

書泉グランデでの講義 第3期 資料1
高校生も十分わかる新しい数論研究 , 2015 年6月12日

飯高 茂

平成27年6月3日

目次

第3期をはじめるにあたって

0.1 開講の辞 3

4,5月を休んで6,7月に第3期をすることになった。

2ヶ月の休みはありがたかった。弱完全数、フェルマーの弱完全数の理論がこのような形をとってきたのは大きな収穫であり、この講座がなければこのような発展は無かったであろう。参加者および書店に深甚なる謝意を表したい。

2015年6月12日

0.2 はじめに

自然数 a の約数の和を $\sigma(a)$ で表す。これを a の関数と見てユークリッド関数という。

$\sigma(a) - 2a = 0$ を満たす自然数 a を完全数 (perfect number) という。

完全数の概念は2300年昔に遡り、多くの研究が行われたが、完全数が無限にあるかどうか未解決で、これは最古のそして未だに解決がされていない数学界最大の難問の1つである。

完全数の概念を究極の形に一般化して研究することがこの講座の目的である。ここで語られ説明される主要な結果はすべて新しい研究の成果である。講座の参加者も一緒になってこの研究に加わってほしい。

次の2つの結果がこの研究の出発点であり、実に古めかしい。

$\sigma(2^e)$ が素数のとき $2^e \sigma(2^e)$ は完全数になる。(ユークリッド)

完全数が偶数なら上の形になる。(オイラー)

0.2.1 研究目標

目標 究極の完全数の探究

P を素数とし $\sigma(P^e)$ が素数 q のとき $a = P^e q$ を底が P の (究極の) 完全数。

究極の完全数を整数 m だけ平行移動する。 $q = \frac{P^{e+1}-1}{P} + m$ は素数とし $a = P^e q$ を m だけ平行移動した底が P の完全数と呼ぶ。ただし $q > P$. ($\bar{P} = P - 1$)

これより a の最大素因子 $\text{Maxp}(a)$ を用いると $q = \text{Maxp}(a)$ になるので

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

m 平行移動した究極の完全数の基本方程式という. 基本方程式を解くことこそ究極の課題である.

$e + 1$ が素数のとき $Q = \sigma(P^e)$ として $a = P^e Q$ を弱完全数という.

$e + 1$ が奇数のとき $Q = \sigma(P^e)$ として $a = P^e Q$ を弱弱完全数という.

P を奇素数とし $E > 0$ について $R = P^E + 1$ とおく. これは偶数なので $L_E = \frac{R}{2}$ とする. L_E を素数とすると, E は 2 のべきになるので $E = 2^m, m > 0$ とかける.

一般に $E = 2^m$ とかけるとき L_E は奇数である.

$E = 2^m$ 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数と理解する.

$a_m = P^{2^m-1} L_m$ を P が底のフェルマの弱完全数と定義する.

L_m が素数の場合には, a_m を P が底のフェルマの完全数と呼ぶ.

底が P の弱完全数と底が P がないフェルマの弱完全数には意外な関連性と類似性がある.

とくに一般の Wieferich 素数, Sophie Germain の素数の性質を述べる.

このほかに下記の話題があるが, 今期は時間がなく説明はできない.

- 完全数の平行移動
- 底が 3 以上の素数について完全数を定義しまたその平行移動も研究する.
- 概完全数の一般化
- 亜完全数
- 疑似完全数
- φ 完全数を導入しその平行移動, 底の一般化を研究する.

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

第1章 P を底とする弱完全数

一般に P を奇素数とし, $p = e + 1$ が素数のとき, $N_p = \frac{P^p - 1}{P}$ に関して $a = p^e N_p$ を P を底とする弱完全数という.

しかしながら $P = 2$ のときは $p = e + 1$ が素数の場合, $q = 2^p - 1$ とおく. $a = 2^e q$ を P を底とする弱完全数という.

1.1 素数べきの約数の和

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

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

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

数値例

1.1.1 $P = 2$ 表 1.1: $P = 2$, 弱完全数

p	$(2p + 1) =$	$2^p - 1 =$ 分解	a
2	(5)=5	(3)=3	6
3	(7)=7	(7)=7	28
5	(11)=11	(31)=31	496
7	(15)=3*5	(127)=127	8128
11	(23)=23	(2047)=23*89	2096128
13	(27) = 3 ³	(8191)=8191	33550336
17	(35)=5*7	(131071)=131071	8589869056
19	(39)=3*13	(524287)=524287	137438691328
23	(47)=47	(8388607)=47*178481	35184367894528
29	(59)=59	(536870911)=233*1103*2089	144115187807420416
31	(63)=3 ² * 7	(2147483647)=2147483647	2305843008139952128
37	(75)=3 * 5 ²	(137438953471)=223*616318177	9444732965670570950656
41	(83)=83	(2199023255551)=13367*164511353	2417851639228158837784576
43	(87)=3*29	(8796093022207)=431*9719*2099863	38685626227663735544086528
47	(95)=5*19	(140737488355327)=2351*4513*13264529	9903520314282971830448816128
53	(107)=107	(9007199254740991)=6361*69431*20394401	40564819207303336344294875201536

表 1.2: $P = 2$

p	$(2p+1)=$	$2^p - 1 =$ 分解	a
59	(119)=7*17	(576460752303423487)=179951*3203431780337	A
61	(123)=3*41	(2305843009213693951)=2305843009213693951	B
67	(135) = $3^3 * 5$	(147573952589676412927)=193707721*761838257287	C
71	(143)=11*13	D	E
73	(147)=3 * 7^2	F	G
79	(159)=3*53	I	J
83	(167)=167	K	L
89	(179)=179	M	N
97	(195)=3*5*13	O	P
101	(203)=7*29	Q	R
103	(207)= $3^2 * 23$	S	T
107	(215)=5*43	U	V
109	(219)=3*73	W	X
113	(227)=227	Y	Z
127	(255)=3*5*17	$A1$	$B1$
131	(263)=263	$C1$	$D1$

$$A = 166153499473114483824745506383331328$$

$$B = 2658455991569831744654692615953842176$$

$$C = 10889035741470030830754200461521744560128$$

$$D = (2361183241434822606847) = 228479 * 48544121 * 212885833$$

$$E = 2787593149816327892690784192460327776944128$$

$$F = (9444732965739290427391) = 439 * 2298041 * 9361973132609$$

$$G = 44601490397061246283066714178813853366747136$$

$$I = (604462909807314587353087) = 2687 * 202029703 * 1113491139767$$

$$J = 182687704666362864775460301858080473799697891328$$

$$K = (9671406556917033397649407) = 167 * 57912614113275649087721$$

$$L = 46768052394588893382517909811217778170473142550528$$

$$M = (618970019642690137449562111) = 618970019642690137449562111$$

$$N = 191561942608236107294793378084303638130997321548169216$$

$$O = (158456325028528675187087900671) = 11447 * 13842607235828485645766393$$

$$P = 12554203470773361527671578846336104669690446551334525075456$$

$$Q = (2535301200456458802993406410751) = 7432339208719 * 341117531003194129$$

$$R = 3213876088517980551083924184681057554444177758164088967397376$$

$$S = (10141204801825835211973625643007) = 2550183799 * 3976656429941438590393$$

$$T = 51422017416287688817342786954912132678309582883443383916822528$$

$$U = (162259276829213363391578010288127) = 162259276829213363391578010288127$$

$$V = 13164036458569648337239753460458722910223472318386943117783728128$$

$$W = (649037107316853453566312041152511) = 745988807 * 870035986098720987332873$$

$$X = 210624583337114373395836055367340540119236532374371439352601378816$$

$$Y = (10384593717069655257060992658440191) = 3391 * 23279 * 65993 * 1868569 * 1066818132868207$$

$$Z = 53919893334301279589334030174039256154977430310253516431710891278336$$

$$A1 = (170141183460469231731687303715884105727) = 170141183460469231731687303715884105727$$

$$B1 = 14474011154664524427946373126085988481573677491474835889066354349131199152128$$

$$C1 = (2722258935367507707706996859454145691647) = 263 * 10350794431055162386718619237468234569$$

$$D1 = 3705346855594118253554271520278013051303278379832814295408789189823493075632128$$

1.1.2 末尾1桁の数

完全数の末尾1桁の数は、6または8という性質は完全数の理論の中でも注目を集めた初等的な結果である。弱完全数でも同じ結果が成り立つことを示す。

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

Proof.

弱完全数の仮定のもとでこの結果を示す。 $e+1=p$ は素数、という性質を用いるが $q=2^p-1$ は素数という性質は使えない。

$2^4 = 16 \equiv 1 \pmod{5}$ を以下用いる。

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

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

2). $e = 4k + 1$. $p = e + 1 = 4k + 2$ が素数なので、 $q = 3, k = 0, e = 1$. $a = 2 * q = 6$. これは例外的な場合.

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

4). $e = 4k + 3$. $p = e + 1 = 4(k + 1)$ は素数ではない。

1.2 フェルマとオイラーの結果

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

さらに $Q \equiv \pm 1 \pmod{8}$.

Proof.

条件より,

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

p は素数なので 2 の \pmod{Q} での位数は p . ゆえに

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

$Q - 1 = 2Lp$ により

$$2^{\frac{Q-1}{2}} \equiv 2^{Lp} \equiv 1 \pmod{Q}.$$

ルジャンドルの記号を用いるとオイラーの基準によって

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

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

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

ゆえに $Q \equiv \pm 1 \pmod{8}$.

例

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

$$23 - 1 = 22 = 2 * 11 = 2q, 89 - 1 = 88 = 8 * 11 = 8p.$$

$p = 23$ とする. $A = 2^{23} - 1$ の素因数分解は $47, 178481$. このとき

$$47 - 1 = 46 = 2 * 23 = 2p, 178480 = 178481 - 1 = 2^4 * 5 * 23 * 97 = 2^4 * 5 * 97 * p.$$

1.2.1 ラグランジュの結果

次の結果はオイラーが予想し 25 年後ラグランジュが証明した.

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

$q = 2p + 1$ が素数, かつ $q \equiv \pm 1 \pmod{8}$ のとき, ($q = 2p + 1$ により $q = 1 + 8k'$ は起きない. *By Mizutani*) $q = 2p + 1$ は M_p の約数. とくに M_p はメルセンヌ素数にならない.

逆に $q = 2p + 1$ が M_p の因子なら q は素数.

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

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

このとき $q \equiv -1 \pmod{8}$ なら q は M_p の素因子になる.

[注] $q \equiv -1 \pmod{8}$ かつ $q = 2p + 1$ によって $p \equiv 3 \pmod{4}$, なのでこれを条件にしてもよい.
 $p \equiv 1 \pmod{4}$, $q = 2p + 1$: 素数のとき $\left(\frac{2}{q}\right) = -1$.

表 1.3: $q = 2p + 1$ が素数とする

$\left(\frac{2}{q}\right)$	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	Z
(-)	5	11	31
(-)	29	59	233*1103*2089
(-)	41	83	13367*164511353
(-)	53	107	6361*69431*20394401
(-)	89	179	A
(-)	113	227	3391*23279*65993*1868569*1066818132868207

$$Z = 263 * 10350794431055162386718619237468234569$$

$$A = 618970019642690137449562111$$

$\left(\frac{2}{q}\right) = 1$ のとき $p \equiv 3 \pmod{4}$. このとき, $q = 2p + 1$ が M_p の最小素因子として出ている. 実に壮観である.

$\left(\frac{2}{q}\right) = -1$ のとき $p \equiv 1 \pmod{4}$. このとき, M_p の最小素因子がどうなるか誰も分からない. 悲しい限り.

1.2.2 $P = 3$

$N_p = \frac{P^p - 1}{P}$ とおく. $p \geq 2$ を仮定する. $p = e + 1$ は素数と仮定している.

$P = 3$ のとき弱完全数の数表は次の通り.

表 1.4: $P = 3$; 弱完全数の数表

p	$(2p+1)=$	$N_p =$ 分解	a
2	(5)=5	(4)= 2^2	12
3	(7)=7	(13)=13	117
5	(11)=11	(121)= 11^2	9801
7	(15)= $3*5$	(1093)=1093	796797
11	(23)=23	(88573)= $23*3851$	5230147077
13	(27)= 3^3	(797161)=797161	423644039001
17	(35)= $5*7$	(64570081)= $1871*34511$	2779530261754401
19	(39)= $3*13$	(581130733)= $1597*363889$	225141952751788437
23	(47)=47	(47071589413)= $47*1001523179$	1477156353259726319517
29	(59)=59	(34315188682441)= $59*28537*20381027$	785021449541029367424039801
31	(63)= $3^2 * 7$	(308836698141973)= $683*102673*4404047$	63586737412824202325875602477
37	(75)= $3 * 5^2$	(225141952945498681)= $13097927*17189128703$	A
41	(83)=83	(18236498188585393201)= $83*2526913*86950696619$	B
43	(87)= $3*29$	C	D
47	(95)= $5*19$	E	F

1.2.3 $P = 3$ 続き表 1.5: $P = 3$

p	$(2p + 1) =$	$\frac{P^p - 1}{P} =$ 分解	a
53	(107)=107	G	H
59	(119)=7*17	I	J
61	(123)=3*41	K	L
67	(135)=3 ³ * 5	M	N
71	(143)=11*13	O	P
73	(147)=3 * 7 ²	Q	R
79	(159)=3*53	S	T
83	(167)=167	U	V
89	(179)=179	W	X
97	(195)=3*5*13	Y	Z
101	(203)=7*29	$A1$	$B1$
103	(207)=3 ² * 23	$C1$	$D1$
107	(215)=5*43	$E1$	$F1$
109	(219)=3*73	$G1$	$H1$
113	(227)=227	$I1$	$J1$
127	(255)=3*5*17	$K1$	$L1$
131	(263)=263	$M1$	$N1$

$$A = 33792599317408761542712904163659401$$

$$B = 221713244121518884968045982580046482001$$

$$C = (164128483697268538813) = 431 * 380808546861411923$$

$$D = 17958772773843029682849400545509814478917$$

$$E = (13294407179478751643893) = 1223 * 21997 * 5112661 * 96656723$$

$$F = 117827508169184117749529434503875992840011597$$

$$G = (9691622833840009948398361) = 107 * 24169 * 3747607031112307667$$

$$H = 62618368768939376720930024035982040019969414457001$$

$$I = (7065193045869367252382405533) = 14425532687 * 489769993189671059$$

$$J = 33277968516933911303947774618193177127885685499906811237$$

$$K = (63586737412824305271441649801) = 603901 * 105293313660391861035901$$

$$L = 2695515449871646815619769744243211980459605339549629443001$$

$$M = (46354731573948918542880962705293) = 221101 * 441019876741 * 475384700124973$$

$$N = 1432507426195237855339786052661605566302711392155333734434378997$$

$$\begin{aligned}
O &= (3754733257489862401973357979128773) = 3754733257489862401973357979128773 \\
P &= 9398681223266955568884336291512894246732289173595197254503404033277 \\
Q &= (33792599317408761617760221812158961) = 11243*20149*15768033143*9460375336977361 \\
R &= 761293179084623401079631239612544524098913602817908624975367225786001 \\
S &= (24634804902390987219347201701063882933) \\
&= 432853009 * 392038110671 * 145171177264407947 \\
T &= 40458240838591134489316030561093028040969 \\
&- - 6733642031742793788413297107082637 \\
U &= (1995419197093669964767123337786174517613) \\
&= 167 * 12119 * 1036745531 * 950996059627210897943351 \\
V &= 2654465181419964333844024765113313569821231448014534796863835735316617556317717 \\
W &= (1454660594681285404315232913246121223340241) \\
&= 179 * 1611479891519807 * 5042939439565996049162197 \\
X &= 1410691630479007265542402365196584476859718059601935045571560890199346276163907738801 \\
Y &= (9544028161703913537712243143807801346335324481) \\
&= 76631 * 2549755542947 * 48845962828028421155731228333 \\
Z &= 607256490342649221167767082843574821283112603199541158927322029723 \\
&61234658808964021817054401 \\
A1 &= (773066281098016996554691694648431909053161283001) \\
&= 33034273 * 465092326319 * 50316775668019759306202964023 \\
B1 &= 39842098331381215400817198305366944024385017897983405520149643694312 \\
&0505787070463855225994805001 \\
C1 &= (6957596529882152968992225251835887181478451547013) \\
&= 6957596529882152968992225251835887181478451547013 \\
D1 &= 32272099648418784474661930627347224659751864497385112062067563800310 \\
&073569424269938090581449997117 \\
E1 &= (563565318920454390488370245398706861699754575308093) = \\
&50077 * 229837 * 48965028505045123993421250406516036571557 \\
F1 &= 211737245793275644938256926846[42digits]895536600580124298348772633797 \\
G1 &= (5072087870284089514395332208588361755297791177772841) \\
&= 1091 * 521402591 * 3499901929 * 239789806103 * 10624346875389299603 \\
H1 &= 171507169092553272399988110745[44digits]424354215954748960360390731801 \\
I1 &= (410839117493011250666021908895657302179121085399600161) \\
&= 227 * 1583 * 2172539 * 526256453012063980796131127321354599535039 \\
J1 &= 112525853641624202021632199459[48digits]758561740499372153467580684001 \\
K1 &= (1965030762956430528586812143568753110946368598712640184849493) \\
&= 5843 * 681229 * 21520151 * 76082653 * 301515315752300874236564235591357673 \\
L1 &= 257423059957675431046184790351[61digits]973215046058831272463436521197 \\
M1 &= (159167491799470872815531783629069001986655856495723854972808973) \\
&= 263 * 605199588591144003100881306574406851660288427740394885828171
\end{aligned}$$

$N1 = 168895269638230850309401840949[65digits]983561348165197935406290479477$

$p = 5$ のときの $a = 9801 = 3^4 \times 11^2$. 昔懐かしき 9801 が登場.

