3, 19]$	324
39609	$[3^5, 163]$	26244
355023	$[3^6, 487]$	--

ここでまた 6(最初の完全数)が出てきた. 今回は 3 を底とし, $\varphi(a) = \frac{\bar{p}}{p}a - \overline{\text{Maxp}(a)}$ を満たす最初の解であって, 後に微小解と呼ばれるものなのである.

11.3.4 5 を底とするとき

表 11.21:

a	素因数分解	$\varphi(a)$
10	[2, 5]	4
15	[3, 5]	8
12625	$[5^3, 101]$	10000

11.3.5 7 を底とするとき

表 11.22: $[p = 7, m = 0]$

a	素因数分解	$\varphi(a)$
14	[2, 7]	6
21	[3, 7]	12
35	[5, 7]	24
2107	$[7^2, 43]$	1764

11.3.6 11 を底とするとき

表 11.23: $[p = 11, m = 0]$

a	素因数分解	$\varphi(a)$
22	[2, 11]	10
33	[3, 11]	20
55	[5, 11]	40
77	[7, 11]	60

$[p, 11]$, ($p = 2, 3, 5, 7$) という解がでてきた. 実に不思議である.

11.3.7 13 を底とするとき

表 11.24: $P = 13, m = 0$

a	素因数分解	$\varphi(a)$
26	[2, 13]	12
39	[3, 13]	24
65	[5, 13]	48
91	[7, 13]	72
143	[11, 13]	120
26533	[13 ² , 157]	24336

$[p, 13], (p = 2, 3, 5, 7, 11)$ という解がでてきた.

11.4 $p \geq 3, m > 0$ の場合11.4.1 $m = 2$ の場合

表 11.25: $[p = 3, 5, 11, 17; m = 2]$

a	素因数分解	$\varphi(a)$
$P = 3$		
3	[3]	2
9	[3 ²]	6
15	[3, 5]	8
27	[3 ³]	18
81	[3 ⁴]	54
243	[3 ⁵]	162
729	[3 ⁶]	486
2187	[3 ⁷]	1458
6561	[3 ⁸]	4374
19683	[3 ⁹]	13122
$P = 5$		
35	[5, 7]	24
575	[5 ² , 23]	440
12875	[5 ³ , 103]	10200
$P = 11$		
143	[11, 13]	120
13673	[11 ² , 113]	12320
$P = 17$		
323	[17, 19]	288

11.4.2 $m = 4$ の場合

表 11.26: $[p = 3, 5, 7; m = 4]$

a	素因数分解	$\varphi(a)$
$P = 3$		
21	$[3, 7]$	12
99	$[3^2, 11]$	60
621	$[3^3, 23]$	396
4779	$[3^4, 59]$	3132
$P = 5$		
5	$[5]$	4
25	$[5^2]$	20
125	$[5^3]$	100
625	$[5^4]$	500
3125	$[5^5]$	2500
15625	$[5^6]$	12500
$P = 7$		
77	$[7, 11]$	60
2303	$[7^2, 47]$	1932
$P = 13$		
221	$[13, 17]$	192
$P = 19$		
437	$[19, 23]$	396

11.4.3 $m = 6$ の場合

11.4.4 $m = 8$ の場合

表 11.27: $P = 3, 5, 7, ; m = 6$

a	素因数分解	$\varphi(a)$
$P = 3$		
117	$[3^2, 13]$	72
4941	$[3^4, 61]$	3240
$P = 5$		
55	$[5, 11]$	40
13375	$[5^3, 107]$	10600
$P = 7$		
7	$[7]$	6
49	$[7^2]$	42
91	$[7, 13]$	72
343	$[7^3]$	294
2401	$[7^4]$	2058
16807	$[7^5]$	14406
$P = 11$		
209	$[11, 19]$	180

表 11.28: $P = 3, 5, 11, ; m = 8$

a	素因数分解	$\varphi(a)$
$P = 3$		
33	$[3, 11]$	20
$P = 5$		
65	$[5, 13]$	48
725	$[5^2, 29]$	560
13625	$[5^3, 109]$	10800
$P = 11$		
209	$[11, 19]$	180

