# 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 2 月 26 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　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 $p = 1 + 2 + 2^2 + \cdots + 2^n$ 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 Goldbacher への手紙で 7 個の完全数は $2^{p-1}(2^p - 1), p = 2, 3, 5, 7, 13, 17, 19$ 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.

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, $a = p^3 (p : \text{素数})$ 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 $p^rq^s, (r \leq e, s \leq f)$ 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.

$\sigma(a)$ 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)

### 1.1.1　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.

### 1.1.2　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. $\overline{p} = p - 1$ 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.
$a = p^e q^f (p < q)$,$\overline{p} = p - 1, \overline{q} = p - 1$ 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.

$\sigma(a) - 2a; a < 2000; |\sigma(a) - 2a| < 10$ 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, $a=2^eL(L:$ 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.

### 1.3.2　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.

### 1.3.3　$\sigma(a) - a = 1$

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.

### 1.3.4　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が問われている.

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,$\cdots$ 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)

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

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

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

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

したがって $\alpha$ 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 $p \equiv \pm 1 \bmod 8$.

Proof.

条件より,

$$2^q \equiv 1 \mod p.$$

$q$ は素数なので 2 の mod$p$ での位数は $q$. ゆえに

フェルマーの小定理によると $2^{p-1} \equiv 1 \mod p$. 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

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

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 $p \equiv \pm 1 \bmod 8$.

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 $q \equiv \pm 1 \bmod 8$ 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.

$q = 2p + 1$ が素数になる素数 $p$ を Germann 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: $p$ : Germann 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*1035079443105516238671861923746823456 9 |
| (-) | 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 $a=2^eq$ 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 $a=p^eq^f$ 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,$a=XY=2^eq, q=2^{e+1}-1$ 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 |

$A = 2^{30} * 2147483647$
$B = 2305843008139952128$
$C = 2^{60} * 2305843009213693951$
$D = 26584559915698317446546926159538421 76$
$E = 2^{88} * 6189700196426901374495621 11$
$F = 19156194260823610729479337808430363813099732154816921 6$
$G = 2^{106} * 16225927682921336339157801028812 7$
$H = 13164036458569648337239753460458722910223472318386943117783728128$
$I = 2^{126} * 17014118346046923173168730371588410572 7$
$J = 14474011154664524427946373126085988481573677491474835889066354349131199152128.$
$K = 2^{520} * 68647976601306097149819007990813932172694353001 43$
$-- 30540939446345918554318339765605212255964066145455497729 6$
$-- 31139148085803712198799971664381257402829111505715 1.$
$L = 2^{606} * 53113799281676709868958820655246862732959 31$
$-- 17727031923199444138200403559860852242739162 5$
$-- 02265229285668889329486246501015346579337652 7$
$-- 07239409519978766587351943831270835393219031 7$
$-- 28127.$
$M = 2^{1278} * 10407932194664399081925240327364085538615 2$
$-- 62247266704805319112350403608059673360298 0$
$-- 12239441732324184842421613954281007791383$
$-- 56624832346490813990660567732076292412950 9$
$-- 38922034577318334966158355047295942054768 98$
$-- 11211693677147548478866962501384438260291732$
$-- 34888531116082853841658502825560466622483189$
$-- 09188018470682220314052102669843548873295 80$
$-- 28878050869736186900714720710555703168729087$

$a$ 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.

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.

Lukas 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.

- $e\equiv 0 \mod 4$ 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.

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.

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 だけ平行移動した 3,10,136,32896,2147516416 をフェルマーの完全数と呼んでやりたい.

$e \geq 3$ のとき $q \equiv 7, a \equiv 6 \mod 10$.
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 $a \equiv 6 \mod 10$.

### 1.6.2　オイラーの結果

$2^{e+1}+1$ が素数になるとき, $e+1=2^m$ と書ける. 一般に $F_m=2^{2^m}+1$ とおきこれをフェルマー数, これが素数のときフェルマー素数という. $m=0,1,2,3,4$ のとき $F_m$ はフェルマー素数になる. 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.

$2^{2^m}+1\equiv 0 \mod Q$ なので $2^{2^m}\equiv -1 \mod Q$ .
$\mathrm{mod}Q$ 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 $s=2^{m+1}$.
$2^{Q-1}\equiv 1 \mod Q$ によれば $Q-1$ は $2^{m+1}$ の倍数なので $Q=1+2^{m+1}k$.

### 1.6.3　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.
$641-1=640=2^7*5$
$6700417-1=6700416=2^7*3*17449$
$F_6=18446744073709551617=274177*67280421310721$ が素因数分解.
$F_7=340282366920938463463374607431768211457$
$F_7=59649589127497217*5704689200685129054721$ が素因数分解.

```
 ?- 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]
A = 274177,
B = 274176,
C = [2, 2, 2, 2, 2, 2, 2, 2, 3|...],
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,
C = [2, 2, 2, 2, 2, 2, 2, 2, 5|...],
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,
C = [2, 2, 2, 2, 2, 2, 2, 2, 2|...],
D = [2^9, 116503103764643].
```

### 1.6.4　$m = 4$

$q = 2^{e+1} + 3$ 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 |

$A = 2^{27} * 268435459, B = 36028797421617152$
$C = 2^{29} * 1073741827, D = 576460753914036224$
$E = 2^{54} * 36028797018963971, F = 576460753914036224$
$G = 2^{66} * 147573952589676412931$
$H = 649037107316853507609507569598464$
$I = 2^{83} * 193428131138340667952988 19$
$J = 187072209578355573530071687601903897267059558449152$
$K = 2^{98} * 6338253001141147007483516026 91$
$L = 2008672555323737844427452615435960632654465462739716318167 04$
(
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,
$q \equiv 1 + 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.
$a = 2^e q \equiv 3 * 4 = 12 \equiv 2 \bmod 5$, $a \equiv 2 \mod 10$.

### 1.6.5　$m = 6$

$q = 2^{e+1} + 5$ 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 |

$A = 2^{46} * 140737488355333$
$B = 990352031428339404291388 2112$
$C = 2^{52} * 9007199254740997$
$D = 405648192073033633658926394245 12$

### 1.6.6　$m = 8$

$q = 2^{e+1} + 7$ 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 |

### 1.6.7　$m = -2$

$q = 2^{e+1} - 3$ 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 1.13: $q = 2^{e+1} - 3$ 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 |

$A = 2^{19} * 1048573, B = 549754241024$
$C = 2^{21} * 4194301, D = 8796086730752$
$E = 2^{23} * 16777213, F = 140737463189504$
$G = 2^{28} * 536870909, H = 144115187270549504$
$I = 2^{93} * 19807040628566084398385987581$
$J = 1961594292308337738698684194455290145603494810419220971 52$
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,

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

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

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

### 1.6.8　$m = -4$

$q = 2^{e+1} - 5$ 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 |

$A = 811296384146066760662894709309 44$
$B = 272225893536750770752252941871705017 5488$
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,
$q \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.
$a = 2^e q \equiv 3 * 1 \bmod 5$, $a \equiv 8 \mod 10$.

### 1.6.9　$m = -6$

$q = 2^{e+1} - 7$ が素数の場合

表 1.15: $q = 2^{e+1} - 7$ が素数

| $e \bmod 4$ | $e$ | $2^e * q$ | $a$ | $a \bmod 10$ |
|---|---|---|---|---|
| 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 |

$A = 2^{714} * 172364133221937103085272756482[156digits]353486799545737272878084128761$
$B = 148546972106748408784527026025[371digits]871159239450829038055508148224$
$C = 2^{1982} * 875954204768565768610254822675[537digits]949667135757182722184637841401$
$D = 383647884425865224359990619773[1134digits]165116463409179288256647266304$
$E = 2^{2318} * 122619614032433428311834616579[639digits]105574484775025248995836428281$
$E = 5177848727314724608197959528 2[1336digits]568219992473923005215055806464$
(
$a = 4$ 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.
$q = 2^{e+1} - 7 = (2^2)^{k+1} - 7 \equiv 1 - 1 = 0 \bmod 3$ 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.

### 1.6.10　$m = -8$

$q = 2^{e+1} - 9$ 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 | $B$ | $C$ |

$A = 904625697166532776746648320380374279912262923807289020860114158381451706368$

$B = 2^{140} * 27875931498163278926919647840810451882475 43$

$C = 38853377844514581418389238136470378132848011339351048690281077056362802057070698823 68$

## 1.7　$m$ 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

## 1.8　$s(a)=2$ 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 $a=2^eq$ 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 $a=p^eq^f$ 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

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

書き直して

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

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

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

$p=2, q=3, m=8$ とおくとき

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

により, $2XY+17=2X+3Y$.

$(2X-3)Y=2X-17$ により

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

$p=2, q=5, m=8$ とおくとき $2XY=2X+5Y-1-32$. 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

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

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

$$2X\overline{q}=\overline{q}\widetilde{q}-\overline{q}m.$$

よって

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

$Y > q$ のとき $Y \geq q^2$ なので

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

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

$\overline{q}$ で割ると

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

$2X - q > 1$ と組み合わせると

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

よって $m < -q$.
$m$ が負の値になるとどうなるか?

## 1.9　例

### 1.9.1　$\sigma(a) = 2a - 2$

$m = 2$ 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.

### 1.9.2　$\sigma(a) = 2a - 4$

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

### 1.9.3　$\sigma(a) = 2a - 6$

$m = 6$; $\sigma(a) = 2a - 6$ 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 ($[3^2, 5, 7]$) 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.

### 1.9.4　$\sigma(a) = 2a - 8$

$m = 8$; $\sigma(a) = 2a - 8$ 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 ( $[2^3, 23]$ ),2272 ( $[2^5, 71]$),33664 $[2^7, 263]$ に注目.

$s(a) = 4$ の解 70564( $[2^2, 13, 23, 59]$ ) が登場.

$m$ が大きい場合も計算してみた.

### 1.9.5　$\sigma(a) = 2a - 32$

$m = 32$; $\sigma(a) = 2a - 32$ 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 | $[2^8, 479]$ |

$2^e q, 3^e qr$ の解のみなのがうれしい.

### 1.9.6　$\sigma(a) = 2a - 64$

$m = 64$; $\sigma(a) = 2a - 64$ 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.

### 1.9.7　$\sigma(a) = 2a + 2$

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

### 1.9.8　$\sigma(a) = 2a + 4$

$m = -4$; $\sigma(a) = 2a + 4$ 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.

### 1.9.9　$\sigma(a) = 2a + 6$

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

### 1.9.10　$\sigma(a) = 2a + 8$

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.

### 1.9.11　$\sigma(a) = 2a + 32$

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

表 1.27: $\sigma(a) = 2a + 16$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| | 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 | $[2^3, 17, 151]$ |

## 1.10　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 | $[2^7, 269]$ |

## 1.11　$a = 2^e qr$ 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.

$\sigma(a) = \sigma(2^e qr) = (2^{e+1} - 1)\widetilde{qr}, 2a = 2^{e+1}qr$ 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=[2,2,2,2,2] (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; a1=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.

### 1.11.1　$p = 2, m = 4; a = 2^e qr$

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.

### 1.11.2　$p = 2, m = 8; a = 2^e qr$

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 |
| 30481177495530451763 2 | $2^{18} * 524411 * 2217277373$ | 60962354991060903525 6 |

### 1.11.3　$p = 2, m = -8; a = 2^e qr$

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.

### 1.11.4　$p = 2, m = 32; a = 2^e qr$

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ここでは 3 のべきの場合を扱う.
$a = 3^e$ 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.

### 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 $a$ 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 $a=p^eq^f(2<p<q)$ 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

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

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 $p=3, R=6, \rho'=2\overline{q}$.

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

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.

$s(a)=3$ 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, どちらかというと解がある方に私は 1 票入れたい.

## 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 $2\sigma(a)-3a$ を亜完全度という.

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: $2\sigma(a)-3a$(亜完全度) の表

| 亜完全度 | $a$ | 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 $a=2^eL$ とおき $L$ は奇数とする.

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

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 11 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.
$a=3^e*q, (q>3:\text{素数})$ 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.

### 2.5.2　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 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

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

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

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

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 $a = 2^2 q$.
$m - 3 = q + 4$ 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 $a = 2^3 q$.
$2(m-3) = 6(q+4)$ 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 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 $Rq^2 - 4 = q^2(q+3) - 4 = (q^2 + 4q + 4)\overline{q}$ 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 $m - 3 = 33$ , $2(m-3) = 2 * 3 * 11 = (q+4)(2^e - 2)$ 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 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

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

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 $a = 2p, (p : \text{奇素数})$ 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 4** $k$ 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.

$$3^k - 1 = 2L = 4l' \equiv 0 \mod 4.$$

$3^k - 1 \equiv (-1)^k - 1 = -2 \mod 4$, 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 5** $q$ 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 $p \equiv \pm 1 \bmod 12$.

**Proof.**
条件より,

$$3^q \equiv 1 \mod p.$$

$q$ は素数なので 3 の $\bmod p$ での位数は $q$.

フェルマーの小定理によると $3^{p-1} \equiv 1 \mod p$. 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.

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

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 $p \equiv \pm 1 \bmod 12$.

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 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 6** *$p$ を素数とし, $q = 2p + 1$ も素数とする. $N_p = 3^p - 1$ とおくとき, $q$ 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 $3 \equiv n^2 \mod q$ を満たす整数 $n$ がある. フェルマーの小定理を用いて

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

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 $q \equiv \pm 1 \mod 12$)

この逆も成立する.

**補題 7** *$p$ 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 $q_0 \neq 3$.

$$3^p - 1 = N_p \equiv 0 \mod q_0.$$

$p$ 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

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

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.

