書泉グランデでの講義

高校生も十分わかる新しい数論研究 訂正済み

講師:飯高 茂, 2014 年11月12月

飯高 茂

平成 27 年 12 月 15 日

目 次

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 定年前の不安

私は 2012 年度末に 70 歳で定年となり引退教授となった. 数年前から引退後の生活をあれこれ想像し、生き甲斐の喪失をいかにして防ぐか考えてきた. そして, 藁をもつかむ気持ちで, 引退 1 年前自分のホームページに

「2013 年 4 月から退職して暇になります. 数学や数学教育についての助言、講演などどんな仕事も無報酬で行います」

というアナウンスを載せた.

これに気づいた知人は「仕事が津波のように押し寄せて来て、飯高さんは破滅するだろう」と言った.

私もそれなりに，仕事が来ないことを心配したのだが私の方が当たった. 半年たっても問い合わせが全くなかったのである.

それまでの私の生き方は世間から無価値のものとしか評価されなかったのかと思い暗い気持ちで正月を過ごした. 休みのとき, 自宅から西武線の一橋学園駅近くにある放送大学多摩学習センターに歩いて行ってみたら 1 時間弱であった. 弁当をもって朝 9 時に家を出て多摩学習センターに行き, 学生控え室で仕事をし夕方歩いて帰れば運動不足にならないだろう. そしてまだ現役の教授のうちに,1 年ごとに入学金 (年額 9000 円, 更新ならさらに安くなる) を払う専科履修生の登録を行い, 教授と学生の 2 足のわらじをはいた生活を始めた.

0.3　都内のある私立高校

年が明けると都内のある私立高校が「高校生の数学クラブで助言してもらえないか」と密かに打診してきた．この高校には私の教え子である理学博士が数学の教員をしている．私はぶしつけな質問をした．

「数学クラブなら活動は放課後でしょう．準備する必要があるので午後から高校に行きたい. 弁当を持って行くのでそこで食べてもいいか.」

すると「講師室の中に専用の机を用意する. いつ来てもいいし、弁当を食べてよい」とのことだった.

この他に特段の事務手続きは無く, 4 月の月曜日にさっそく高校に行った.

0.3.1　数学クラブ

数学クラブには 10 名前後の生徒がいて、グループに別れて研究活動をしている．意外なことに，数年前から高校生もオリジナルな研究を行うこと．研究成果を本当の学会で発表することを国が推奨しているそうである.

こんなことも動機となりこの学校では数学研究のクラブができて、オイラー関数の研究、置換群とくにバイグラスマニアンの研究、微分方程式をもちいて伝染病の拡散の状況のシミュレーションなどをそれぞれしていて校内や校外で研究発表している．そこでオイラー関数の班の活動には数回、参加させてもらった.

いざ高校に行ってみると, 自分は助言者であり高校生に指図はできない．求められれば助言するだけ．そこで自分は何ができるか、何をすべきかで戸惑いがあった．自分の立ち位置がどこにあるか、悩みは深かった．しかし高校の先生方は私をフランクに受け入れてくれた.

0.4　高校生の数学研究

さて, 高校生は数学研究をすべきか ？

これに対する答えは,No であろう. 圧倒的な No に違いない.

高校生は, 学ぶべきです．研究は大学や大学院に入ってからすればよい.

そもそも大学に入ることが大切で, わけの分からない研究をして時間をつぶすのはもったいない

志のある生徒は受験勉強の他に, 大学レベルの数学書を読むのがよい. その方がよいだろう．あえて, 学会発表までする研究活動をすべきだろうか.

これらはもっともなことである

少ない人数ではあるが, 高校生でも数学の研究に熱心で成果がでると真実に感動しさらに努力したいという人がいる.

そういう欲求や要望に応えてやりたい.

その結果, 私は高校 2 年生なら理解できる範囲で新しい数学研究を行う必要が生じた．これは私にとって全く新しいチャレンジであって, 高校生が理解可能な問題を探し, 発展させた. そして私自身も成長し新しい数学の研究ができ広がった.

最近は私は秋葉原にある事務所に籍をおかせてもらい, そこで朝から夕方まで数学研究に専念している. 現役の教授時代に比べて 2 倍も 3 倍も数学の研究をしている. 定年後に数学の研究にほとんどの時間をささげ至福の時を過ごすようになった.

0.5 雑誌『現代数学』

2012 年の冬、現代数学社から雑誌『理系への数学』をリニューアルする予定なので、テーマは何でもよいから長期連載をしてくれないか、というメールが届いた. これも私のＨＰでの自爆的広告の効果である.

学生の研究活動を活発にするための記事を書きたい.28 年間学習院大学に勤務したので学生の数学研究の論文がたくさんある. それらを紹介することを主な目的とし題名は「数学の研究を始めよう」ではどうか、と返事をだした.

それでよいと返事が来たので直ちに原稿を書き始め「10 のべきの階乗の研究」、「オイラー関数の評価」、「誕生日を遊ぶ」、「完全数の一般化」などができた.

「完全数の一般化」の原稿は高校生にも読める形で書いたので彼らに読んでもらったところミスプリントをいくつか指摘してくれた. これはきちんと高校生が読んでいることの証拠のひとつである.

数学の研究をしても世間に結果を公開しないと意味が無い. フェルマーは晩年になって, それまで得てきた数学上の数々の結果が自分の死後忘れられていくのではないか, と思いひどくあせったそうである.

私の場合は「数学の研究を始めよう」で世の中に公表するという機会ができた. しかも稿料が入るのである. 数学の研究で生活費を稼ぐことになった. これは小川洋子さんの小説に出てくる博士の境遇である.

0.6 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 $p = 1 + 2 + 2^2 + \cdots + 2^n$ が素数なら $a = 2^n p$ は完全数になることを示した.

a の約数は

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

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 Paciuolo (1494 年 ?) は $1+2+2^2+\cdots+2^n$ 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) $1+2+4, 1+2+4+8, 1+2+4+8+16, \cdots$ は交互に素数か合成数になる, と述べた.

F.Maurolucus (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

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

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であった.

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.

L.Euler は 1752 年の Goldbacher への手紙で 7 個の完全数は $2^{p-1}(2^p-1), p = 2, 3, 5, 7, 13, 17, 19$ であるが $p = 31$ 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.

Servaias 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 $1, 2, 2^2 = 4, 2^3 = 8, \cdots$ 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 $1, 3, 3^2 = 9, 3^3 = 27, \cdots$ 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.

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

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

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

$$\sigma(a) = \sigma(p^e)\sigma(q^f). \tag{1.1}$$

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.

$\sigma(a)$ は奇数になるのは少ない.

1.1.1　$\sigma(a)$ の表

$\sigma(a)$ に親しむため 素因数分解 , $\sigma(a)$ を横に並べている.
素因数分解がわかれば $\sigma(a)$ は直ちに計算できる.

表 1.1: a の順

a	素因数分解	$\sigma(a)$	a	素因数分解	$\sigma(a)$
2	$[2]$	3	27	$[3^3]$	40
3	$[3]$	4	28	$[2^2, 7]$	56
4	$[2^2]$	7	29	$[29]$	30
5	$[5]$	6	30	$[2, 3, 5]$	72
6	$[2, 3]$	12	31	$[31]$	32
7	$[7]$	8	32	$[2^5]$	63
8	$[2^3]$	15	33	$[3, 11]$	48
9	$[3^2]$	13	34	$[2, 17]$	54
10	$[2, 5]$	18	35	$[5, 7]$	48
11	$[11]$	12	36	$[2^2, 3^2]$	91
12	$[2^2, 3]$	28	37	$[37]$	38
13	$[13]$	14	38	$[2, 19]$	60
14	$[2, 7]$	24	39	$[3, 13]$	56
15	$[3, 5]$	24	40	$[2^3, 5]$	90
16	$[2^4]$	31	41	$[41]$	42
17	$[17]$	18	42	$[2, 3, 7]$	96
18	$[2, 3^2]$	39	43	$[43]$	44
19	$[19]$	20	44	$[2^2, 11]$	84
20	$[2^2, 5]$	42	45	$[3^2, 5]$	78
21	$[3, 7]$	32	46	$[2, 23]$	72
22	$[2, 11]$	36	47	$[47]$	48
23	$[23]$	24	48	$[2^4, 3]$	124
24	$[2^3, 3]$	60	49	$[7^2]$	57
25	$[5^2]$	31	50	$[2, 5^2]$	93
26	$[2, 13]$	42	51	$[3, 17]$	72