11.5 微小解

$m = 0$ のとき $p = \text{Maxp}(a)$ とおくと $a = pq (p > q)$ は

$$\varphi(a) = \frac{\bar{p}a}{p} - \overline{\text{Maxp}(a)}$$

の解になることは一般的に証明できる。

実際, $\varphi(a) = \overline{pq}$, $\text{Maxp}(a) = p$ によって

$$\frac{\overline{pa}}{p} - \overline{\text{Maxp}(a)} = \overline{pq} - \overline{p} = \overline{pq} = \varphi(a).$$

よって $\varphi(a) = \frac{\overline{pa}}{p} - \overline{\text{Maxp}(a)}$.

$m = 0$ のときの解 $a = pq (p > q)$ を微小解という. 微小解は φ 完全数の方程式 (*) に特有の解である.

11.5.1 $p = 2, m = 0$ のときの予想

$p = 2, m = 0$ なら微小解はない. したがって,

$$\varphi(a) = \frac{a}{2} - \overline{\text{Maxp}(a)} \quad (11.3)$$

を満たす解は フェルマー素数 $p = 2^{e-1} + 1$ によって $a = 2^e p$ と書ける, という予想をたてることは可能である.

これは古代ギリシャ時に起源を持つ完全数の形の問題の類似である.

完全数は $\sigma(a) = 2a$ で定義されるが, a が偶数なら $p = 2^{e+1} - 1$ が素数になるモノによって $a = 2^e p$ と書けることはほぼ 2000 年に長きにわたって予想されてきたがオイラーが完璧な証明を与えた.

φ 完全数の考察の中からでて来た式 (11.3) はずっと易しい問題に見える. そもそも問題自身から a が偶数であることはわかってしまう. 実際式 (11.3) を 2 倍すると

$$2\varphi(a) = a - 2\overline{\text{Maxp}(a)} \quad (11.4)$$

となるからである.

11.6 予想の解決

$a = 2^e L$, (L : 奇数) の形に書くとき,

$$2\varphi(a) = 2^e \varphi(L), a = 2^e L, \overline{\text{Maxp}(a)} = \overline{\text{Maxp}(L)}.$$

整理して

$$\overline{\text{Maxp}(L)} = 2^{e-1}(L - \varphi(L)).$$

次の補題に注目する.

補題 15 $a > 1$ が素数でないとき

$$a - \varphi(a) \geq \text{Maxp}(a)$$

Proof. $a = p^e, (e > 1)$ のとき $a - \varphi(a) = p^{e-1} \geq p$ となり正しい.

$s(a) \geq 2$ なら $\text{Maxp}(a) = p$ とすれば $a = \alpha p^e, (e > 0, \text{Maxp}(\alpha) < p)$ と書けて

$$\begin{aligned} a - \varphi(a) &= \alpha p^e - \varphi(\alpha) p^{e-1} \bar{p} \\ &= p^{e-1} (\alpha p - \varphi(\alpha) \bar{p}) \\ &= p^{e-1} (\alpha p - \varphi(\alpha) p + \varphi(\alpha)) \\ &= p^{e-1} (\alpha - \varphi(\alpha) p + \varphi(\alpha)) \\ &> p^{e-1} (p + \varphi(\alpha)) \\ &> p^e \\ &\geq \text{Maxp}(a). \end{aligned}$$

定理の証明の続き.

L が素数でないとすると,

$$\text{Maxp}(L) \leq 2^{e-1} \text{Maxp}(L) \leq 2^{e-1} (L - \varphi(L)) = \overline{\text{Maxp}(L)}.$$

これは矛盾.

L が素数ならば

$$L - 1 = \overline{\text{Maxp}(L)} = 2^{e-1} (L - \varphi(L)) = 2^{e-1}$$

ゆえに $L = 2^{e-1} + 1$ は素数. $L = \varphi(2^e) + 1$. したがって $a = 2^e L$ は φ 完全数.