$p$ : 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

| $p$ | $q = 2p + 1$ | $q + 1$ | $q + 1 \bmod 12$ | $N_p$ 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 | $G$ |

$A = 2 * 167 * 12119 * 1036745531 * 950996059627210897943351$
$B = 2 * 179 * 1611479891519807 * 5042939439565996049162197$
$C = 2 * 227 * 1583 * 2172539 * 526256453012063980796131127321354599535039$
$D = 2 * 263 * 605199588591144003100881306574406851660288427740394885828171$
$E = 2*347*762239*2125048865543*309854287003880455089590180543928107620331492803069077467668 19$
$F = 2*359*56207*100957*19510643*291066066130451*6779963644378513811*161868664744491655705858963594 33$
190 383
$G = 2*383*311713*9593931911*589086859176036543433200507492971040054890918146821485888880034836950031$

## 2.7　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.

### 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

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

$A = 3^{70} * 375473325748986240197335797912877 3$
$B = 939868122326695556888433629151289424673228917359519725450340403327 7$
$C = 3^{102} * 695759652988215296899222525183588718147845154701 3$
$D = 322720996484187844746619306273472246597518644973851120620$
$-- 675638003100735694242699380905814499971 17$
$E = 663084395471818436731691851499754503355465637904747079717256778$
$-- 420962351634164023840051028850346300844173685211922100000030110 2$
$-- 907948169398408014645814376158251490141606616528088759064995410 6$
$-- 127657939605016069105854900863398930585910640912412558322079038082 01.$
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 $q \equiv 3 \mod 10$.
$a = 3^e q \equiv 3^2 q \equiv -q \equiv 2 \mod 5$ により $a = 2 + 5L$.
$a$ は素数なので $L$ は奇数. よって $a \equiv 7 \mod 10$.

2. $e = 4k$ のとき

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

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

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

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

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

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

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

$q$ が素数に矛盾.

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

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

### 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 $a=3^eq$ 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 $a$ の最大素因子を $\mathrm{Maxp}(a)$ 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.

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

次の大きな問題はこの方程式を満たす $\alpha$ 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.

## 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 $a=3^eq$ 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.

### 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 |

$X = 572280636715419056279672990187$
$A = 3^{63} * 1716841910146256242328924544641$
$B = 19650307629564305285868121435693253915830840174600831596977 07$

$q$ 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. $e = 4k + 3$.

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

$q = 1 + 5L$ 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.

### 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.
このい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.

### 2.8.3　オイラーの結果

$3^{e+1} + 1 = 2N_{e+1}$ とおくとき $N_{e+1}$ 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, これが素数のときフェルマー素数という. オイラーはの結果と類似した結果が成り立つ.

**補題 8** $G_m$ の素因数 $Q$ は $1 + 2^{m+1}K$ と書ける.

$3^{2^m} + 1 \equiv 0 \mod Q$ なので $3^{2^m} \equiv -1 \mod Q$ .
mod$Q$ での 3 の位数 $u$ は $2^{m+1}$ の約数である.
$u = 2^s$ とおくと $s \leq 2^{m+1}$ だが $3^{2^m} \equiv -1$ により $s = 2^{m+1}$.
$3^{Q-1} \equiv 1 \mod Q$ によれば $Q - 1$ は $2^{m+1}$ の倍数なので $Q = 1 + 2^{m+1}k$.
$G_m = (3^{2^m} + 1)/2$ $m = 1, 2, 3, 4, 5, 6$
$m = 7$ 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.

### 2.8.4　$p = 3, m = 3$

表 2.22: $p = 3, m = 3$

| $e \mod 4$ | $e$ | 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 | $3^{155} * H$ | $--$ |

$A = 3^{59} * 211955791376081017571472166 03,$
$B = 299501716652405201735529971620260138517926107518220545401$
$C = 3^{65} * 154515771913163061809603209017 67$
$D = 159167491799470872815531783629094754615308050339358788840978581$
$E = 3^{99} * 257688760366005665518230564882810636351053761003$
$F = 442689981459791282231302203392966044715389 08$
$-- 77599523059637250306571246609168838155964920610900 1$
$G = 253764393028207800359877079870848178454371125095831943631813721057443$

$H = 134860802795303781631053435203643426805969445092054023955634715732487236763$

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

### 2.8.5　$p = 3, m = 4$

$A = 3^{74} * 304133393856678854559841996309430657$
$B = 61664747505854495487450130408616108074056769063871156275495392272296233$

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 | $D$ | $--$ |

$C = 3^{190} * 67472943371405469018640786982619424587012511 47$
$-- 01505095703335268351096100445313679302912917 7$
$D = 3^{394} * 14516623680360766607502936538258188521915215969709 3$
$-- 24231043461565691787150531467933452530561614636658056574554$
$-- 49081397363517073931519024006052367992891671955307824800900$
$-- 41796692270130317057$
$p = 3, m = 6$

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 | $3^{32} * 2779530283277767$ | 515052573043877891859781231 9047 |
| 0 | 40 | $A$ | $B$ |
| 0 | 136 | $C$ | $D$ |

$A = 3^{40} * 18236498188585393207$
$B = 22171324412151888504099197533438805 4807$
$C = 3^{136} * 11603310152181426628252267026559130244827211938538269027517774 1687$
$D = 89757870991811041319278823756 0[70 digits]0668863760170538556292133511 27$

### 2.8.6　$p = 3, m = 7$

$A = 3^{69} * 12515777524966208006577859930429 31$
$B = 10442979136963283965427040323903271455380432264919137295492361944 73$
$C = 3^{93} * 35348252450755235324860159791880745727167869 1$
$D = 83299930088154900023013317262493116774089521865276753817089242886050887332772275251707993$

表 2.25: $p = 3, m = 7$

| $e \mod 4$ | $e$ | 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 | $C$ | $D$ |

### 2.8.7　$p = 3, m = 9$

表 2.26: $p = 3, m = 9$

| $e \mod 4$ | $e$ | 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 | $A$ | $B$ |

$A = 3^{65} * 154515771913163061809603209017 73$

$B = 15916749179947087281553178362915656092407331556408263012458563 9$

### 2.8.8　$p = 3, m = -2$

表 2.27: $p = 3, m = -2$

| $e \mod 4$ | $e$ | 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 | $G$ | $H$ |

$A = 3^{30} * 308836698141971$

$B = 635867374128237905436114131 79$
$C = 3^{44} * 1477156353275416849319$
$D = 145466059468128540431277098599066219525 8039$
$E = 3^{48} * 119649664615308764795039$
$F = 954402816170391353771204372770010916506066 6079$
$G = 2^{126} * 196503076295643052858681214356875311094636859871264018484 9491$
$H = 257423059957675431046184790351[61digits]969067117567366322276523388539$
解が急に増えた.

### 2.8.9　$p = 3.m = -3$

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

表 2.28: $m = -3$

| $e \mod 4$ | $e$ | 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 | $C$ | $D$ |

$A = 3^{105} * 187855106306818130162790081799568953899918191769361$
$B = 2352636064369729388202854742 73[41digits]232655623244560699998326360723$
$C = 3^{163}$*8848217271399881112813415883711045232739655292489664511729193699208487603856 37
$D = 52193965921266104919096424366 6[96digits]293165758751776686426411496999$
さて

- $e \equiv 3 \mod 4$ なら $q$ の末尾の数は 7. $a$ の末尾の数は 9
- $e \equiv 1 \mod 4$ 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. $e = 4k + 3$.
$2q = 3^{e+1} - 7 \equiv 1 - 7 = -6 \equiv \quad 4 \mod 5$ 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.

### 2.8.10　$p = 3, m = -5$

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 | $D$ | $E$ |

$A = 199541919709366996456652185771173519239 7$

$B = 3^{49} * 35894899384592629438 5119$

$C = 85896253455335221839408872147959443720605174877$

$D = 3^{89} * 43639817840438562129456987397383636700207 19$

$E = 126962246743110653898816212867692602917374508991326579598608134899308105165053829 27$

### 2.8.11　$p = 3, m = -6$

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 | $A$ | $B$ |

$A = 3^{50} * 554982727552690459387051173677544966279709650584584460722776607952622367$
$B = 20533721858788256398698904107 3[84 digits]83853102093930044990920048538 3$

### 2.8.12　$p = 3, m = -8$

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 | $3^{28} * 34315188682433$ | 7850214495408463530844001 13 |

### 2.8.13　$p = 3, m = -9$

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 | $A$ | $B$ |

$A = 3^{99} * 257688760366005665518230564882810636351053760991$
$B = 44268998145979128223130220339296604471538908773933720 5$
$- - 13444457741566621572625896468840776020997$

## 2.9　$m$ 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 $q = \mathrm{Maxp}(a)$ を使うと方程式

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

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.

## 2.10　方程式を満たす解

$a \leq 200000$ の範囲で解を探索する.

### 2.10.1　$m = 0$ のとき

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

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.

### 2.10.2　$m = 1$ のとき

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

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

### 2.10.3　$m = 3$ 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 |

### 2.10.4　$m = 4$ 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 |

### 2.10.5　$m = 6$ 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 |

### 2.10.6　$m = 7$ 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 |

### 2.10.7　$m = 9$ 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 |

### 2.10.8　$m = -1$ 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 つだけでてきた. 説明がつかないであろう.
1 つだけの解ということが証明できるだろうか.

### 2.10.9　$m = -2$ 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 |

### 2.10.10　$m = -3$ のとき

表 2.42: $[p = 3, m = -3]$

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

### 2.10.11　$m = -5$ 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 |

### 2.10.12　$m = -6$ 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 |

### 2.10.13　$m = -8$ 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 |

### 2.10.14　$m = -9$ 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 |

## 2.11　$a = 3^e qr$ の解

$m = 1$ 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.

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

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

$\Delta = q + r$ 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 |

### 2.11.1　$m = -2$ のとき

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

この結果を受けて $m = -2$ のき $a = 3^e qr$ 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 |
| 436123392252707027348851 59 | $3^13 * 4782971 * 5719200505223$ | 65418508837908913702580352 |

### 2.11.2　$m = 4$ 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 |

### 2.11.3　$m = 8$ 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 |

### 2.11.4　$m=-8$ 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 |

### 2.11.5　$m=-5$ 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 |

### 2.11.6　$m = 2$ 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 $2\sigma(a) = 3 * 3^f - 1, 3a + \mathrm{Maxp}(a) - 4 = 3 * 3^f + 3 - 4.$

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 |

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

### 2.11.7　$m = -1$ 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.

## 2.12　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

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

に関して $2\sigma(a) - 3a - \mathrm{Maxp}(a)$ 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
$\sigma(a) = \sigma(P^E) = \frac{aP-1}{\overline{P}}$ 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.

$P = 5$ 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 $\overline{p} = p - 1, \overline{q} = q - 1$ 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 $a = 77$.

しかしながら $s(a) = 3$ の解がまだある可能性が残る.

### 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, $59 + 1 \equiv 0 \mod 5$. すなわち $q \equiv \pm 1 \mod 5$ なので $(\frac{5}{q}) = 1$ 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 9** $k$ が 奇数のとき $5^k - 1 = 4L$ と書ける. ここで $L$ は奇数

**Proof.**
$L$ は偶数 $2L'$ とする.

$$5^k - 1 = 4L = 8l' \equiv 0 \mod 8.$$

$5^2 = 25 \equiv 1 \mod 8$ によって
$5^k - 1 \equiv 5 - 1 = 4 \mod 8$ により矛盾.

5 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 10** $q$ が素数のとき $\frac{5^q-1}{2}$ の奇数素因数 $p$ については $p - 1 = 2Lq$ と書ける.
さらに $p \equiv \pm 1 \bmod 5$.

**Proof.**
条件より,

$$5^q \equiv 1 \mod p.$$

$q$ は素数なので 5 の mod$p$ での位数は $q$.
フェルマーの小定理によると $5^{p-1} \equiv 1 \mod p$. 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.

$$5^{\frac{p-1}{2}} \equiv 5^{Lq} \equiv 1 \bmod q.$$

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

$$5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right)$$

$5^{\frac{p-1}{2}} \equiv 1$ なので $\left(\frac{5}{p}\right) = 1$. 平方剰余の法則から $p \equiv \pm 1 \bmod 5$.

### 3.1.4　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 5 でも成り立つ.

**補題 11** $p$ を素数とし, $q = 2p+1$ も素数とする. $L_p = 5^p - 1$ とおくとき, $q$ を法として $5$ 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 $5 \equiv n^2 \mod q$ を満たす整数 $n$ がある. フェルマーの小定理を用いて

$$5^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \mod q$$

ゆえに $L_p = 5^p - 1 = qk$ 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 $q \equiv \pm 1 \mod 5$)

この逆も成立する.

**補題 12** $p$ を素数とし, $q = 2p+1$ が $L_p = 5^p - 1$ 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 $q_0 \neq 5$.

$$5^p - 1 = N_p \equiv 0 \mod q_0.$$

$p$ は素数なので $q_0$ を法とした 5 の位数である. フェルマーの小定理を用いて

$$5^{q_0-1} \equiv 1 \mod q_0.$$

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.

$A = 2^2 * 2238236249 * 5079304643216687969512641 * 172827552198815888791$
$p = 29, q = 59 \equiv -1 \mod 5$ なので $q$ を法として 5 は平方剰余.
$q = 59$ は $L_p$ の素因子.

$B = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 * 231669654363683130095909$
$p = 89, q = 179 \equiv +1 \mod 5$ なので $q$ を法として 5 は平方剰余.

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 | $2^2*59*35671*2212599644432962555252508473588471$ |
| 41 | 83 | 82 | 84 | $A$ |
| 53 | 107 | 106 | 108 | $2^2*5960555749*17154094481*27145365052629449$ |
| 89 | 179 | 108 | 180 | $2^2*B$ |

$q=179$ は $L_p$ の素因子.

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.

## 3.2　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 $\mathrm{Maxp}(a)$ と書きこれを使うことにする. すると

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

を満たす.

### 3.2.1　$s(a)=2$ 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 $a = p^e q^f (2 < p < q)$ 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

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

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

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

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

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

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. $Y \geq q^3$ なら

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

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

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

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

$Y \geq q$ により

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

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

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

i. $X \geq 3^2 = 9$ のとき

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

これから矛盾が出る.
ii. $X = 3$ のとき

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

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
例

## 3.3　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 $m$ だけ平行移動しよう.
$q = \frac{P^{e+1}-1}{P} + m$ 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.

## 3.4　例

### 3.4.1　$[p = 5, m = 0]$

表 3.4: $P = 5, m = 0$

| $e$ | 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 | $5^{46} * 17763568394002504646778106689453 1$ | $A$ |
| 126 | $B$ | $C$ |

$A = 252435489670723777731753140890491238224058179184794425964355468 75$
$B = 5^{126}$*14693679385278593849609206715278070972733319459651094018859396328480215743184089660644531
$C = 17272337110188889250772703725 6$[117$digits$]66189579945057630538940429687 5$
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. $a = 5^e * q = 625 * 5^{e-3} * (31 + 50k) = 625K$, $K$ は奇数.

$$a = 625(2s + 1) \equiv 625 \equiv 625 + 50 = 675 \equiv 5 \mod 25.$$

よって $q \equiv 31, a \equiv 25 \mod 50$.
表の観察から

- $e \equiv 2 \mod 4$ なら $q \equiv 31, a \equiv 75 \mod 100$,
- $e \equiv 0 \mod 4$ なら $q \equiv 81, a \equiv 25 \mod 100$.