表 1.2: $\sigma(a)$ の順

a	素因数分解	$\sigma(a)$	a	素因数分解	$\sigma(a)$
2	$[2]$	3	27	$[3^3]$	40
3	$[3]$	4	20	$[2^2, 5]$	42
5	$[5]$	6	26	$[2, 13]$	42
4	$[2^2]$	7	41	$[41]$	42
7	$[7]$	8	43	$[43]$	44
6	$[2, 3]$	12	33	$[3, 11]$	48
11	$[11]$	12	35	$[5, 7]$	48
9	$[3^2]$	13	47	$[47]$	48
13	$[13]$	14	34	$[2, 17]$	54
8	$[2^3]$	15	28	$[2^2, 7]$	56
10	$[2, 5]$	18	39	$[3, 13]$	56
17	$[17]$	18	49	$[7^2]$	57
19	$[19]$	20	24	$[2^3, 3]$	60
14	$[2, 7]$	24	38	$[2, 19]$	60
15	$[3, 5]$	24	32	$[2^5]$	63
23	$[23]$	24	30	$[2, 3, 5]$	72
12	$[2^2, 3]$	28	46	$[2, 23]$	72
29	$[29]$	30	51	$[3, 17]$	72
16	$[2^4]$	31	45	$[3^2, 5]$	78
25	$[5^2]$	31	44	$[2^2, 11]$	84
21	$[3, 7]$	32	40	$[2^3, 5]$	90
31	$[31]$	32	36	$[2^2, 3^2]$	91
22	$[2, 11]$	36	50	$[2, 5^2]$	93
37	$[37]$	38	42	$[2, 3, 7]$	96
18	$[2, 3^2]$	39	48	$[2^4, 3]$	124

$\sigma(a)$ にしたがって並べてみた.

$\sigma(a)$ 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. こられ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)

1.1.2　$\sigma(a)$ のグラフ

ユークリッド関数 $\sigma(a)$ のグラフを描いて見た．きわめて複雑な形をしている．

図 1.1: $\sigma(a)$

$x = a, y = \sigma(a)$ とおく．

$a = p > 1$ が素数なら $\sigma(a) = a + 1$ なので $y = x + 1$: これが素数の直線.

$a = p > 1$ が素数でないなら $\sigma(a) \geq a + 2$ なので $y \geq x + 2$. 素数の直線の上側になる．

$m(\neq p)$ を素数として $a = mp$ について

$b = \sigma(a) = \sigma(m)\sigma(p) = \widetilde{m}\widetilde{p}$ となるので $p = \frac{a}{m}$ を用いて

$$b = \widetilde{m}(\frac{a}{m} + 1) = \frac{\widetilde{m}x}{m} + \widetilde{m}$$

したがって, 素数 m に対して $a = mp, b = \sigma(a)$ とおけば (a, b) は直線

$$y = \frac{\widetilde{m}x}{m} + \widetilde{m}$$

の上にある.

$m=2$ に対して直線 $y=\frac{3x}{2}+3$,

$m=3$, に対して直線 $y=\frac{4x}{3}+4$,

$m=5$, に対して直線 $y=\frac{6x}{5}+6$,$\cdots$ などが対応する.

1.1.3　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うと次の表ができた.

表 1.3:

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して 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, 一見やさしそうで意外に難しい問題として残されている.

1.1.4　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．$\overline{p}=p-1$ とおくと $\sigma(a)=\frac{pa-1}{\overline{p}}$ となるので,

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

よって

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

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

$p-2\overline{p}=2-p$ 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.

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

$X=p^e,Y=q^f$, $A=pX-1,B=qY-1$, $\rho'=\overline{pq}$ 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 $R=pq-2\rho'=2-(p-2)(q-2)$.

$$RXY-(pX+qY-1)=-\rho'. \tag{1.2}$$

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 $\rho'=\overline{q},R=2$.

式 (1.2) より

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

これを変形して

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

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,$a = 2^e$ に関しての 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.

$\sigma(a) - 2a; a < 100$ の順に並べた表をみて見よう.

表 1.4:

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$
7	$[7]$	8	-6
15	$[3, 5]$	24	-6
9	$[3^2]$	13	-5
5	$[5]$	6	-4
14	$[2, 7]$	24	-4
44	$[2^2, 11]$	84	-4
3	$[3]$	4	-2
10	$[2, 5]$	18	-2
2	$[2]$	3	-1 (2 のべき)
4	$[2^2]$	7	-1
8	$[2^3]$	15	-1
16	$[2^4]$	31	-1
32	$[2^5]$	63	-1
6	$[2, 3]$	12	0 (完全数)
28	$[2^2, 7]$	56	0
20	$[2^2, 5]$	42	2
18	$[2, 3^2]$	39	3
12	$[2^2, 3]$	28	4
40	$[2^3, 5]$	90	10

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.

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, $a=2^eL(L:$ 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

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

$d=\sigma(L)-L$ とおくとき $Nd=L$. 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 $a=2^ep$. 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.

Dickson にある完全数の証明:
$(2^{e+1}-1)\sigma(L)=2^{e+1}L$ により

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

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

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

となってしまい矛盾.

1.3.2　$\sigma(a)-a=1$

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なのだ.

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見た.

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

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.

1.3.3　疑似完全数

$\sigma(a) - 2a = 1$ を満たす自然数は 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が問われている.

$\sigma(a) - 2a = -1, 0, 1$ を満たす自然数 a を求める問題はどれも未解決の難問である. 完全数の問題は 2300 年かかっても解けない難問だが, その前後の問題 (3 点セット) も未だに解けない. 実は, これ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.

1.3.4　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,$\cdots$ 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)

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

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

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

表 1.5: $\sigma(2^e) = 2^{e+1} - 1$, $e+1$: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]

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

したがって α は完全数になる.

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 $s(a)$ とおくと, 先ほどの奇数完全数の非存在問題は $s(a) < 8$ なら解けているらしい.

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

1.3.5　$s(a) = 2$ 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. $\overline{p} = p - 1, \overline{q} = q - 1$ を使うと

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

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

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

書き直して

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

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

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

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.

1.5 完全数の数表

表 1.6: 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	6
0	16	17	$2^{16}*131071$	8589869056	6
2	18	19	$2^{18}*524287$	137438691328	8
2	30	31	A	B	8
0	60	61	C	D	6
0	88	89	E	F	6

$A = 2^{30} * 2147483647$
$B = 2305843008139952128$
$C = 2^{60} * 2305843009213693951$
$D = 26584559915698317446546926159538421 76$
$E = 2^{88} * 618970019642690137449562111$
$F = 191561942608236107294793378084303638130997321548169216$
a の末尾の数は 6 か 8. 言い換えると $a \equiv 6$ または $8 \mod 10$. これは完全数の持つ周知の性質のひとつ.

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.

- $e \equiv 0 \mod 4$ なら $q \equiv 1 \mod 10$. $a \equiv 6 \mod 10$.
- $e \equiv 2 \mod 4$ なら $q \equiv 7 \mod 10$. $a \equiv 8 \mod 10$.

Proof. (金子元さんの援助による)

$2^4 = 16 \equiv 1 \mod 5$ を以下用いる.
1). $e = 4k$. $q = 2^{e+1} - 1 \equiv 1 \mod 5$ によって $q = 1 + 5L$. q は奇数なので L は偶数. $q \equiv 1 \mod 10$.
$a = 2^e q \equiv q \equiv 1 \mod 5$; $a = 1+5L$. a は偶数なので $L = 2m+1$. $a = 1+5(2m+1) \equiv 6 \mod 10$.

2). $e = 4k + 1$. $c = 2^{2k+1}$ とおくとき

$q = 2^{e+1} - 1 = 2^{4k+2} - 1 = c^2 - 1 = (c-1)(c+1)$ 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). $e = 4k+2$. $q = 2^{e+1} - 1 \equiv 2 \mod 5$ によって $q = 2+5L$. L は奇数になり, $q \equiv 7 \mod 10$.
$a = 2^e q \equiv -q \equiv 3 \mod 5$; $a = 3 + 5L$. a は偶数なので $L = 2m + 1$. $a = 3 + 5(2m+1) \equiv 8 \mod 10$.

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

偶数完全数の末尾の 1 桁は 6, または 8 になるという結果は完全数の中でもやさしいが美しい性質である.

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.

表 1.7:

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

1.5.1　$m = 2$

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.

表 1.8: $q = 2^{e+1} + 1$ 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.

$e \geq 3$ のとき $q \equiv 7, a \equiv 6 \mod 10$.
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
$q = 2^{e+1} + 1 \equiv 2 \bmod 5$. 一方, q は奇数なので $2^e \equiv 3 \times 2^{e+1}$ なので $q \equiv 7 \mod 10$.
$a = 2^e * q \equiv 3 * q \equiv 6 \bmod 5$, a は偶数なので $a \equiv 6 \mod 10$.