11.7 定理と証明

一般の場合は次の定理にまとめられる.

定理 3 $m = 0$ のとき.

$$p\varphi(a) = \bar{p}a - p\overline{\text{Maxp}(a)}$$

を満たす解は微小解または φ 完全数である.

Proof.

a は式より p の倍数なので $a = p^e L (p, L : \text{は互いに素})$ と書ける.

$p\varphi(a) = p^e \bar{p} \varphi(L), \bar{p}a = p^e L \bar{p}$ により,

$$\overline{\text{Maxp}(a)} = p^{e-1} \bar{p} (L - \varphi(L)).$$

L が素数でないなら $L - \varphi(L) \geq \text{Maxp}(L)$ となり矛盾.

L は素数であり, $L - \varphi(L) = 1$ によって $\overline{\text{Maxp}(a)} = p^{e-1}\bar{p}$. さらに $\text{Maxp}(L) = L$ が成り立つ
ここで $\text{Maxp}(a) = p$ または $\text{Maxp}(a) = \text{Maxp}(L)$ が成り立つ.

- 1) $\text{Maxp}(a) = p$ とすると, $p > L, p - 1 = p^{e-1}\bar{p}$ となり $e = 1$. このとき $a = pL$ は微小解.
- 2) $\text{Maxp}(a) = \text{Maxp}(L) = L$ が成り立つとき $\overline{\text{Maxp}(a)} = p^{e-1}\bar{p}(L - \varphi(L)) = p^{e-1}\bar{p}$ によって
 $\overline{\text{Maxp}(a)} = \bar{L}$ によって $L = p^{e-1}\bar{p} + 1$. L は素数なので $a = p^e L$ は φ 完全数.

11.8 諸例

11.8.1 $p = 2, m = -4$ のとき

表 11.29: $p = 2, m = -4$ のとき

a	素因数分解	$\varphi(a)$
36	$[2^2, 3^2]$	12
80	$[2^4, 5]$	32
416	$[2^5, 13]$	192
1856	$[2^6, 29]$	896
7808	$[2^7, 61]$	3840
521216	$[2^{10}, 509]$	—

ここで $a = 36 (= [2^2, 3^2])$ 非通常解.

11.9 $p = 2, m = -q$; (奇素数) のとき

$p = 2$ のとき本来の m だけ平行移動した φ 完全数の定義は次の通り.

$q = \varphi(2^e) + 1 + m = 2^{e-1} + 1 + m$ が素数になるとき $a = 2^e q$ を (2 を底とする) m だけ平行移動した φ 完全数とする. したがって, m はこのとき必ず偶数である.

m だけ平行移動した φ 完全数の満たす方程式は

$$p\varphi(a) = \bar{p}a - \overline{p\text{Maxp}(a)} + pm. \quad (11.5)$$

であり, $p = 2$ とすれば

$$2\varphi(a) = a - \overline{2\text{Maxp}(a)} + 2m.$$

$m < 0$ かつ m : 奇数 の場合にこの方程式の解を探す. これはそもそも違反行為なので何が出てくるか分からない.

とくに $-m$ が奇素数の場合にパソコンで例を計算させた. その結果は, いかなる想像も超えた豊かな大地が見えてきた.

11.9.1 $p = 2, m = -3$ のとき

表 11.30: $p = 2, m = -3$ のとき

a	素因数分解	$\varphi(a)$
30	[2, 3, 5]	8
42	[2, 3, 7]	12
66	[2, 3, 11]	20

通常解は $6p$ とかける. 非通常解はない.

11.9.2 $p = 2, m = -5$ のとき

表 11.31: $p = 2, m = -5$ のとき

a	素因数分解	$\varphi(a)$
70	[2, 5, 7]	24
110	[2, 5, 11]	40
130	[2, 5, 13]	48

通常解は $10p$ とかける. 非通常解はない.