しかし証明には至らなかった.

### 3.4.2　$[p = 5, m = 1]$

表 3.5: $P = 5, m = 1$

| $e$ | 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 | $5^{27} * 9313225746154785157$ | 693889390390722837820649147033691406 25 |
| 153 | $A$ | $B$ |

$A = 5^{153} * 109476442525376333665916373694[48digits]859491143608465790748596191407$
$B = 9588073174409622174015179599 58[154digits]2945956764742732048034667968 75$

$q \equiv 7, 32 \mod 50$ 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,

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

$a \equiv 25 \mod 50$ は読者への課題.
しかし表の観察から

- $e \equiv 3 \mod 4$ なら $q \equiv 57, a \equiv 25 \mod 100$,
- $e \equiv 1 \mod 4$ なら $q \equiv 7, a \equiv 65 \mod 100$.

証明は ?

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

表 3.6: $P = 5, m = -2$

| $e$ | 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 | $5^{42} * 28421709430404007434844970702 9$ | $C$ |

$A = 27755575615628913477063179016113281 25$
$B = 67762635780344027125460561364889144897460 9375$
$C = 64623485355705287099328804067454257165081799030303955078125$
以下で, $q \equiv 9 \mod 10$ を示す.
$q = \frac{5^{e+1}-1}{4} - 2 = \frac{5^{e+1}-9}{4}$ 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

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

### 3.4.3　$[p = 7, m = 0]$

表 3.7: $P = 7, m = 0$

| $e$ | 素因数分解 | $a$ |
|---|---|---|
| 4 | $7^4 * 2801$ | 6725201 |
| 12 | $7^{12} * 16148168401$ | 223511436608353935601 |
| 130 | $A$ | $B$ |
| 148 | $C$ | $--$ |

$A = 7^{130} * 850534611647968019495395416395428057706663 9$
$-- 2330682673302530819774105141531698707146930307290253537320447270457$
$B = 62006496480956552247752200100 4[160digits]14986751101246418648152531479 3$
$C = 7^{149}*13850221271010340870077438103313550392666332499331763172 92 --27790657325163310341833227775 9$

$e \equiv 0 \bmod 4$ なら $a, q$ は末尾が 1.
$e \equiv 2 \bmod 4$ なら $q \equiv 7, b \equiv 3 \mod 10$.
証明できるか?

$[p = 7, m = 1]$

表 3.8: $P = 7, m = 1$

| $e$ | 素因数分解 | $a$ |
|---|---|---|
| 3 | $7^3 * 401$ | 137543 |
| 5 | $7^5 * 19609$ | 329568463 |
| 11 | $7^{11} * 2306881201$ | 4561457891661258343 |
| 35 | $7^{35} * 44195514097660891196317056360 1$ | $X$ |
| 41 | $A$ | $B$ |

$X = 16742086854484650666653692241643193260697833501385600910 0743$
$A = 7^{41} * 51995580380757061883555053636996009$
$B = 23173203249700874472330986792321198894230671439855207043157069580840 63$

$q$ の末尾は 1,9 ;$a$ の末尾は 3 .
証明できるか?

### 3.4.4　$[p = 11, m = 0]$

表 3.9: $P = 11, m = 0$

| $e$ | 素因数分解 | $a$ |
|---|---|---|
| 16 | $11^{16} * 50544702849929377$ | $A$ |
| 18 | $11^{18} * 6115909044841454629$ | $B$ |
| 72 | $C$ | $D$ |
| 138 | $E$ | $F$ |

$A = 232251544198878080950520379327369 7,$
$B = 340039485861577398986846964992269755 49.$

$C = 11^{72}$*105115319950005359840318840721759019070767114728555170234108965018594521595 3
$D = 496393063768024261910916388812210934417238517638790071036123979591088 – 624762214910080919555329 2$
$E = 11^{138} * 56700023252179573962582828126717134448680538588121757508114966$
$- - 016304621746554457335571059207976993265198915383361219833484346786109 19$
$−02034340949$
$F = 19757074551525286274108978674 5[126 digits]4190905748424729000260728258 56$

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

表 3.10: $P = 11, m = -1$

| $e$ | 素因数分解 | $a$ |
|---|---|---|
| 7 | $11^{16} * 21435889$ | $A$ |
| 136 | $B$ | $C$ |

$A = 984973308935517986686129$
$B = 11^{136} * 339670648186281055704283718218[92 digits]1781625986574972433077371783 61$
$C = 295894866274296553472802883472[133 digits]2145775486530648179290889256 96$

### 3.4.5　$[p = 13, m = 0]$

表 3.11: $P = 13, m = 0$

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

## 3.5　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.
$q = \frac{P^{e+1}-1}{\overline{P}} + m$ であって

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

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

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

これより $q = \mathrm{Maxp}(a)$ を用いて

$$\overline{P}\sigma(a) - Pa = (P-2)\mathrm{Maxp}(a) - m(P-1). \tag{3.1}$$

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 $\mathrm{Maxp}(a)$ が消えた.
$P = 3$ なら

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

### 3.5.1　究極の完全数の基本問題

(3.1) を満たすとき
素数 $q = \frac{P^{e+1}-1}{\overline{P}} + m$ 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.

## 3.6　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.

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

### 3.6.1　$[P = 5, m = 0]$

表 3.12: $[P = 5, m = 0]$

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

微小解は無い.

### 3.6.2　$[P = 7, m = 0]$

表 3.13: $[P = 7, m = 0]$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 9 | $[3^2]$ | 13 |

$a = 3^2$ は微小解.

### 3.6.3　$[P = 43, m = 0]$

表 3.14: $[P = 43, m = 0]$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 49 | $[7^2]$ | 57 |

## 3.7　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.

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. $s(a) = 1$ 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. $q$ 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 $P = 1 + wq$

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

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

$w = 1$ のとき.

$P = 1 + q$ となり $P, q$ はともに素数だから $q = 2, P = 3, a = Y = 2^f$.

$2\sigma(a) = 3a + 2$ なので $2(2Y-1) = 3Y + 2$. これより $a = Y = 4$.

$w \geq 2$ のとき.

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

これより

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

$$q^{f-1}(q+1) \leq 2q^2 - 3q + 3.$$

$f \geq 3$ 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

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

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

### 3.7.1　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.

表 3.15: $P, q$ 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．

### 3.7.2　$s(a) = 2$ 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.$\rho'$ 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.

## 3.8　例

### 3.8.1　$[m = p - 1]$ の解

$\overline{P}\sigma(a) - Pa = (P-2)\mathrm{Maxp}(a) - m(P-1)$ おいて微小解として $s(a) = 1$ の解 $a = P^e$ があるとする.

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

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

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

### 3.8.2　$[p = 5, m = 1]$

表 3.16: $[p = 5, m = 1]$

| $a$ | 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 |

### 3.8.3　$[p = 5, m = 3]$

表 3.17: $[p = 5, m = 3]$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 847 | $[7, 11^2]$ | 1064 |

### 3.8.4　$[p = 5, m = 4]$

表 3.18: $[p = 5, m = 4]$

| $a$ | 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 3.19: $[p = 5, m = -2]$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 539 | $[7^2, 11]$ | 684 |
| 725 | $[5^2, 29]$ | 930 |
| 12905 | $[5, 29, 89]$ | 16200 |

### 3.8.5　$[p = 5, m = -2]$

### 3.8.6　$[p = 7, m = 1]$

表 3.20: $[p = 7, m = 1]$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 2 | [2] | 3 |
| 126293 | $[17^2, 19, 23]$ | $--$ |
| 137543 | $[7^3, 401]$ | $--$ |

### 3.8.7　$[p = 7, m = 2]$

[p=7,m=2]

表 3.21:

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 3 | [3] | 4 |
| 2891 | $[7^2, 59]$ | 3420 |
| 59171 | $[7, 79, 107]$ | 69120 |

### 3.8.8　$[p = 7, m = 3]$

表 3.22:

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 77 | $[7, 11]$ | 96 |
| 13651 | $[11, 17, 73]$ | 15984 |

## 3.9　$p$ 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

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

の解を $p^e qr(p < q, r : \text{素数})$ の形に限って求めよう.

$\overline{p}\sigma(a) = (p^{e+1}-1)\widetilde{qr}, pa = (p^e-1)qr, (p-2)\mathrm{Maxp}(a) - m(p-1) = (p-2)r - m(p-1)$ によって

$\Delta = q + r, \Gamma = p^{e+1} - 1$ を用いて

$$\begin{aligned}\overline{p}\sigma(a) - pa &= \Gamma(qr + \Delta + 1) - (\Gamma + 1)qr \\ &= \Gamma\Delta + \Gamma - qr \qquad\qquad = (p-2)r - m(p-1)\end{aligned}$$

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 $D = \Gamma^2 + \Gamma(3-p) + m\overline{p}$ を用いて

$$q'r = \Gamma\Delta' + \Gamma(3-p) + m\overline{p}$$

から $q_0 = q' - \Gamma, r_0 = r - \Gamma$ より

$$q_0 r_0 = \Gamma^2 + \Gamma(3-p) + m\overline{p} = D.$$

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 $D = \Gamma^2 + \Gamma(3-p) + m\overline{p}$ 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.

## 3.10　例

表 3.23: $p = 3, m = 1; a = 3^e qr$

| $a$ | 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 3.24: $p = 3, m = -2; a = 3^e qr$

| $a$ | 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 3.25: $p = 3, m = 4; a = 3^e qr$

| $a$ | 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 3.26: $p = 3, m = -4; a = 3^e qr$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 50373 | $3^2 * 29 * 193$ | 75660 |
| 283176230906781 | $3^9 * 100511 * 143137$ | 424764346431744 |

表 3.27: $p = 3, m = -5; a = 3^e qr$

| $a$ | 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 |

### 3.10.1　$p = 5, m = -2; a = 5^e qr$

表 3.28: $p = 5, m = -2; a = 5^e qr$

| $a$ | 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 3.29: $p = 5, m = 2; a = 5^e qr$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 244917625 | $5^3 * 853 * 2297$ | 306148752 |

表 3.30: $p = 5, m = -2; a = 5^e qr$

| $a$ | 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 |
| 55460673931324184785156 25 | $5^9 * 9765949 * 290764011289$ | 69325842414157411711530 00 |
| 30068550191905103515625 | $5^9 * 9826877 * 1566631769$ | 37585687739882554368360 |
| 766585572748771484375 | $5^9 * 16727981 * 23463191$ | 958231965935981952864 |

表 3.31: $p = 5, m = -7; a = 5^e qr$

| $a$ | 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 |

### 3.10.2　$p = 7, m = 2; a = 7^e qr$

表 3.32: $p = 7, m = 2; a = 7^e qr$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 59171 | $7 * 79 * 107$ | 69120 |
| $A$ | $7^8 * 43244809 * 603583009$ | $B$ |

$A = 150471866868680839759081$
$B = 175550511346794816038100$

### 3.10.3　$p = 7, m = 3; a = 7^e qr$

表 3.33: $p = 7, m = 3; a = 7^e qr$

| $a$ | 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 |

### 3.10.4　$p = 7, m = 4; a = 7^e qr$

表 3.34: $p = 7, m = 4; a = 7^e qr$

| $a$ | 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 |

### 3.10.5　$p = 7, m = -1; a = 7^e qr$

表 3.35: $p = 7, m = -1; a = 7^e qr$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 64570497397 | $7^3 * 2473 * 76123$ | 75332310400 |
| 19060639997 | $7^3 * 2713 * 20483$ | 22237430400 |

表 3.36: $p = 7, m = -6; a = 7^e qr$

| $a$ | 素因数分解 | $\sigma(a)$ |
|---|---|---|
| 324579681723559549 | $7^6 * 1458697 * 1891333$ | 378676295345728924 |

表 3.37: $p = 7, m = -7; a = 7^e qr$

| $a$ | 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.

そこで一般に $E=2^m$ とかけるとき $L_E$ は奇数であることがを証明する.

実際,$L_E=\frac{Q}{2}=2L'$ とすると $Q=4L'$ なので

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

ゆえに, $P^E\equiv -1$.

一方, $P=2k+1$ とおくとき

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

これで前の式に矛盾した.

$E=2^m$ 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.

### 4.0.6　例

表 4.1:

| $m$ | $2^m$ | $2^{2^m}+1$ | 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 | $A$ | $B$ |

$A = 340282366920938463463374607431768211457$
$B = 59649589127497217 * 5704689200685129054721$
$m = 0, 1, 2, 3, 4$ のときのみ素数 (フェルマー素数)
$P = 3$

表 4.2: $P = 3$

| $m$ | $2^m$ | $2L_E$ | 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 | $A$ | $B$ |

$A = 117901845777385831715208728614125186656782115922758411090969 62$

$B = 2 * 257 * 275201 * 138424618868737 * 3913786281514524929 * 153849834853910661121$

$m = 2$ のときのみ素数.

### 4.0.7　オイラーの結果

$L_E$ は奇数なのでその素因子を $\rho$ とおくと

$$P^E + 1 = 2L_E \equiv 0 \mod \rho.$$

表 4.3: $P = 5$

| $m$ | $2^m$ | $2L_E$ | 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 | $2 * 641 * 75068993 * 241931001601$ |

表 4.4: $P = 7$

| $m$ | $2^m$ | $2L_E$ | 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 | $2 * 7699649 * 134818753 * 531968664833$ |

表 4.5: $P = 11$

| $m$ | $2^m$ | $2L_E$ | 素因数分解 |
|---|---|---|---|
| 1 | 2 | 122 | $2 * 61$ |
| 2 | 4 | 14642 | $2 * 7321$ |
| 3 | 8 | 214358882 | $2 * 17 * 6304673$ |
| 4 | 16 | 45949729863572162 | $2 * 51329 * 447600088289$ |

$E = 2^m$ によって

$$P^E = P^{2^m} \quad \equiv -1 \mod \rho.$$

ゆえに

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

$\rho$ 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 $2^{m+1}$.

$P^E = P^{2^m} \quad \equiv -1 \mod \rho$ により $\rho \neq P$. フェルマーの小定理によって

$P^{\rho-1} \quad \equiv 1 \mod \rho$. $\rho - 1$ は位数 $2^{m+1}$ の倍数なので, $\rho - 1 = 2^{m+1}K$.