1.5.2　$m = 4$

$q = 2^{e+1} + 3$ が素数の場合

表 1.9:

$e \bmod 4$	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

$A = 2^{27} * 268435459, B = 36028797421617152$
$C = 2^{29} * 1073741827, D = 576460753914036224$
$E = 2^{54} * 36028797018963971, F = 576460753914036224$
$G = 2^{66} * 147573952589676412931$
$H = 6490371073168535076095075695598464$
$I = 2^{83} * 19342813113834066795298819$
$J = 187072209578355573530071687601903897267059558449152$
$K = 2^{98} * 633825300114114700748351602691$
$L = 200867255532373784442745261543596063265446546273971631816704$
表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 7, a \equiv 4 \mod 10.$
- $e \equiv 2 \bmod 4$ なら $q \equiv 1, a \equiv 4 \mod 10.$
- $e \equiv 3 \bmod 4$ なら $q \equiv 9, a \equiv 2 \mod 10.$

Proof.

$e = 4k + 1$ のとき,
$q \equiv 4 + 3 \equiv 7 \bmod 5$, $q \equiv 7 \mod 10.$
$a = 2^e q \equiv 2 * 7 = 14 \equiv 4 \bmod 5$, $a \equiv 4 \mod 10.$

$e = 4k + 2$ のとき,
$q \equiv -2 + 3 \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.
$a = 2^e q \equiv 4 * q \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 3$ のとき,
$q \equiv 1 + 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.
$a = 2^e q \equiv 3 * 4 = 12 \equiv 2 \bmod 5$, $a \equiv 2 \mod 10$.

1.5.3　$m = -2$

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

表 1.10: $q = 2^{e+1} - 3$ 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

- $e \equiv 1 \bmod 4$ なら $q \equiv 1, a \equiv 2 \mod 10$.
- $e \equiv 0 \bmod 4$ なら $q \equiv 9, a \equiv 4 \mod 10$.
- $e \equiv 3 \bmod 4$ なら $q \equiv 3, a \equiv 4 \mod 10$.

Proof.
$e = 4k + 1$ のとき,
$q = 2^{e+1} - 3 \equiv 4 - 3 \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.
$a = 2^e q \equiv 2 * 1 = 2 \bmod 5$, $a \equiv 2 \mod 10$.

$e = 4k$ のとき,

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

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

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

1.5.4　$m = -4$

$q = 2^{e+1} - 5$ が素数の場合

表 1.11: $q = 2^{e+1} - 5$

e mod 4	e	$2^e * q$	a	a mod 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

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. $2^{2N+1} = 4^N \times 2 \equiv 2, 5 \equiv 2 \mod 3$.
これらにより $q = 2^{2N+1} - 5 \equiv 0 \mod 3$ したがって q が 3 の倍数; 矛盾が導かれた.

表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 9, a \equiv 8 \mod 10$.
- $e \equiv 3 \bmod 4$ なら $q \equiv 1, a \equiv 8 \mod 10$.

Proof.
$e = 4k + 1$ のとき,
$q \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.
$a = 2^e q \equiv 2 * 9 \equiv 3 \bmod 5$, $a \equiv 8 \mod 10$.

$e = 4k + 3$ のとき,
$q \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.
$a = 2^e q \equiv 3 * 1 \bmod 5$, $a \equiv 8 \mod 10$.

1.5.5　$m = -6$

$q = 2^{e+1} - 7$ が素数の場合

表 1.12: $q = 2^{e+1} - 7$ が素数

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
2	2	$2^2 * 1$	4	4
2	38	$2^{38} * 549755813881$	151115727449904501489664	4

$a = 4$ 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.
$q = 2^{e+1} - 7 = (2^2)^{k+1} - 7 \equiv 1 - 1 = 0 \bmod 3$ なので矛盾.

$e = 4k + 2$ の証明
$e = 4k$ として矛盾を導く.
$q = 2^{e+1} - 7 = (2^4)^k \times 2 - 7 \equiv 2 - 2 = 0 \bmod 5$ 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.

- $N = 2^{42+1} - 7$ の最小素因子 107
- $N = 2^{46+1} - 7$ の最小素因子 11
- $N = 2^{50+1} - 7$ の最小素因子 17174671
- $N = 2^{54+1} - 7$ の最小素因子 896723
- $N = 2^{58+1} - 7$ の最小素因子 13
- $N = 2^{62+1} - 7$ の最小素因子 157

$e = 160$ まで試みたが $q = 2^{e+1} - 7$ が素数となる場合は見つからなかった.

1.6　m だけ平行移動した完全数の定義式

パラメータ m に対して $q=2^{e+1}-1+m$ が素数のとき $a=2^eq$ を m だけ平行移動した完全数という. これの満たす方程式を求めよう. ただし m は偶数の整数.

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

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

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なるか?

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ので, 次に $m=4$ の場合を扱う.

1.6.1　$\sigma(a)=2a-4$

$\sigma(a)=2a-4$ を満たす解の表を作った.

表 1.13: $\sigma(a)=2a-4$

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.

1.7 3^e のとき

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

1.7.1 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う.

表 1.14: $2\sigma(a) - 3a = -1$

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えて 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 3 のべきになることはすぐわかる.

1.7.2 $s(a) = 2$ 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.

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

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

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

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

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 $R>0$. $0<R=6-(p-3)(q-3)$ により $p=3, R=6$. $\rho'=2\overline{q}$

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

を 2 で割って

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

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

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

$3X=q$ となり矛盾.

$s(a)\geq 3$ のときも矛盾が導けるとよいのだが, 難しそうである.

$s(a)\geq 3$ なら解のない証明は難しそうなので解がある方に私は 1 票入れたい.

1.7.3 $2\sigma(a) - 3a$ 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．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 1.15: $2\sigma(a) - 3a$ の値

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$	$2\sigma(a) - 3a$(亜完全度)
51	$[3, 17]$	72	-30	-9
35	$[5, 7]$	48	-22	-9
11	$[11]$	12	-10	-9
39	$[3, 13]$	56	-22	-5
7	$[7]$	8	-6	-5
33	$[3, 11]$	48	-18	-3
5	$[5]$	6	-4	-3
27	$[3^3]$	40	-14	-1(3 のべき)
9	$[3^2]$	13	-5	-1
3	$[3]$	4	-2	-1
2	$[2]$	3	-1	0
21	$[3, 7]$	32	-10	1
4	$[2^2]$	7	-1	2
15	$[3, 5]$	24	-6	3
46	$[2, 23]$	72	-20	6 ($a = 2p$)
38	$[2, 19]$	60	-16	6
34	$[2, 17]$	54	-14	6
26	$[2, 13]$	42	-10	6
22	$[2, 11]$	36	-8	6
14	$[2, 7]$	24	-4	6
10	$[2, 5]$	18	-2	6

表によれば $2\sigma(a) = 3a$ を満たす a は 2 だけらしい．
やってみたら簡単に証明できた．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.

1.8　$2\sigma(a) - 3a = 1$ 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 1.16: $2\sigma(a) - 3a = 1$

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 $3^e * q$ の形になっているのでこのような解があるとしてそれを決めよう.
$a = 3^e * q, (q > 3:$ 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.

1.9　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.

1.10　亜完全度

$W = 2\sigma(a) - 3a$ とおき W を 亜完全度とよぶ. 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.

$s(a) = 2$ と仮定したので a を素因数分解し $a = p^e q^f$ とする.

1.10.1　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 とおくとき $R = 2pq - 3\rho'$ 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

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

移項して

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

(1) $Y = q$ と仮定すると

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

により, $\overline{q}$ 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.

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

これより $\overline{q}$ 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

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

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.

1.10.2　奇数の例

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

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

$W = 23$ なら $a = 75$ になるか?

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

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

この場合 $s(a) = 3$ の解も出てきた.

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

表 1.17: $W = 23$ の場合

a	$\sigma(a)$	素因数分解
75	124	$[3, 5^2]$

表 1.18: $W = 131$ 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 1.19: $W = 455$ 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.

1.10.3　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

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

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

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

書き直して

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

$R = 4q - 3\rho'$ とおくとき $R = q + 3$.

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

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

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

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

$$2(m-3)=(q+4)(2^e-2). \tag{1.3}$$

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 1.20: $W=20$ の場合

a	$\sigma(a)$	素因数分解
12	28	$[2^2,3]$

.