$p = 7$ のとき $N_p = 1093$. これは Wieferich 素数のひとつ. Wieferich 素数は 2 つしかないから貴重な素数.

1.2.4 末尾の数

3 が底の弱完全数の場合, $q = \frac{3^p-1}{2}$ は素数でなくても $p = e + 1$ が素数を仮定するとき q の末尾の数が 3 または 1, も同様に成立する. また, 3 を底とする弱完全数では末尾の数が 7 または 1 になる.

Proof.

$e > 1$ とする. $p = e + 1$ が素数は使える. しかし $q = \frac{3^p-1}{2}$ が素数とは言えない.

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

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

1. $e = 4k + 2$ のとき

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

よって $q \equiv 3 \pmod{5}$. $q = 3 + 5L$ となる.

$$q = \frac{3^p - 1}{2} = 1 + 3 \cdots 3^{p-1} \equiv p \pmod{2}.$$

ゆえに q は奇数. その結果 L は偶数になるので $q \equiv 3 \pmod{10}$.

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

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

2. $e = 4k$ のとき

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

よって $q \equiv 1 \pmod{5}$. $q = 1 + 5L$ となるが q は奇数. L は偶数になるので $q \equiv 1 \pmod{10}$.

$a = 3^e q \equiv q \equiv 1 \pmod{5}$ により a は奇数なので $a \equiv 1 \pmod{10}$.

3. $e = 4k + 3$ のとき $e + 1 = 4(k + 1)$ は素数ではない.

4. $e = 4k + 1$ のとき $e + 1 = 4k + 2$ は素数なので $k = 0, e = 1$.

$e = 1$

しかし, $q = 2^p - 1$ が合成数のとき, 各素因子の末尾の数はさまざまである. 素因子の数が 2 個の場合, Q_1, Q_2 とおく.

$q = Q_1 Q_2$ の末尾の数が 1, 3 なら可能性は絞られる.

- $q = Q_1 Q_2$ の末尾の数 1 なら (Q_1, Q_2) の末尾の数 $(1, 1), (3, 7), (9, 9)$

- $q = Q_1 Q_2$ の末尾の数 3 なら (Q_1, Q_2) の末尾の数 $(1,3), (7,9)$

$q = Q_1 Q_2 Q_3$ の末尾の数が 1,3 ならどんな可能性があるか例と対応させて調べるとよい.

表 1.6: mod10 での乗算表

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$q = Q_1 Q_2 Q_3$ の末尾の数が 1,7 ならどんな可能性があるか例と対応させて良く調べるとよい.

次は課題:

- $e \equiv 2 \pmod{4}$ のとき $q \equiv 13, 33, 73, 93 \pmod{100}$.
- $e \equiv 0 \pmod{4}$ のとき $q \equiv 01, 41, 61, 81 \pmod{100}$.

N_p 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.

底が 3, 一般には奇素数 P のときにもオイラーとラグランジュの結果が成立する. これは弱完全数に関して後に取り上げて証明する.

ここでは, $P = 3$ の場合を取り上げる.

$P = 3$ のとき p が Sophie Germain 素数ならば 素数 $q = 2p + 1$ は $q + 1 \equiv 0 \pmod{12}$ を満たし q は すべて N_p の因子となる. これは意外な結果である.

表 1.7: $P = 3, q = 2p + 1$: 素数

p	$q = 2p + 1$	$q + 1$	$q + 1 \pmod{12}$	N_p の素因数分解
5	11	12	0	11^2
11	23	24	0	$23 * 3851$
23	47	48	0	$47 * 1001523179$
29	59	60	0	$59 * 28537 * 20381027$
41	83	84	0	$83 * 2526913 * 86950696619$
53	107	108	0	$107 * 24169 * 3747607031112307667$
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

$A = 167 * 12119 * 1036745531 * 950996059627210897943351$
 $B = 179 * 1611479891519807 * 5042939439565996049162197$
 $C = 227 * 1583 * 2172539 * 526256453012063980796131127321354599535039$
 $D = 263 * 605199588591144003100881306574406851660288427740394885828171$
 $E = 347 * 762239 * 2125048865543 * 30985428700388045508959018054392810762$
 $-- 033149280306907746766819$
 $F = 359 * 56207 * 100957 * 19510643 * 291066066130451 * 6779963644378513811*$
 $-- 161868664744491655705858963594331$
 $G = 383 * 311713 * 9593931911 * 589086859176036543433200507492971040054890$
 $-- 918146821485888800348369500317$

1.2.5 証明

参加者の水谷氏の指摘により, 次の結果を証明する.

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

3 より大きい素数 q を $\pmod{12}$ で分類すると $q \equiv 1, 5, 7, 11 \pmod{12}$ である.

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

矛盾.

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

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

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

一方、メルセンヌ数 $M_p = 2^p - 1$ には平方因子が無い. という予想がある.
しかし底が3のとき $p = 5$ の場合 $N_5 = 11^2$. これは平方因子なので反例.
これは Wieferich の素数の一般化としてのちにとりあげる.

1.2.6 $P = 5$

$$N_p = \frac{P^p - 1}{P}$$

表 1.8: $P = 5$

p	$(2p + 1) =$	$N_p =$ 分解	a
2	(5)=5	(6)=2*3	30
3	(7)=7	(31)=31	775
5	(11)=11	(781)=11*71	488125
7	(15)=3*5	(19531)=19531	305171875
11	(23)=23	(12207031)=12207031	119209287109375
13	(27)=3 ³	(305175781)=305175781	74505805908203125
17	(35)=5*7	(190734863281)=409*466344409	29103830456695556640625
19	(39)=3*13	(4768371582031)=191*6271*3981071	A
23	(47)=47	B	C
29	(59)=59	D	E
31	(63)=3 ² * 7	F	G

表 1.9: $P = 5$ 続き

p	$(2p + 1) =$	$(P^p - 1) =$ 分解	a
37	(75)=3 * 5 ²	H	I
41	(83)=83	J	K
43	(87)=3*29	L	M
47	(95)=5*19	N	O
53	(107)=107	P	Q
59	(119)=7*17	R	S
61	(123)=3*41	T	U
67	(135)=3 ³ * 5	V	W
71	(143)=11*13	X	Y
73	(147)=3 * 7 ²	Z	$A1$
79	(159)=3*53	$B1$	$C1$

$$A = 18189894035457611083984375$$

$$B = (2980232238769531) = 8971 * 332207361361$$

$$C = 7105427357601001262664794921875$$

$$D = (46566128730773925781) = 59 * 35671 * 22125996444329$$

$$E = 1734723475976807094402611255645751953125$$

$$\begin{aligned}
F &= (1164153218269348144531) = 1861 * 625552508473588471 \\
G &= 1084202172485504434007219970226287841796875 \\
H &= (18189894035458564758300781) = 149 * 13971969971 * 8737481256739 \\
I &= 264697796016968855958850777824409306049346923828125 \\
J &= (11368683772161602973937988281) = 2238236249 * 5079304643216687969 \\
K &= 103397576569128459358926086506471619941294193267822265625 \\
L &= (284217094304040074348449707031) = 1644512641 * 172827552198815888791 \\
M &= 64623485355705287099328804067909004515968263149261474609375 \\
N &= (177635683940025046467781066894531) \\
&= 177635683940025046467781066894531 \\
O &= 25243548967072377773175314089049123822405817918479442596435546875 \\
P &= (2775557561562891351059079170227050781) \\
&= 5960555749 * 17154094481 * 27145365052629449 \\
Q &= 6162975822039154729779129416271767418766813761976663954555988311767578125 \\
R &= (43368086899420177360298112034797668457031) = 21180247636732981*2047572230657338751575051 \\
S &= 1504632769052528010199982767644474467607883239050892143495730124413967132568359375 \\
T &= (1084202172485504434007452800869941711425781) = 8419*918585913061*140194179307171898833699259 \\
U &= 94039548065783000637498922977796542254932228577235520106114563532173633575439453125 \\
V &= (16940658945086006781366450013592839241027832031) \\
&= 269 * 1609 * 26399 * 2454335007529 * 604088623657497125653141 \\
W &= 229588740394978028900143854926219858948958116553660212255660866276230080984532833099365234375 \\
X &= (10587911840678754238354031258495524525642395019531) \\
&= 569 * 18607929421228039083223253529869111644362732899 \\
Y &= 89683101716788292539118693330554632401936764280094891810084234418098958485643379390239715576171 \\
Z &= (264697796016968855958850781462388113141059875488281) \\
&= 4853479 * 5729041 * 9519524151770349914726200576714027279 \\
A1 &= 560519385729926828369491833315[41digits]537278131581842899322509765625 \\
B1 &= (4135903062765138374357043460349814267829060554504394531) \\
&= 205367807127911 * 58523123221688392679 * 344120456368919234899 \\
C1 &= 136845553156720417082395467118[50digits]744322988204658031463623046875
\end{aligned}$$

1.2.7 末尾の数

$a \equiv 25, 75 \pmod{100}$ は成り立つ.

より詳しく,

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

が成り立つ事を参加者の一人である高嶋耕司氏が詳しく証明した.

多分, 弱完全数でも証明は通用する.

1.2.8 $P = 7$

$$N_p = \frac{P^p - 1}{P}$$

表 1.10: $P = 7$

p	$(2p + 1) =$	$(N_p) =$ 分解	a
2	(5)=5	(8)= 2^3	56
3	(7)=7	(57)= $3 \cdot 19$	2793
5	(11)=11	(2801)=2801	6725201
7	(15)= $3 \cdot 5$	(137257)= $29 \cdot 4733$	16148148793
11	(23)=23	(329554457)= $1123 \cdot 293459$	93090977300134793
13	(27)= 3^3	(16148168401)=16148168401	AA
17	(35)= $5 \cdot 7$	(38771752331201)= $14009 \cdot 2767631689$	BB
19	(39)= $3 \cdot 13$	(1899815864228857)= $419 \cdot 4534166740403$	CC

AA = 223511436608353935601

BB = 1288498953284568548534420801

CC = 3093685986836262112339927626793

表 1.11: $P = 7$; 続き

p	$(2p+1)=$	$(N_p) =$ 分解	a
23	$(47)=47$	$(4561457890013486057)=47*3083*31479823396757$	A
29	$(59)=59$	$(536650959302196621139601)=59*127540261*71316922984999$	B
31	$(63)=3^2 * 7$	C	D
37	$(75)=3 * 5^2$	E	F
41	$(83)=83$	G	H
43	$(87)=3*29$	I	J
47	$(95)=5*19$	K	L
53	$(107)=107$	M	N
59	$(119)=7*17$	O	P
61	$(123)=3*41$	Q	R
67	$(135)=3^3 * 5$	S	T
71	$(143)=11*13$	U	V
73	$(147)=3 * 7^2$	W	X

$$\begin{aligned}
A &= 17834484070599672225407746556059132793 \\
B &= 246852216102829623577350845421202364881743396401 \\
C &= (26295897005807634435840457) = 311 * 21143 * 3999088279399464409 \\
D &= 592692170862893926209219560171029203619130597664793 \\
E &= (3093685986836262383742193945201) = 223 * 2887 * 4805345109492315767981401 \\
F &= 8203622558697478826660309198389254312666780494848270305646801 \\
G &= (7427940054393865983365007662428001) = 83 * 20515909 * 4362139336229068656094783 \\
H &= 47292251530001784637410177127186118373220132474676100080318673652001 \\
I &= (363969062665299433184885375458972057) \\
&= 166003607842448777 * 2192537062271178641 \\
J &= 113548695923534284914421835282373872709889396348036286703487710014262793 \\
K &= (873889719459383939076909786476991909257) \\
&= 13722816749522711 * 63681511996418550459487 \\
L &= 6545856358086863692089439104576641840714624343426304270223 \\
&50295255757960808793 \\
M &= (102812251604677061048459359469231621132196401) \\
&= 8269 * 319591 * 38904276017035188056372051839841219 \\
N &= 9060307782877217926754915842544557323346169012644208670628797275051 \\
&070279034171965187601 \\
O &= (12095758589038651555290195182195630994581774400857) \\
&= 459257 * 134927809 * 550413361 * 354639323684545612988577649 \\
P &= 1254063221522591234440805721152441125518421478503867792800074932 \\
&27585324645254553813463672815486793 \\
Q &= (592692170862893926209219563927585918734506945642001) \\
&= 367 * 4759 * 177237331 * 1914662449813727660680530326064591907 \\
R &= 301100579487574155389237453648[42digits]978837401438140457906182478001 \\
S &= (69729641209848607524588472476516555753196007647835795257) \\
&= 228337 * 147300841 * 206244761 * 10052011757370829033540932021825161 \\
T &= 416761959707504329552743754033[52digits]988654120686252470466511138793 \\
U &= (167420868544846506666536922416116250363423614362453744412457) \\
&= 990643452963163 * 169002145064468556765676975247413756542145739 \\
V &= 240254976208378066650998674599[59digits]692282259881493512306080724793 \\
W &= (8203622558697478826660309198389696267807757103760233476210401) \\
&= 439 * 3675989 * 359390389 * 1958423494433591 * 7222605228105536202757606969 \\
X &= 576852197876315738029047817714[62digits]229828085800348831357942813601
\end{aligned}$$

1.2.9 末尾の数

$p = e + 1$ は素数を仮定しているので, $e \equiv 0, 2 \pmod{4}$ の場合はおきない.

- $e \equiv 1 \pmod{4}$ なら $q \equiv 01, a \equiv 93 \pmod{100}$.
- $e \equiv 3 \pmod{4}$ なら $q \equiv 57, a \equiv 01 \pmod{100}$.

証明.

$7^2 = 49 \equiv -1 \pmod{50}, 7^4 = 2401 \equiv 1 \pmod{100}$, に注意する.

(1) $e \equiv 2, \pmod{4}$ のとき, $p = e + 1 = 4k + 3$. $7^p = 7^{4k+3} = 2401^k \cdot 7^3 \equiv 343 \pmod{600}$.
これより

$$6N_p = 7^p - 1 \equiv 342 = 6 \times 57 \pmod{600}$$

ゆえに

$$N_p \equiv 57 \pmod{100}.$$

よって

$$a_p = 7^e N_p = 7^{4k+2} N_p \equiv 49 \times 57 = 2793 \equiv 93 \pmod{100}.$$

(1) $e \equiv 0, \pmod{4}$ のとき, $p = e + 1 = 4k + 1$. $7^p = 7^{4k+1} = 2401^k \cdot 7 \equiv 7 \pmod{600}$.
これより

$$N_p = \frac{7^p - 1}{6} \equiv 1 \pmod{100}.$$

ゆえに

$$a_p = 7^{p-1} N_p = 7^{4k} N_p \equiv 1 \pmod{100}.$$

高嶋耕司氏もこの場合の証明に成功した. 飯高とほぼ同時に証明した (2015/3/27).