この結果は $P = 2$ のときオイラーによる.

### 4.0.8　$P = 5$ のとき

$P = 5$ のとき, $L_E$ が合成数の場合に確認する.

表 4.6: $P = 5$

| $m$ | $2^m$ | $2L_E$ | 素因数分解 |
|---|---|---|---|
| 3 | 8 | 390626 | $2 * 17 * 11489$ |
| 4 | 16 | 152587890626 | $2 * 2593 * 29423041$ |
| 5 | 32 | 23283064365386962890626 | $2 * 641 * 75068993 * 241931001601$ |

```
 ?- A=17,B is A-1,factorize(B,C),exps(C,D).
A = 17,
B = 16,
D = [2^4].

?- A=2593,B is A-1,factorize(B,C),exps(C,D).
A = 2593,
B = 2592,
D = [2^5, 3^4].

?- A=11489,B is A-1,factorize(B,C),exps(C,D).
A = 11489,
B = 11488,
D = [2^5, 359].

 ?- A=17,B is A-1,factorize(B,C),exps(C,D).
A = 17,
B = 16,
D = [2^4].

?- A=29423041,B is A-1,factorize(B,C),exps(C,D).
A = 29423041,
B = 29423040,
D = [2^6, 3, 5, 30649].

 ?- A=641,B is A-1,factorize(B,C),exps(C,D).
A = 641,
B = 640,
D = [2^7, 5].
```

```
?- A=75068993,B is A-1,factorize(B,C),exps(C,D).
A = 75068993,
B = 75068992,
D = [2^6, 1172953].

 ?- A=241931001601,B is A-1,factorize(B,C),exps(C,D).
A = 241931001601,
B = 241931001600,
D = [2^8, 3^2, 5^2, 23, 182617].
```

## 4.1　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.

$P^{e+1} - 1 = 2q$ により,$2q + 2 = P^{e+1} + 3$. さらに $\sigma(a) = \frac{P^{e+1}-1}{\overline{P}}(q+1)$ によって

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

よって,

$$\overline{P}\sigma(a) - aP = q - 2.$$

これが $P$ を底とするフェルマーの完全数の方程式である.

# 第5章　$P$ を底とする概完全数

## 5.1　$P=5$ の場合

$P$ を素数とし $E>0$ について $a=P^E$ とおくと $\sigma(a)=\sigma(P^E)=\frac{aP-1}{\overline{P}}$ 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 $P$ 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 5.1: $4\sigma(a)-5a=-1$

| $a$ | $\sigma(a)$ | 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.

### 5.1.1　$s(a)=2$ 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 $a=p^eq^f(2<p<q)$ 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 $a = 77$.

しかしながら $s(a) = 3$ の解がまだある可能性が残る.

## 5.2　$p = 7$ 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 5.2: $6\sigma(a) - 7a = -1$

| $a$ | $\sigma(a)$ | 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 5.3: $10\sigma(a) - 11a = -1$

| $a$ | $\sigma(a)$ | 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 5.4: $16\sigma(a) - 17a = -1$

| $a$ | $\sigma(a)$ | 素因数分解 |
|---|---|---|
| 17 | 18 | $[17]$ |
| 289 | 307 | $[17^2]$ |
| 1073 | 1140 | $[29, 37]$ |
| 2033 | 2160 | $[19, 107]$ |
| 4913 | 5220 | $[17^3]$ |

## 5.3　$pq$ 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

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

$D = P(P-1)+1$, $p_0 = p - \overline{P}, p_0 = p - \overline{P}$ 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 $D = p_0 q_0$ 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.

### 5.3.1　非べき概完全数の数表

表 5.5: 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 |

## 5.4　$s(a)=3, a=p^eqr$ の場合

素数 $P$ に対して $\overline{P}\sigma(a)-Pa=-1$ 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

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

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 $\Delta$ 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 $q_0r_0$ に分解し $q=q_0+u, r=r_0+u$ がともに素因数になるとき $a=p^eqr$ が求まる.

### 5.4.1　$p=2$ 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 $u\equiv 1 \mod 2$ なので $v\equiv 1 \mod 2$.

$q,r$ は奇素数なので $q_0=q+u\equiv 0, r_0=r+u\equiv 0, \mod 2$ $v=q_0r_0\equiv 0, \mod 2$ 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.

### 5.4.2　$a=p^eqr$ 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 5.6: $a = p^e qr$ 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6章　亜完全数

## 6.1　$p$ 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, $-m = \overline{p}\sigma(a) - pa$ と $m$ を定めるとき $\sigma(a) = \frac{(pX-1)(q+1)}{\overline{p}}$ により

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

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.

### 6.1.1　$p = 3, m = 3$ の例

例を与える.

表 6.1: $p = m = 3$

| $e$ | 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 |

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

- $e \equiv 3 \mod 4$　ならば $, q \equiv 3, a \equiv 1 \mod 10$,
- $e \equiv 1 \mod 4$ ならば $, q \equiv 1, a \equiv 3 \mod 10$.

### 6.1.2　$p = 3, m = 5$ の例

表 6.2: $p = 3, m = 5$

| $e \bmod 4$ | $e$ | 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 |

- $e \equiv 2 \mod 4$ ならば $, q \equiv 1, a \equiv 9 \mod 10$,
- $e \equiv 1 \mod 4$　ならば $, q \equiv 3, a \equiv 9 \mod 10$,
- $e \equiv 0 \mod 4$ ならば $, q \equiv 7, a \equiv 7 \mod 10$.

### 6.1.3　$p = 3, m = -3$ の例

表 6.3: $m = -3$

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

- $e \equiv 2 \mod 4$ ならば $, q \equiv 3, a \equiv 7 \mod 10$,
- $e \equiv 0 \mod 4$ ならば $, q \equiv 9, a \equiv 9 \mod 10$.

証明はまだ

### 6.1.4　$p = 5, m = 3$ の例

例を与える.

表 6.4: $p = 5, m = 3$

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

- $e \equiv 2 \mod 4$ ならば , $q \equiv 127, a \equiv 175 \mod 1000$,
- $e \equiv 0 \mod 4$ ならば , $q \equiv 127, a \equiv 375 \mod 1000$.

証明はまだ

### 6.1.5　$p = 5, m = -3$ の例

表 6.5: $p = 5, m = -3$

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

- $e \equiv 2 \mod 4$ ならば , $q \equiv 121, a \equiv 625 \mod 1000$,
- $e \equiv 0 \mod 4$ ならば , $q \equiv 121, a \equiv 625 \mod 1000$.

証明はまだ

## 6.2　$m = -1$ の例

このとき $q = p^{e+1} - 2$ が素数になる.

### 6.2.1　$p = 3, m = -1$ 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 6.6: $p = 3, m = -1$

| $a$ | $\sigma(a)$ | 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 6.7: $m = -1$

| $e$ | 素因数分解 | $a$ |
|---|---|---|
| 13 | $5^{13} * 6103515623$ | 74505805944824218 75 |
| 25 | $5^{25} * 1490116119384765623$ | 4440892098500626155734062194824218 75 |

### 6.2.2　$p = 5, m = -1$ の例

```
 ?- A is 5^14-2, factorize(A,B).
A = 6103515623,
B = [6103515623].
```

### 6.2.3　$p = 7, m = -1$ の例

表 6.8: $p = 7, W = 1$

| $e$ | 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 | $7^{27} * 34522673169589$ | 22685664090778948984172523930239 57827 |
| 30 | $7^{30} * 157775382034845806615042741$ | 3556153025177363557255317338486834931022525498125509 |

```
 ?- A is 7^7-2, factorize(A,B).
A = 823541,
```

```
B = [823541].
```

### 6.2.4　$p = 11, m = -1$ の例

表 6.9: $p = 11, m = -1$

| $e$ | 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].
```

### 6.2.5　$p = 13, m = -1$ の例

表 6.10: $p = 13, m = -1$

| $e$ | 素因数分解 | $a$ |
|---|---|---|
| 3 | $13^3 * 28559$ | 62744123 |
| 4 | $13^4 * 371291$ | 10604442251 |
| 11 | $13^{11} * 23298085122479$ | 417539054134095320462577 23 |

```
 ?- A is 13^4-2, factorize(A,B).
A = 28559,
B = [28559].
```

### 6.2.6　$p = 17, m = -1$ の例

表 6.11: $p = 17, m = -1$

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