表 1.21: $W=24$ の場合

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

表 1.22: $W = 28$ の場合

a	$\sigma(a)$	素因数分解
28	56	$[2^2, 7]$

表 1.23: $W = 36$ 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 $a = 2^3 q$.
$2(m-3) = 6(q+4)$ 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 1.24: $W = 48$ 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 1.25: $W = 60$ 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 $Rq^2 - 4 = q^2(q+3) - 4 = (q^2 + 4q + 4)\overline{q}$ により

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

よって

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

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 $m = 36X = 2, q = 11, Y = 121$.
$a = 242, \sigma(a) = 399$. $2\sigma(a) - 3a = 2 \times 399 - 3 * 242 = 72 = W$.

(3) $Y = q^3$ などについても考える.

1.10.4　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 $m - 3 = 33$, $2(m-3) = 2 * 3 * 11 = (q+4)(2^e-2)$ 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 1.26: $W = 72$ 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 1.27: $X = 2$ 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 1.28: $X = 4$ 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 1.29: $X = 8$ の場合

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

1.10.5　亜完全度 4,6 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

$$(2^{e+1} - 1)\sigma(L) - 3 \cdot 2^{e-1} L = m. \tag{1.4}$$

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 (1.4) 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 (1.4) 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 $a=4$.

1.11　3 のべきとそのユークリッド関数の値

表 1.30: $3^e = a$

$3^e = a$	$\sigma(a)$	$\sigma(a)$ 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]
$3^{30} = 205891132094649$	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．

$9 * 13 = 117, 729 * 1093 = 796797$ などは完全数の類似とみなすことができる．

1.12　3 を底とする完全数

$a = 3^e$ に対して $\sigma(3^e) = \dfrac{3^{e+1} - 1}{2}$ 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言うことにする．

1.12.1　3 を底とする完全数の数表

表 1.31: 3 を底とする完全数

e mod 4	e	素因数分解	q mod 10	a	a mod 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

$A = 3^{70} * 3754733257489862401973357979128773$
$B = 939868122326695556888433629151289424673228917359519725450340403327$
$C = 3^{102} * 6957596529882152968992225251835887181478451547013$
$D = 3227209964841878447466193062734722465975186449738511$
$--2062067563800310073569424269938090581449997117$
これらから次の結論を導くことができる.

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

$3^2 = 9 \equiv -1 \mod 5$ により $3^4 \equiv 1 \mod 5$. 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

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

よって $q \equiv 3 \mod 5$. $q = 3+5L$ となるが q は素数なので奇数. L は偶数になるので $q \equiv 3 \mod 10$.
$a = 3^e q \equiv -q \equiv 2 \mod 5$ により $a = 2 + 5L$. L は奇数になるので $a \equiv 7 \mod 10$.

2. $e = 4k$ のとき

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

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

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

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

$A - 1 = 3^{k+1} - 1 = 2(3^k + 3^{k-1} + \cdots 1)$ 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 $A = 3^{2k+1}$ とおくとき

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

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

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

q が素数に矛盾.

1.12.2　$s(a) = 1$ 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 $2\sigma(a) = 3a + \mathrm{Maxp}(a)$ を満たすと仮定する.
$Y = q^f$ とおくと

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

これより

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

$2q - 3\overline{q} > 0$ により, $q = 2$.
$Y(2q - 3\overline{q}) = 2 + q\overline{q}$ 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.

1.12.3　$s(a) = 2$ 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.
$2\sigma(a) = 3a + \mathrm{Maxp}(a)$ を満たすと仮定する.
ここで a は奇数である. なぜなら $\mathrm{Maxp}(a)$ 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 $\overline{p} = p - 1, \overline{q} = q - 1$ を使うと

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

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

$\mathrm{Maxp}(a) = q$ 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 $p = 3, R = 6$. $\rho' = 2\overline{q}$.

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

を 2 で割って

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

$3X > q$ かつ $Y \geq q$ によって

$$\overline{q}q \geq (3X - q)q - 3X + 1 = 3X\overline{q} - \widetilde{q}\overline{q}.$$

$\overline{q}q \geq 3X\overline{q} - \widetilde{q}\overline{q}$ から $\overline{q}$ を消すと

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

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.

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

よって

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

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

1.12.4　3 を底とする完全数の公式

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 $a=3^eq$ 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.

.

$q=\sigma(3^e)=\dfrac{3^{e+1}-1}{2}$ より $q+1=\dfrac{3^{e+1}+1}{2}$ 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 $\mathrm{Maxp}(a)$ と書くことにすると次の公式の形にまとめられた.

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

すると次の大きな問題はこの公式を満たす α は $\sigma(3^e)$ が素数 q になるのを用いて $\alpha=aq$ 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.

1.13　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 $a=3^eq$ 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.

$q=\frac{3^{e+1}-1}{2}+m$ が素数 q のとき $a=3^eq$ を m だけ **平行移動した 3 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.

1.13.1　$p=3.m=1$

$p=3.m=1$ のとき

$X=5722806367154190562796729901 87$

$A=3^{63}*171684191014625624232892454464 1$

$B=1965030762956430528586812143569325391583084017460083159697707$

q の末尾の数は 1, a の末尾の数は 7 になることを証明したい.

Proof.

$m=1$ なので $2q=3^{e+1}+1$ になる.

表 1.32: $m = 1$

$e \bmod 4$	e	素因数分解	$q \bmod 10$	a	$a \bmod 10$
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

1.
$e = 4k + 3$.

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

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

$$a = 3^e q \equiv 2q \equiv 2 \mod 5.$$

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

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

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

q は素数に反する.

3. $e = 4k + 2$.

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

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.

$m = 2$ 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.

1.13.2 $p = 3.m = 3$

$p = 3.m = 3$ のときは $q = \frac{3^{e+1}+5}{2}$.

表 1.33: $m = 3$

e	素因数分解	a
3	$3^3 * 43$	1161
5	$3^5 * 367$	89181
9	$3^9 * 29527$	581179941
59	A	B

$A = 3^{59} * 21195579137608101757147216603$
$B = 2995017166524052017355299716202601385179261075182205454 01$

[研究課題]
$q \equiv 3, 7; a \equiv 1 \mod 10$ を示す.

1.13.3　$p = 3.m = -2$

$p = 3.m = -2$ のときは $q = \frac{3^{e+1}-5}{2}$.

表 1.34: $m = -2$

e	素因数分解	a
2	$3^2 * 11$	99
6	$3^6 * 1091$	795339
8	$3^8 * 9839$	64553679
30	A	B
44	C	D
48	E	F

$A = 3^{30} * 308836698141971$
$B = 63586737412823790543611413179$
$C = 3^{44} * 1477156353275416849319$
$D = 1454660594681285404312770985990662195258039$
$E = 3^{48} * 1196496646153087647950 39$
$F = 954402816170391353771204372770010916506066 6079$
さて

- q の末尾の数は 1,9.
- a の末尾の数は 9.

正しいか? 証明できるか?

1.13.4　$p = 3.m = -3$

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

表 1.35: $m = -3$

e	素因数分解	a
3	$3^3 * 37$	999
11	$3^{11} * 265717$	47070969399
17	$3^{17} * 193710241$	25015772097509283
25	$3^{25} * 1270932914161$	1076846981534813373022323

$2q = 3^{e+1} - 7, a = 3^e q$ が成り立つ.

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

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

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

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

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

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

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

1.14　m だけ平行移動した完全数の公式

$q = \frac{3^{e+1}-1}{2} + m$ が素数 q のとき $a = 3^e q$ とおく. これが満たす形式を決定しよう.
$q + 1 = \frac{3^{e+1}+1}{2} + m$ 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

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

かくして $q = \mathrm{Maxp}(a)$ を使うと公式

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

がえられた.
この公式を満たす解を探す. 一種の逆問題を考えることになる.

1.15　公式を満たす解

1.15.1　$m = 0$ のとき

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

表 1.36: $[p = 3, m = 0]$

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

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.

1.15.2　$m = 1$ のとき

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

表 1.37: $[p = 3, m = 1]$

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

1.15.3　$3^e qr$ のとき

$m = 1$ のとき $2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2$ になるが, この解 a を素因数分解すると $[3, 13, 19]$ と $[3, 11^2, 41]$ があったのでこの形の解,$3^e qr$ と書ける解を探す.
$= 3^e qr (3 < q, r :$ 素数$)$ とおくと $\mathrm{Maxp}(a) = r$ になるので

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

$\Delta = q + r$ 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

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

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

$$q''r'' = \Gamma^2 + 2.$$

そこで, 与えられた e に対して, $\Gamma = 3^{e+1}-1, U = \Gamma^2+2$ を求め 2 因数分解: $q''r'' = U, q'' < r''$ を行い, $q = q''+\Gamma-1, r = r''+\Gamma$ がともに素数になるもの探すと次の結果をえた.