11.9.3 $p = 2, m = -7$ のとき表 11.32: $p = 2, m = -7$ のとき

a	素因数分解	$\varphi(a)$
54	$[2, 3^3]$	18
154	$[2, 7, 11]$	60
182	$[2, 7, 13]$	72

$a = 54 = 2 * 3^3$ が非通常解として先頭に出てきた. 通常解は $14p$ とかける.

11.9.4 $p = 2, m = -11$ のとき表 11.33: $p = 2, m = -11$ のとき

a	素因数分解	$\varphi(a)$
286	$[2, 11, 13]$	120
374	$[2, 11, 17]$	160
418	$[2, 11, 19]$	180

解は $22p$ だけらしい.

11.9.5 $p = 2, m = -13$ のとき表 11.34: $p = 2, m = -13$ のとき

a	素因数分解	$\varphi(a)$
442	$[2, 13, 17]$	192
494	$[2, 13, 19]$	216
598	$[2, 13, 23]$	264

解は $26p$ だけらしい.

表 11.35: $p = 2, m = -17$ のとき

a	素因数分解	$\varphi(a)$
90	$[2, 3^2, 5]$	24
646	$[2, 17, 19]$	288
782	$[2, 17, 23]$	352

11.9.6 $p = 2, m = -19$ のとき

解は $38p$ だけらしい.

表 11.36: $p = 2, m = -19$ のとき

a	素因数分解	$\varphi(a)$
874	[2, 19, 23]	396
1102	[2, 19, 29]	504
1178	[2, 19, 31]	540

11.9.7 $p = 2, m = -23$ のとき表 11.37: $p = 2, m = -23$ のとき

a	素因数分解	$\varphi(a)$
1334	[2, 23, 29]	616
1426	[2, 23, 31]	660
1702	[2, 23, 37]	792

解は $46p$ だけらしい.

11.9.8 $p = 2, m = -29$ のとき表 11.38: $p = 2, m = -29$ のとき

a	素因数分解	$\varphi(a)$
198	[2, 3^2 , 11]	60
1798	[2, 29, 31]	840

解は $2 \times 29p$ の他に非通常解 $198 = 2 * 3^2 * 11$ が出了.

11.9.9 $p = 2, m = -31$ のとき

通常解 $2 \times 31p$ の他に非通常解 $150 = 2 * 3 * 5^2$ が出了.

表 11.39: $p = 2, m = -31$ のとき

a	素因数分解	$\varphi(a)$
150	$[2, 3, 5^2]$	40
2294	$[2, 31, 37]$	1080
2542	$[2, 31, 41]$	1200

11.9.10 $p = 2, m = -37$ のとき表 11.40: $p = 2, m = -37$ のとき

a	素因数分解	$\varphi(a)$
3034	$[2, 37, 41]$	1440
3182	$[2, 37, 43]$	1512
3478	$[2, 37, 47]$	1656

解は $2 \times 37p$, 通常解のみ.

11.9.11 $p = 2, m = -41$ のとき表 11.41: $p = 2, m = -41$ のとき

a	素因数分解	$\varphi(a)$
306	$[2, 3^2, 17]$	96
3526	$[2, 41, 43]$	1680
3854	$[2, 41, 47]$	1840

解は $2 \times 41p$ の他に非通常解 $306 = 2 * 3^2 * 17$ が出た.

11.9.12 $p = 2, m = -43$ のとき

解は $2 \times 43p$ の他に非通常解 $686 = 2 * 7^3$ が出た.

以上の結果を次に証明する. その根拠は copm の表である. これらから一般的な解の形を求めることは難しそうである.