1.2.10 $P = 11$

$$N_p = \frac{P^p - 1}{P}$$

表 1.12: $P = 11$

e	p	$(2p + 1)$	$(N_p) = \text{分解}$	a
1	2	(5)=5	(12)=2 ² *3	132
2	3	(7)=7	(133)=7*19	16093
4	5	(11)=11	(16105)=5*3221	235793305
6	7	(15)=3*5	(1948717)=43*45319	3452271037237
10	11	(23)=23	(28531167061)=15797*1806113	740024994423222267661
12	13	(27)=3 ³	(3452271214393)=1093*3158528101	10834705943388058361345353
16	17	(35)=5*7	(50544702849929377)=50544702849929377	A0
18	19	(39)=3*13	(6115909044841454629)=6115909044841454629	A
22	23	(47)=47	B	C
28	29	(59)=59	D	E
30	31	(63)=3 ² * 7	F	G
36	37	(75)=3 * 5 ²	H	I
40	41	(83)=83	J	K
42	43	(87)=3*29	L	M
46	47	(95)=5*19	N	O

$$A0 = 2322515441988780809505203793273697$$

$$A = 34003948586157739898684696499226975549$$

$$B = (89543024325523737224653) = 829 * 28878847 * 3740221981231$$

$$C = 7289048368510305214290278538501245253967902613$$

$$D = (158630929717149157441443670489) = 523 * 303309617049998388989376043$$

$$E = 22876156239024650606645326473334848325625895160495412605609$$

$$F = (19194342495775048050414684129181) = 50159 * 2428541 * 157571957584602258799$$

$$G = 334929803495559909531894224896304907162715367932636041603766981$$

$$H = (34003948586157739899240688230576198697) = 2591*36855109*136151713*2615418118891695851$$

$$I = 1051153199500053598403188407217590190704579879232264635077522314892256470617$$

$$J = (497851811249935469864782916383866125124241)$$

$$= 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$$

$$K = 225324023604401248793730853803334956796672939988861482205529251845184623522089398641$$

$$L = (60240069161242191853638732882447801140033173)$$

$$= 1416258521793067 * 42534656091583268045915654719$$

$$M = 3298969029592038683589013430534627102460089171541311810885973997778797699690196049501133$$

$$\begin{aligned}
 N &= (881974852589746930929124688131918256491225687357) \\
 &= 2069 * 22666879066355177 * 18806327041824690595747113889 \\
 O &= 7071633096370052987228539828633738974356170631456409943 \\
 &-- 18500556468267327181081133208187483831077
 \end{aligned}$$

1.2.11 末尾の数

表を観察してもきれいな結果が見えてこない.

$$e \equiv 0 \pmod{4} \text{ のとき } q \equiv 1, 3, 5, 7, 9 \pmod{10}$$

$$e \equiv 2 \pmod{4} \text{ のとき } q \equiv 1, 3, 7, 9 \pmod{10}$$

$P = 11$ がこれほど期待を裏切る素数とは思わなかった. しかしこのように末尾の数の 1,2 桁の数の性質は 10 進展開で得られた性質なので, 皮相的な結果にすぎない, という事もできる.

この困難さは弱弱完全数によって解決される. これはささやかな結果ではあるが, まったく予想外の良い結果になるのである.

1.2.12 $P = 13$

$$N_p = \frac{P^p - 1}{P}$$

表 1.13: $P = 13$

p	$(2p+1)=$	$(N_p) =$ 分解	a
2	(5)=5	(14)=2*7	182
3	(7)=7	(183)=3*61	30927
5	(11)=11	(30941)=30941	883705901
7	(15)=3*5	(5229043)=5229043	25239591813787
11	(23)=23	(149346699503)=23*419*859*18041	20588710756109377851047
13	(27)=3 ³	(25239592216021)=53*264031*1803647	588034167905566113995468101
17	(35)=5*7	(720867993281778161)=103*443*15798461357509	A
19	(39)=3*13	(121826690864620509223)=12865927*9468940004449	B
23	(47)=47	C	D
29	(59)=59	E	F
31	(63)=3 ² * 7	G	H
37	(75)=3 * 5 ²	I	J
41	(83)=83	K	L
43	(87)=3*29	M	N
47	(95)=5*19	O	P

$$\begin{aligned}
A &= 479677535758244089774221240729252401 \\
B &= 13700070098791209449615908553795581328767 \\
C &= (3479492117784426363920483) = 1381 * 2519545342349331183143 \\
D &= 11175568059437494512804842434187269399079517489227 \\
E &= (16794843869550929233208663030981) = 1973 * 2843 * 3539 * 846041103974872866961 \\
F &= 260369335940854550834324579101958487505450742744381795527146101 \\
G &= (2838328613954107040412264052235803) = 311 * 1117 * 8170509011431363408568150369 \\
H &= 7436408603806746826379144303731073041582189762751733789770879453347 \\
I &= (13700070098791209449625279837708244444861) = 1481 * 67495678093 * 4287755796749 * \\
&31964044249933 \\
J &= 173254080657039673337315704257336335416015022123686381380502857325209484698165901 \\
K &= (391287702091575733090747617444785169589677401) \\
&= 6740847065723 * 58047259977349384372529747126587 \\
L &= 141328676130559126457053015638459738428404628572768084246239884360142050818445913276235001 \\
M &= (66127621653476298892336347348168693660655480783) \\
&= 119627 * 552781743698966779174737704265497702530829 \\
N &= 4036488318964899210739891179650048589253664597521401595524858 \\
&738280209909925044539466403307527 \\
O &= (1888671002044936572664018416611046059641981186645643) \\
&= 183959 * 19216136497 * 534280344481909234853671069326391741 \\
P &= 329268752673731520686918237543[43digits]852840982402455585532753634387
\end{aligned}$$

1.2.13 末尾の数

表を観察すると,

- $e \equiv 0 \pmod{4}$ なら $q \equiv 1, a \equiv 1 \pmod{10}$.
- $e \equiv 2 \pmod{4}$ なら $q \equiv 3, q \equiv 7 \pmod{10}$.

$13^4 \equiv 1 \pmod{10}$. この性質を使って証明できるだろう.

1.2.14 $P = 17$ の弱完全数表 1.14: $P = 17$

p	$(2p+1)=$	$(N_p) =$ 分解	a
2	(5)=5	(18)= $2 * 3^2$	306
3	(7)=7	(307)=307	88723
5	(11)=11	(88741)=88741	7411737061
7	(15)= $3*5$	(25646167)=25646167	619036125548023
11	(23)=23	(2141993519227)=2141993519227	4318245869562919805432923
13	(27)= 3^3	A	B
17	(35)= $5*7$	C	D
19	(39)= $3*13$	E	F
23	(47)=47	G	H

$$A = (619036127056621) = 212057 * 2919196853$$

$$B = 360664213271775112269833297581$$

$$C = (51702516367896047761) = 10949 * 1749233 * 2699538733$$

$$D = 2515906069432996448706321616411281521041$$

$$E = (14942027230321957802947) = 229 * 1103 * 202607147 * 291973723$$

$$F = 210130990825113296392653823244423862968703523$$

$$G = (1247973056303720237659941607) = 47 * 26552618219228090162977481$$

$$H = 1465822822832986806979099496452603964256853795297401223$$

1.2.15 末尾の数

- $p \equiv 1 \pmod{4}$ なら $q \equiv 1, a \equiv 1 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ なら $q \equiv 7, a \equiv 3 \pmod{100}$.

1.2.16 $P = 19$ の弱完全数表 1.15: $P = 19$

p	$(2p+1)=$	$(N_p) =$ 分解	a
2	(5)=5	(20)= $2^2 \cdot 5$	380
3	(7)=7	(381)= $3 \cdot 127$	137541
5	(11)=11	(137561)= $151 \cdot 911$	17927087081
7	(15)= $3 \cdot 5$	(49659541)= $701 \cdot 70841$	2336276856400621
11	(23)=23	(6471681049901)= $104281 \cdot 62060021$	39678305316298170811527701
13	(27)= 3^3	A	B
17	(35)= $5 \cdot 7$	C	D
19	(39)= $3 \cdot 13$	E	F

$$A = (2336276859014281) = 599 * 29251 * 133338869$$

$$B = 5170916427125338184627482845241$$

$$C = (304465936543600121441) = 3044803 * 99995282631947$$

$$D = 87820585119825665555381186232873824348321$$

$$E = (109912203092239643840221) = 109912203092239643840221$$

$$F = 11444866473400800560844914118060307887728197861$$

1.2.17 末尾の数

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

1.2.18 $P = 23$ の弱完全数表 1.16: $P = 23$

p	$(2p+1)=$	$(N_p) =$ 分解	a
2	(5)=5	(24)= $2^3 \cdot 3$	552
3	(7)=7	(553)= $7 \cdot 79$	292537
5	(11)=11	(292561)=292561	81870562801
7	(15)= $3 \cdot 5$	(154764793)= $29 \cdot 5336717$	22910743717655977
11	(23)=23	A	B
13	(27)= 3^3	C	D
17	(35)= $5 \cdot 7$	E	F
19	(39)= $3 \cdot 13$	G	H

$$A = (43309534450633) = 11 * 3937230404603$$

$$B = 1794162914577065657306289817$$

$$C = (22910743724384881) = 47691619 * 480393499$$

$$D = 502080344178161156557235817166801$$

$$E = (6411365434575589496641) = 103 * 62246266355102810647$$

$$F = 39318406442815392450806435199657663047640001$$

$$G = (3391612314890486843723113) = 2129 * 63877469 * 24939218613613$$

$$H = 11002902177363902238826201492329237570873472728697$$

1.2.19 末尾の数

- $p \equiv 1 \pmod{4}$ なら $q \equiv 1, a \equiv 1 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ なら $q \equiv 3, a \equiv 7 \pmod{100}$.

以上から次の推察が可能:

N_p は $p = 2, P \equiv -1 \pmod{4}$ ($P=3,7,11,19,23, \dots$) のとき $p^2 = 4$ で割れる.

$p > 2$ は奇数.

1.3 フェルマとオイラーの結果 (一般の場合)

底が奇素数 P で, $N_p = \frac{P^p-1}{P}$ の素数因子 (奇数) Q について $P-1 \not\equiv 0 \pmod{Q}$ かつ

$$P^p \equiv 1 \pmod{Q}$$

になる. よって \pmod{Q} で P の位数は素数 p である. $P \neq Q$ により, フェルマの小定理によれば $P^{Q-1} \equiv 1 \pmod{Q}$ なので $Q-1$ は位数 p で割れる. よって $Q-1 = kp$ と書けるが Q, p はともに奇数なので k は偶数. したがって, $Q = 1 + 2k'p$ と書ける. オイラーの基準によって

$$P^{\frac{Q-1}{2}} = \left(\frac{P}{Q}\right)$$

$P^{\frac{Q-1}{2}} = P^{pk'} \equiv 1 \pmod{Q}$. ゆえに

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

逆に素数 $Q = 2p + 1$ が素数 (p : Sophie Germain) とする. さらに $P-1 \not\equiv 0 \pmod{Q}$ かつ $\left(\frac{P}{Q}\right) = 1$ を仮定すると, $P \equiv n^2 \pmod{Q}$ を満たす n がある.

$$P^p = P^{\frac{Q-1}{2}} \equiv n^{Q-1} \equiv 1 \pmod{Q}$$

これより, 素因子 Q は $P^p - 1$ の素因子になる. $P-1 \not\equiv 0 \pmod{Q}$ なので Q は $N_p = \frac{P^p-1}{P}$ の素因子.

したがって次の結果が証明できた.

定理 1 底が奇素数 P のとき

(1) $N_p = \frac{P^p-1}{P}$ の素因子 (奇数) Q について $\left(\frac{P}{Q}\right) = 1$.

(2) 素数 Q は $2p + 1$ と書けるとき $\left(\frac{P}{Q}\right) = 1$ を仮定すると, Q は N_p の素数因子.

第1章で示したようこの結果は $P = 2$ のとき, フェルマとオイラーにより示された. 底が P でも同じ証明が成立することがわかった.

次は Lagrange の結果の一般化.

定理 2 p を素数とし, $N_p = \frac{P^p-1}{P}$ とおく. $Q = 2p + 1$ は 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 $Q_0 \neq P$.

$$P^p = \overline{P}N_p + 1 \equiv 1 \pmod{Q_0}.$$

p は素数なので Q_0 を法とした P の位数である. フェルマの小定理を用いて

$$P^{Q_0-1} \equiv 1 \pmod{Q_0}.$$

ゆえに, $Q_0 - 1$ は p の倍数. とくに $Q_0 - 1 > p$ になり

$$2p + 1 \geq Q_0^2 > p^2 + 2p + 1 > 2(p + 1) + 1.$$

これで矛盾した.

1.4 p : Sophie Germain 素数

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

1.4.1 $P = 3$

表 1.17: $P = 3, Q = 2p + 1$ も素数

p	$Q = 2p + 1$	(N_p) =素因数分解
2	5	$(4) = 2^2$
3	7	$(13) = 13$
5	11	$(121) = 11^2$
11	23	$(88573) = 23 * 3851$
23	47	$(47071589413) = 47 * 1001523179$
29	59	$(34315188682441) = 59 * 28537 * 20381027$
41	83	$(18236498188585393201) = 83 * 2526913 * 86950696619$
53	107	$(9691622833840009948398361) = 107 * 24169 * 3747607031112307667$
83	167	$A = B$
89	179	$C = D$

$$A = (1995419197093669964767123337786174517613)$$

$$B = 167 * 12119 * 1036745531 * 950996059627210897943351$$

$$C = (1454660594681285404315232913246121223340241)$$

$$D = 179 * 1611479891519807 * 5042939439565996049162197$$

$Q = 2p + 1$ が N_p の最小素因子となる。

1.4.2 $P = 5$

表 1.18: $P = 5, Q = 2p + 1$ も素数

p	$Q = 2p + 1$	(N_p) =素因数分解
2	5	(6)=2*3
5	11	(781)=11*71
23	47	(2980232238769531)=8971*332207361361
29	59	A
41	83	B
53	107	C
83	167	$D = E$
89	179	$F = G$
113	(227)=227	$H = I$
131	(263)=263	$J = K$

$$A = (46566128730773925781) = 59 * 35671 * 22125996444329$$

$$B = (11368683772161602973937988281) = 2238236249 * 5079304643216687969$$

$$C = (2775557561562891351059079170227050781) = 960555749*17154094481*27145365052629449$$

$$D = (2584939414228211483973152162718633917393162846565246582031)$$

$$E = 20515111 * 1431185706701868962383741 * 88040095945103834627376781$$

$$F = (40389678347315804437080502542478654959268169477581977844238281)$$

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

$$H = (2407412430484044816319972428231159148172627060269235244049923494458198547363281)$$

$$I = 2939 * 6329 * 129499 * 308491 * 304247586761 * 2084303944451$$

$$- * 620216264269531 * 8237123176890810696379$$

$$J = 918354961579912115600575419704879435795832466228193$$

-

$$3761787122705300134839490056037902832031)$$

$$K = 2621 * 23928199 * 34720241 * 16815642611861 * -$$

$$250805666433416532678429525124977090318975999001796354124089$$

$Q = 2p + 1$ が N_p の最小素因子となるのは $Q = 11, 179$,
 $p = 23$ での (N_p) の素因数分解 $8971 * 332207361361$ について各素因子 Q の $Q - 1$ の素因数分解を行う.

?- Q=8971,B is Q-1, factorize(B, BB), exps(BB, J).
 Q = 8971,
 B = 8970,
 J = [2, 3, 5, 13, 23].

3 ?- Q=332207361361,B is Q-1, factorize(B, BB), exps(BB, J).
 Q = 332207361361,
 J = [2^4, 3^2, 5, 7, 23, 293, 9781].

$B = Q - 1$ がどれも 2×23 を因数に持つ.

$p = 29$ での (N_p) の素因数分解 $59 * 35671 * 22125996444329$ について

4 ?- Q=59,B is Q-1, factorize(B, BB), exps(BB, J).
 Q = 59,
 B=Q-1 = [2, 29].

5 ?- Q=35671,B is Q-1, factorize(B, BB), exps(BB, J).
 Q = 35671,
 B = 35670,
 J = [2, 3, 5, 29, 41].

6 ?- Q=22125996444329,B is Q-1, factorize(B, BB), exps(BB, J).
 Q = 22125996444329,
 B = Q-1,
 J = [2^3, 7, 29, 13624382047].

B はどれも 2×29 を因数に持つ.