$e = 1, 2, 11$ について解が発見された.

表 1.38: $[p=3, m=1]$

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

$m \neq 1$ のとき $2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2m$ の解で $3^e qr$ と書けるものの方程式を求める.

1.15.4　$m = -2$ のとき

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

表 1.39: $[p=3, m=-2]$

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

表 1.40: $[p = 3, m = -2]$

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 1.41: $[p = 3, m = 4; a = 3^e qr]$

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

1.15.5　$m = 2$ のとき

$m = 2$ のとき

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

$a = 3^f$ はこの式を満たす.

実際に $2\sigma(a) = 3 * 3^f - 1, 3a + \mathrm{Maxp}(a) - 4 = 3 * 3^f + 3 - 4$.

$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 4$ 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, 公式が $2\sigma(a) = 3a + \mathrm{Maxp}(a) \quad - 2m$ 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.

1.15.6　$m = -1$ のとき

$s(a) = 2$ の解はない.

表 1.42: $[p = 3, m = 2]$

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

表 1.43: $[p = 3, m = -1]$

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

1.16　5 べき 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
$\sigma(a) = \sigma(P^E) = \frac{aP-1}{\overline{P}}$ によって

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

これが $a = P^E$ に関しての方程式である.

$P = 5$ 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.

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 AKB 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驚かざるを得ない.

表 1.44: $4\sigma(a)-5a=-1$

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	$[5^6]$

1.16.1　$s(a)=2$ 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.

[$s(a)=1$ のときに求めるのは良い演習問題である.]

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

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

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

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

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

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

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

次の基本等式

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

を各場合ごとに調べる.

1. $p=5, R=20.\ \rho'=4\overline{q}$ の場合.
基本等式を 4 で割って

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

$(5X-q)Y-5X=-\overline{q}-1=q$ により

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

よって $5X=5^{f+1}=q$ となり矛盾.

2. $p=3, R=30+2q.\ \rho'=2\overline{q}.$
$R_1=R/2=5+q$ とおくと

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

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

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

$q=11$ 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 $a=77$.

証明は適当に難しい. しかしながら $s(a)=3$ の解がある可能性が残る.

1.16.2 $\sigma(5^e)$ が素数になる場合

表 1.45: $5^e a$ 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	$[8971, 332207361361]$

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

1.17　5 を底とする完全数

$a=5^e$ 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 $\mathrm{Maxp}(a)$ と書きこれを使う．すると

$$4\sigma(\alpha)=5\alpha+3\mathrm{Maxp}(\alpha)$$

を満たす．

1.17.1　$s(a)=2$ の場合

$4\sigma(\alpha)=5\alpha+3\mathrm{Maxp}(\alpha)$ の解を $s(a)=2$ の場合に求めよう.

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

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

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

$$\frac{4AB}{\rho'}=5XY+3q$$

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

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

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

$$RXY-4(pX+qY-1)=3q\rho'.$$

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

$$(20X-4q)Y-20X=12q\overline{q}-4.$$

4 で割って

$$(5X-q)Y-5X=(5X-q)Y-(5X-q)-q=3q\overline{q}-1.$$

変形して

$$(5X-q)(Y-1)=3q\overline{q}+\overline{q}.$$

$Y-1\geq\overline{q}$ により

$$3q\overline{q}+\overline{q}\geq(5X-q)\overline{q}$$

$\overline{q}$ を除して

$$3q+1 \ge (5X-q).$$

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

$$(5X-q)(q^2-1)=(5X-q)(Y-1)=3q\overline{q}+\overline{q}$$

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. $Y \ge q^3$ なら

$$(5X-q)(Y-1)=3q\overline{q}+\overline{q} \ge (5X-q)(q^3-1)=(5X-q)(q^2+q+1)\overline{q}.$$

$\overline{q}$ を除すると $3q+1 \ge q^2+q+1$; 矛盾.

2. $p=3, R=30+2q$. $\rho'=2\overline{q}$,
$R_1=15+q$ とおくとき

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

$Y \ge q$ により

$$(R_1X-2q)Y=6X+3q\overline{q}-2 \ge (R_1X-2q)q.$$

$6X+3q\overline{q}-2 \ge (R_1X-2q)q$ により

$$3q\overline{q}-2+2q^2 \ge (R_1q-6)X.$$

i. $X \ge 3^2=9$ のとき

$$3q\overline{q}-2+2q^2 \ge 9(R_1q-6)=9(q^2+15q-6).$$

これから矛盾が出る.
ii. $X=3$ のとき

$$3R_1Y-2(9+qY-1)=3q\overline{q}-2.$$

これより

$$Y(3R_1-2q)=3q\overline{q}-4.$$

$3R_1-2q=q+45$ なので $q_1=q+45$ とおいて

$$q_1Y=3q^2-3q-4=\overline{q}-4=3q_1^2-273q_1+6226.$$

$\frac{6226}{q_1}$ 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. $p = 7, R = 30-2q; q = 11, 13\ \rho' = 6\overline{q}$.
$p = 7$ より $R_1 = 15-q$ とおくと

$$R_1XY - 2(7X+qY-1) = 9q\overline{q}$$

i. $q = 11$ なら

$$4XY - 2(7X+11Y-1) = 9q\overline{q} = 90\times 11.$$

$X_1 = 2X, Y_1 = 2Y$ とすると

$$X_1Y_1 - 7X_1 - 11Y_1 = 9q\overline{q} = 90\times 11 - 2 = 988.$$

$$X_1(Y_1-7) - 11(Y_1-7) = (X_1-11)(Y_1-7) = 988+77 = 1065 = 3*5*71.$$

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 $R_1 = 2$.

$$4XY - 4(7X+13Y-1) = 18q\overline{q} = 2808.$$

$$XY - (7X+13Y) = 3^2*6*13-1 = 701.$$

$$(X-13)(Y-7) = 701+13*7 = 792 = 8*9*11.$$

$X-13 = 36, Y-7 = 22; Y = 29$. 矛盾

第2章　究極の完全数

2.1　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 $a=P^eq$ 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 だけ平行移動する.
$q=\frac{P^{e+1}-1}{P}+m$ は素数として $a=P^eq$ を m だけ平行移動した底が P の完全数と呼ぶ.

2.1.1　例

$[p=5,m=0]$

表 2.1: $P=5,m=0$

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

$A=252435489670723777731753140890491238224058179184794425964355468 75$
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, $q\equiv 31 \mod 50$ を証明する.
$e\geq 2$ により

$$4q=5^{e+1}-1\equiv -1 \mod 25$$

6倍して

$$24q\equiv -6 \mod 25$$

$24q\equiv -q$ により

$$q \equiv 6 \equiv 31 \mod 25$$

q は奇数なので $q \equiv 31 \mod 50$.
$e \geq 3$ を仮定する.
$a = 5^e * q = 625 * 5^{e-3} * (31 + 50k)$
a の末尾はどれも 5.(これは当然のこと)

$[p = 5, m = 1]$

表 2.2: $P = 5, m = 1$

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

$q \equiv 7, 32 \mod 50$ を以下で証明する.
$q = \frac{5^{e+1}-1}{4} + 1 = \frac{5^{e+1}+3}{4}$ により
$e \geq 2, 5^2 \equiv 0 \mod 25$ を用いて

$$4q = 5^{e+1} + 3 \equiv 3 \mod 25.$$

6 倍して

$$24q \equiv -q \equiv 18 \mod 25$$

$q \equiv 7$ により

$$q \equiv 7 \mod 25.$$

$q = 7 + 25k$. q は奇数なので k は偶数になり,

$$q \equiv 7 \mod 50.$$

$[p = 5, m = -2]$

$A = 277555756156289134770631790161132812 5$
$B = 677626357803440271254605613648891448974609375$
$C = 6462348535570528709932880406745425716508179903030395507812 5$
以下で, $q \equiv 9 \mod 10$ を示す.

表 2.3: $P = 5, m = -2$

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	$5^{32} * 291038304567337036113279$	B
42	$5^{42} * 2842170943040400743484497070 29$	C

$q = \frac{5^{e+1}-1}{4} - 2 = \frac{5^{e+1}-9}{4}$ により
$4q = 5^{e+1} - 9$ により
6 倍して

$$24q \equiv -q \equiv -54 \equiv -4 \mod 25.$$

$$q \equiv 4 \equiv 29 \mod 25.$$

$q = 19 + 25k$ となるが, q は奇数なので k は偶数. ゆえに

$$q \equiv 29 \mod 50.$$

2.1.2 $[p = 7, m = 0]$

表 2.4: $P = 7, m = 0$

e	素因数分解	a
4	$7^4 * 2801$	6725201
12	$7^{12} * 16148168401$	223511436608353935601

a, q は末尾が 1. 証明できるか?