11.9.13 copm の表

表 11.42: $p = 2, m = -43$ のとき

a	素因数分解	$\varphi(a)$
686	$[2, 7^3]$	294
4042	$[2, 43, 47]$	1932
4558	$[2, 43, 53]$	2184

表 11.43: copm1

a	素因数分解	$\varphi(a)$	$\sigma(a)$	Maxp	copm
15	$[3, 5]$	8	24	5	2
21	$[3, 7]$	12	32	7	2
27	$[3^3]$	18	40	3	6
77	$[7, 11]$	60	96	11	6
91	$[7, 13]$	72	112	13	6
143	$[11, 13]$	120	168	13	10
187	$[11, 17]$	160	216	17	10
209	$[11, 19]$	180	240	19	10
221	$[13, 17]$	192	252	17	12
247	$[13, 19]$	216	280	19	12
299	$[13, 23]$	264	336	23	12
45	$[3^2, 5]$	24	78	5	16
323	$[17, 19]$	288	360	19	16
391	$[17, 23]$	352	432	23	16
493	$[17, 29]$	448	540	29	16

11.10 $p = 2, m = -s$: 奇素数

s : 奇素数とする. $s < p$ を満たす素数 p をとり $a = 2sp$ とする.

$$\begin{aligned} 2\varphi(a) - a + 2\text{Maxp}(a) - 1 &= 2s\bar{p} - 2sp + 2p - 2 \\ &= 2(2 - p - s) - 2p + 2 = -2s \end{aligned}$$

よって

$$2\varphi(a) = a - 2\text{Maxp}(a) - 1 - 2s.$$

逆にこの式を満たすとき, a は偶数. そこでいつものように $a = 2^e L, L$: 奇数, とおけば $2^e \varphi(L) = 2^e La - 2\overline{\text{Maxp}(a)} - 2s$ により

表 11.44: copm2

a	素因数分解	$\varphi(a)$	$\sigma(a)$	Maxp	copm
437	[19, 23]	396	480	23	18
551	[19, 29]	504	600	29	18
589	[19, 31]	540	640	31	18
667	[23, 29]	616	720	29	22
713	[23, 31]	660	768	31	22
851	[23, 37]	792	912	37	22
99	[3 ² , 11]	60	156	11	28
899	[29, 31]	840	960	31	28
1073	[29, 37]	1008	1140	37	28
1189	[29, 41]	1120	1260	41	28
75	[3, 5 ²]	40	124	5	30
1147	[31, 37]	1080	1216	37	30
1271	[31, 41]	1200	1344	41	30

$$2^{e-1}co\varphi(L) = \text{Maxp}(L) - 1 + s.$$

$e > 1$ とすると, 左辺は偶数. $L > 2$ とすると $\text{Maxp}(L) - 1 + s$ は奇数. よって, $e = 1$.

$$co\varphi(L) = \text{Maxp}(L) - 1 + s.$$

L : 素数なら $co\varphi(L) = 1 = \text{Maxp}(L) - 1 + s$. これは矛盾.

L : 素数でないなら $co\varphi(L)\text{Maxp}(L) > 0$.

かくて

$$co\varphi(L) - \text{Maxp}(L) = -1 + s.$$

$s = 3$ なら $copm = 2$. このとき $L = 3p$ となるので, $a = 6p$.

$s = 5$ なら $copm = 4$. このとき $L = 5p$ となるので, $a = 10p$.

$s = 7$ なら $copm = 6$. このとき $L = 3^3, a = 2 \times 3^3$. または $L = 7p$ となるので, $a = 14p$.

$s = 11$ なら $copm = 10$. このとき $L = 11p$ となるので, $a = 22p$.

$s = 13$ なら $copm = 12$. このとき $L = 13p$ となるので, $a = 26p$.

$s = 17$ なら $copm = 16$. このとき $L = 45 = [3^2, 5], a = 90$ または $L = 17p$ となるので, $a = 34p$.

$s = 31$ なら $copm = 30$. このとき $L = 75 = [3, 5^2], a = 150$ または $L = 31p$ となるので, $a = 62p$.

$s = 41$ なら $copm = 40$. このとき $L = 343 = [3^2, 17], a = 486$ または $L = 41p$ となるので, $a = 2 * 41p$.

$s = 47$ なら $copm = 46$. このとき $L = 343 = [7^3], a = 486$ または $L = 47p$ となるので, $a = 2 * 47p$.