```
 ?- A is 17^6-2, factorize(A,B).
A = 24137567,
B = [24137567].
```

## 6.3　亜完全度

$W = \overline{p}\sigma(a) - pa$ 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 $W = \overline{p}\sigma(a) - pa$ 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,Maxp($a$) が出てこない.
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.

### 6.3.1　$p = 3, W = 1$ の例

表 6.12: $p = 3, W = 1$

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

(

### 6.3.2　$p = 5, W = 1$ 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)

### 6.3.3　$p = 7, W = 1$ の例

$a = 5$ が微小解. (5,7) は双子素数.

表 6.13: $p = 5, W = 1$

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

表 6.14: $p = 7, W = 1$

| $a$ | $\sigma(a)$ | $a$ の素因数分解 |
|---|---|---|
| 5 | 6 | [5] |
| 329 | 384 | [7, 47] |
| 822857 | 960000 | [$7^3$, 2399] |

### 6.3.4　$p = 11, W = 1$ の例

表 6.15: $p = 11, W = 1$

| $a$ | $\sigma(a)$ | $a$ の素因数分解 |
|---|---|---|
| 174109 | 191520 | [13,59,227] |

### 6.3.5　$p = 13, W = 1$ の例

表 6.16: $p = 13, W = 1$

| $a$ | $\sigma(a)$ | $a$ 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.

## 6.4　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.

## 6.5　$a = p^e qr$ 型の亜完全数

$a = p^e qr, p < q, r$:(素数) を底が $p$ の $p^e qr$ 型の**亜完全数**という.
$\overline{p}\sigma(a) - ap = W$ とおくとき,$\Gamma = p^{e+1} - 1, \Delta = q + r$ 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 6.17: $p = 7, W = 1; a = 7^e qr$

| $a$ | $\sigma(a)$ | $a$ の素因数分解 |
|---|---|---|
| 27466313 | 32044032 | $[7^2, 487, 1151]$ |

表 6.18: $p = 19, W = -1; a = 19^e qr$

| $a$ | $\sigma(a)$ | $a$ の素因数分解 |
|---|---|---|
| 73400059 | 77477840 | $19 * 373 * 10357$ |

表 6.19: $p = 3, W = 3; a = 3^e qr$

| $a$ | $\sigma(a)$ | $a$ 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 6.20: $p = 3, W = -3; a = 3^e qr$

| $a$ | $\sigma(a)$ | $a$ 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7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:

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

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 $\alpha$ 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.

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

$$g_m\sigma(a) = \widetilde{g_m}a - m - 1. \tag{7.1}$$

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 $a = P^eL$ 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.

### 7.0.1　$m = -2$ 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.

### 7.0.2　$s(a) = 2$ 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

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

$q_0 = q - \widetilde{P}, r_0 = r - \widetilde{P}$ とおけば

$$q_0 r_0 = \widetilde{P}^2 + \widetilde{P} - 1.$$

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 $q_0, r_0$ の積に分解し $q = q_0 + \widetilde{P}, r = r_0 + \widetilde{P}$ がともに素数の場合に $a = qr$ として解がえられる.

### 7.0.3　$m = -2$

表 7.1: $m = -2$ の例

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

### 7.0.4　$m = 1$ の例

表 7.2: $m = 1$

| 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いる.

### 7.0.5　$m = 2$ の例

表 7.3: $m = 2$ 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 7.4: $m = 2$ 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 |

### 7.0.6　$P = 5, m = 2$ 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. $\Gamma = 3^{e+1} - 1, \Delta = q + r$ おくとき
$2\sigma(a) = \Gamma(qr + \Delta + 1), 3a - 3 = (\Gamma + 1)qr - 3$ を使うと

$$qr = \Gamma\Delta + \Gamma + 3.$$

$q_0 = q - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + \Gamma + 3.$ とおくとき

$$q_0 r_0 = D. \tag{7.2}$$

表 7.5: $m = 2, P = 5; 3^e qr$ 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 |

### 7.0.7　$m = -3$

表 7.6: $m = -3$ 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 7.7: $m = -3$ 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 |

### 7.0.8　$m = 3$

表 7.8: $m=-3$ 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 |

### 7.0.9　$m=qr$ 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
$(v-1)\sigma(a)=(v-1)\widetilde{qr}=(v-1)(qr+\Delta+1), va=vqr$ 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

$$q_0r_0=D. \tag{7.3}$$

表 7.9: $m = -3$

| $a$ | 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 |

### 7.0.10　例

表 7.10: $m = -3$; 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 7.11: $m = 3$ 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 7.12: $m = 3$ 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 7.13: $m = -6$

| $a$ | 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 7.14: $m = -3$; 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8章　疑似完全数

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

### 8.1.1　$X = 0$

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

### 8.1.2　$X = 1$

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

表 8.1: $X - 1$

| $p = 3$ | | |
|---|---|---|
| $a$ | $\sigma(a)$ | 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.

$\overline{P}\sigma(a) = Pa$ 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,

$$P + 2^{e+1} - 1 \geq P2^e. \tag{8.1}$$

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

によれば

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

よって, $e = 1$. (8.1) によれば,$P + 4 - 1 \geq 2P$. $3 \geq P$ なので $p = 3$. $a = 2$.

この結果は $\overline{P}\sigma(a) = Pa$ 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.

### 8.1.3　$X = 2$

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

表 8.2:

| $a$ | $\sigma(a)$ | 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.

### 8.1.4　$X = -1$

$X = -1$ 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

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

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.

### 8.1.5　$X = -2$

$X = -2$

$p = 3$ 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.

表 8.3: $\overline{P}\sigma(a) = Pa - 3$

| $a$ | $\sigma(a)$ | 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9章　オイラー関数と素数兄弟

## 9.1　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.

## 9.2　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).

### 9.2.1　オイラー関数数表

表 9.1:

| $a$ | 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 9.2:

| $a$ | 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 |

### 9.2.2　オイラーの公式

オイラー関数に関した次の公式は定義からすぐ導かれる.

$$a = \sum_{a'|a} \varphi(a') \tag{9.1}$$

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 $\varphi(pq)=pq-p-q+1=(p-1)(q-1)$.

### 9.2.3　乗法性

$a,b$ を互いに素な自然数とするとき, $\varphi(ab)=\varphi(a)\varphi(b)$ 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.

### 9.2.4　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 $p_1,\cdots,p_s$ とする. $A_j=p_jS(a/p_j)$ とおくとき和集合 $A_1\cup\cdots\cup A_s$ 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 $A_1\cup\cdots\cup A_s$ 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 $\varphi(a)=a-|A_1\cup\cdots\cup A_s|$ と書ける.

$p=p_j$ とおくとき $|A_j|=\frac{a}{p}$ 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

$$\begin{aligned}\varphi(a)=a-|A_1\cup A_2|&=a-|A_1|-|A_2|+|A_1\cap A_2|\\&=a-\frac{a}{p}-\frac{a}{q}+\frac{a}{pq}\\&=a(1-\frac{1}{p})(1-\frac{1}{q})\end{aligned}$$

書き直すと

$$\varphi(a)=a(1-\frac{1}{p})(1-\frac{1}{q})$$

一般に $\overline{a} = a - 1$ と書く.
さて , $a = p^e q^f$ と書くとき

$$\varphi(a) = a(1 - \frac{1}{p})(1 - \frac{1}{q}) = p^e(1 - \frac{1}{p})q^f(1 - \frac{1}{q}) = p^{e-1}\overline{p}q^{f-1}\overline{q}$$

となる. ここで $\overline{p} = p - 1, \overline{q} = q - 1$.
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 $p_1, p_2, \cdots, p_s$ のべきの積で書くと次のようになる:

$$\varphi(a) = p_1^{e_1-1}\overline{p_1}p_1^{e_2-1}\overline{p_2}\cdots p_s^{e_s-1}\overline{p_s}.$$

これからオイラー関数の乗法性は直ちに導かれる.

## 9.3　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 $a = 2^e$.

## 9.4　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 $a_j = F_0 F_1 \cdots F_j$ とおくとき

$$\varphi(a_j) = f_0 f_1 \cdots f_j = 2^{1+2+\cdots 2^j} = 2^{2^{j+1}-1}$$

$$2\varphi(a_j) = f_{j+1}.$$

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 $f_{j+1} - 1 = F_0F_1 \cdots F_j = a_j$. 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 $a_0, a_1, \cdots, a_4$ 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 9.3: $a - 2\varphi(a) = -1$ 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.

$a = p_1p_2 \cdots p_s$ とおくとき $\overline{p_1} = p_1 - 1$ を使うと
$\varphi(a) = \overline{p_1p_2} \cdots \overline{p_s}$ により

$$2\overline{p_1p_2} \cdots \overline{p_s} - p_1p_2 \cdots p_s = 1$$

を解けばよい.

### 9.4.1　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 $1+pq=2\overline{p}\ \overline{q}$ は偶数なので, $p,q$ はともに奇数.

$3\le p<q$ とする.

$\overline{p}=p-1$, によって

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

これより

$$2q-1=2\overline{q}+1=p(2\overline{q}-q)\ge 3(q-2)=3q-6.$$

$q\le 5$ をえるが $3\le p<q$ によれば $q\ge 5$. 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.

$$2\overline{p}\ \overline{q}\ \overline{r}=pqr+1.$$

これより $p,q,r$ はともに奇数.

$p=3$ を仮定するとき

$$4\overline{q}\ \overline{r}=3qr+1.$$

$q(4\overline{r}-3r)=4\overline{r}+1$ により

$$q=\frac{4\overline{r}+1}{r-4}=\frac{4r-3}{r-4}=4+\frac{13}{r-4}.$$

$r\ge q+2\ge 7$ 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 $p\ge 5$ を仮定して矛盾を導く.

このとき $q\ge 7,r\ge 11$. $A=\overline{q}\ \overline{r},B=pq$ とおくとき $2\overline{p}A=pB+1$ から

$$5(2A-B)\le p(2A-B)=2A+1.$$

$8A\le 5B+1$ を変形して

$$q(3r-8)\le 8r-7<9r-7.$$

ゆえに $r\ge 11$ なので

$$q<3+\frac{17}{3r-8}<3+\frac{17}{33-8}<4.$$

$q\ge 7$ に矛盾.

$s>5$ なら解が無いことを示したい.

### 9.4.2　不存在性

$2\varphi(a)-a=-1$ を満たす自然数 $a$ はないことを示したい.

$$2\overline{p_1p_2}\cdots\overline{p_s}-p_1p_2\cdots p_s=-1$$

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.

## 9.5　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.

## 9.6　$a = P^e$

素数 $P$ に対して $a = P^e$ とおけば $P\varphi(a) = a\overline{P}$ を満たす.

$$P\varphi(a) = a\overline{P}$$

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

$$P\varphi(a) = P\varphi(P^e L) = P^e \overline{P}\varphi(L) = \overline{P}a = \overline{P}P^e L$$

によれば $\varphi(L) = L$. よって $L = 1; a = P^e$.

### 9.6.1　$a = P^e$ の 3 点セット

3 点セットにして

(1)  $P\varphi(a) - \overline{P}a = -1$ を満たす自然数 $a$ は何か,

(2)  $P\varphi(a) - \overline{P}a = 1$ を満たす自然数 $a$ は 何か,

(3)  $P\varphi(a) - \overline{P}a = 0$ 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.

### 9.6.2　$P = 3$ 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 9.4: $3\varphi(a)-2a=0$

| $a$ | $\varphi(a)$ | 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 9.5: $3\varphi(a)-2a=-1$

| $a$ | $\varphi(a)$ | 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.

### 9.6.3　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 9.6: $3\varphi(a)-2a=-2$

| $a$ | $\varphi(a)$ | 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. $3 * 2\varphi(L) - 2^3 L - 2$ によると $\varphi(L)$ は奇数なので $L = 1$. ゆえに $a = 4$.

$e = 1$ のとき. $3\varphi(L) - 2^2 L - 2$ 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.

## 9.7　$P = 3$ 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 9.7: $3\varphi(a) - 2a = 2$ 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 $a = p(p \neq 5, 7, 37$: 素数) が $3\varphi(a) - 2a = 2$ の解とすると,

$$3\varphi(p) - 2p - 2 = 3\overline{P} - 2 = p - 5 = 0$$

により $p = 5$.

$a = 5q(q$ : 素数) が $3\varphi(a) - 2a = 2$ の解のとき,

$$3\varphi(5q) - 10q - 2 = 12\overline{q} - 10q - 2 = 2q - 14 = 0$$

より $q = 7$.

$a = 5 \times 7q(q$: 素数) が $3\varphi(a) - 2a = 2$ の解とき,

$$0 = 3\varphi(35q) - 70q - 2 = 72\overline{q} - 70q - 2 = 2(q - 37) = 0$$

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,

$$3\varphi(5 \times 7 \times 37q) - 2 \times 5 \times 7 \times 37q - 2 = 36^2\overline{q} - 35 \times 37q - 2 = 2(q - 36^2 - 1) = 0.$$

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, $a = 5\times7\times37\times1297$ が新しい $3\varphi(a)-2a = 2$ の解になることが確定した.

表 9.8: $3\varphi(a) - 2a = 2$ 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,

$$\begin{aligned} 3\varphi(5 \times 7 \times 37 \times 1297Q) - 5 \times 7 \times 37 \times 1297Q - 2 &= 36^2 \times 1296\overline{Q} - 70 \times 37 \times 1297Q - 2 \\ &= 2(Q - 36^2 \times 1296 - 1) = 0. \end{aligned}$$

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 $36^2 * 1296 + 1 = 36^4 + 1 = 6^8 + 1 = 1679617$ の素因数分解は [17, 98801] であった.
もうひとつ先も $36^8 + 1 = 6^{16} + 1 = 2821109907457 = 353 * 1697 * 409377$ となり合成数.

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.

### 9.7.1　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) とおくとき
$g^m = (g^{2^e})^L$ 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 $H_0, H_1, \cdots, H_t$ 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 $B_0, B_1, \cdots, B_t$ がすべて解になる.