$[p = 7, m = 1]$

$A = 329568463,$
$B = 4561457891661258343,$
$C = 167420868544846506666536922416431932606978335013856009100743$
q の末尾は 1,9 ;a の末尾は 3 .
証明できるか?

表 2.5: $P = 7, m = 1$

e	素因数分解	a
3	$7^3 * 401$	137543
5	$7^5 * 19609$	A
11	$7^{11} * 2306881201$	B
35	$7^{35} * 441955140976608911963170563601$	C

2.1.3 $[p = 11, m = 0]$

表 2.6: $P = 11, m = 0$

e	素因数分解	a
16	$11^{16} * 50544702849929377$	A
18	$11^{18} * 6115909044841454629$	B

$A = 2322515441988780809505203793273697$,
$B = 34003948586157739898684696499226975549$.

$[p = 11, m = -1]$

表 2.7: $P = 11, m = 1$

e	素因数分解	a
7	$11^{16} * 21435889$	A

$A = 984973308935517986686129$

2.1.4 $[p = 13, m = 0]$

表 2.8: $P = 13, m = 0$

e	素因数分解	a
4	$13^4 * 30941$	883705901
6	$13^6 * 5229043$	25239591813787

2.2　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.

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

になり, $q+1 = \frac{P^{e+1}+P-2}{\overline{P}} + m$ を用いて次のように式変形する.

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

これより

$$\overline{P}\sigma(a) - Pa = (P-2)\mathrm{Maxp}(a) - m(P-1). \tag{2.1}$$

例えば $P=2$ なら

$$\sigma(a) = 2a - m.$$

$P=2$ に限って不愉快な $\mathrm{Maxp}(a)$ が消えた.

$P=3$ なら

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

2.2.1　究極の完全数の基本問題

(2.1) を満たすとき

素数 $q = \frac{P^{e+1}-1}{\overline{P}} + m$ 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.

2.3 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.

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

2.3.1 $[P=2, m=0]$

表 2.9: $\sigma(a) - 2a = 0$

a	素因数分解	$\sigma(a)$
6	$[2,3]$	12
28	$[2^2,7]$	56
496	$[2^4,31]$	992
8128	$[2^6,127]$	16256

おなじみの完全数 4 人組 6,28,496(仕組むね),8128(やい, にやけるな) が登場する.

2.3.2 $[P=3, m=0]$

表 2.10: $[P=3, m=0]$

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

$a=4$ は微小解.

2.3.3 $[P=5, m=0]$

表 2.11: $[P=5, m=0]$

a	素因数分解	$\sigma(a)$
775	$[5^2,31]$	992

微小解は無い.

2.3.4 $[P = 7, m = 0]$

表 2.12: $[P = 7, m = 0]$

a	素因数分解	$\sigma(a)$
9	$[3^2]$	13

$a = 3^2$ は微小解.

2.3.5 $[P = 43, m = 0]$

表 2.13: $[P = 43, m = 0]$

a	素因数分解	$\sigma(a)$
49	$[7^2]$	57

2.4　微小解

平行移動しない場合を扱う. したがって

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

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.
$f = 1$ のとき.

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

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 $a = Y, \overline{q}\sigma(a) = qY - 1$ を満たし $\mathrm{Maxp}(a) = q$ によって

$$\frac{\overline{P}(qY-1)}{\overline{q}} = PY + (P-2)q.$$

整理して

$$Y(\overline{P}q - P\overline{q}) = \overline{P} + (P-2)q\overline{q}.$$

これより

$$\overline{P} = Y(P-q) - (P-2)q\overline{q} = q(q^{f-1}(P-q) - (P-2)\overline{q}).$$

よって $\overline{P} = wq$ を満たす自然数 w がある. $P - 1 = wq$ なので

$$\overline{P} = Y(P-q) - (P-2)q\overline{q} = q(q^{f-1}(P-q) - (P-2)\overline{q}).$$

$\overline{P} = wq$ により q を払って

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

よって

$$w = (1+wq)(q^{f-1} - \overline{q}) - q^f + 2\overline{q}.$$

$$w(1 - q^f + q\overline{q}) = -q^f + q^{f-1} - \overline{q}.$$

$w = 1$ のとき.
$P = 1 + q$ となり P, q はともに素数だから $q = 2, P = 3, Y = 2^f$.
$2\sigma(a) = 3a + 2$ なので $a = Y = 2^f$. よって $2(2Y-1) = 3Y + 2$. これより $a = Y = 4$.

$w \geq 2$ のとき.

$$2(q^f - q\overline{q} - 1) \leq w(q^f - q\overline{q} - 1) = q^f - q^{f-1} + \overline{q}.$$

これより

$$q^f - 2q\overline{q} - 2 \leq -q^{f-1} + \overline{q}.$$

$$q^{f-1}(q+1) \leq 2q^2 - q + 1.$$

$f \geq 3$ のとき.

$$q^2(q+1) \leq 2q^2 - q + 1.$$

変形して

$$q^3 - q^2 \leq 1 - q.$$

これは矛盾.

$f = 2$ のとき

$$w(q^2 - q(q-1) - 1) = q^2 - q - (q-1) = \overline{q}^2.$$

$q^2 - q(q-1) - 1 = q - 1, w\overline{q} = \overline{q}^2$ によって $w = \overline{q}$.

$P - 1 = wq = q(q-1)$ 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.

2.4.1　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 $\{an + b\}$ $(n = 1, 2, 3, \cdots)$ 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.

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.

表 2.14: 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

2.4.2　$s(a) = 2$ 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.

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

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.

2.4.3　反例

m が 0 でないと反例がでて来やすい. $m = 0$ でも反例がありそうだが構成が難しい. 最も簡単な $P = 2$ のときを扱う.

すなわち, $\sigma(a) = 2a - m$ を満たす数 a は m だけ平行移動した 底が 2 の完全数になるか. という問題を提起できる.

$m = 0$ ならこの問題は古来からの難問であり未だに解けない「奇数完全数はあるか」 という問題である.

しかし,m だけ平行移動すると反例を作りやすい.

$[p = 2, m = 1]$ であれば $\sigma(a) = 2a - 1$ を満たす数を探すことになるがこれを満たす数は概完全数とよばれ, これが 2 のべきになるかは未だに解けない難問中の難問である. パソコンで結果を探索する.

$[p=2, m=1]$

表 2.15: $[p=2, m=1]$

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

$p=2$ のとき m だけ平行移動すると $q=2^{e+1}-1-m$ になるが q が素数になるためには m は偶数でないといけない. したがって, ここで $m=1$ の場合を考えるのは違反行為なのだが違反した結果, 概完全数の式というおもしろい例がでてきた. 不思議なことだ.

$[p=2, m=2]$

$[p=2, m=2]$ であれば $\sigma(a)=2a-2$ を満たす数を探す.

表 2.16: $\sigma(a)=2a-2$

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

2 のべきとフェルマー素数の積で書けるらしいが, 証明は難しいであろう.

$[p=2, m=4]$

2 のべき 2^e と素数 q の積で書ける解以外に $s(a)=1, s(a)=3$ の解がでてきた.
$s(a)=3$ の解でも $a=2^e qr, 2<q<r$ に特化した解をパソコンで探索して出た結果を次に示す.

2.4.4　$m=8$

$\sigma(a)=2a-8$ の解をパソコンで探索した.

表 2.17: $\sigma(a) = 2a - 4$

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

表 2.18: $m = 4, a = 2^e qr$

a	素因数分解	$\sigma(a)$
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

表 2.19: $\sigma(a) = 2a - 8$ の解

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
100804	$[2^2, 11, 29, 79]$	201600

$a = 2^e q, (q:$ 素数$)$ の解とすると $q = 2^{e+1} + 7$ が素数ならよい. たぶん無限にある.
$s(a) = 4, a = 2^e qrs$ の解が出てきた. これを統制するのは難しい.

$a = 2^e qr$ の解のみを探索した結果は次の通り.

2.4.5 $m = 8, a = 2^e qr$

表 2.20: $m = 8, a = 2^e qr$

a	素因数分解	$\sigma(a)$
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

2.4.6 $m = 4$ の場合

2.5 P を底とする概完全数

2.5.1 $a = 5^e$ 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
$\sigma(a) = \sigma(P^E) = \frac{aP-1}{\overline{P}}$ によって

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

これが $a = P^E$ に関しての方程式である.

この解を P 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. 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.

$s(a) = 1$ 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.