1.4.3 $P = 7$

表 1.19: $P = 7, Q = 2p + 1$ も素数

p	$Q = 2p + 1$	(N_p) =素因数分解
2	5	$(8)=2^3$
3	7	$(57)=3*19$
11	23	$(329554457)=1123*293459$
23	47	$(4561457890013486057)=47*3083*31479823396757$
29	59	$(536650959302196621139601)=59*127540261*71316922984999$
41	83	A
53	107	$B = C$
83	167	$D = E$

$A = (7427940054393865983365007662428001) = 83 * 20515909 * 4362139336229068656094783$
 $B = (102812251604677061048459359469231621132196401)$
 $C = 8269 * 319591 * 8904276017035188056372051839841219$
 $D = (2317320324970087447233098679232119852283366872016190787490668645944057)$
 $E = 167*66733*76066181*7685542369*62911130477521*303567967057423*18624275418445601$

$Q = 2p + 1$ が N_p の最小素因子となるのは $Q = 47, 59, 83, 167$.

- $e \equiv 1 \pmod{4}$ なら $Q \equiv 01, a \equiv 93 \pmod{100}$.
- $e \equiv 3 \pmod{4}$ なら $Q \equiv 57, a \equiv 01 \pmod{100}$.

証明.

$7^2 = 49 \equiv -1 \pmod{50}, 7^4 = 2401 \equiv 1 \pmod{100}$, に注意する.

(1) $e \equiv 2, \pmod{4}$ のとき, $p = e + 1 = 4k + 3, 7^p = 7^{4k+3} = 2401^k \cdot 7^3 \equiv 343 \pmod{600}$.
これより

$$6N_p = 7^p - 1 \equiv 342 = 6 \times 57 \pmod{600}$$

ゆえに

$$N_p \equiv 57 \pmod{100}.$$

よって

$$a_p = 7^e N_p = 7^{4k+2} N_p \equiv 49 \times 57 = 2793 \equiv 93 \pmod{100}.$$

(1) $e \equiv 0, \pmod{4}$ のとき, $p = e + 1 = 4k + 1, 7^p = 7^{4k+1} = 2401^k \cdot 7 \equiv 7 \pmod{600}$.

これより

$$N_p = \frac{7^p - 1}{6} \equiv 1 \pmod{100}.$$

ゆえに

$$a_p = 7^{p-1} N_p = 7^{4k} N_p \equiv 1 \pmod{100}.$$

高嶋耕司氏もこの場合の証明に成功した。飯高とほぼ同時に証明した (2015/3/27)。

1.4.4 実例

$P = 7, p = 73$ のときの $W = N_p$ の各素因子 Q について $Q - 1$ の素因子分解を実行した結果 $2, 73$ を素因子に持っていることの確認。

$p = 73, W = 439 * 3675989 * 359390389 * 1958423494433591 * 7222605228105536202757606969$
について

1 ?- $Q=439, A$ is $Q-1, \text{factorize}(A,S), \text{exps}(S,SX).$

$SX = [2, 3, 73].$

2 ?- $Q=3675989, A$ is $Q-1, \text{factorize}(A,S), \text{exps}(S,SX).$

$SX = [2^2, 73, 12589].$

3 ?- $Q=3675989, A$ is $Q-1, \text{factorize}(A,S), \text{exps}(S,SX).$

$SX = [2^2, 73, 12589].$

4 ?- $Q=359390389, A$ is $Q-1, \text{factorize}(A,S), \text{exps}(S,SX).$

$SX = [2^2, 3, 7, 29, 43, 47, 73].$

5 ?- $Q=1958423494433591, A$ is $Q-1, \text{factorize}(A,S), \text{exps}(S,SX).$

$SX = [2, 5, 73, 2682771910183].$

1.4.5 $P = 11$

表 1.20: $P = 11, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(12)=2^2 * 3$
3	7	$(133)=7*19$
5	11	$(16105)=5*3221$
11	23	$(28531167061)=15797*1806113$
23	47	$(89543024325523737224653)=829*28878847*3740221981231$
29	59	$(158630929717149157441443670489)=523*303309617049998388989376043$
41	83	$X = Y$
53	107	$A = B$
83	167	$C = D$

$$X = (497851811249935469864782916383866125124241)$$

$$Y = 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$$

$$A = (1562472251828744662703731061631669238387852269920031433)$$

$$B = 107 * 351497 * 6005113 * 6918082374901313855125397665325977135579$$

$$C = (27264206856132551104041433310203529772397431215022163096159$$

$$-- 207985879419668700193602213)$$

$$D = 167 * 12119 * 178057577 * 52447614013*$$

$$1442525225996981034595894901431683672700025887063977893738081$$

$q = 2p + 1$ が N_p の最小素因子となるのは $q = 7, 83, 107, 167$

1.4.6 $P = 13$

$$A = (7427940054393865983365007662428001) = 83 * 20515909 * 4362139336229068656094783$$

$$B = (102812251604677061048459359469231621132196401)$$

$$C = 8269 * 319591 * 38904276017035188056372051839841219$$

$$D = (2317320324970087447233098679232119852283366872016190787490668645944057)$$

$$E = 167*66733*76066181*7685542369*62911130477521*303567967057423*18624275418445601$$

$$F = (272630418912405818079526826512979668501285829125832829957489675526672381601)$$

$$G = 1805633*18489605314740987765913*8166146875847876762859119015147004762656450569$$

$q = 2p + 1$ が N_p の最小素因子となるのは $q = 47, 59, 83, 167$

$p = 89$ のときの $G = 1805633*18489605314740987765913*8166146875847876762859119015147004762656450569$
 の各素因数 Q について

?- Q=1805633,B is Q-1, factorize(B, BB),exps(BB,J).

表 1.21: $P = 13, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p) =素因数分解
2	5	$(8)=2^3$
3	7	$(57)=3*19$
11	23	$(329554457)=1123*293459$
23	47	$(4561457890013486057)=47*3083*31479823396757$
29	59	$(536650959302196621139601)=59*127540261*71316922984999$
41	83	A
53	107	$B = C$
83	167	$D = E$
89	179	$F = G$

$Q = 1805633,$

$B = 1805632,$

$J = [2^6, 89, 317].$

?- $Q=18489605314740987765913, B$ is $Q-1, \text{factorize}(B, BB), \text{exps}(BB, J).$

$Q = 18489605314740987765913,$

$B = 18489605314740987765912,$

$J = [2^3, 3, 7, 89, 89839, 13764595178129].$

$B = Q - 1$ はどちらも 2×89 を因数に持つ.

第2章 弱弱完全数

2.1 条件を弱める

条件をさらに弱めて, $\varepsilon + 1$ を奇数 ($\varepsilon + 1 = 2$ はあえて付加する) だけにしても次からわかるように 末尾 1 桁が 6 または 8, はやはり成立している.

$\varepsilon + 1$ を奇数とだけ仮定している場合, 弱々しいが完全な数, (弱々完全数; ww-perfect number) と呼んでみたい.

表 2.1: $P = 2$

$2\varepsilon - 1$	$Q = 2^{2\varepsilon-1} - 1$	素因数分解	a : 弱弱完全数
2	3	3	6
3	7	7	28
5	31	31	496
7	127	127	8128
9	511	7*73	130816
11	2047	23*89	2096128
13	8191	8191	33550336
15	32767	7*31*151	536854528
17	131071	131071	8589869056
19	524287	524287	137438691328
21	2097151	$7^2 * 127 * 337$	2199022206976
23	8388607	47*178481	35184367894528
25	33554431	31*601*1801	562949936644096
27	134217727	7*73*262657	9007199187632128
29	536870911	233*1103*2089	144115187807420416
31	2147483647	2147483647	2305843008139952128
33	8589934591	7*23*89*599479	36893488143124135936
35	34359738367	31*71*127*122921	590295810341525782528
37	137438953471	223*616318177	9444732965670570950656
39	549755813887	7*79*8191*121369	151115727451553768931328

弱弱完全数 a の末尾の数は 6, 8, 6, 8, \dots が正確に繰り返され, $Q = 2^{2\varepsilon-1} - 1$ の末尾の数は 最初を飛ばすと 7, 1, 7, 1, \dots となり正確に繰り返されている.

そこで欲を出して $Q = 2^{2^\varepsilon - 1} - 1$ と弱弱完全数 a の下2桁の数を並べてみた.

表 2.2: $P = 2$

$2\varepsilon - 1$	$Q = 2^{2\varepsilon-1} - 1$	素因数分解	Q の下 2 桁	a	a の下 2 桁
3	7	7	7	28	28
5	31	31	31	496	96
7	127	127	27	8128	28
9	511	$7*73$	11	130816	16
11	2047	$23*89$	47	2096128	28
13	8191	8191	91	33550336	36
15	32767	$7*31*151$	67	536854528	28
17	131071	131071	71	8589869056	56
19	524287	524287	87	137438691328	28
21	2097151	$7^2 * 127 * 337$	51	2199022206976	76
23	8388607	$47*178481$	7	35184367894528	28

Q の下 2 桁 の数は 7,31,27,11,47,67,71,87,37,7;(周期は 10)

a の下 2 桁 の数は 28,96,28,16,28,36,28,56,28,76,28;(周期は 10); 28 が 1 つおきに出る.28 は第 2 の完全数.

完全数の下 2 桁 の数を研究した結果はあるようだ.

弱弱完全数と仮定した結果, 下 2 桁 の数の変化の推移が具体的に見えてきた.

指数部分が奇数で等差数列にすぎない. その結果, 下 2 桁の数が周期 10 で正しく変化する.

弱完全数, あるいは真正完全数では, 素数条件がつくため周期性の性質が虫食い状態になり変化の状況が見えづらくなっている.

2.1.1 周期性の証明

以下ではこの周期性の結果を証明する.

$Q = 2^{2^\varepsilon - 1} - 1$ となる Q を $Q_{2^\varepsilon - 1}$ と書き, 弱弱完全数 a を $a_{2^\varepsilon - 1}$ と書くことにする.

$Q_3 = 2^3 - 1 = 7, Q_{23} = 2^{23} - 1$ なので $Q_{23} - Q_3 = 2^{23} - 2^3 = 2^3(2^{20} - 1)$. この数が 100 の倍数であることを確認しよう.

$2^{10} = 1024 \equiv 24 \pmod{100}$ を利用すると $2^{20} \equiv 24^2 = 576 \equiv 76$ により $2^{20} - 1 \equiv 75$.

4 倍すると

$$4(2^{20} - 1) \equiv 300 \equiv 0 \pmod{100}$$

$$Q_{23} - Q_3 = 2^3(2^{20} - 1) \equiv 0 \pmod{100}$$

$20 + 3 = 23$ を一般にして $20m + 3$ を考えると $Q_{20m+3} - Q_3 \equiv 0$. これに 2^{2L} を掛けると

$$Q_{20m+3+2L} - Q_{3+2L} \equiv 0 \pmod{100}.$$

$L = 1, 2, 3, 4$ に応じて $Q_{3+2L} = Q_5 = 2^5 - 1 = 31, Q_7 = 2^7 - 1 = 32 \times 4 - 1 \equiv 17$, と計算した結果,

27, 11, 47, 67, 71, 87, 37, 7.

これから 周期が 10 もわかった.

$\xi = 20m + 3 + 2L$ とおくと

$$Q_\xi \equiv Q_{3+2L} \pmod{100}.$$

$a_\xi = 2^{\xi-1} Q_\xi$ が成り立つ.

$$a_\xi \equiv a_{3+2L} = 2^{2+2L} Q_{3+2L} \pmod{100}.$$

が成り立つことを以下で示す.

$Q_\xi - Q_{3+2L} \equiv 2^{\xi-1} - 2^{2+2L} = (2^{20m} - 1) * 2^{2L+2} \equiv 0 \pmod{100}$ に注意して

$$\begin{aligned} a_\xi - a_{3+2L} &= 2^{\xi-1} Q_\xi - 2^{2+2L} Q_{3+2L} \\ &\equiv 2^{\xi-1} Q_\xi - (Q_{3+2L}) + 2^{\xi-1} - (2^{2+2L}) Q_{3+2L} \\ &\equiv 0. \pmod{100}. \end{aligned}$$

2.1.2 $P = 2$; 弱弱完全数の p, Q, a 変化表 2.3: $P = 2$

$p = 2\varepsilon - 1$	$Q = 2^p - 1$	$a = 2^{p-1}Q$
3	7	28
5	31	96
7	27	28
9	11	16
11	47	28
13	91	36
15	67	28
17	71	56
19	87	28
21	51	76
23	7	28
25	31	96

周期は $(21 - 1)/2 = 10$.

これより完全数の下2桁は, 28,96,16,36,56,76 のどれかになる.

2.2 P を底とする弱弱完全数

一般に P を奇素数とし, $p = e + 1$ が奇数のとき, $q = \frac{P^p - 1}{P}$ に関して $a = p^e q$ を P を底とする弱弱完全数 (ww-perfect number) という.

2.2.1 $P = 3$ 弱弱完全数の表

表 2.4: $P = 3$

$2\varepsilon - 1$	$(3^{2\varepsilon-1} - 1)/2 =$ 素因数分解	a : 弱弱完全数
3	(13)=13	117
5	(121) = 11^2	9801
7	(1093)=1093	796797
9	(9841)= $13 \cdot 757$	64566801
11	(88573)= $23 \cdot 3851$	5230147077
13	(797161)=79716	423644039001
15	(7174453)= $11^2 \cdot 13 \cdot 4561$	34315186290957
17	(64570081)= $1871 \cdot 34511$	2779530261754401
19	(581130733)= $1597 \cdot 363889$	225141952751788437
21	(5230176601)= $13 \cdot 1093 \cdot 368089$	18236498186842001001
23	(47071589413)= $47 \cdot 1001523179$	1477156353259726319517
25	A	B
27	C	D
29	E	F
31	G	H
33	I	J
35	K	L
37	M	N
39	O	P

$$A = (423644304721) = 11^2 \cdot 8951 \cdot 391151$$

$$B = 119649664615167550026801$$

$$C = (3812798742493) = 13 \cdot 109 \cdot 433 \cdot 757 \cdot 8209$$

$$D = 9691622833838739015484197$$

$$E = (34315188682441) = 59 \cdot 28537 \cdot 20381027$$

$$F = 785021449541029367424039801$$

$$G = 308836698141973 = 683 \cdot 102673 \cdot 4404047$$

$$H = 63586737412824202325875602477$$

$$I = 2779530283277761 = 13 \cdot 23 \cdot 3851 \cdot 2413941289$$

$$J = 5150525730438767800476679208001$$

$$K = 25015772549499853 = 11^2 * 71 * 1093 * 2664097031$$

$$L = 417192584165540258547337814514357$$

$$M = 225141952945498681 = 13097927 * 17189128703$$

$$N = 33792599317408761542712904163659401$$

$$O = 2026277576509488133 = 13^2 * 313 * 6553 * 7333 * 797161$$

$$P = 2737200544710109690363152107948379837$$

弱弱完全数の Q 下 2 桁 と a 下 2 桁 を書き出した.

表 2.5: $P = 3$

$2\varepsilon - 1$	$Q = (3^{2\varepsilon-1} - 1)/2$	Q の素因数分解	a : 弱弱完全数	Q 下 2 桁	a 下 2 桁
3	13	13	117	13	17
5	121	11^2	9801	21	1
7	1093	1093	796797	93	97
9	9841	$13*757$	64566801	41	1
11	88573	$23*3851$	5230147077	73	77
13	797161	79716	423644039001	61	1
15	7174453	$11^2 * 13 * 4561$	34315186290957	53	57
17	64570081	$1871*34511$	A	81	1
19	581130733	$1597*363889$	B	33	37
21	5230176601	$13*1093*368089$	C	1	1
23	47071589413	$47*1001523179$	D	13	17
25	423644304721	$11^2 * 8951 * 391151$	E	21	1
27	3812798742493	$13*109*433*757*8209$	F	93	97
29	34315188682441	$59*28537*20381027$	G	41	1

$$A = 2779530261754401$$

$$B = 225141952751788437$$

$$C = 18236498186842001001$$

$$D = 1477156353259726319517$$

$$E = 119649664615167550026801$$

$$F = 9691622833838739015484197$$

$$G = 785021449541029367424039801$$

2.3 $P = 3$; 弱弱完全数の p, Q, a 変化表 2.6: $P = 3$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	13	17
5	21	1
7	93	97
9	41	1
11	73	77
13	61	1
15	53	57
17	81	1
19	33	37
21	1	1
23*	13	17
25	21	1

周期は $(21 - 1)/2 = 10$.