### 9.7.2　2 素数の追加

$H_0, H_1, \cdots, H_t$ が全て素数の時これらと異なる 2 素数 $p, q$ を追加し $a = B_tpq$ も $g\varphi(a) = (g-1)a+1$ の解であると仮定する.

$g\varphi(a) = g\varphi(B_tpq) = g\varphi(B_t)\varphi(pq)$,$\Delta = p+q$ と定めると $\varphi(pq) = \overline{pq} = pq - \Delta + 1$.

$$g\varphi(B_t) = h_{t+1}, \overline{g}B_t = h_{t+1} - 1$$

によって, $L = h_{t+1}$ を用いて $g\varphi(a) = \overline{g}a + 1$ を書き直すと

$$g\varphi(a) = L(pq - \Delta + 1), \overline{g}a = \overline{g}B_tpq = (L-1)pq$$

によって

$$L(pq - \Delta + 1) = (L-1)pq + 1.$$

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 $a = B_tpq$ も $g\varphi(a) = (g-1)a+1$ の解になる.

### 9.7.3　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.

### 9.7.4　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 9.9: $a - 2\varphi(a) = -1$ 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.

### 9.7.5　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.

### 9.7.6　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.
$g\varphi(a_1) = g\varphi(apq) = g\varphi(a)\overline{pq}$, $\overline{g}a_1 + 1 = \overline{g}apq + 1$ なので

$$g\varphi(a)\overline{pq} = \overline{g}apq + 1.$$

$g\varphi(a) = \overline{g}a + 1$ によって

$$(\overline{g}a + 1)\overline{pq} = \overline{g}apq + 1.$$

$\overline{pq} = pq - \Delta + 1, (\Delta = p + q)$ を代入すると

$$(\overline{g}a + 1)(pq - \Delta + 1) = \overline{g}apq + 1.$$

これより

$$(\overline{g}a + 1)(pq - \Delta + 1) = \overline{g}(pq - \Delta + 1) + pq - \Delta + 1 = \overline{g}apq + 1$$

$$pq = ((\overline{g}a + 1)\Delta - \overline{g}a.$$

$\Gamma = \overline{g}a + 1$ とおけば

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

### 9.7.7　計算例

表 9.10:

| $g$ | $a$ | $\overline{g}a + 1$ | $\Gamma$ | $pq$ | $\sigma(pq)$ |
|---|---|---|---|---|---|
| 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 |

## 9.8　$P = 5$ 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 9.11: $5\varphi(a) - 4a = 4$

| $a$ | $\varphi(a)$ | 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,

$$5\overline{P}(q-1)=4pq+4$$

$pq-5(p+q-1)=4$ 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.

## 9.9　$P=7$ 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 9.12: $7\varphi(a)-6a=6$ 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.

$7\varphi(a)=7\times 180\overline{q}, 6a=6\times 11\times 19q$ により

$$7\varphi(a)-6a=7\times 180\overline{q}-6\times 11\times 19q=6(7\times 30\overline{q}-11\times 19q)=6(q-211).$$

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.

$$7\varphi(a)-6a=7\times 180\times 210\overline{q}-6\times 11\times 19\times 211q$$

$g=210$ 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.

$7\varphi(a) - 6a = 6$ を満たす $a$ は 210. これを $\alpha$ 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

$$\gamma, \gamma * (\alpha + 1), \gamma * (\alpha + 1)(\alpha^2 + 1), \gamma * (\alpha + 1)(\alpha^2 + 1)(\alpha^4 + 1).$$

## 9.10　$a = pqr$ 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 $7\overline{p}A = 6pB + 6$ となるので $7\overline{p}A = 7pA - 7A$ 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, $7A + 6 = 7\overline{qr} + 6 > 7q_1 r_1 + 6$ 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

$(p - 7)q_1 r_1 > 6 + 42p$. $p > 7$ 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.

## 9.11　$p = 11$

$p = 11$.

$r > q > p = 11$ により $q \geq 13, r \geq 17$.

$\overline{q} = q - 1 = q_1 + 6, \overline{r} = r - 1 = r_1 + 6$ を代入して

$$\begin{aligned} pC = 11(q_1 r_1 - 42) = 7A + 6 &= 7\overline{qr} + 6 \\ &= 7(q_1 + 6)(r_1 + 6) + 6 \\ &= 7q_1 r_1 + 42(q_1 + r_1) + 7 * 36 + 6 \end{aligned}$$

これより

$$4q_1 r_1 = 42(q_1 + r_1) + 7 * 36 + 6 + 11 * 42.$$

2 で割って

$$2q_1 r_1 = 21(q_1 + r_1) + 7 * 18 + 3 + 11 * 21.$$

$7 * 18 + 3 + 11 * 21 = 360$ 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

表 9.13:

| $\alpha$ | $\beta > 0$ | $q_1$ | $r_1$ | $q$ | $r$ |
|---|---|---|---|---|---|
| 3 | 387 | 12 | 204 | 19 | 211 |
| 9 | 129 | 15 | 75 | 22 | 82 |
| 27 | 43 | 24 | 32 | 31 | 39 |

$q$ , $r$ がともに素数になるのは $q = 19, r = 211$.

### 9.11.1　$p \geq 13$.

$$p(q_1r_1 - 42) = 7A + 6 = 7\overline{qr} + 6 \geq 13(q_1r_1 - 42)$$

によって

$$p = \frac{7(q_1 + 6)(r_1 + 6) + 6}{q_1r_1 - 42}.$$

かつ

$$7(q_1 + 6)(r_1 + 6) + 6 \geq 13q_1r_1 - 13 * 42.$$

$$7(6(q_1 + r_1) + 6^2) + 6 \geq 6q_1r_1 - 13 * 42$$

を 6 で割ると

$$7(q_1 + r_1) + 6) + \geq q_1r_1 - 13 * 7 - 1.$$

$$134 \geq (q_1 - 7)(r_1 - 7) - 49.$$

$q_2 = q_1 - 7r_2 = r_1 - 7$ 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 $r \leq 14 + 61 = 75$.

$$p = \frac{7(q_1 + 6)(r_1 + 6) + 6}{q_1r_1 - 42} = p_0. \tag{9.2}$$

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.

表 9.14: $q = 17$

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $q$ | 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 |

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 $s(a) = 3$ であり $s(a) \geq 4$ の場合に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のでひたすらため息をはくだけ.

表 9.15: $q = 19$

| $q$ | 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 9.16: $q = 23$

| $q$ | 29 | 31 |
|---|---|---|
| $q_1$ | 22 | 24 |
| $p_0 =$ | 13.9 | 13.5 |

## 9.12　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 $B_1 = g+1, B_2 = B_1(g^2+1), B_3 = B_2(g^4+1) = (g+1)(g^2+1)(g^4+1)$ とおくとき

$$(g-1)B_1 = g^2-1, (g-1)B_2 = g^4-1, (g-1)B_3 = g^8-1.$$

$B_3 = (g+1)(g^2+1)(g^4+1)$ 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

$$g\varphi(B_1) - (g-1)B_1 = g^2 - (g-1)(g+1) = 1,$$

$$g\varphi(B_2) - (g-1)B_2 = g^4 - (g-1)(g+1)(g^2+1) = 1.$$

### 9.12.1　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.

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.

表 9.17: $g < 1000$ 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 |

### 9.12.2　$g = 180$

$g = 180$ 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.

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.

表 9.18: $90\varphi(a) = 89(a+1)$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 179 | 178 | [179] |
| 32399 | 32040 | [179, 181] |
| 1049759999 | 1038096000 | [179, 181, 32401] |
| 11019960575999999999 | 10897516569600000000 | [179, 181, 32401, 1049760001] |

### 9.12.3　$g = 430$

$g = 430$ 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

$429, 429 * B1, 429 * B2, 429 * B4$ 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 9.19: $43\varphi(a) = 24(a+1)$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 429 | 240 | [3, 11, 13] |
| 184899 | 103200 | [3, 11, 13, 431] |

### 9.12.4　$g = 936$

$g = 936$ 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 9.20: $117\varphi(a) = 80(a+1)$

| $a$ | $\varphi(a)$ | 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.

## 9.13　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.

### 9.13.1　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.

### 9.13.2　$3\varphi(a)=2a+2$ 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 9.21: $3\varphi(a)=2(a+1)$ 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.

$6\overline{p}'\overline{q}=5pq+1$ 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.

$\varphi(L)=\overline{p}'\overline{q}'\overline{r}$ により $A=\overline{q}'\overline{r}, B=qr$ とおけば $6\varphi(L)=5L+1$ は次の形になる.

$$6\overline{p}A=5pB+1.$$

これより

$$p(6A-5B)=6A+1$$

をえて,

$$6A-5B=q(6\overline{r}-5r)-6\overline{r}=q_6r_6-30$$

により

$$p(q_6r_6-30)=6A+1=6\overline{q}'\overline{r}+1.$$

$\overline{q}=q_6+5,\overline{r}=r_6+5,\Delta_6=q_6+r_6,\beta=q_6r_6-30$ を用いて

$$6\overline{q}'\overline{r}+1=6(q_6+5)(r_6+5)+1=6q_6r_6+5\Delta_6+25)+1$$

と

$$p=6+\frac{6(55+\Delta_6)+1}{\beta}>6$$

をえる.

$p=7$ のとき,

$$6(55+\Delta_6)+1=\beta=q_6r_6-30.$$

$x=q_6,y=r_6$ とおけば

$$xy=30+6\times5(11+x+y)+1=30(x+y)+30\times12+1.$$

$x'=x-30,y'=y-30$ とすると

$$x'y'=900+361=1261=13\times97. \tag{9.3}$$

$x'=13,y'=97$ 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 $p\geq11$.

$$6(55+\Delta_6)+1\geq5\beta.$$

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れて, パソコン計算で矛盾が出る.

### 9.13.3　$7\varphi(a)-6a=6$ 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, $e=2,p=2.3$. これよる直ちに矛盾.
$a=p$ 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 $p=11,q=19$.

## 9.14　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. ($a_2$ 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.

$B_2=a_1a_2$ とおくと $a_1,a_2$ が素数なので

$$\varphi(B_2)=\varphi(a_1)\varphi(a_2)=g^3.$$

$\overline{g}=g-1=a_0$ , $\overline{g}B_2=\overline{g}(g+1)(g^2+1)=g^4-1$

$$g\varphi(B_2)=g^4-1+1=\overline{g}B_2+1.$$

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.

$$g\varphi(a)=\overline{g}a+1$$

### 9.14.1　数値例

### 9.14.2　$a_0=g-1$

$a_0=g-1$ も入れて $C_2=a_0B_2$ とおけば $g\varphi(B_2)=\overline{g}(B_2)+1$ によって,

$$g\varphi(C_2)=\varphi(a_0)g\varphi(B_2)=\varphi(g-1)(\overline{g}(B_2)+1)=\varphi(g-1)(C_2+1)$$

表 9.22: 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 9.23: $g=6; 6\varphi(a)-5a=1$

| $a$ | $\varphi(a)$ | 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

$$g\varphi(a) = \varphi(g-1)(a+1) \tag{9.4}$$

の解として

$$C_2, C_1, C_0 = g-1$$

が得られた.

表 9.24: $g = 40; 40\varphi(a) - 39a = 1$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 41 | 40 | $[41]$ |
| 12361 | 12052 | $[47, 263]$ |
| 65641 | 64000 | $[41, 1601]$ |

表 9.25: $g = 10; 10\varphi(a) - 9a = 1$

| $a$ | $\varphi(a)$ | 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.

$$\alpha\varphi(a) = \beta(a+1).$$

## 9.15　$5\varphi(a)=3(a+1)$ 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 9.26: $5\varphi(a)=3(a+1)$ 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, $g-1=39=3\times13$,, $g+1=41, g^2+1=1601$ 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. $a=3L,(L:3$ で割れない$)$. と ii. $a=3^2L,(L:3$ で割れない$)$ の 2 つの場合がある.

### 9.15.1　$a = 3L$ 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, $10\overline{p} = 9p + 3$ によって $p = 13$.

$s(L) = 2$. $L = pq$ とおくとき, $10\overline{pq} = 9pq + 3$ 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, $A = \overline{q}'\overline{r}, B = qr$ とおけば

$$10\overline{q}A = 9pB + 3.$$

$$p(10A - 9B) = 10A + 3$$

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 $p\gamma = 10A + 3$. $\Delta_1 0 = q_{10} + r_{10}$ 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 9.27: $5\varphi(a) = 3(a + 1)$ 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.

### 9.15.2　$a = 3^2L$ の場合

ii. $a = 3^2L, (L : 3$ 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 $L = pqr$.
$A = \overline{q}'\overline{r}, B = qr$ とおけば

$$10\overline{q}A = 9pB + 1.$$

$$p(10A - 9B) = 10A + 1$$

となり $10A - 9B = xy - 90$. ここで $x = q - 10, y = r - 10$.

$$10A + 1 = 10\overline{q}'\overline{r} + 1 = 10(x+9)(y+9) + 1 = 10xy + 90(x+y) + 811.$$

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.

## 9.16　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.

$\overline{p} = p - 1 = g$ とおき $a = p$ が素数のとき $g\varphi(a) = \overline{P}^2 = (p-2)p + 1 = \overline{g}a + 1$ と表される.

素数 $p$ が与えられたとき $g = p - 1$ とおく.

$$g\varphi(a) = \overline{g}a + 1 \tag{9.5}$$

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. この他の解はあれば $p$ 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.

素数ひとりはたしているか, ひとりと思っていても探索すると親戚筋がでてくるかもしれない.

### 9.16.1　数値解の例

$P - 3$ のとき $2\varphi(a) = a + 1$.

表 9.28: $P = 3$

| $a$ | $\varphi(a)$ | 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 9.29: $P = 5$

| $a$ | $\varphi(a)$ | 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 9.30: $P = 7$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 7 | 6 | [7] |
| 259 | 216 | [7, 37] |
| 335923 | 279936 | [7, 37, 1297] |

表 9.31: $P = 11$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 11 | 10 | [11] |
| 391∗ | 352 | [17, 23] |
| 1111 | 1000 | [11, 101] |

表 9.32: $P = 13$

| $a$ | $\varphi(a)$ | 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りは認めることができない.

表 9.33: $P = 17$

| $a$ | $\varphi(a)$ | 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 9.34: $P = 19$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 19 | 18 | [19] |
| 167743∗ | 158424 | [43, 47, 83] |

$g = 18$ で $s(a) = 3$ という扱いづらい例がでている.

表 9.35: $P = 23$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 23 | 22 | [23] |
| 2279∗ | 2184 | [43, 53] |

表 9.36: $P = 29$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 29 | 28 | [29] |
| 4469∗ | 4320 | [41, 109] |

### 9.16.2　$s(a) = 2$ の解

$g\varphi(a) = \overline{p}a + 1$ に $s(a) = 2$ の解 $a = qr, (q < r)$ があるとしよう.
$\varphi(a) = \overline{qr} = qr - \Delta + 1$ 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 9.37:

| $P = 3$ | | | |