表 11.45: copm3

a	素因数分解	$\varphi(a)$	$\sigma(a)$	Maxp	copm
1517	[37, 41]	1440	1596	41	36
1591	[37, 43]	1512	1672	43	36
153	[3 ² , 17]	96	234	17	40
1763	[41, 43]	1680	1848	43	40
1927	[41, 47]	1840	2016	47	40
343	[7 ³]	294	400	7	42
2021	[43, 47]	1932	2112	47	42
2279	[43, 53]	2184	2376	53	42

11.11 $p = 3, m \neq 0$ のとき

$$3\varphi(a) = 2a - 3\overline{\text{Maxp}(a)} + 6.$$

11.11.1 $p = 3, m = -3$ のとき

表 11.46: $m = -3; 3\varphi(a) = 2a - 3\overline{\text{Maxp}(a)} + 6$

a	素因数分解	$\varphi(a)$
3	[3]	2
9	[3 ²]	6
15	[3, 5]	8
27	[3 ³]	18
81	[3 ⁴]	54
243	[3 ⁵]	162
729	[3 ⁶]	486
2187	[3 ⁷]	1458
6561	[3 ⁸]	4374
19683	[3 ⁹]	13122

$$3\varphi(a) = 2a - 3\overline{\text{Maxp}(a)} - 6.$$

11.11.2 $p = 3, m = -2$ のとき

表 11.47: $p = 3, m = -2$

a	素因数分解	$\varphi(a)$
12	$[2^2, 3]$	4
45	$[3^2, 5]$	24
459	$[3^3, 17]$	288
4293	$[3^4, 53]$	2808

11.12 $p = 5, m \neq 0$ のとき

11.12.1 $p = 5, m = -2$ のとき

表 11.48: $P = 5; m = -2$

a	素因数分解	$\varphi(a)$
475	$[5^2, 19]$	360

11.12.2 $p = 5, m = 2$ のとき

表 11.49: $[P = 5, m = 2]$

a	素因数分解	$\varphi(a)$
35	$[5, 7]$	24
575	$[5^2, 23]$	440
12875	$[5^3, 103]$	10200

$e \geq 2$ のとき $q \equiv 3 \pmod{10}$ を満たすであろう.

解に $a = 5^e q$ があると仮定すれば $q = 4 * 5^{e-1} + 3$ を満たす.

$4 * 5^{e-1} + 3$ が素数になる e は無限にあるかが問題となりうる.

11.13 $co\varphi(a) - \text{Maxp}(a)$ の値変化

$copm = co\varphi(a) - \text{Maxp}(a)$, $cosm = co\sigma(a) - \text{Maxp}(a)$ とおく.

$co\varphi(a) - \text{Maxp}(a)$, $co\sigma(a) - \text{Maxp}(a)$ の $s(a) \geq 2$ の場合について, 値の変化を調べた.

これから一般的な結論を導き証明することが課題である.

表 11.50: $p = 5, m = 2$

e	a	素因子分解	$\varphi(a)$
1	35	$5 * 7$	24
2	575	$5^2 * 23$	440
3	12875	$5^3 * 103$	10200
4	314375	$5^4 * 503$	251000
5	7821875	$5^5 * 2503$	6255000
6	195359375	$5^6 * 12503$	156275000
11	1907348779296875	$5^{11} * 39062503$	1525878984375000

表 11.51: copm, cosm の表

a	factor	$s(a)$	$\varphi(a)$	$\sigma(a)$	$\text{Maxp}(a)$	$\text{co}\varphi(a)$	$\text{co}\sigma$	copm	cosm
$2p, p > 2$	$[2, p]$	2	—	—	—	—	—	1	3
$3p, p > 3$	$[3, p]$	2	—	—	—	—	—	2	4
$5p, p > 5$	$[5, p]$	2	—	—	—	—	—	4	6
12	$[2^2, 3]$	2	4	28	3	8	16	5	13
$7p, p > 7$	$[7, p]$	2	—	—	—	—	—	6	8
20	$[2^2, 5]$	2	8	42	5	12	22	7	17
18	$[2, 3^2]$	2	6	39	3	12	21	9	18
28	$[2^2, 7]$	2	12	56	7	16	28	9	21
$11p, p > 11$	$[11, p]$	2	—	—	—	—	—	10	12

定理 4 $\text{copm} = \text{co}\varphi(a) - \text{Maxp}(a)$, $\text{cosm} = \text{co}\sigma(a) - \text{Maxp}(a)$ とおく.