$3^5 = 243, 43^4 = 3418801$ より

$$3^5 \equiv 43 \pmod{200}, 43^4 - 1 \equiv 0 \pmod{200}.$$

よって $3^{20} - 1 \equiv 0 \pmod{200}$.

$$\frac{3^{20} - 1}{2} \equiv 0 \pmod{100}.$$

2.3.1 $P = 5$ の弱弱完全数の p, Q, a 変化表 2.7: $P = 5$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
5	81	25
7	31	75
9	81	25

周期は 2

2.3.2 $P = 7$; 弱弱完全数の p, Q, a 変化表 2.8: $P = 7$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	57	93
5	1	1
7	57	93

2.3.3 $P = 11$; 弱弱完全数の p, Q, a 変化表 2.9: $P = 11$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	33	93
5	5	5
7	17	37
9	69	89
11	61	61
13	93	53
15	65	65
17	77	97
19	29	49
21	21	21
23	53	13
25	25	25
27	37	57
29	89	9
31	81	81
33	13	73
35	85	85
37	97	17
39	49	69
41	41	41
43	73	33
45	45	45
47	57	77
49	9	29
51	1	1
53 *	33	93
55	5	5

周期は $(53 - 3)/2 = 25$

$$A = 11^{10} = 25937424601, B = 4601^5 = 2061869461571623001.$$

これより

$$11^{50} - 1 \equiv 0 \pmod{1000}.$$

$$\frac{11^{50} - 1}{10} \equiv 0 \pmod{100}.$$

2.3.4 $P = 11$ 弱弱完全数の表

表 2.10: $P = 11$

$2e + 1$	$(11^{2e+1} - 1)/10$	分解	a
3	133	$7 \cdot 19$	16093
5	16105	$5 \cdot 3221$	235793305
7	1948717	$43 \cdot 45319$	3452271037237
9	235794769	$7 \cdot 19 \cdot 1772893$	U
11	28531167061	$15797 \cdot 1806113$	V
13	3452271214393	$1093 \cdot 3158528101$	W
15	417724816941565	$5 \cdot 7 \cdot 19 \cdot 3221 \cdot 195019441$	X
17	50544702849929377	50544702849929377	Y
19	6115909044841454629	6115909044841454629	Z
21	740024994425816010121	A	B
23	89543024325523737224653	C	D
25	10834705943388372204183025	E	F
27	1310999419149993036706146037	G	H

$$U = 50544702828493489$$

$$V = 740024994423222267661$$

$$W = 10834705943388058361345353$$

$$X = 158630929717149119466460312165$$

$$Y = 2322515441988780809505203793273697$$

$$Z = 34003948586157739898684696499226975549$$

$$A = 7^2 \cdot 19 \cdot 43 \cdot 1723 \cdot 8527 \cdot 27763 \cdot 45319$$

$$B = 497851811249935469864715641384372869123321$$

$$C = 829 \cdot 28878847 \cdot 3740221981231$$

$$D = 7289048368510305214290278538501245253967902613$$

$$E = 5^2 \cdot 3001 \cdot 3221 \cdot 24151 \cdot 1856458657451$$

$$F = 106718957163359378642424086278988841454677198699025$$

$$G = 7 \cdot 19 \cdot 1772893 \cdot 5559917315850179173$$

$$H = 1562472251828744662703731061512487473010580175674018157$$

2.3.5 $P = 13$; 弱弱完全数の p, Q, a 変化表 2.11: $P = 13$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	83	27
5	41	1
7	43	87
9	81	1
11	3	47
13	21	1
15	63	7
17	61	1
19	23	67
21	1	1
23*	83	27

周期は $(23 - 3)/2 = 10$

2.3.6 $P = 13$ のときの弱弱完全数表 2.12: $P = 13$

$2e + 1$	$Q = (13^{2e+1} - 1)/12$	分解	a
3	183	$3 \cdot 61$	30927
5	30941	30941	883705901
7	5229043	5229043	25239591813787
9	883708281	A	B
11	149346699503	C	D
13	25239592216021	E	F
15	4265491084507563	G	H
17	720867993281778161	I	J
19	121826690864620509223	K	L
21	20588710756120866058701	M	N
23	3479492117784426363920483	O	P
25	588034167905568055502561641	Q	R
27	9937774376041001379932917343	S	T
29	16794843869550929233208663030981	U	V
31	2838328613954107040412264052235803	W	X
33	479677535758244089829672624827850721	Y	Z

$$A = 3^2 * 61 * 1609669$$

$$B = 720867993213800601$$

$$C = 23 * 419 * 859 * 18041$$

$$D = 20588710756109377851047$$

$$E = 53 * 264031 * 1803647$$

$$F = 588034167905566113995468101$$

$$G = 3 * 61 * 4651 * 30941 * 161971$$

$$H = 16794843869550928905093964222707$$

$$I = 103 * 443 * 15798461357509$$

$$J = 479677535758244089774221240729252401$$

$$K = 12865927 * 9468940004449$$

$$L = 13700070098791209449615908553795581328767$$

$$M = 3 * 43 * 61 * 337 * 547 * 2714377 * 5229043$$

$$N = 391287702091575733090746033697803929523057501$$

$$O = 1381 * 2519545342349331183143$$

$$P = 11175568059437494512804842434187269399079517489227$$

$$Q = 701 * 9851 * 30941 * 2752135920929651$$

$$R = 319185399345594280780219112362033386548297277812147401$$

$$S = 3^3 * 61 * 650971 * 1609669 * 57583418699431$$

$$T = 9116254190709518253363838069456302175911679184810336544087$$

$$U = 1973 * 2843 * 3539 * 846041103974872866961$$

$$V = 260369335940854550834324579101958487505450742744381795527146101$$

$$W = 311 * 1117 * 8170509011431363408568150369$$

$$X = 7436408603806746826379144303731073041582189762751733789770879453347$$

$$Y = 3 * 23 * 61 * 419 * 859 * 18041 * 17551032119981679046729$$

$$Z = 212391266133324496108214740458863183339538614689722045030030778150037601$$

2 ?- A is $(13^{20}-1)/12$.

$$A = 1583746981240066619900$$

2.3.7 $P = 17$; 弱弱完全数の p, Q, a 変化表 2.13: $P = 17$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	7	23
5	41	61
7	67	23
9	81	21
11	27	23
13	21	81
15	87	23
17	61	41
19	47	23
21	1	1
23*	7	23

周期は $(23 - 3)/2 = 10$

2.3.8 $P = 19$; 弱弱完全数の p, Q, a 変化表 2.14: $P = 3$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	81	41
5	61	81
7	41	21
9	21	61
11	1	1
13	81	41
15	61	81
17	41	21
19	21	61
21	1	1
23*	81	41

周期は $(23 - 3)/2 = 10$

2.3.9 $P = 23$; 弱弱完全数の p, Q, a 変化表 2.15: $P = 23$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	53	37
5	61	1
7	93	77
9	21	1
11	33	17
13	81	1
15	73	57
17	41	1
19	13	97
21	1	1
23	53	37

周期は $(23 - 3)/2 = 10$

2.3.10 $P = 31$; 弱弱完全数の p, Q, a 変化表 2.16: $P = 31$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	93	73
5	5	5
7	37	97
9	89	49
11	61	61
13	53	33
15	65	65
17	97	57
19	49	9
21	21	21
23	13	93
25	25	25
27	57	17
29	9	69
31	81	81
33	73	53
35	85	85
37	17	77
39	69	29
41	41	41
43	33	13
45	45	45
47	77	37
49	29	89
51	1	1
53*	93	73

周期は $(53 - 3)/2 = 25$

2.3.11 $P = 37$; 弱弱完全数の p, Q, a 変化表 2.17: $P = 37$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	7	83
5	21	81
7	87	83
9	41	61
11	67	83
13	61	41
15	47	83
17	81	21
19	27	83
21	1	1
23*	7	83
25	21	81

周期は $(23 - 3)/10$

2.3.12 $P = 41$; 弱弱完全数の p, Q, a 変化

$P = 41$ のとき弱弱完全数の周期は 50. 本当だろうか.

表 2.18: $P = 41$ 前半分

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	23	63
5	5	5
7	47	27
9	49	29
11	11	11
13	33	73
15	15	15
17	57	37
19	59	39
21	21	21
23	43	83
25	25	25
27	67	47
29	69	49
31	31	31
33	53	93
35	35	35
37	77	57
39	79	59
41	41	41
43	63	3
45	45	45

周期は $(103 - 3)/2 = 50$

表 2.19: $P = 41$ 後半分

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
47	87	67
49	89	69
51	51	51
53	73	13
55	55	55
57	97	77
59	99	79
61	61	61
63	83	23
65	65	65
67	7	87
69	9	89
71	71	71
73	93	33
75	75	75
77	17	97
79	19	99
81	81	81
83	3	43
85	85	85
87	27	7
89	29	9
91	91	91
93	13	53
95	95	95
97	37	17
99	39	19
101	1	1
103*	23	63
105	5	5

2.3.13 $P = 43$; 弱弱完全数の p, Q, a 変化

表 2.20: $P = 43$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	93	57
5	1	1

2.4 弱弱完全数の周期

$p = 2\varepsilon - 1$ を奇数として, $Q = N_p = \frac{P^p - 1}{P}$, $a = P^{p-1}Q$ とおく. 周期を T とおくと, p に $2T$ を加えても法を 100 として Q が不変であればよい. 周期なので不変にする T の中で最小を選ぶ. 100 を一般化して H とおき $M = \bar{P} \times H$ とする.

$$N_{p+2T} = \frac{P^{p+2T} - 1}{P} \equiv N_p = \frac{P^p - 1}{P} \pmod{H}$$

により

$$P^p - 1 \equiv P^{p+2T} - 1 \pmod{M}.$$

故に $P^p(P^{2T} - 1) \equiv 0 \pmod{M}$.

ここで, P と M は互いに素, とする. $H = 100$ なら $P \neq 2, 5$ なので妥当であろう. $H = 10, 100, 1000$ のときを主に扱うが, $P = 2, P = 5$ は別扱いする.

2.4.1 $P = 5$ のときの周期

$P = 5$ のとき $\bar{P} = 4, M = 4H$ になり, $H = 400$ のとき $5^p(P^{2T} - 1) \equiv 0 \pmod{400}$. $l = 2, p = 3$ のとき

$$5(5^{2T} - 1) \equiv 0 \pmod{16}$$

これより

$$5^2 \equiv 9, 5^4 \equiv 81 \equiv 1 \pmod{16}$$

したがって, $T = 2$.

2.4.2 周期の計算

一般に $H = 100$ について $M = \overline{P} \times H$ とする.

$P^{2T} \equiv 1 \pmod{M}$ を満たす最小の T をパソコンで計算する.

表 2.21: 弱弱完全数の周期 1

p	周期	周期の順	素数
3	10	1	199
7	2	2	7
11	25	2	43
13	10	2	107
17	10	2	149
19	5	2	157
23	10	2	193
29	10	2	257
31	25	2	293
37	10	5	19
41	50	5	59
43	2	5	79
47	10	5	139
53	10	5	179
59	5	5	239
61	50	10	3
67	10	10	13
71	25	10	17
73	10	10	23
79	5	10	29
83	10	10	37
89	10	10	47
97	10	10	53

表 2.22: 弱弱完全数の周期 2

p	周期	周期の順	素数
101	50	10	67
103	10	10	73
107	2	10	83
109	10	10	89
113	10	10	97
127	10	10	103
131	25	10	109
137	10	10	113
139	5	10	127
149	2	10	137
151	25	10	163
157	2	10	167
163	10	10	173
167	10	10	197
173	10	10	223
179	5	10	227
181	50	10	229

表 2.23: 弱弱完全数の周期 3

p	周期	周期の順	素数
191	25	10	233
193	2	10	263
197	10	10	269
199	1	10	277
211	25	10	283
223	10	25	11
227	10	25	31
229	10	25	71
233	10	25	131
239	5	25	151
241	50	25	191
251	25	25	211
257	2	25	251
263	10	25	271
269	10	50	41
271	25	50	61
277	10	50	101
281	50	50	181
283	10	50	241
293	2	50	281

2.4.3 下3桁

下3桁 すなわち $H = 1000, M = (P - 1)H$ を法として周期を求めてみた.

表 2.24:

p 素数	周期
3	50
7	10
11	250
13	100
17	100
19	50
23	50
29	100
31	125
37	100
41	500
43	10
47	50
53	100
59	50
61	500
67	50
71	125
73	100
79	25
83	50
89	100
97	100

2.4.4 $P = 7$ のときの弱弱完全数

$P = 7$ のとき周期が 10 なのでこの場合に数表を求めてみた.

表 2.25: $P = 7$; 弱弱完全数

$p = 2\varepsilon + 1$	$Q = (7^{2\varepsilon+1} - 1)/6$	素因数分解	a
3	(57)	$3 \cdot 19$	2793
5	(2801)	2801	6725201
7	(137257)	$29 \cdot 4733$	16148148793
9	(6725601)	$3^2 \cdot 19 \cdot 37 \cdot 1063$	38771751370401
11	(329554457)	$1123 \cdot 293459$	93090977300134793
13	(16148168401)	A	B
15	(791260251657)	C	D
17	(38771752331201)	E	F
19	(1899815864228857)	G	H
21	(93090977347214001)	I	J
23	(4561457890013486057)	K	L
25	(223511436610660816801)	M	N

$$A = 16148168401$$

$$B = 223511436608353935601$$

$$C = 3 \cdot 19 \cdot 31 \cdot 2801 \cdot 159871$$

$$D = 536650959302083583960793$$

$$E = 14009 \cdot 2767631689$$

$$F = 1288498953284568548534420801$$

$$G = 419 \cdot 4534166740403$$

$$H = 3093685986836262112339927626793$$

$$I = 3 \cdot 19 \cdot 29 \cdot 4733 \cdot 11898664849$$

$$J = 7427940054393865970066296612826001$$

$$K = 47 \cdot 3083 \cdot 31479823396757$$

$$L = 17834484070599672225407746556059132793$$

$$M = 2551 \cdot 2801 \cdot 31280679788951$$

$$N = 42820596253509813014736649332142509151201$$

この表から

$$p = 3, Q \text{ の下 3 桁} = 057, a \text{ の下 3 桁} = 793,$$

$$p = 5, Q \text{ の下 3 桁} = 801, a \text{ の下 3 桁} = 201,$$

$$p = 23, Q \text{ の下 3 桁} = 057, a \text{ の下 3 桁} = 793,$$

$$p = 25, Q \text{ の下 3 桁} = 801, a \text{ の下 3 桁} = 201,$$

したがって 周期は $23 - 3 = 10$.

第3章 Wieferich の素数とその一般化

3.1 Wieferich の素数の定義

奇素数 p に対して $2^{p-1} - 1$ は p の倍数になるという主張がフェルマの小定理である。

$2^{p-1} - 1$ が p^2 の倍数になる場合の素数 p を Wieferich の素数¹ という。

Wieferich の素数は希少価値のある素数とされている。実例は2つだけで 1093,3511.(3番目の Wieferich の素数はあるとすると 3×10^{17} より大きい)

abc-予想が解けると Wieferich の素数にならない素数は無限にあることが分かるそうである。望月新一さんによって abc-予想が示された現在, 非 Wieferich 素数は無限にあることが分かった。

Wieferich 素数は2個しか見つからない現在, 非 Wieferich 素数は無限にあることは肯定しやすい結果と言ってよい。

ここでは $2^{\frac{p-1}{2}} - 1$ が p^2 の倍数になる場合の素数 p を 強い意味での Wieferich の素数という。
計算機での実行例:

```
?- wieferich_loop3(2,1=<20000).
wieferich = 1093
wieferich = 3511
```

これは Wieferich の素数 は 1093,3511.

```
?- wieferich_loop2(2,1=<20000).
wieferich2 = 3511
```

強い意味での Wieferich の素数は 3511.

3.1.1 Wieferich の素数と完全数の関係

完全数については多くの難問があるが「 p :素数のときメルセンヌ数 $2^p - 1$ には平方因子があるか。」という問題があり, たぶん無いと想像されている。

素数 p に対して $2^p - 1$ が素数の平方 Q^2 で割れるとき

$$2^p - 1 \equiv 0 \pmod{Q^2}$$

Fermat によれば $2^{Q-1} - 1 \equiv 0 \pmod{Q}$ なので $Q - 1 = pk$. Q, p は奇数なので k は偶数.
 $k = 2k'$.