|---|---|---|---|
| $g$ | $qr$ | 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 9.38:

| | | | |
|---|---|---|---|
| $P=13$ | | | |
| 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 |

## 9.17　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 $\widetilde{p},p,\overline{p}$ のどれかを考える.

1. $\widetilde{p}\varphi(a)=p^2-1=pa-1$ と変形すると中抜きして

$$\widetilde{p}\varphi(a)=pa-1. \tag{9.6}$$

2. $p\varphi(a)=p^2-p=\overline{p}a$ と変形すると

$$p\varphi(a)=\overline{p}a.$$

この解は $a=p^e$ であることは既知の事実である.

3. $\overline{p}\varphi(a)=p^2-2p+1=(\overline{p}-1)a+1$ と変形できる.
$g=p-1$ とおけば

$$g\varphi(a)=\overline{g}a+1$$

となってこれはすでに扱われたものである.
結局 方程式 (9.6) のみが新しい. これをパソコン君の計算で求めよう.

表 9.39:

| | | |
|---|---|---|
| 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 9.40:

| | | |
|---|---|---|
| $P$ =29 | | |
| 29 | 28 | [29] |
| 4469 | 4320 | [41, 109] |
| $P$ =31 | | |
| 31 | 30 | [31] |
| $P$ =37 | | |
| 37 | 36 | [37] |
| $P$ =41 | | |
| 41 | 40 | [41] |
| $P$ =43 | | |
| 43 | 42 | [43] |
| $P$ =47 | | |
| 47 | 46 | [47] |
| 9167 | 8976 | [89, 103] |
| 26447 | 25896 | [53, 499] |

## 9.18　$P$ が 11 を超えた世界

表 9.41: $11\varphi(a) = 10(a+1)$ 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 | $[19, 41, 61]$ |

理屈がつかない解が並んでいる.

このまま負けたくないので $s(a) = 2$ 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 $\alpha, \beta$ 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 9.42:

| 奇数 | 奇数 | $\alpha$ | $\beta$ | $\alpha_1$ | $\beta_1$ | $p$ | $q$ | $p$ | $q$ |
|---|---|---|---|---|---|---|---|---|---|
| 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 9.43: $13\varphi(a) = 12a + 12$ を満たす $a$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 779 | 720 | $[19, 41]$ |
| 74359 | 68640 | $[23, 53, 61]$ |

本当に理屈がつかない解が並んでいる.

表 9.44: $17\varphi(a) = 16a + 16$ 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.

## 9.19　$6^e$ 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.

$$3\varphi(a) = 3\varphi(6^e) = 3\varphi(3^e)\varphi(2^e) = 6^e = a.$$

$W = 3\varphi(a) - a$ とおいてパソコン君に計算してもらう.

表 9.45: $3\varphi(a)-a=0$

| $a$ | $\varphi(a)$ | 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 $a=2^e3^f, e, f>0$ らしい.

実際, $a=3\varphi(a)$ によって $a$ は 3 の倍数だから $a=3^fL$ とかける. ここで $L$ は 3 で割れない.

$3\varphi(a)=3\varphi(3^fL)=2\times3^f\varphi(L)$, $a=3^fL$ によれば $2\varphi(L)=L$. このとき $L=2^e$ となる. その結果, $a=2^e3^f$.

### 9.19.1　$3\varphi(a)-a=1$ の場合

表 9.46: $3\varphi(a)-a=1$

| $a$ | $\varphi(a)$ | 素因数分解 |
|---|---|---|
| 2 | 1 | [2] |

表 9.47: $3\varphi(a)-a=2$

| $a$ | $\varphi(a)$ | 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 $a=2^eL$ とおけば

$$2=3\varphi(a)-a=3\varphi(2^eL)-2^eL=3\times 2^{e-1}\varphi(L)-2^eL=2^e(\frac{3}{2}\varphi(L)-L).$$

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.

### 9.19.2　$3\varphi(a)-a=4$ の場合

表 9.48: $3\varphi(a)-a=4$

| $a$ | $\varphi(a)$ | 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, $p=2$. $0=3\varphi(a)-a-4=3*2^{e-1}-2^e-4$ . 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てない.
$L = q$ とすれば $3(q - 1) = 2q + 4$. ゆえに $q = 7; a = 14$.

### 9.19.3　$3\varphi(a)-a=8,16$

表 9.49: $3\varphi(a)-a=8$

| $a$ | $\varphi(a)$ | 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 9.50: $3\varphi(a)-a=16$

| $a$ | $\varphi(a)$ | 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 | $[2^4,5,7]$ |

## 9.20　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 $\alpha$ 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.

$g_m\overline{P}=\overline{g_m}P+\alpha$ により $\alpha=P-g_m=m+1$. かくて

$$g_m\varphi(a)=\overline{g_m}a+m+1. \tag{9.7}$$

### 9.20.1　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 9.51: $(P-2)\varphi(a) = (P-3)a + 2$

| $a$ | $\varphi(a)$ | 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 9.52: $(P-3)\varphi(a) = (P-4)a + 3$

| $a$ | $\varphi(a)$ | 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 $a = 9qr, 3 < q, r$ : 素数, となる解を求めよ.
問題 $a = 15qr, 7 < q, r$ : 素数, となる解を求めよ.

# 第10章　$\varphi$ 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 $\varphi$ **完全数**と定義する.

$\varphi$ 完全数は次の方程式を持つ:

$$p\varphi(a) = \overline{p}a - p\overline{\mathrm{Maxp}(a)}.$$

これはとくに微小解をもち $\varphi$ **完全数**ではない.

$p = 2$ の場合は微小解がない. したがって, $\varphi$ 完全数の方程式を満たす解は $\varphi$ 完全数に限ることは正しいかもしれない.

## 10.1　$p$ を底とする $\varphi$ 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.

### 10.1.1　2 を底とするとき

表 10.1: 2 を底とする $\varphi$ 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 $q \equiv 7; a \equiv 6 \mod 10$ が成り立つ.

5 つのフェルマー素数に応じて 5 つの $\varphi$ 完全数ができた. これらはフェルマー $\varphi$ 完全数 と呼ぶ方がよい. 後で本物の $\varphi$ 完全数がでてくる.

### 10.1.2　3 を底とするとき

$$q = 2 * 3^{e-1} + 1, a = 3^e q.$$

表 10.2: 3 を底とする $\varphi$ 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 | $D$ | $3^{61} * 847823165504324070285888664 03$ | −− |
| 66 | $E$ | $3^{66} * 2060210292175507490794709453 5687$ | −− |

$A = 254346949651297838759162883153,$
$B = 202883514811363580575813290088026580303113437822 61873,$
$C = 147902082297484050239767887249537915756946030930720 9503,$
$D = 107820617994865872624790789771848037132145023757699899380 09.$
$E = 6366699671978834912621271345163069111010060585952573405330394 23$

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

**Proof.**
$e \equiv 2 \bmod 4.$
$e = 4k + 2$ となるので, $q = 2(3^{e-1}) + 1 \equiv 1 + 1 = 2 \bmod 5.$ よって $q \equiv 2 + 5 = 7 \bmod 10.$
$a = 3^e q \equiv -4 \times 7 \equiv 3 \bmod 5.$ $a$ は奇数なので $a \equiv 3 \bmod 10.$

$e \equiv 1 \bmod 4.$
$e = 4k + 1$ となるので, $q = 2(3^{e-1}) + 1 \equiv 2 + 1 = 3 \bmod 5.$ よって $q \equiv 3 \bmod 10.$
$a = 3^e q \equiv 3 \times 3 \equiv -1 \bmod 5.$ $a$ は奇数なので $a \equiv 9 \bmod 10.$

$e \equiv 3 \bmod 4$.
$e = 4k + 3$ となるので, $q = 2(3^{e-1}) + 1 \equiv -2 + 1 = 4 \bmod 5$. よって $q \equiv 9 \bmod 10$.
$a = 3^e q \equiv 2 \times -1 \equiv 3 \bmod 5$. $a$ は奇数なので $a \equiv 3 \bmod 10$.

### 10.1.3　5 を底とするとき

$$q = 4 * 5^{e-1} + 1, a = 5^e q.$$

表 10.3: 5 を底とする $\varphi$ 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 | $C$ | $5^{51} * 3552713678800500929355621337890625 01$ | $--$ |

$A = 291038304567356109619140625,$
$B = 232830643653869628906250000$
$C = 157772181044202361082345713056557246378730496871867217123508453369140625$

次は表の観察結果 (証明は不明)
$a \equiv 625 \mod 1000$
$e > 3$ なら $q \equiv 501 \mod 1000$

### 10.1.4　7 を底とするとき

表 10.4: $[p = 7, m = 0]$

| $e \bmod 4$ | $e$ | $a$ | 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 | $C$ | $7^{100} * C$ | $--$ |

$A = 68393371394714107,$
$B = 58622889524776164$
$C = 277240843682122113543826951637161440930617417048967891508619599833573553683165262285 9$

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

### 10.1.5　11 を底とするとき

表 10.5: $[p = 11, m = 0]$

| $e \bmod 4$ | $e$ | $a$ | 素因数分解 | $\varphi(a)$ |
|---|---|---|---|---|
| 3 | 11 | $A$ | $11^{11} * 259374246011$ | $B$ |
| 3 | 25 | $C$ | $11^{25} * D$ | $--$ |

$A = 74002499442866912682721,$
$B = 67274999493256000920100,$
$C = 10671895716335937864242408834743270337427552858851161$
$D = 98497326758076110947118411.$

- $e \equiv 3 \bmod 4$ のとき $q \equiv 1, a \equiv 1 \bmod 10.$
- $e \equiv 1 \bmod 4$ のとき $q \equiv 1, a \equiv 1 \bmod 10.$

### 10.1.6　13 を底とするとき

表 10.6: $[p = 13, m = 0]$

| $e \bmod 4$ | $e$ | $a$ | 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 | $E$ | $13^{54} * F$ | $--$ |

$A = 873519401092878854401927853123365158780648390553335676472198548937712602981233$
$B = 897956346939432936161147153677736549869$
$C = 135421125769648021857682633667[50digits]522259722098657982526674878569$
$D = 353559211582812126402704247589587822364978878140064385 3$
$E = 18668952163097425672866315191 5[61digits]7178216364962713573687620438 93$
$F = 131274060346217062848439268200280831329360102601258925774063 7$

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

$e = 4k + 2$. $q = 12 * 13^{4k+1} + 1 \equiv 12 * 13 + 1 \equiv 7 \mod 5$. $q \equiv 7 \mod 10$.
$a = 13^{4k+2} * q \equiv 3 \mod 5$; $a \equiv 3 \mod 10$.
$e = 4k + 3$. $q = 12 * 13^{4k+2} + 1 \equiv 2 * 9 + 1 \equiv 9 \mod 5$. $q \equiv 9 \mod 10$.
$a = 13^{4k+3} * q \equiv 3 \mod 5$; $a \equiv 3 \mod 10$.
$e = 4k + 1$. $q = 12 * 13^{4k} + 1 \equiv 2 + 1 \equiv 3 \mod 5$. $q \equiv 3 \mod 10$.
$a = 13^{4k+1} * q \equiv 3 * 3 \mod 5$; $a \equiv 9 \mod 10$.

### 10.1.7　17 を底とするとき

表 10.7: $[p = 17, m = 0]$

| $e \bmod 4$ | $e$ | $a$ | 素因数分解 | $\varphi(a)$ |
|---|---|---|---|---|
| 5 | 1897407443809 | $17^5 * 1336337$ | 1785793904896 | |
| 21 | $A$ | $17^{21} * B$ | $--$ | |

$A = 449288972408429763277079389472452476889040272361788 9,$
$B = 650277025063611603584256 17.$

## 10.2　$\varphi$ 完全数の平行移動

$m$ だけ平行移動した $\varphi$ 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 $a=p^eq$ を ($p$ を底とする) $m$ だけ平行移動した $\varphi$ 完全数の定義とする.

### 10.2.1　$[p=2,m=2]$

表 10.8: $p=2,m=2$

| $e \mod 4$ | $e$ | $a$ | 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 | $2^{29}*268435459$ | −− |

### 10.2.2　$[p=2,m=4]$

表 10.9: $p=2,m=4$

| $e \mod 4$ | $e$ | $a$ | 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 | 396140812571335761716555528448 | $2^{48}*140737488355333$ | −− |

### 10.2.3　$[p = 2, m = -2]$

表 10.10: $p = 2, m = -2$

| $e \mod 4$ | $e$ | $a$ | 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 $a = 24, 112, 1984, \cdots$ は $\varphi$ 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

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

$e = 4k + 4, (k \geq 0)$ のとき, $q = 2^{4k+3} - 1 \equiv 8 - 1 = 7 \bmod 5$. $q$ は奇数なので $q \equiv 7 \mod 10$. $a = 2^e q = 2^{4k+4} q \equiv q \equiv 7 \bmod 5$.

$a$ は奇数なので $a \equiv 2 \bmod 10$.

### 10.2.4　$[p = 2, m = -4]$

### 10.2.5　$[p = 3, m = 4]$

$A = 53177628719327154257979$

$B = 31400857981645063751678935 41$

$q = p^{e-1}\overline{p} + 1 + m = 3^{e-1} \times 2 + 5$ : 素数

表 10.11: $[p=2,m=-4]$

| $e \mod 4$ | $e$ | $a$ | 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 10.12: $p=3,m=4$

| $e \mod 4$ | $e$ | $a$ | 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 | $B$ | $3^{29}*45753584909927$ | $-$ |

### 10.2.6　$[p=3,m=6]$

$A=478598658467166079446267$

表 10.13: $p=3, m=6$

| $e \mod 4$ | $e$ | $a$ | 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 | $A$ | $3^{25} * 564859072969$ | − |

### 10.2.7　$[p=3, m=-2]$

表 10.14: $p=3, m=-2$

| $e \mod 4$ | $e$ | $a$ | 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 | $C$ | $3^{36} * 100063090197999413$ | − |

$A = 53177628717632577039093$
$B = 34889842201821748134988 6053$
$C = 150189330299594494577987966195159 73$
$q = p^{e-1}\overline{p} + 1 + m = 3^{e-1} \times 2 - 1$ : 素数

### 10.2.8　$[p = 3, m = -8]$

表 10.15: $[p = 3, m = -8]$

| $a$ | 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.

### 10.2.9　$[p = 5, m = 2]$

表 10.16: $p = 5, m = 2$

| $e \mod 4$ | $e$ | $a$ | 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 | $H$ | $5^{28} * 29802322387695312503$ | $--$ |

$A = 745058059783935546875$
$B = 596046447802734375000$
$C = 18626451492767333984375$
$D = 1490116119409179687500 0$
$E = 4656612873100280761718 75$
$F = 3725290298474121093750 00$
$G = 1818989403545870780944824 21875$
$H = 1110223024625156540535390377044677734375$

### 10.2.10　$[p = 5, m = 6]$

表 10.17: $p = 5, m = 6$

| $e \mod 4$ | $e$ | $a$ | 素因数分解 | $\varphi(a)$ |
|---|---|---|---|---|
| 3 | 3 | 13375 | $5^3 * 107$ | 10600 |
| 3 | 23 | $A$ | $5^{23} * 9536743164062507$ | $--$ |
| 3 | 43 | $B$ | $5^{43} * 90949470177292823791503906250 7$ | $--$ |

$A = 1136868377216161131858825683593 75$

$B = 1033975765691284593589260865095411645597778260707855224609375$

表 10.18: $p = 5, m = -2$

| $e \mod 4$ | $e$ | $a$ | 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 | $5^{40} * 7275957614183425903320$ |

## 10.3　$\varphi$ 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 $a=p^eq$ とすると,

$$\begin{aligned}\varphi(a)=\varphi(p^eq)&=p^{e-1}\overline{pq}\\&=p^e\overline{p}(q-1)/p\\&=\overline{p}a/p-(q-1-m).\end{aligned}$$

かくして $\mathrm{Maxp}(a)=q$ に注意し

$$\varphi(a)=\frac{\overline{p}}{p}a-\overline{\mathrm{Maxp}(a)}+m. \tag{10.1}$$

が得られた. 分母を払った次の式もよく使われる.

$$p\varphi(a)=\overline{p}a-p\overline{\mathrm{Maxp}(a)}+pm. \tag{10.2}$$

が得られた.

これが $m$ だけ平行移動した $\varphi$ 完全数の方程式 $(*)$ である.

$\varphi$ 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 $\varphi$ 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.

$\varphi$ 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.

### 10.3.1　$\varphi$ 完全数の方程式 $(*)$ の解

$m = 0$ の場合に $\varphi$ 完全数の方程式 $(*)$