2.5.2 $s(a) = 2$ 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 $\overline{p} = p - 1, \overline{q} = q - 1$ を使うと

表 2.21: $4\sigma(a) - 5a = -1$

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]

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

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

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

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

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

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

次の基本等式

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

を各場合ごとに調べる.

1. $p = 5, R = 20$. $\rho' = 4\overline{q}$ の場合.
基本等式を 4 で割って

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

$(5X-q)Y-5X=-\overline{q}-1=q$ により

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

よって $5X=5^{f+1}=q$ となり矛盾.

2. $p=3, R=30+2q.\ \rho'=2\overline{q}.$
$R_1=R/2=5+q$ とおくと

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

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

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

$q=11$ 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.

2.6　$a = 7^e$ の場合

$6\sigma(a) - 7a = -1$ が方程式である.

表 2.22: $6\sigma(a) - 7a = -1$

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	$[7^6]$

2.6.1　P を底とする概完全数

$a = 5^e$ 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. 一般にして考えてみよう.

$a = P^E$ は

$$\overline{P}\sigma(a) = Pa - 1 \tag{2.2}$$

を満たす. そこで式 (2.2) を満たす自然数 a を p を底とする概完全数と呼ぶことにする.

ここで $a = pq(p < q)$ の形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

$$(p - \overline{P})(q - \overline{P}) = P(P-1) + 1.$$

$D = P(P-1) + 1$, $p_0 = p - \overline{P}, p_0 = p - \overline{P}$ 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 $D=p_0q_0$ として $p_0+\overline{P}, q_0+\overline{P}$ がともに素数となるとき

$p=p_0+\overline{P}, q=q_0+\overline{P}$ 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 $\overline{P}=2$ $D=P(P-1)+1=13, p_0=1, q_0=13; p=3, q=15.$ ここで 15 は素数では無い.

2.6.2　多くの概完全数

表 2.23:

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

$7^e=a$

$\sigma(7^e)$ が素数になるのは 2801,16148168401

$\sigma(11^e)$ が素数になるのは みつけられない.

表 2.24: $7^e = a$

$7^e = a$	$\sigma(a)$	素因数分解
$7^2 = 49$	57	$[3, 19]$
$7^4 = 2401$	2801	$[2801]$
$7^6 = 117649$	137257	$[29, 4733]$
$7^{10} = 282475249$	329554457	$[1123, 293459]$
$7^{12} = 13841287201$	16148168401	$[16148168401]$
$7^{16} = 33232930569601$	38771752331201	$[14009, 2767631689]$
$7^{18} = 1628413597910449$	1899815864228857	$[419, 4534166740403]$

表 2.25: $11^e = a$

$11^e = a$	$\sigma(a)$	素因数分解
$11^2 = 121$	133	$[7, 19]$
$11^4 = 14641$	16105	$[5, 3221]$
$11^6 = 1771561$	1948717	$[43, 45319]$
$11^{10} = 25937424601$	28531167061	$[15797, 1806113]$
$11^{12} = 3138428376721$	3452271214393	$[1093, 3158528101]$

2.7　$s(a) = 3, a = Xqr$ の場合

素数 P に対して $\overline{P}\sigma(a) - Pa = -1$ を満たす自然数を決定しよう.

$s(a) = 3$ 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

$$\overline{p}\sigma(a) = (pX - 1)\widetilde{qr} = \overline{p}(pa - 1) = \overline{p}(Xqr - 1).$$

これより

$$(pX - 1)\widetilde{qr} = \overline{p}(Xqr - 1).$$

移項して

$$pX(\widetilde{qr} - qr) = \widetilde{qr} - 1.$$

$\widetilde{qr} - qr = q + r + 1$ なのでこれを Δ とおく. $\widetilde{qr} - 1 = qr + \Delta - 1$ 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 $q_1 r_1$ に分解し $q = q_1 + u, r = r_1 + u$ がともに素因数になるとき $a = p^e qr$ が求まる.

2.7.1　$p = 2$ 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 $u \equiv 1 \mod 2$ なので $v \equiv 1 \mod 2$.

q, r は奇素数なので $q_1 = q + u \equiv 0, r_1 = r + u \equiv 0, \mod 2$ $v = q_1 r_1 \equiv 0, \mod 2$ となって矛盾.

$p = 3$ のときの計算でも Xqr の解は出てこないようだが証明はできていない.

2.7.2　$a = Xqr$ のときの計算例

表 2.26: $a = Xqr$ 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

$p = 7, e = 1$ 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.

第3章　亜完全数

3.1　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. $X = p^e$ とおくとき, $\sigma(a) = \frac{(pX-1)(q+1)}{\overline{p}}$ により

$$\begin{aligned}\overline{p}\sigma(a) &= (pX-1)(q+1)\\ &= (pX-1)q + pX - 1\\ &= pa - q + pX - 1\end{aligned}$$

そこで $m = q - pX + 1$ とおけば

$$\overline{p}\sigma(a) = pa - m. \tag{3.1}$$

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.

$W = \overline{p}\sigma(a) - pa$ を $a = p^e q$ の**亜完全度**と言う. 意外にも $W = -m$ が成り立つ.

究極の完全数と違い,Maxp(a) が出てこない.

3.1.1　$p = 3, m = 3$ の例

例を与える.

表 3.1: $m = 3$

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

- $e \equiv 2 \mod 4, q \equiv 9, a \equiv 1 \mod 10$
- $e \equiv 3 \mod 4, q \equiv 3, a \equiv 1 \mod 10$
- $e \equiv 1 \mod 4, q \equiv 1, a \equiv 3 \mod 10$

3.1.2　$p = 3, m = 5$ の例

表 3.2: $m = 5$

e	素因数分解	a
2	$3^2 * 31$	279
5	$3^5 * 733$	178119
8	$3^8 * 19687$	129166407
9	$3^9 * 59053$	1162340199

3.1.3　$p = 3, W = 1$ の例

表 3.3: $2\sigma(a) - 3a = 1$

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.

3.1.4　$p = 3, m = -3$ の例

表 3.4: $m = -3$

e	素因数分解	a
2	$3^2 * 23$	207
4	$3^4 * 239$	19359
20	$3^{20} * 10460353199$	36472996363223648799

3.1.5　$p = 5, m = 3$ の例

例を与える.

表 3.5: $p = 5, m = 3$

e	素因数分解	a
2	$5^2 * 127$	3175
16	$5^{16} * 762939453127$	116415321827239990234375

表 3.6: $m = -1$

e	素因数分解	a
13	$5^{13} * 6103515623$	7450580594482421875
25	$5^{25} * 1490116119384765623$	444089209850062615573406219482421875

表 3.7: $p = 5, m = -3$

e	素因数分解	a
4	$5^4 * 3121$	1950625
6	$5^6 * 78121$	1220640625
14	$5^{14} * 30517578121$	186264514898681640625

3.2　亜完全度 1

$m = -1$, すなわち亜完全度 1 のときは $q = p^{e+1} - 2$ を満たす.
このとき, 素数 p に対して $p^{e+1} - 2$ が素数になる指数 $e + 1$ は確実にありそうである.
亜完全度 1 のときとくに真性亜完全数という.

3.2.1　$p = 7, W = 1$ の例

表 3.8: $p = 7, W = 1$

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	$7^{14} * 4747561509941$	321990575581182328069 1909
27	$7^{27} * 34522673169589$	2268566409077894898417252393023957827
30	$7^{30} * 157775382034845806615042741$	35561530251773635572553173384868349310225254981 25509

3.2.2　$p = 11, W = 1$ の例

表 3.9: $p = 11, W = 1$

e	素因数分解	a
3	$11^3 * 14639$	19484509
5	$11^5 * 1771559$	285311348509

3.2.3　$p = 13, W = 1$ の例

表 3.10: $p = 13, W = 1$

e	素因数分解	a
3	$13^3 * 28559$	62744123
4	$13^4 * 371291$	10604442251
11	$13^{11} * 23298085122479$	41753905413409532046257723

表 3.11: $p = 17, W = 1$

e	素因数分解	a
5	$17^5 * 24137567$	34271893467919

3.2.4　$p = 17, W = 1$ の例

3.3　亜完全度 1 の公式

亜完全度 1 のとき次の公式を満たす.

$$\overline{p}\sigma(a) - pa = 1$$

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.