¹Arthur Wieferich in 1909

これより

$2^{\frac{Q-1}{2}} - 1 = 2^p K' - 1 \equiv 0 \pmod{Q^2}$ なので Q は強い意味での Wieferich の素数になる.

ここに希少価値の高い強い意味での Wieferich の素数が出てきたことに感動を覚える. 強い意味での Wieferich の素数は $Q = 3511$ ただ1つ, しか発見されていない.

$Q = 3511$ に対して $Q - 1 = 2pk'$ によって p が定まる.

$3511 - 1 = 3510$ の素因数分解は $2 * 3^3 * 5 * 13$.

$p = 5$ または 13 .

$$p = 5, 2^p - 1 = 31, p = 13, 2^p - 1 = 8191.$$

これらはともに素数. したがって平方因子を持たない.

$1093 - 1 = 1092$ の素因数分解は $2^2 * 3 * 7 * 13$.

$$p = 3, 2^p - 1 = 7, p = 7, 2^p - 1 = 127.$$

3.1.2 P を底とする弱完全数

ここで, 奇素数 P を底とする弱完全数に戻る.

$P = 3$ の数表を見ると2番目, $p = 5$ に堂々と平方数 $N_p = 121 = 11^2$ が出ている.

表 3.1: $p = e + 1, N_p = (3^p - 1)/2$:素数

e	3^e =素因数分解	N_p	N_p の素因数分解
2	$3^2 = 9$	13	[13]
4	$3^4 = 81$	121	[11^2]
6	$3^6 = 729$	1093	[1093]

第3番目の数 $\frac{3^7-1}{2} = 1093$ は Wieferich の素数である. 何という偶然であろうか.

これはうれしい結果である. 次に底をいろいろ変えて N_p が平方因子を持つ場合を探してみよう.

3.2 奇素数 P を底とする Wieferich 素数

奇素数 P に対して P と相異なる素数 Q は $P^{Q-1} - 1$ が Q^2 の倍数になる場合素数 Q を P を底とする Wieferich 素数という.

奇素数 Q は $P^{\frac{Q-1}{2}} - 1$ が Q^2 の倍数になる場合 P を底とする 強い意味の Wieferich 素数という.

3.2.1 $Q = 2$ の場合

底が奇素数 P なので $Q = 2$ もある.

$P - 1$ が 4 の倍数になる場合すなわち $P \equiv 1 \pmod{4}$ のとき 2 が P を底とする Wieferich の素数になる.

しかしこのとき 奇素数 p について N_p は 4 を平方因子に持たない. これを以下で証明する.

p : 奇素数のとき, 各 k について $P^k \equiv 1 \pmod{4}$ によって

$$N_p = (P^p - 1)/\overline{P} = 1 + P + \cdots + P^{p-1} \equiv p \pmod{4}.$$

ゆえに N_p は 4 を平方因子に持たない.

一方, $p = 2$ ならば, $P \equiv 1 \pmod{4}$ のとき

$$N_2 = 1 + P \equiv 2 \pmod{4}.$$

ゆえに N_2 は 4 を平方因子に持たない.

$P \equiv 3 \pmod{4}$ のとき, N_2 が 4 を平方因子に持つ例は次の通りでたくさんある.

表 3.2: $p = 2, Q = 2, P = 3 + 4k$

P	$N_2 = P + 1$ の素因数分解
3	$[2^2]$
7	$[2^3]$
11	$[2^2, 3]$
19	$[2^2, 5]$
23	$[2^3, 3]$
31	$[2^5]$
43	$[2^2, 11]$
47	$[2^4, 3]$
59	$[2^2, 3, 5]$
67	$[2^2, 17]$
71	$[2^3, 3^2]$
79	$[2^4, 5]$
83	$[2^2, 3, 7]$
103	$[2^3, 13]$
107	$[2^2, 3^3]$
127	$[2^7]$
131	$[2^2, 3, 11]$
139	$[2^2, 5, 7]$
151	$[2^3, 19]$
163	$[2^2, 41]$
167	$[2^3, 3, 7]$
179	$[2^2, 3^2, 5]$
191	$[2^6, 3]$
199	$[2^3, 5^2]$

3.2.2 一般の弱完全数と Wieferich の素数

奇素数 P を底にする弱完全数において $p = e + 1$ が素数のとき, $N_p = \frac{P^p - 1}{P}$ が素数の平方 Q^2 を因子として持つとする. このとき

$$P^p \equiv 1 \pmod{Q^2}.$$

1) $P \equiv 1 \pmod{Q}$ でないなら, Q を法として, P の位数は p . 一方, $P \neq Q$ なのでフェルマの小定理により

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

$Q \geq 3, p \geq 3$ のとき $Q - 1 = 2pL$ と整数 L を用いて書ける. よって

$$P^{\frac{Q-1}{2}} = P^{pL} \equiv 1 \pmod{Q^2}.$$

したがって、素数 Q は底が P の強い意味での Wieferich の素数になる。

$p \geq 3$ を仮定しているので、 $Q = 1 + 2pL \geq 7$. $Q - 1 = 2pL \geq 2p$ により $Q - 1$ の奇数素因子 p について $N_p = \frac{P^p - 1}{P}$ の素因数分解を行い、 Q^2 が因数になるものを探索すればよい。

これは簡単にはできないので後で組織的に行う。

2) p が偶数なら $p = 2$. $Q = 1 + 2k$.

たとえば $k = 1, 2, 3, 5, 6$ に応じて $Q = 3, 5, 7, 11, 13$

$N_2 = 1 + P$ なのでこれが Q^2 で割れる場合を以下、列挙する。平方因子を含む場合がこのように簡単に得られる。

3.2.3 平方因子を含む例

表 3.3: $P = -1 + 9N$

P	$N_2 = P + 1$ の素因数分解
17	$[2, 3^2]$
53	$[2, 3^3]$
71	$[2^3, 3^2]$
89	$[2, 3^2, 5]$
107	$[2^2, 3^3]$
179	$[2^2, 3^2, 5]$
197	$[2, 3^2, 11]$

表 3.4: $P = -1 + 5^2N$

P	$N_2 = P + 1$ の素因数分解
149	$[2, 3, 5^2]$
199	$[2^3, 5^2]$
349	$[2, 5^2, 7]$
449	$[2, 3^2, 5^2]$
499	$[2^2, 5^3]$
599	$[2^3, 3, 5^2]$

表 3.5: $P = -1 + 7^2N$

P	$N_2 = P + 1$ の素因数分解
97	$[2, 7^2]$
293	$[2, 3, 7^2]$
587	$[2^2, 3, 7^2]$
881	$[2, 3^2, 7^2]$

表 3.6: $P = -1 + 11^2N$

P	$N_2 = P + 1$ の素因数分解
241	$[2, 11^2]$
967	$[2^3, 11^2]$

表 3.7: $P = -1 + 13^2N$

P	$N_2 = P + 1$ の素因数分解
337	$[2, 13^2]$
1013	$[2, 3, 13^2]$

3.2.4 $Q = 2$ の例3) $Q = 2, p \geq 3, P \equiv 1 \pmod{4}$ のとき

$$N_p = (P^p - 1)/\overline{P} = 1 + P + \cdots + P^{p-1} \equiv p \not\equiv 0 \pmod{4}.$$

 $Q = 2, p \geq 3, P \equiv -1 \pmod{4}$ のとき

$$N_p = (P^p - 1)/\overline{P} = 1 + P + \cdots + P^{p-1} \equiv 1 \not\equiv 0 \pmod{4}.$$

ともに N_p は 4 で割れない。したがって、 $Q = 2$ ならば $p = 2$ になる。4) $Q = 2, p = 2, P \equiv 1 \pmod{4}$ のとき

$$N_2 = P + 1 \equiv 2 \pmod{4}.$$

 N_2 は平方因子 4 を持たない。 $p = 2, P \equiv -1 \pmod{4}$ のとき ($P = 3, 7, 11, 19, 23, 31, 43, \dots$)

$$N_2 = P + 1 \equiv 0 \pmod{4}.$$

 N_2 は平方因子 4 を持つ。5) $P \equiv 1 \pmod{Q}$ なら、各 j につき $P^j \equiv 1 \pmod{Q}$ により

$$N_p = 1 + P + \cdots + P^{p-1} \equiv p \pmod{Q}.$$

 $N_p \equiv 0 \pmod{Q^2}$ によると $p \equiv 0 \pmod{Q}$ が成り立つので $p = Q$. $P = 1 + Qk$ とおくと

$$P^j = 1 + Qkj + \cdots \equiv 1 + Qkj \pmod{Q^2}.$$

$$N_p = 1 + P + \cdots + P^{p-1} \equiv p + \frac{p(p-1)}{2} \times Qk \equiv p = Q \pmod{Q^2}.$$

このとき $N_p \equiv 0 \pmod{Q^2}$ に矛盾。よってこの場合は起きない。

3.2.5 (強い意味で)Wieferich の素数の計算

底が P の (強い意味で)Wieferich の素数も希少価値がありそうなのでこれらをコンピュータで探してみよう.

P, Q が 20 を越えると $P^{\frac{Q-1}{2}} - 1$ の計算は大変で, うっかりコンピュータを信じて, $P^{\frac{Q-1}{2}} - 1$ の素因数分解を実行すると誤差が累積して誤った結果が出るかもしれない.

ここでは, $P^{\frac{Q-1}{2}} - 1$ が Q^2 の整数倍かどうかの問題なので累乗の計算を 2 つの積の計算に置き換え, かつ積の計算を Q^2 を法として行う.

表 3.8: 強い意味の Wieferich 素数 Q の例, $Q \geq 7$

P	prime	prime
P=3	prime = 11	
P=19	prime = 137	
P=23	prime = 13	
P=31	prime = 79	
P=53	prime = 47	prime = 59
P=67	prime = 7	
P=71	prime = 47	prime = 331
P=79	prime = 7	
P=137	prime = 59	
P=179	prime = 17	
P=181	prime = 3	prime = 101
P=191	prime = 13	
P=197	prime = 7	
P=199	prime = 5	

この表にある P に対して $prime = Q$ で与えられる Q に関して, 奇素数 p なら, $Q - 1 = 2pL$ 満たす. $Q - 1$ の素因子 p について $N_p = \frac{P^p - 1}{P}$ の因数分解を行い, Q^2 が因数になるものを探索する.

3.2.6 プログラム

次のプログラムで実行した結果を以下に書く.

```
wief(P,Q,P0,PP):- Q2 is Q*Q,
power(PP=P^P0 mod Q2),
write(PP=P^P0),put(9),
write(mod=Q2),put(9),
( PP=1 -> write(PP=ok); write(no)),
nl.
wief2(P,Q):- P0 is (Q-1)//2,
P0 >=2,
for(2=<P0,PW),
factorize(PW,PW0),
PW0=[PP],
write(prime=PP),put(9),
wief(P,Q,PP,PP),
```



```
fail.
wief2(P,Q):-!.
```

実行例

```
8 ?- wief2(23,13).
prime=2 22=23^2 (mod)=169      no
prime=3 168=23^3      (mod)=169      no
prime=5 147=23^5      (mod)=169      no

9 ?- wief2(53,47).
prime=2 600=53^2      (mod)=2209      no
prime=3 874=53^3      (mod)=2209      no
prime=5 867=53^5      (mod)=2209      no
prime=7 1085=53^7     (mod)=2209      no
prime=11 202=53^11    (mod)=2209      no
prime=13 1914=53^13   (mod)=2209      no
prime=17 2093=53^17   (mod)=2209      no
prime=19 1088=53^19   (mod)=2209      no
prime=23 1=53^23 (mod)=2209      1=ok
```

$P = 53, Q = 47, p = 23$ が見つけられた. さらに計算を続けて次の結果をえた.

表 3.9: Q^2 が N_p の因数

P	Q	p
3	11	5
53	47	23
71	47	23
79	7	3
101	5	2
137	59	29
149	5	2
151	5	2
197	7	3
199	5	2

3.2.7 参考

強い意味の Wieferich 素数 Q はあまりない.

表 3.10: 強い意味の Wieferich 素数 Q の例 ; Q : 500 から 8000 まで

P	prime = Q
P=31	prime = 6451
P=59	prime = 2777
P=71	prime = 331
P=83	prime = 4871
P=173	prime = 3079
P=197	prime = 653

3.2.8 一般の Wieferich 素数

表 3.11: 一般の Wieferich 素数の例

P	prime=Q				
P=3	prime = 11				
P=7	prime = 5				
P=11	prime = 71				
P=13	prime = 863				
P=17	prime = 3				
P=19	prime = 3	prime = 7	prime = 13	prime = 43	prime = 137
P=23	prime = 13				
P=31	prime = 7	prime = 79			
P=37	prime = 3				
P=41	prime = 29				
P=43	prime = 5	prime = 103			
P=53	prime = 3	prime = 47	prime = 59	prime = 97	
P=67	prime = 7	prime = 47			
P=71	prime = 3	prime = 47	prime = 331		
P=73	prime = 3				
P=79	prime = 7	prime = 263			
P=89	prime = 3	prime = 13			
P=97	prime = 7				
P=101	prime = 5				
P=107	prime = 3	prime = 5	prime = 97		
P=109	prime = 3				
P=127	prime = 3	prime = 19	prime = 907		
P=131	prime = 17				
P=137	prime = 29	prime = 59			
P=149	prime = 5				
P=151	prime = 5				
P=157	prime = 5				

私は当初、強い意味の Wieferich 素数は本来の Wieferich 素数よりはるかに少ないと予想した。
 $P = 2$ のときは 3511 のみが強い意味の Wieferich 素数だった。半分は強い意味の Wieferich 素数であるとは意外だった。

3.3 平方因子をもつ弱完全数の例

平方因子をもつ弱完全数の例

3.3.1 $P = 53$

表 3.12: $P = 53$

p	$(2p+1)=$	$N_p =$ 分解	a
2	(5)=5	(54)= $2 \cdot 3^3$	2862
3	(7)=7	(2863)= $7 \cdot 409$	8042167
5	(11)=11	(8042221)= $11 \cdot 131 \cdot 5581$	63456991998301
7	(15)= $3 \cdot 5$	(22590598843)= $29 \cdot 778986167$	500706190876621573747
11	(23)=23	(178250690949465223)= 178250690949465223	31173812431056824238751548578194927
13	(27)= 3^3	A	B
17	(35)= $5 \cdot 7$	C	D
19	(39)= $3 \cdot 13$	E	F
23	(47)=47	G	H

$$A = (500706190877047811461) = 13 \cdot 3297113 \cdot 11681692691969$$

$$B = 245976374684817681602736538606687298140501$$

$$C = (3950812685697719092424754481) = 647 \cdot 4013 \cdot 12479 \cdot 121936356626073149$$

$$D = 15314412936385684029826954552174353350696783028210620401$$

$$E = (11097832834124892930621135337183) = 229 \cdot 32688470798197 \cdot 1482545708952391$$

$$F = 120838084300705448509353018182383219548095580591429385933186087$$

$$G = (87567239118838619296100386576471206763) = 47^2 \cdot 4969 \cdot 21529 \cdot 16055056483 \cdot 23080289344401529$$

$$H = 7523341718463863201525775016855522659535920597794835286613930378332647396067$$

$p = 2$ において $N_2 = 54 + 1 = 2 \cdot 3^3$ ここに平方因子 3^2 ,

G に 47^2 という平方因子があり, $47 = 2p + 1$.

$p = 29$ まですると 59^2 という平方因子がありえるが wxmaxima の能力を超えた.

3.3.2 $P = 71$ 表 3.13: $P = 71$

2	(5)=5	(72)= $2^3 * 3^2$	5112
3	(7)=7	(5113)=5113	25774633
5	(11)=11	(25774705)= $5*11*211*2221$	654978581329105
7	(15)= $3*5$	(129930287977)= $7*883*21020917$	16644106779790992717817
11	(23)=23	(3301747030310022361)= $23*143554218709131407$	10747990727482727047368690334263535561
13	(27)= 3^3	A	B
17	(35)= $5*7$	C	D
19	(39)= $3*13$	E	F
23	(47)=47	G	H

$$A = (16644106779792822721873) = 3202878953 * 5196608121641$$

$$B = 273124511757748992738986545319414474009953393$$

$$C = (422954732018032457097788761537) = 239 * 3652120847 * 484563667343825089$$

$$D = 176371117937340781806990224586174626005792843120041060998977$$

$$E = (2132114804102901616229953146908089) = 1900857799450121 * 1121659287043817009$$

$$F = 4481886586637081935569839157302377956474817214183976021737973255529$$

$$G = (54180621257240427046019992014174494350633) = 47^2 * 242329 * 101214532738371118365636938570353$$

$$H = 2894194089963906004849054026497654260619806809292930186226138112926209752659428153$$

$p = 2$ において $N_2 = 2^3 * 3^2$ が 2 つの平方因子 $2^2, 3^2$ を持っている.