$$\varphi(a) = \frac{\overline{p}}{p}a - \overline{\mathrm{Maxp}(a)}$$

を満たす例の計算結果を与える.

### 10.3.2　2 を底とするとき

表 10.19: $\varphi(a) = \frac{1}{2}a - \overline{\mathrm{Maxp}(a)}$

| $a$ | 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 |

### 10.3.3　3 を底とするとき

表 10.20:

| $a$ | 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, $\varphi(a) = \frac{\overline{p}}{p}a - \overline{\mathrm{Maxp}(a)}$ 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.

### 10.3.4　5 を底とするとき

表 10.21:

| $a$ | 素因数分解 | $\varphi(a)$ |
|---|---|---|
| 10 | $[2,5]$ | 4 |
| 15 | $[3,5]$ | 8 |
| 12625 | $[5^3,101]$ | 10000 |

### 10.3.5　7 を底とするとき

表 10.22: $[p=7,m=0]$

| $a$ | 素因数分解 | $\varphi(a)$ |
|---|---|---|
| 14 | $[2,7]$ | 6 |
| 21 | $[3,7]$ | 12 |
| 35 | $[5,7]$ | 24 |
| 2107 | $[7^2,43]$ | 1764 |

### 10.3.6　11 を底とするとき

表 10.23: $[p=11,m=0]$

| $a$ | 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.

### 10.3.7　13 を底とするとき

表 10.24: $P = 13, m = 0$

| $a$ | 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.

## 10.4　$p \geq 3, m > 0$ の場合

### 10.4.1　$m = 2$ の場合

表 10.25: $[p = 3, 5, 11, 17; m = 2]$

| $a$ | 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 |

### 10.4.2　$m = 4$ の場合

表 10.26: $[p = 3, 5, 7; , m = 4]$

| $a$ | 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 |

### 10.4.3　$m = 6$ の場合

### 10.4.4　$m = 8$ の場合

表 10.27: $P = 3, 5, 7, ; m = 6$

| $a$ | 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 10.28: $P = 3, 5, 11, ; m = 8$

| $a$ | 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 |

## 10.5　微小解

$m = 0$ のとき $p = Maxp(a)$ とおくと $a = pq(p > q)$ は

$$\varphi(a) = \frac{\overline{p}a}{p} - \overline{\mathrm{Maxp}(a)}$$

の解になることは一般的に証明できる.

実際, $\varphi(a) = \overline{pq}$, $\mathrm{Maxp}(a) = p$ によって

$$\frac{\overline{p}a}{p} - \overline{\mathrm{Maxp}(a)} = \overline{p}q - \overline{p} = \overline{pq} = \varphi(a).$$

よって $\varphi(a) = \frac{\overline{p}a}{p} - \overline{\mathrm{Maxp}(a)}$.

$m = 0$ のときの解 $a = pq(p > q)$ を微小解という. 微小解は $\varphi$ 完全数の方程式 $(*)$ に特有の解である.

### 10.5.1　$p = 2, m = 0$ のときの予想

$p = 2, m = 0$ なら微小解はない. したがって,

$$\varphi(a) = \frac{a}{2} - \overline{\mathrm{Maxp}(a)} \tag{10.3}$$

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.

$\varphi$ 完全数の考察の中からでて来た式 (10.3) 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 (10.3) を 2 倍すると

$$2\varphi(a) = a - 2\overline{\mathrm{Maxp}(a)} \tag{10.4}$$

となるからである.

## 10.6　予想の解決

$a = 2^e L, (L : \text{奇数})$ の形に書くとき,

$$2\varphi(a) = 2^e\varphi(L), a = 2^e L, \overline{\mathrm{Maxp}(a)} = \overline{\mathrm{Maxp}(L)}.$$

整理して

$$\overline{\mathrm{Maxp}(L)} = 2^{e-1}(L - \varphi(L)).$$

次の補題に注目する.

**補題 13** $a > 1$ が素数でないとき

$$a - \varphi(a) \geq \mathit{Maxp}(a)$$

**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 $\mathrm{Maxp}(a) = p$ とすれば $a = \alpha p^e (, e > 0, \mathrm{Maxp}(\alpha)) < p$ と書けて

$$\begin{aligned} a - \varphi(a) &= \alpha p^e - \varphi(\alpha) p^{e-1} \overline{p} \\ &= p^{e-1}(\alpha p - \varphi(\alpha)\overline{p}) \\ &= p^{e-1}(\alpha p - \varphi(\alpha)p + \varphi(\alpha)) \\ &= p^{e-1}(\alpha - \varphi(\alpha)p + \varphi(\alpha)) \\ &> p^{e-1}(p + \varphi(\alpha)) \\ &> p^e \\ &\geq \mathrm{Maxp}(a). \end{aligned}$$

定理の証明の続き.
$L$ が素数でないとすると,

$$\mathrm{Maxp}(L) \leq 2^{e-1}\mathrm{Maxp}(L) \leq 2^{e-1}(L - \varphi(L)) = \overline{\mathrm{Maxp}(L)}.$$

これは矛盾.

$L$ が素数ならば

$$L - 1 = \overline{\mathrm{Maxp}(L)} = 2^{e-1}(L - \varphi(L)) = 2^{e-1}$$

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 $\varphi$ 完全数.

## 10.7　定理と証明

一般の場合は次の定理にまとめれる.

**定理 3** $m = 0$ のとき.

$$p\varphi(a) = \overline{p}a - p\overline{Maxp(a)}$$

を満たす解は微小解または $\varphi$ 完全数である.

**Proof.**
$a$ は式より $p$ の倍数なので $a = p^e L(p, L :$ は互いに素$)$ と書ける.
$p\varphi(a) = p^e \overline{p}\varphi(L), \overline{p}a = p^e L\overline{p}$ により,

$$\overline{\mathrm{Maxp}(a)} = p^{e-1}\overline{p}(L - \varphi(L)).$$

$L$ が素数でないなら $L - \varphi(L) \geq \mathrm{Maxp}(L)$ となり矛盾.

$L$ は素数であり, $L-\varphi(L)=1$ によって $\overline{\mathrm{Maxp}(a)}=p^{e-1}\overline{p}$. さらに $\mathrm{Maxp}(L)=L$ が成り立つ
ここで $\mathrm{Maxp}(a)=p$ または $\mathrm{Maxp}(a)=\mathrm{Maxp}(L)$ が成り立つ.

1) $\mathrm{Maxp}(a)=p$ とすると,$p>L, p-1=p^{e-1}\overline{p}$ となり $e=1$. このとき $a=pL$ は微小解.
2) $\mathrm{Maxp}(a)=\mathrm{Maxp}(L)=L$ が成り立つとき $\overline{\mathrm{Maxp}(a)}=p^{e-1}\overline{p}(L-\varphi(L))=p^{e-1}\overline{p}$ によって $\overline{\mathrm{Maxp}(a)}=\overline{L}$ によって $L=p^{e-1}\overline{p}+1$. $L$ は素数なので $a=p^eL$ は $\varphi$ 完全数.

## 10.8　諸例

### 10.8.1　$p=2, m=-4$ のとき

表 10.29: $p=2, m=-4$ 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.

## 10.9　$p=2, m=-q;$ ( 奇素数) のとき

$p=2$ のとき本来の $m$ だけ平行移動した $\varphi$ 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 $a=2^eq$ を (2 を底とする) $m$ だけ平行移動した $\varphi$ 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 $\varphi$ 完全数の満たす方程式は

$$p\varphi(a)=\overline{p}a-p\overline{\mathrm{Maxp}(a)}+pm. \tag{10.5}$$

であり,$p=2$ とすれば

$$2\varphi(a)=a-2\overline{\mathrm{Maxp}(a)}+2m.$$

$m<0$ 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.

### 10.9.1　$p=2, m=-3$ のとき

表 10.30: $p=2, m=-3$ 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.

### 10.9.2　$p=2, m=-5$ のとき

表 10.31: $p=2, m=-5$ 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.

### 10.9.3　$p = 2, m = -7$ のとき

表 10.32: $p = 2, m = -7$ 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.

### 10.9.4　$p = 2, m = -11$ のとき

表 10.33: $p = 2, m = -11$ 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.

### 10.9.5　$p = 2, m = -13$ のとき

表 10.34: $p = 2, m = -13$ 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 10.35: $p = 2, m = -17$ 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 |

### 10.9.6　$p = 2, m = -19$ のとき

解は $38p$ だけらしい.

表 10.36: $p=2, m=-19$ 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 |

### 10.9.7　$p=2, m=-23$ のとき

表 10.37: $p=2, m=-23$ 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.

### 10.9.8　$p=2, m=-29$ のとき

表 10.38: $p=2, m=-29$ 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 $198=2*3^2*11$ が出た.

### 10.9.9　$p=2, m=-31$ のとき

通常解 $2\times 31p$ の他に非通常解 $150=2*3*5^2$ が出た.

表 10.39: $p=2, m=-31$ 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 |

### 10.9.10　$p=2, m=-37$ のとき

表 10.40: $p=2, m=-37$ 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.

### 10.9.11　$p=2, m=-41$ のとき

表 10.41: $p=2, m=-41$ 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.

### 10.9.12　$p=2, m=-43$ 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.

### 10.9.13　copm の表

表 10.42: $p=2, m=-43$ 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 10.43: 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 |

## 10.10　$p=2, m=-s$ : 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.

$$2\varphi(a)-a+2\mathrm{Maxp}(a)-1=2\overline{sp}-2sp+2p-2$$
$$=2(2-p-s)-2p+2=-2s$$

よって

$$2\varphi(a)=a-2\mathrm{Maxp}(a)-1-2s.$$

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 $a=2^eL, L$:奇数, とおけば $2^e\varphi(L)=2^eLa-2\overline{\mathrm{Maxp}(a)}-2s$ により

表 10.44: 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 |

$$2^{e-1}co\varphi(L) = \mathrm{Maxp}(L) - 1 + s.$$

$e > 1$ とすると, 左辺は偶数. $L > 2$ とすると $\mathrm{Maxp}(L) - 1 + s$ は奇数. よって, $e = 1$.

$$co\varphi(L) = \mathrm{Maxp}(L) - 1 + s.$$

$L$ : 素数なら $co\varphi(L) = 1 = \mathrm{Maxp}(L) - 1 + s$. これは矛盾.
$L$ : 素数でないなら $co\varphi(L)\mathrm{Maxp}(L) > 0$.
かくて

$$co\varphi(L) - \mathrm{Maxp}(L) = -1 + s.$$

$s = 3$ 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 10.45: 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 |

## 10.11　$p = 3, m \neq 0$ のとき

$3\varphi(a) = 2a - 3\overline{\mathrm{Maxp}(a)} + 6.$

### 10.11.1　$p = 3, m = -3$ のとき

表 10.46: $m = -3; 3\varphi(a) = 2a - 3\overline{\mathrm{Maxp}(a)} + 6$

| $a$ | 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 |

$3\varphi(a) = 2a - 3\overline{\mathrm{Maxp}(a)} - 6.$

### 10.11.2　$p = 3, m = -2$ のとき

表 10.47: $p=3, m=-2$

| $a$ | 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 |

## 10.12　$p=5, m\neq 0$ のとき

### 10.12.1　$p=5, m=-2$ のとき

表 10.48: $P=5; m=-2$

| $a$ | 素因数分解 | $\varphi(a)$ |
|---|---|---|
| 475 | $[5^2, 19]$ | 360 |

### 10.12.2　$p=5, m=2$ のとき

表 10.49: $[P=5, m=2]$

| $a$ | 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 $q\equiv 3 \mod 10$ 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.

## 10.13　$co\varphi(a)-\mathbf{Maxp}(a)$ の値変化

copm= $co\varphi(a)-\mathrm{Maxp}(a)$, cosm= $co\sigma(a)-\mathrm{Maxp}(a)$ とおく.
$co\varphi(a)-\mathrm{Maxp}(a), co\sigma(a)-\mathrm{Maxp}(a)$ 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 10.50: $p=5, m=2$

| $e$ | $a$ | 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 10.51: copm,cosm の表

| $a$ | factor | $s(a)$ | $\varphi(a)$ | $\sigma(a)$ | Maxp$(a)$ | co$\varphi(a)$ | 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** *copm*$=co\varphi(a)-Maxp(a)$, *cosm*$=co\sigma(a)-Maxp(a)$ とおく.

$s(a)=1$ のとき. $a=p^e, e\geq 2$ なら *copm*$=p(p^{e-2}-1)$.
とくに $a=p^2$ なら *copm*$=0$.

$s(a)\geq 2$ のとき
*copm*$\geq 1$. *copm*$=1$ なら $a=2p, p>2$.
*copm*$=2$ なら $a=3p, p>3$.
*copm*$>2$ なら *copm*$\geq 4$. *copm*$=4$ なら $a=5p, p>5$.
*copm*$>4$ なら *copm*$\geq 5$. *copm*$=5$ なら $a=12$.
*copm*$>5$ なら *copm*$\geq 6$. *copm*$=6$ なら $a=7p, p>11$.

## 10.14　$co\sigma(a) - \mathbf{Maxp}(a)$ の値変化

$s(a) = 1$ のとき $s = p^e$ とおけば

$$co\sigma(a) - \mathrm{Maxp}(a) = \frac{p^{e+1} - 1}{\overline{p}} - p^e - p = \frac{p^2(p^{e-2} - 1) + \overline{p}}{\overline{p}} \geq 1.$$

$e = 2$ なら $co\sigma(a) - \mathrm{Maxp}(a) = 1$.
$e \geq 3$ なら $co\sigma(a) - \mathrm{Maxp}(a) \geq p^2 + 1$.

$s(a) \geq 2$ のとき $co\sigma(a) - \mathrm{Maxp}(a) \geq 3$ を示そう.
$p = \mathrm{Maxp}(a), a = \alpha p^e, \mathrm{Maxp}(\alpha) < p$ とする.

$e = 1$ のとき

$$co\sigma(a) = \sigma(\alpha p) - \alpha p = \sigma(\alpha)(p + 1) - \alpha p = (co\sigma(\alpha))p + \sigma(\alpha).$$

$\alpha$ が素数なら , $co\sigma(a) = p + \sigma(\alpha)$. よって
$\mathrm{cosm} = co\sigma(a) - \mathrm{Maxp}(a) = \sigma(\alpha)$.
とくに $a = \alpha p (p \neq \alpha)$;( 両者は素数なら) のとき $\mathrm{cosm} = \sigma(\alpha p)$.
$\mathrm{cosm} = \sigma(2p) = 3$ .$p > 2$ は素数.
$\mathrm{cosm} = \sigma(3p) = 4$ .$p > 3$ は素数.
$\mathrm{cosm} = \sigma(5p) = 6$ .$p > 5$ は素数.

$\alpha$ が素数でないなら , $co\sigma(\alpha) \geq 2$ によって $co\sigma(a) = 2p + \sigma(\alpha)$.

$e \quad \geq 2$ のとき

$$co\sigma(a) = \sigma(\alpha p^e) - \alpha p^e = \frac{\sigma(\alpha)(p^{e+1} - 1) - p^e \alpha \overline{p}}{\overline{p}}$$

## 10.15　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

$$p\varphi(a) - \overline{p}a = -p\overline{\mathrm{Maxp}(a)} + p(p - 1). \tag{10.6}$$

これは容易に確かめられる. 実際,
$p\varphi(a) - \overline{p}a = p^e\varphi(a) - \overline{p}p^e = 0$ および $-p\overline{\mathrm{Maxp}(a)} + p(p - 1) = -p(p - 1) + p(p - 1) = 0$ が成り立つ.
(式 10.6) の解の $s(a) = 1$ の場合は $a = p^e$.

表 10.52: $[P=5, m=4]$

| $a$ | 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 |

### 10.15.1　$s(a) > 1$ の場合

(式 10.6) の解は $p$ の倍数なので $a = p^e L(, L > 1, p, L$ は互いに素) と書ける.

$$p\varphi(a) - \overline{p}a = p^e\overline{p}\varphi(L) - \overline{p}p^e L = p^e\overline{p}(\varphi(L) - L) < 0.$$

よって, $-p\overline{\mathrm{Maxp}(a)} + p(p-1) = -p(\overline{\mathrm{Maxp}(a)} - \overline{p}) < 0.$

$\overline{\mathrm{Maxp}(a)} > \overline{p}$ なので $\mathrm{Maxp}(a) = \mathrm{Maxp}(L) > p$..

$co\varphi(L) = L - \varphi(L)$ を使うと,

$$p^{e-1}\overline{p}(co\varphi(L)) = \overline{\mathrm{Maxp}(L)} - \overline{p}.$$

$L$ が素数でないなら補題から $co\varphi(L) \geq \mathrm{Maxp}(L)$.

よって

$$\overline{\mathrm{Maxp}(L)} - \overline{p} = p^{e-1}\overline{p}(co\varphi(L)) \geq p^{e-1}\overline{p}\mathrm{Maxp}(L).$$

これは矛盾.

$L$ が素数なら $co\varphi(L) = 1$.

$$p^{e-1}\overline{p} = \overline{\mathrm{Maxp}(L)} - \overline{p} = \overline{L} - \overline{p} = L - p.$$

$L = p + p^{e-1}\overline{p}$, $L$ は素数なので $e = 1$. $L = p + \overline{p} = 2p - 1$.

$a = p^e L = pL$ が特異解なのである.

たとえば $p = 7, L = 13$ のとき $a = 7 * 13$.

### 10.15.2　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 10.53: $P=7, m=6$

| $a$ | 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 $co\varphi(L) \geq \mathrm{Maxp}(L)$.

$$p^{e-1}\overline{p}\mathrm{Maxp}(L) \leq p^{e-1}\overline{p}(co\varphi(L)) = \overline{\mathrm{Maxp}(L)} - \overline{p}.$$

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.

### 10.15.3　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

$$p\varphi(a) - \overline{p}a = -p\overline{Maxp(a)} + p(p-1)$$

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.