$s(a) = 1$ のとき. $a = p^e, e \geq 2$ なら $\text{copm} = p(p^{e-2} - 1)$.
とくに $a = p^2$ なら $\text{copm} = 0$.

$s(a) \geq 2$ のとき

$\text{copm} \geq 1$. $\text{copm} = 1$ なら $a = 2p, p > 2$.

$\text{copm} = 2$ なら $a = 3p, p > 3$.

$\text{copm} > 2$ なら $\text{copm} \geq 4$. $\text{copm} = 4$ なら $a = 5p, p > 5$.

$\text{copm} > 4$ なら $\text{copm} \geq 5$. $\text{copm} = 5$ なら $a = 12$.

$\text{copm} > 5$ なら $\text{copm} \geq 6$. $\text{copm} = 6$ なら $a = 7p, p > 11$.

11.14 $\text{cos}\sigma(a) - \text{Maxp}(a)$ の値変化

$s(a) = 1$ のとき $s = p^e$ とおけば

$$\text{cos}\sigma(a) - \text{Maxp}(a) = \frac{p^{e+1} - 1}{\bar{p}} - p^e - p = \frac{p^2(p^{e-2} - 1) + \bar{p}}{\bar{p}} \geq 1.$$

$e = 2$ なら $\text{cos}\sigma(a) - \text{Maxp}(a) = 1$.

$e \geq 3$ なら $\text{cos}\sigma(a) - \text{Maxp}(a) \geq p^2 + 1$.

$s(a) \geq 2$ のとき $\text{cos}\sigma(a) - \text{Maxp}(a) \geq 3$ を示そう.

$p = \text{Maxp}(a), a = \alpha p^e, \text{Maxp}(\alpha) < p$ とする.

$e = 1$ のとき

$$\text{cos}\sigma(a) = \sigma(\alpha p) - \alpha p = \sigma(\alpha)(p + 1) - \alpha p = (\text{cos}\sigma(\alpha))p + \sigma(\alpha).$$

α が素数なら, $\text{cos}\sigma(a) = p + \sigma(\alpha)$. よって

$$\text{cosm} = \text{cos}\sigma(a) - \text{Maxp}(a) = \sigma(\alpha).$$

とくに $a = \alpha p (p \neq \alpha)$; (両者は素数なら) のとき $\text{cosm} = \sigma(\alpha p)$.

$$\text{cosm} = \sigma(2p) = 3. p > 2 \text{ は素数.}$$

$$\text{cosm} = \sigma(3p) = 4. p > 3 \text{ は素数.}$$

$$\text{cosm} = \sigma(5p) = 6. p > 5 \text{ は素数.}$$

α が素数でないなら, $\text{cos}\sigma(\alpha) \geq 2$ によって $\text{cos}\sigma(a) = 2p + \sigma(\alpha)$.

$e \geq 2$ のとき

$$\text{cos}\sigma(a) = \sigma(\alpha p^e) - \alpha p^e = \frac{\sigma(\alpha)(p^{e+1} - 1) - p^e \alpha \bar{p}}{\bar{p}}$$

11.15 素数べきの問題

$m = p - 1$ のときの解に $a = p^e$ がある.

このときの方程式は

$$p\varphi(a) - \bar{p}a = -p\overline{\text{Maxp}(a)} + p(p - 1). \tag{11.6}$$

これは容易に確かめられる. 実際,

$p\varphi(a) - \bar{p}a = p^e\varphi(a) - \bar{p}p^e = 0$ および $-p\overline{\text{Maxp}(a)} + p(p - 1) = -p(p - 1) + p(p - 1) = 0$ が成り立つ.