$p = 23$ において G に 47^2 という平方因子がある. $47 = 2 * 23 + 1$.

3.3.3 $P = 79$ 表 3.14: $P = 79$

p	$(2p+1)=$	$N_p =$ 分解	a
2	(5)=5	(80) = $2^4 * 5$	6320
3	(7)=7	(6321) = $3 * 7^2 * 43$	39449361
5	(11)=11	(39449441)=39449441	1536558922354721
7	(15)= $3*5$	(246203961361)= $281*337*1289*2017$	59849094506436090124081

$p = 3$ において 7^2 という平方因子がある. $7 = 2 * 3 + 1$.

3.3.4 $P = 137$

表 3.15: $P = 137$

p	$(2p + 1) =$	$N_p =$ 分解	a
2	(5)=5	(138)=2*3*23	18906
3	(7)=7	(18907)=7*37*73	354865483
5	(11)=11	(354865621)=11*101*319411	125010414744264181
7	(15)=3*5	(6660472840687)=8933*745603139	44038088983707823203728383
11	(23)=23	A	B
13	(27) = 3 ³	C	D
17	(35)=5*7	E	F
19	(39)=3*13	G	H
23	(47)=47	I	J
29	(59)=59	K	L

$A=(2346320474383711003267)=2346320474383711003267$

$B= 5465035682610653717879961178365556122821683$

$C = (44038088983707871820318461) = 864319 * 19805293 * 2572605139183$

$D= 1925197417969549460912161511671456536120639693634141$

$E = (15513533694485813664044412986329681) = 17*103*8859813646194068340402291825431$

$F= 238913014349144128571410485112685260256845095745917501392062668019921$

$G=(291173513911804236660449587340421782827)=291173513911804236660449587340421782827$

$H= 84163168377442927933524042922256325776247704876773687945116498292399482547483$

$I = (102573254726919359630889312802648113437647615807)$

$= 1381 * 143235060131 * 518550578298278365204966204101137$

$J = 104444749751619994641076050602515305522087006896962812$

$- - 24738478203470769145406043274426557803983$

$K = (678199615411490923350187085927605536880232074954687758366541)$

$= 59^2 * 616367 * 316092460536539293043853391060042444716569284439483$

$L = 456597384633751903346547654483[60digits]475472486261488580834605020461$

$p = 23$ で $K = 59^2 * 616367 * 316092460536539293043853391060042444716569284439483$

平方因子 59^2 .

3.3.5 $P = 197$

表 3.16: $P = 197$

p	$(2p+1)=$	$N_p =$ 分解	a
2	(5)=5	(198)= $2 * 3^2 * 11$	39006
3	(7)=7	(39007)= $19*2053$	1513822663
5	(11)=11	(1513822861)= $661*991*2311$	2280026864369614141
7	(15)= $3*5$	(58749951412747)= $7*29*97847*2957767$	3434036198152417107087067363

$p = 2$ で 平方因子 3^2 .

3.3.6 $P = 199$

表 3.17: $P = 199$

p	$(2p+1)=$	$N_p =$ 分解	a
2	(5)=5	(200)= $2^3 * 5^2$	39800
3	(7)=7	(39801)= $3*13267$	1576159401

$p = 2$ で 平方因子 $2^3 * 5^2$. 2 重の平方因子.

第4章 フェルマの(弱)完全数について

4.1 P を底とするフェルマの(弱)完全数

P を奇素数とし $E > 0$ について $R = P^E + 1$ とおく. これは偶数なので $L_E = \frac{R}{2}$ とする. L_E を素数とすると, E は2のべきになるので $E = 2^m, m > 0$ とかける.

一般に $E = 2^m$ とかけるとき L_E は奇数であることが証明できる.

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

$$R = P^E + 1 = 4L' \equiv 0 \pmod{4}.$$

ゆえに, $P^E \equiv -1$.

一方, $P = 2k + 1$ とおくと

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

これで前の式に矛盾した.

以上を踏まえて, $E = 2^m$ のとき $L_m = \frac{P^E + 1}{2}$ とする. $F_m(P)$;¹

ただし, $P = 2$ のとき $E = 2^m, L_m = F_m = P^E + 1$ とおく.

補題 4 $e > 1$ について L_m の素因子 Q は $P - 1$ の因子にならない.

$a_m = P^{2^m - 1} L_m$ を P が底のフェルマの弱完全数と定義する.

L_m が素数の場合なら, a_m を P が底のフェルマの完全数と呼ぶ.

フェルマの弱完全数はフェルマの完全数に比べて豊富な例を持っている. しかも, フェルマの完全数で言えたことは弱完全数でも成り立つ事がある.

一般の底の場合でもフェルマの完全数は数が少ない. 研究対象が少ないのは研究上不利だ.

一方, フェルマの弱完全数は無限にあるので研究材料として有利である.

4.2 オイラーの結果の一般化

L_E は奇数なのでその素因子を Q とおくと

$$P^E + 1 = 2L_E \equiv 0 \pmod{Q}.$$

¹a half generalized Fermat number to base P . (By Wikipedia).

$E = 2^m$ によって

$$P^E = P^{2^m} \equiv -1 \pmod{Q}.$$

ゆえに

$$(P^E)^2 = P^{2^{m+1}} \equiv 1 \pmod{Q}.$$

Q を法とすると P の位数は 2^{m+1} 以下であるが $P^E = P^{2^m} \equiv -1$ によって位数は 2^m より大なので、 P の位数は 2^{m+1} .

$P^E = P^{2^m} \equiv -1 \pmod{Q}$ により $Q \neq P$. フェルマの小定理によって $P^{Q-1} \equiv 1 \pmod{Q}$.

したがって $Q-1$ は位数 2^{m+1} の倍数なので、 $Q-1 = 2^{m+1}K$.

この結果は $P=2$ のときオイラーによる.

$\frac{Q-1}{2} = 2^m K$ によれば

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

オイラーの基準にしたがい

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

次のようにまとめる.

定理 3 $Q = 1 + 2^{m+1}K$ において K が奇数なら ($Q-1$ の 2 の指数は $m+1$ のとき) $\left(\frac{P}{Q}\right) = -1$.
すなわち、 Q を法とするとき P は平方非剰余.

$Q = 1 + 2^{m+1}K$ において K が偶数なら ($Q-1$ の 2 の指数は $m+2$ 以上のとき) $\left(\frac{P}{Q}\right) = 1$.
すなわち、 Q を法とするとき P は平方剰余.

4.3 例

4.3.1 $P = 2$

$F_m = 2^{2^m} + 1$ とおきこれをフェルマ数という.

$a = 2^{2^m - 1} * F_m$ をフェルマ弱完全数という.

F_m が素数ならフェルマ素数といいこの場合 a_m をフェルマ完全数という.

表 4.1: Fermat 弱完全

m	2^m	a_m	(F_m) =素因数分解
0	1	3	(3)=3
1	2	10	(5)=5
2	4	136	(17)=17
3	8	32896	(257)=257
4	16	2147516416	(65537)=65537
5	32	9223372039002259456	(4294967297)=641*6700417
6	64	A	B
7	128	C	D
8	256	E	F

$A = 170141183460469231740910675752738881536$

$B = (18446744073709551617) = 274177 * 67280421310721$

$C = 57896044618658097711785492504343953926805133516280751251460479307672448925696$

$D = (340282366920938463463374607431768211457) = 59649589127497217 * 5704689200685129054721$

$E = 670390396497129854978701249910$ [94 digits] $761687993013765220781067862016$

$F = (115792089237316195423570985008687907853269984665640564039457584007913129639937)$

$= 1238926361552897 * 9346163971535797769163558199606896584051237541638188580280321$.

$m = 5, 6$ のフェルマ数について各素因子を素因数分解した結果を次に述べる.

表 4.2: 素因子 Q

m	Q	$Q - 1$	素因数分解
5	641	640	$[2^7, 5]$
5	6700417	6700416	$[2^7, 3, 17449]$
6	274177	274176	$[2^8, 3^2, 7, 17]$
6	67280421310721	67280421310720	$[2^8, 5, 47, 373, 2998279]$
7	59649589127497217	59649589127497216	A

$$A = [2^9, 116503103764643]$$

ここで $m = 5$ のとき素因子の1つは 641 という例外的に小さい値を持っている. このためオーダーによって発見されたのである. 彼にとって僥倖としかいいようがない.

4.3.2 末尾2桁

$f_m = 2^{2^m}, F_m = f_m + 1, B_m = 2^{2^m - 1}$ とおくと, $B_{m+1} = B_m \times f_m, a_m = B_m \times F_m$.
これを 100 を法としてエクセルで計算すると次の表ができる.

表 4.3: $P = 2$

m	2^m	f_m	F_m	B_m	a_m
2	4	16	17	8	36
3	8	56	57	28	96
4	16	36	37	68	16
5	32	96	97	48	56
6	64	16	17	8	36

$m, 2^m$ には周期性がないが, この表により f_m, F_m, B_m, a_m には周期 4 の周期性があることが分かる. 案外短い.

- $m \equiv 2 \pmod{4}$ ならば $F_m = 17, a_m = 36$.
- $m \equiv 3 \pmod{4}$ ならば $F_m = 57, a_m = 96$.
- $m \equiv 0 \pmod{4}$ ならば $F_m = 37, a_m = 16$.
- $m \equiv 1 \pmod{4}$ ならば $F_m = 97, a_m = 56$.

4.3.3 末尾3桁

表 4.4: $P = 2, \text{mod} = 1000$

m	2^m	f_m	F_m	B_m	a_m
2	4	16	17	8	136
3	8	256	257	128	896
4	16	536	537	768	416
5	32	296	297	648	456
6	64	616	17	808	736
7	28	456	457	728	696
8	56	936	937	968	16
9	12	96	97	48	656
10	24	216	217	608	936
11	48	656	657	328	496
12	96	336	337	168	616
13	92	896	897	448	856
14	84	816	817	408	336
15	68	856	857	928	296
16	36	736	737	368	216
17	72	696	697	848	56
18	44	416	417	208	736
19	88	56	57	528	96
20	76	136	137	568	816
21	52	496	497	248	256
22	4	16	17	8	136
23	8	256	257	128	896

$m = 2$ の行の3項以後の 16,17,8,136 が $m = 22$ の行の3項以後の 16,17,8,136 と同じなので以後繰り返しが起こる.

$22 - 2 = 20$ なので周期 20 である.

4.3.4 $P = 3$ 表 4.5: $P = 3$; Fermat 弱完全数

m	2^m	a	(L_m) =素因数分解
1	2	$15=3*5$	$(5)=5$
2	4	$1107 = 3^3 * 41$	$(41)=41$
3	8	$7175547 = 3^7 * 17 * 193$	$(3281) = 17 * 193$
4	16	$(308836705316427) = 3^{15} * 21523361$	$(21523361)=21523361$
5	32	A	B
6	64	C	D
7	128	E	F

$$A = 572280636715419056279672990187 = 3^{31} * 926510094425921$$

$$B = (926510094425921) = 926510094425921$$

$$C = 1965030762956430528586812143569325391583084017460083159697707$$

$$D = (1716841910146256242328924544641) = 1716841910146256242328924544641$$

$$E = 231680753961907887941566311316[62digits]771379200003876302731668088747$$

$$F = (5895092288869291585760436430706259332839105796137920554548481)$$

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

$L_1 = 5, L_2 = 41, L_4 = 21523361, L_5, L_6$ は新しい素数 5 兄弟である.

$m = 0$ のとき $L_0 = 2$ なのでこれをいれてもよい.

4.3.5 素因数分解

一般のメルセンヌ数 L_m が素数でないとき、各素因子 Q について $Q - 1$ の素因数分解を行う。 2^m を因子とする。

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

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

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

```
10 ?- A is 641,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

```
641,640,[2^7,5]
```

```
A = 641,
```

```
B = 640,
```

```
D = [2^7, 5].
```

```
11 ?- A is 75068993,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

```
75068993,75068992,[2^6,1172953]
```

```
A = 75068993,
```

```
B = 75068992,
```

```
D = [2^6, 1172953].
```

```
12 ?- A is 241931001601,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

```
241931001601,241931001600,[2^8,3^2,5^2,23,182617]
```

```
A = 241931001601,
```

```
B = 241931001600,
```

```
D = [2^8, 3^2, 5^2, 23, 182617].
```


4.3.6 一般の場合

奇素数 P について $h_m = P^{2^m}$, $B_m = P^{2^m-1}$, $L_m = \frac{h_m+1}{2}$ とおくと、 $h_{m+1} = h_m^2$, $h_m = 2L_m - 1$, $L_{m+1} = 2L_m^2 - 2L_m + 1$ が成り立つ。

これらを表計算を用いて計算する。

4.3.7 素因数分解

$m = 7$ に出てくる F の素因数 A について $A - 1$ の素因数分解を行う。

?- 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].

見所は 2 の指数が $m + 1$ を超えるところ。

?- 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。

4.3.8 末尾2桁

L_m, a_m の末尾を調べるため、次の数列を導入する。

$$h_m = 3^{2^m}, L_m = \frac{1+h_m}{2}, h_{m+1} = h_m^2, K_m = 3^{2^m-1} \text{ とおく.}$$

$h_m = 2L_m - 1, (h_m)^2 + 1 = 4L_m^2 - 4L_m + 1$. ゆえに $L_{m+1} = 2L_m^2 - 2L_m + 1$. $a_m = K_m L_m$ に注して次の表を作る。

表 4.6: $P = 3$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	81	82	41	27	7
3	8	61	62	81	87	47
4	16	21	22	61	7	27
5	32	41	42	21	47	87
6	64	81	82	41	27	7

$6 - 2 = 4$ なので周期が 4.

$22 - 2 = 20$ が周期なので案外短い.

表 4.7: $P = 3$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	81	82	41	27	107
3	8	561	562	281	187	547
4	16	721	722	361	907	427
5	32	841	842	921	947	187
6	64	281	282	641	427	707
7	128	961	962	481	987	747
8	256	521	522	761	507	827
9	512	441	442	721	147	987
10	1024	481	482	241	827	307
11	2048	361	362	681	787	947
12	4096	321	322	161	107	227
13	8192	41	42	521	347	787
14	16384	681	682	841	227	907
15	32768	761	762	881	587	147
16	65536	121	122	561	707	627
17	131072	641	642	321	547	587
18	262144	881	882	441	627	507
19	524288	161	162	81	387	347
20	1048576	921	922	961	307	27
21	2097152	241	242	121	747	387
22	4194304	81	82	41	27	107

4.3.9 $P = 5$

表 4.8: $P = 5$; Fermat 弱完全数

m	2^m	a	(L_m) =素因数分解
1	2	$(65)=5*13$	$(13)=13$
2	4	$(39125) = 5^3 * 313$	$(313)=313$
3	8	$(15258828125) = 5^7 * 17 * 11489$	$(195313)=17*11489$
4	16	$(2328306436553955078125) = 5^{15} * 2593 * 29423041$	$(76293945313)=2593*29423041$
5	32	A	B
6	64	C	D

$$A = (54210108624275221700374968349933624267578125) = 5^{31} * 641 * 75068993 * 241931001601$$

$$B = (11641532182693481445313) = 641 * 75068993 * 241931001601$$

$$C = (29387358770557187699218413430556141945466638973512296661994014357333071529865264892578125) = 5^{63} * 769 * 3666499598977 * 96132956782643741951225664001$$

$$D = (271050543121376108501863200217485427856445313) = 769 * 3666499598977 * 96132956782643741951225664001$$

驚くべきはことに $m \geq 2$ について L_m の末尾 3 桁は 313 となり変化しない。 a_m の末尾 3 桁も 125 で変化しない。

4.3.10 素因数分解

$$P = 5, m = 3$$

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

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

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

```
10 ?- A is 641,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

```
641,640,[2^7,5]
```

```
A = 641,
```

```
B = 640,
```

```
D = [2^7, 5].
```

```
11 ?- A is 75068993,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