3.3.1　$p = 3, W = 1$ の例

表 3.12: $p = 3, W = 1$

a	$\sigma(a)$	a の素因数分解
21	32	$[3, 7]$
2133	3200	$[3^3, 79]$
19521	29282	$[3^4, 241]$

3.3.2　$p = 5, W = 1$ の例

表 3.13: $p = 5, W = 1$

a	$\sigma(a)$	a の素因数分解
3	4	$[3]$
115	144	$[5, 23]$
29491	36864	$[7, 11, 383]$

$a = 3$ 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)

3.3.3　$p = 7, W = 1$ の例

表 3.14: $p = 7, W = 1$

a	$\sigma(a)$	a の素因数分解
5	6	$[5]$
329	384	$[7, 47]$

$a = 5$ が微小解. (5,7) は双子素数.

3.3.4　$p = 13, W = 1$ の例

表 3.15: $p = 13, W = 1$

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.

3.4　亜完全度 1 の微小解

$W = 1$ を満たすとき

$$\overline{p}\sigma(a) - pa = 1$$

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,

$$\overline{p}\sigma(a) - pa = \frac{\overline{p}(qa-1)}{\overline{q}} - pa$$

によって,

$$\overline{p}(qa-1) - \overline{q}(pa-1) = \overline{q}.$$

これより

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

$p > q$ なので $f \geq 2$ とすると,

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

$p(1-q^2) \geq -q^3 - q + 2$ により,

$$p \leq q + \frac{2}{q-1}.$$

$q-1 \geq 3$ 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,

$$\overline{p}\sigma(a) - pa = \overline{p}(q+1) - pq = p - q - 1 = 1.$$

$p = q+2$ 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 $\overline{p}\sigma(a) - pa = 1$ 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.

3.5　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:

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

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 $a = P$ を解に持つとする.

$g_m(P+1) = \widetilde{g_m}P + \alpha$ を解けば $\alpha = -(m+1)$.

$$g_m\sigma(a) = \widetilde{g_m}a - m - 1. \tag{3.2}$$

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 $a = P^eL$ とかけ, L は P の倍数ではない, としてよい.

$$\overline{P}\sigma(a) = (P^{e+1}-1)\sigma(L), \widetilde{P}a = \widetilde{P}P^eL$$

によれば

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

$\sigma(L) \geq L$ 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.

3.5.1　$m = -2$ 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.

3.5.2　$s(a) = 2$ の解

$s(a) = 2$ の解を $a = qr$ として探す.
$\widetilde{P} = P + 1$ を用いると $\sigma(a) = \widetilde{qr}$ によって
$\widetilde{P}\widetilde{qr} = (\widetilde{P}+1)qr + 1$, $\widetilde{qr} = qr + \Delta + 1$ となる．そこで

$$\widetilde{P}(\Delta + 1) = qr + 1.$$

$q' = q - \widetilde{P}, r' = r - \widetilde{P}$ とおけば

$$q'r' = \widetilde{P}^2 + \widetilde{P} - 1.$$

これをアルゴリズムとみて解を探す。

素数 P に対して $D = \widetilde{P}^2 + \widetilde{P} - 1$ とおきこれを異なる因数 q', r' の積に分解し $q = q' + \widetilde{P}, r = r' + \widetilde{P}$ がともに素数の場合に $a = qr$ として解がえられる.

表 3.16: $m = -2$, $P = 3, 5$

P=3		
a	σ	素因数分解
3	4	$[3]$
115	144	$[5, 23]$
29491	36864	$[7, 11, 383]$
P=5		
5	6	$[5]$
329	384	$[7, 47]$

表 3.17: $m = -2$, prime ≥ 7

P=7		
7	8	$[7]$
P=11		
11	12	$[11]$
731	792	$[17, 43]$
2171	2352	$[13, 167]$

3.5.3　$m = 1$ の例

$$(P-2)\sigma(a) = (P-1)a - 2$$

$P = 2$ なら $a = 2$.
$P = 3$ なら $a = 2$.

表 3.18:

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

表 3.19:

P=5		
5	6	$[5]$
P=7		
7	8	$[7]$
P=11		
11	12	$[11]$

3.5.4　$m = 2$ の例

表 3.20: $m = 2$,P=3,5

P=3		
a	$\sigma(a)$	素因数分解
3	4	[3]
P=5		
5	6	[5]
33	48	$[3, 11]$
261	390	$[3^2, 29]$
385	576	$[5, 7, 11]$
897	1344	$[3, 13, 23]$
2241	3360	$[3^3, 83]$
26937	40404	$[3^2, 41, 73]$
46593	69888	$[3^2, 31, 167]$

$P = 5$ のとき方程式は $2\sigma(a) = 3a - 3$.
$a = 3^e q$ の形の解があるとすると $q = 3^{e+1} + 2$.

表 3.21: $m = 2$,P=7,11

P=7		
7	8	[7]
3175	3968	$[5^2, 127]$
P=11		
11	12	[11]
299	336	$[13, 23]$

3.6　疑似完全数

$\sigma(a) = 2a + 1$ 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 $\overline{P}\sigma(a) = Pa - 1$ である. これの定数を X だけ変化させて

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

3.6.1　$X = 0$

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

3.6.2　$X = 1$

$X = 1$ のとき $\overline{P}\sigma(a) = Pa$ になりパソコンによる解は

表 3.22: $X - 1$

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.
$\overline{P}\sigma(a) = Pa$ なので $\overline{P}$ は偶数に注意して $a = 2^e L$, (L:奇数), と書ける.
$\overline{P}(2^{e+1} - 1)\sigma(L) = P2^e L$.
$\sigma(L) \geq L$ によって

$$P2^e L \geq \overline{P}(2^{e+1} - 1)L.$$

$$P2^e \geq \overline{P}(2^{e+1} - 1) = (2 \times 2^e - 1)P - 2^{e+1} + 1,$$

によって,

$$P + 2^{e+1} - 1 \geq P2^e. \tag{3.3}$$

$$2^{e+1} - 1 \geq P(2^e - 1) \geq 3(2^e - 1)$$

によれば

$$3 \geq 2^e + 1.$$

よって, $e = 1$. (3.3) によれば,$P + 4 - 1 \geq 2P$. $3 \geq P$ なので $P = 3$. $a = 2$.
この結果は $\overline{P}\sigma(a) = Pa$ の解を疑義完全数と呼ぶと, この場合の疑義完全数は $P = 3$ で $a = 2$, と言い換えられる.

3.6.3　$X = 2$

$X = 2$ のとき $\overline{P}\sigma(a) = Pa + 1$ になりパソコンによる解は
急に解が増えた.

表 3.23:

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	$[13,167]$	

3.6.4　$X=-1$

$X=-1$ 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. $a=2^eL$, (L:奇数), と書ける

$$\overline{P}(2^{e+1}-1)\sigma(L)=P2^eL-2.$$

i. $L>1, L$: 非素数と仮定する. $\sigma(L)\geq L+2$ によって

$$P2^eL-2=\overline{P}(2^{e+1}-1)\sigma(L)\geq\overline{P}(2^{e+1}-1)(L+2).$$

$N=2^{e+1}-1$ とおくと $2^e=\frac{N+1}{2}$.

$$P2^eL-2=PL\frac{N+1}{2}-2\geq\overline{P}N(L+2).$$

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

$$L(P(N+1)-2NP+2N)\geq 4(N\overline{P}+1)>0.$$

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

$$PL\frac{N+1}{2}-2=\overline{P}N(L+1).$$

変形して

$$PL(N+1)-4=2\overline{P}N(L+1).$$

$P\geq 3$ 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.

$$\overline{P}(2^{e+1}-1)\sigma(L)=P2^eL-2$$

に $L=1$ を代入して

$$\overline{P}(2^{e+1}-1)=P2^e-2.$$

$2^{e+1}-1=N$ を用いて,

$$2N\overline{P}=P(N+1)-4.$$

$N=\frac{P-4}{P-2}$ が出て矛盾.

3.6.5　$X=-2$

$X=-2$
$P=3$ のとき $2\sigma(a)=3a-3$ となる.$a=3^eq$ が解とすると $q=3^{e+1}+2$ が素数なら良い.

3.7　$\sigma(a)-2a$ の値

表 3.24: $\overline{P}\sigma(a) = Pa - 3$

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	$[19]$

表 3.25: $\sigma(a) - 2a = -4$

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

表 3.26: $\sigma(a) - 2a = -2$

a	$\sigma(a)$	素因数分解
3	4	$[3]$
10	18	$[2, 5]$
136	270	$[2^3, 17]$

表 3.27: $\sigma(a) - a = -6$

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

表 3.28: $\sigma(a) - a = 2$

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

表 3.29: $\sigma(a) - a = 3$

a	$\sigma(a)$	素因数分解
18	39	$[2, 3^2]$

表 3.30: $\sigma(a) - a = 4$

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

表 3.31: $\sigma(a) - a = 6$

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

第4章　オイラー関数と素数兄弟