(式 11.6) の解の $s(a) = 1$ の場合は $a = p^e$.

表 11.52: $[P = 5, m = 4]$

a	素因数分解	$\varphi(a)$
5	[5]	4
25	[5 ²]	20
125	[5 ³]	100
625	[5 ⁴]	500
3125	[5 ⁵]	2500
15625	[5 ⁶]	12500

11.15.1 $s(a) > 1$ の場合

(式 11.6) の解は p の倍数なので $a = p^e L, (L > 1, p, L \text{ は互いに素})$ と書ける.

$$p\varphi(a) - \bar{p}a = p^e \bar{p} \varphi(L) - \bar{p} p^e L = p^e \bar{p} (\varphi(L) - L) < 0.$$

よって, $-\overline{p \text{Maxp}(a)} + p(p-1) = -p(\overline{\text{Maxp}(a)} - \bar{p}) < 0.$

$\overline{\text{Maxp}(a)} > \bar{p}$ なので $\text{Maxp}(a) = \text{Maxp}(L) > p.$

$co\varphi(L) = L - \varphi(L)$ を使うと,

$$p^{e-1} \bar{p} (co\varphi(L)) = \overline{\text{Maxp}(L)} - \bar{p}.$$

L が素数でないなら補題から $co\varphi(L) \geq \text{Maxp}(L).$

よって

$$\overline{\text{Maxp}(L)} - \bar{p} = p^{e-1} \bar{p} (co\varphi(L)) \geq p^{e-1} \bar{p} \text{Maxp}(L).$$

これは矛盾.

L が素数なら $co\varphi(L) = 1.$

$$p^{e-1} \bar{p} = \overline{\text{Maxp}(L)} - \bar{p} = L - \bar{p} = L - p.$$

$L = p + p^{e-1} \bar{p}, L$ は素数なので $e = 1. L = p + \bar{p} = 2p - 1.$

$a = p^e L = pL$ が特異解なのである.

たとえば $p = 7, L = 13$ のとき $a = 7 * 13.$

11.15.2 ソフィーの素数

$p, 2p-1$ がともに素数になるとき, これをソフィーの素数という. ソフィーの素数は無限にあり
 そうなのだが証明はできていない.

実は $p, 2p+1$ がともに素数になるとき, ソフィー・ジェルマンの素数という. Sophie Germain
 はガウスに親しかった女流数学者として有名.

ここでは $p, 2p - 1$ がともに素数になるので, 仮にソフィーの素数と言うことにした.
例

表 11.53: $P = 7, m = 6$

a	素因数分解	$\varphi(a)$
7	[7]	6
49	[7 ²]	42
91	[7, 13]	72
343	[7 ³]	294
2401	[7 ⁴]	2058
16807	[7 ⁵]	14406

$13 = 2 * 7 - 1$ なので 7 はソフィーの素数である.

L が素数でないなら $co\varphi(L) \geq \text{Maxp}(L)$.

$$p^{e-1}\bar{p}\text{Maxp}(L) \leq p^{e-1}\bar{p}(co\varphi(L)) = \overline{\text{Maxp}(L)} - \bar{p}.$$

これで矛盾.

しかし, $p = 5$ のとき $2p - 1 = 9$ は素数ではないので, $p = 5, m = 4$ のとき特異解はない.

11.15.3 最後の定理

以上の結果をまとめて次の定理ができた.

定理 5 素数 p に対して

$$p\varphi(a) - \bar{p}a = -p\overline{\text{Maxp}(a)} + p(p - 1)$$

の通常解は p^e .

p がソフィーの素数ならば $q = 2p - 1$ も素数で $a = p * q$ が非通常解.

双子素数, ソフィーの素数, そして (P, q) が素数のペアで $(P = q^2 - q + 1)$ 満たす対がそれぞれ無限にあるか?

このような興味ある素数の問題が微小解の存在としてでてきたことは実に興味深く, ここまで展開された理論があながち的を外れていないことの傍証と言えるかも知れない.