```
75068993,75068992,[2^6,1172953]
```

```
A = 75068993,
```

```
B = 75068992,
```

```
D = [2^6, 1172953].
```

```
12 ?- A is 241931001601,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).
```

```
241931001601,241931001600,[2^8,3^2,5^2,23,182617]
```

```
A = 241931001601,
```

```
B = 241931001600,
```

```
D = [2^8, 3^2, 5^2, 23, 182617].
```

4.3.11 $P = 7$ 表 4.9: $P = 7$; Fermat 弱完全数

m	2^m	a	(L_m) =素因数分解
1	2	$(175) = 5^2 * 7$	$(25) = 5^2$
2	4	$(411943) = 7^3 * 1201$	$(1201)=1201$
3	8	$(2373781166743) = 7^7 * 17 * 169553$	$(2882401)=17*169553$
4	16	A	B
5	32	C	D
6	64	E	F

$$A = (78887691017425277088276343) = 7^{15} * 353 * 47072139617$$

$$B = (16616465284801) = 353 * 47072139617$$

$$C = (87125749116845407152755275976242821071395424316895543) = 7^3 * 1 * 7699649 * 134818753 * 531968664833$$

$$D = (552213837121960323152649601) = 7699649 * 134818753 * 531968664833$$

$$E = (106272546228400835422165191552[48\text{digits}]633015552098763160614287733943) = 7^{63} * 35969 * 1110623386241 * 15266848196793556098085000332888634369$$

$$F = (609880243817917850069286931281485910377807647065619201) = 35969 * 1110623386241 * 15266848196793556098085000332888634369$$

驚くべきはことに $m \geq 2$ について L_m の末尾 2 桁は 01 となりで変化しない. a_m の末尾 2 桁も 43 で変化しない.

4.3.12 $P = 11$

表 4.10: $P = 11$; Fermat 弱完全数

m	2^m	a	$(L_m)=$ 素因数分解
1	2	$(671)=11*61$	$(61)=61$
2	4	$(9744251)=11^3 * 7321$	$(7321)=7321$
3	8	$(2088624094451411)=11^7 * 17 * 6304673$	$(107179441)=17*6304673$
4	16	A	B
5	32	C	D
6	64	E	F

$$A = (95971712478875242340697505353731) = 11^{15} * 51329 * 447600088289$$

$$B = (22974864931786081) = 51329 * 447600088289$$

$$C = (202632531114813745266796006062265620493992544102127830051326774371) = 11^{31} * 193 * 257 * 21283620033217629539178799361$$

$$D = (1055688837267627642772807627104961) = 193 * 257 * 21283620033217629539178799361$$

$$E = (903318738651911133358014692888[72digits]318199357308617680403672591651) = 11^{63} * 316955440822738177 * 7032401262704707649518767703756385761576062060673$$

$$F = (2228957842262951197934756066684920769745080717495763357756967413121) = 316955440822738177 * 7032401262704707649518767703756385761576062060673$$

驚くべきはことに $m \geq 2$ について L_m の末尾桁は 1 となりで変化しない. a_m の末尾 1 桁も 1 で変化しない.

4.3.13 末尾 3 桁

表 4.11: $P = 5$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	625	626	313	125	125
3	8	625	626	313	125	125

$$m \geq 2 \text{ のとき, } L_m \equiv 313; a_m \equiv 125 \pmod{1000}$$

4.3.14 $P = 7$

$$A = 125749116845407152755275976242821071395424316895543$$

$$B = (552213837121960323152649601) = 7699649 * 134818753 * 531968664833$$

表 4.12: $P = 7$

m	2^m	a	$(L_m)=$ 素因数分解
1	2	175	$(25)=5^2$
2	4	411943	$(1201)=1201$
3	8	2373781166743	$(2882401)=17*169553$
4	16	78887691017425277088276343	$(16616465284801)=353*47072139617$
5	32	A	B
6	64	C	D

$C = 106272546228400835422165191552[48digits]633015552098763160614287733943$

$D = (609880243817917850069286931281485910377807647065619201)$

$= 35969 * 1110623386241 * 15266848196793556098085000332888634369$

$P = 7, m = 1$ 平方因子 5^2 あり.

4.3.15 素因数分解

14 ?- A is 353,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

353,352,[2^5,11]

A = 353,

B = 352,

D = [2^5, 11].

15 ?- A is 47072139617,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

47072139617,47072139616,[2^5,67,1847,11887]

A = 47072139617,

B = 47072139616,

D = [2^5, 67, 1847, 11887].

16 ?- A is 7699649,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

7699649,7699648,[2^6,11,10937]

A = 7699649,

B = 7699648,

D = [2^6, 11, 10937].

$m \geq 2$ のとき $q = \frac{7^{2^m} + 1}{2}$, $a = 7^{2^m - 1} q$ とおく

$q \equiv 1, a \equiv 43 \pmod{100}$. を以下で証明する.

$$7^3 = 343 \equiv 43 \pmod{100}.$$

$$7^4 = 2401 = 1 + 200 \times 12 \equiv 1 \pmod{200}.$$

$$(7^{2^e})^{2^f} = 7^{2^{e+f}} \text{ を使う.}$$

$$(7^{2^{m-2}})^4 = 7^{2^m} \equiv 1 \pmod{200} \text{ と変形すると}$$

$$q = \frac{7^{2^m} + 1}{2} \equiv 1 \pmod{100}.$$

$m \geq 3$ のとき,

$$2^m - 1 = 1 + 2 + \dots + 2^{m-1} = 3 + 2^2 + \dots + 2^{m-1} = 3 + 4(1 + 2 + \dots + 2^{m-3}) = 3 + 4K$$

$$a = q7^{2^m-1} \equiv 7^{2^m-1} = 7^{3+4K} = 7^3 \cdot (7^4)^K \equiv 7^3 \equiv 43 \pmod{100}.$$

$$m = 2 \text{ のとき } 2^m - 1 = 3 \text{ なので } a = 7^3 q \equiv 343 \equiv 43 \pmod{100}.$$

[課題]

$q \equiv 201, 401, 601, 801, \pmod{1000}$ が成り立つか?

4.3.16 末尾2桁

表 4.13: $P = 7$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	1	2	1	43	43
3	8	1	2	1	43	43

4.3.17 末尾3桁

表 4.14: $P = 7$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	401	402	201	343	943
3	8	801	802	401	543	743
4	16	601	602	801	943	343
5	32	201	202	601	743	543
6	64	401	402	201	343	943

4.3.18 $P = 11$ 表 4.15: $P = 11$

m	2^m	a	(L_m) =素因数分解
1	2	671	(61)=61
2	4	9744251	(7321)=7321
3	8	2088624094451411	(107179441)=17*6304673
4	16	A	B
5	32	C	D
6	64	E	F

$$A = 95971712478875242340697505353731$$

$$B = (22974864931786081) = 51329 * 447600088289$$

$$C = 202632531114813745266796006062265620493992544102127830051326774371$$

$$D = (1055688837267627642772807627104961) = 193 * 257 * 21283620033217629539178799361$$

$$E = 903318738651911133358014692888[72\text{digits}]318199357308617680403672591651$$

$$F = (2228957842262951197934756066684920769745080717495763357756967413121) \\ = 316955440822738177 * 7032401262704707649518767703756385761576062060673$$

17 ?- A is 6304673,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

6304673,6304672,[2^5,11,17911]

A = 6304673,

B = 6304672,

D = [2^5, 11, 17911].

18 ?- A is 51329,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

51329,51328,[2^7,401]

A = 51329,

B = 51328,

D = [2^7, 401].

19 ?- A is 447600088289,B is A-1,factorize(B,C),exps(C,D),write((A,B,D)).

447600088289,447600088288,[2^5,127,110137817]

A = 447600088289,

B = 447600088288,

D = [2^5, 127, 110137817].

4.3.19 末尾2桁

表 4.16: $P = 11$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	41	42	21	31	51
3	8	81	82	41	71	11
4	16	61	62	81	51	31
5	32	21	22	61	11	71
6	64	41	42	21	31	51

周期4である.

4.3.20 末尾3桁

周期20である.

表 4.17: $P = 11$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	641	642	321	331	251
3	8	881	882	441	171	411
4	16	161	162	81	651	731
5	32	921	922	961	811	371
6	64	241	242	121	931	651
7	128	81	82	41	371	211
8	256	561	562	281	51	331
9	512	721	722	361	611	571
10	1024	841	842	921	531	51
11	2048	281	282	641	571	11
12	4096	961	962	481	451	931
13	8192	521	522	761	411	771
14	16384	441	442	721	131	451
15	32768	481	482	241	771	811
16	65536	361	362	681	851	531
17	131072	321	322	161	211	971
18	262144	41	42	521	731	851
19	524288	681	682	841	971	611
20	1048576	761	762	881	251	131
21	2097152	121	122	561	11	171
22	4194304	641	642	321	331	251

4.3.21 $P = 13$

表 4.18: $P = 13$

m	2^m	a	$(L_m)=$ 素因数分解
1	2	1105	$(85)=5*17$
2	4	31375357	$(14281)=14281$
3	8	25592946538419637	$(407865361)=407865361$
4	16	A	B
5	32	C	D
6	64	E	F

$A = 17029971683724642268066530820460197$

$$B = (332708304591589921) = 2657 * 441281 * 283763713$$

$$C = 7540518324260041281948452323983308302583943991575249457457852153501317$$

$$D = (221389631888420349152156596074392641) = 193 * 1601 * 10433 * 68675120456139881482562689$$

$$E = 147834483156103798805725342714[82\text{digits}]066972978558588555890851839557$$

$$F = (98026738215380536665329880211783007712201640002057893794795481921124481)$$

$$= 257 * 3230593 * 36713826768408543617 * 3215877717636198473712500018174097551256193$$

18 ?- B = [2657, 441281, 283763713], fer_euler_list(B).

2657=[2^5, 83] 441281=[2^6, 5, 7, 197] 283763713=[2^10, 3, 71, 1301]

B = [2657, 441281, 283763713] .

19 ?- B = [193, 1601, 10433], fer_euler_list(B).

193=[2^6, 3] 1601=[2^6, 5^2] 10433=[2^6, 163]

B = [193, 1601, 10433] .

4.3.22 末尾2桁

表 4.19: $P = 13$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	61	62	81	97	57
3	8	21	22	61	17	37
4	16	41	42	21	57	97
5	32	81	82	41	37	17
6	64	61	62	81	97	57

周期4である.

4.3.23 末尾3桁

表 4.20: $P = 13$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	561	562	281	197	357
3	8	721	722	361	517	637
4	16	841	842	921	757	197
5	32	281	282	641	637	317
6	64	961	962	481	997	557
7	128	521	522	761	117	37
8	256	441	442	721	957	997
9	512	481	482	241	37	917
10	1024	361	362	681	797	757
11	2048	321	322	161	717	437
12	4096	41	42	521	157	797
13	8192	681	682	841	437	517
14	16384	761	762	881	597	957
15	32768	121	122	561	317	837
16	65536	641	642	321	357	597
17	131072	881	882	441	837	117
18	262144	161	162	81	397	157
19	524288	921	922	961	917	237
20	1048576	241	242	121	557	397
21	2097152	81	82	41	237	717
22	4194304	561	562	281	197	357

周期 20 である.

4.4 フェルマの弱完全数の平方因子

$E = 2^m$ のとき $L_m = \frac{P^E+1}{2}$ に素数の平方因子 Q^2 (Q :素数) があるとしよう.

$$P^E + 1 \equiv 0 \pmod{Q^2}.$$

$P^E \equiv -1 \pmod{Q}$ により $(P^E)^2 \equiv 1 \pmod{Q}$ なので Q を法としてみると P の位数は 2^{m+1} .
 $Q \geq 3$ を仮定しておく.

フェルマの小定理によると $P^{Q-1} \equiv 1 \pmod{Q}$ が成り立つので $Q-1$ は 2^{m+1} の倍数. よって $Q-1 = 2^{m+1}k$.

$$P^{Q-1} = P^{2^{m+1}k} \equiv 1 \pmod{Q^2}$$

$P^{Q-1} - 1$ は Q^2 の倍数なので Q は P を Wieferich 素数である.

$Q > 2$, すなわち Q は 2 にならない.

$Q = 2$ とすると $P^{2^{m+1}k} - 1 \equiv 0 \pmod{4}$ になるが $m > 0$ のとき P が奇数なら $\frac{P^{2^{m+1}k}-1}{2}$ は奇数になるからである.

4.4.1 P を底とする Wieferich 素数

Q は P を底とする Wieferich 素数とする.

$Q-1$ の 2 の指数を s とおく.

$m \leq s$ を満たす m について $L_m = \frac{P^E+1}{2}$ が Q^2 を因子とする場合を探す.

```
fer_wief3(P,Q):- Q0 is (Q-1),
Q2 is Q*Q,
factorize(Q0,SS),
exps(SS,SS0),
SS0=[2^LL1|_],
for(1=<LL1,LL),
    EE is 2^LL,
write(2^LL=EE),put(9),
power(PP=P^EE mod Q2),
PP1 is PP+1,
PPP is mod(PP1,Q2),
( PPP ==0 -> write(ok) ; write(n0)),nl,
fail.
fer_wief3(P,Q):-!.
```

```
66 ?- fer_wief3(7,5).
```

```
2^1=2 ok
```

```
2^2=4 n0
```

4.4.2 一般の Wieferich 素数

表 4.21: 一般の Wieferich 素数の例

P	prime=Q				
P=3	prime = 11				
P=7	prime = 5				
P=11	prime = 71				
P=13	prime = 863				
P=17	prime = 3				
P=19	prime = 3	prime = 7	prime = 13	prime = 43	prime = 137
P=23	prime = 13				
P=31	prime = 7	prime = 79			
P=37	prime = 3				
P=41	prime = 29				
P=43	prime = 5	prime = 103			
P=53	prime = 3	prime = 47	prime = 59	prime = 97	
P=67	prime = 7	prime = 47			
P=71	prime = 3	prime = 47	prime = 331		
P=73	prime = 3				
P=79	prime = 7	prime = 263			
P=89	prime = 3	prime = 13			
P=97	prime = 7				
P=101	prime = 5				
P=107	prime = 3	prime = 5	prime = 97		
P=109	prime = 3				
P=127	prime = 3	prime = 19	prime = 907		
P=131	prime = 17				
P=137	prime = 29	prime = 59			
P=149	prime = 5				
P=151	prime = 5				
P=157	prime = 5				

72 ?- fer_wief3(19,43).

73 ?- fer_wief3(19,137).

2^1=2 n0

2^2=4 n0

$2^3=8$ n0

74 ?- fer_wief3(23,13).

$2^1=2$ n0

$2^2=4$ n0

75 ?- fer_wief3(31,7).

76 ?- fer_wief3(31,79).

77 ?- fer_wief3(37,3).

78 ?- fer_wief3(41,29).

$2^1=2$ ok

$2^2=4$ n0

表 4.22: $m = 1$ の場合

P	L_1 素因数分解
7	$[5^2]$
41	$[29^2]$
43	$[5^2, 37]$
107	$[5^2, 229]$
157	$[5^2, 17, 29]$
193	$[5^3, 149]$
239	$[13^4]$
251	$[17^2, 109]$
257	$[5^2, 1321]$
293	$[5^2, 17, 101]$
307	$[5^3, 13, 29]$

表 4.23: $m = 2$ の場合

P	L_2 素因数分解
179	$[17^2, 1776169]$

表 4.24: $m = 3$ の場合

P	L_3 素因数分解
131	$[17^2, 7841, 19136877329]$

4.4.3 $P = 41$

表 4.25: $P = 41$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	34481	$41 * 29^2$	$(841)=29^2$
2	4	97377171401	$41^3 * 137 * 10313$	$(1412881)=137*10313$
3	8	A	B	C

$$A = 777549157495866332581241$$

$$B = 17 * 41^7 * 234850742033$$

$$C = (3992462614561) = 17 * 234850742033$$

$$m = 1 \text{ に平方因子 } 29^2$$

4.4.4 $P = 43$

表 4.26: $P = 43$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	39775	$5^2 * 37 * 43$	$(925)=5^2 * 37$
2	4	A	B	C

$$A = 135909345307$$

$$B = 17 * 43^3 * 193 * 521$$

$$C = (1709401) = 17 * 193 * 521$$

$$m = 1 \text{ に平方因子 } 5^2$$

4.4.5 $P = 107$

表 4.27: $P = 107$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	612575	$5^2 * 107 * 229$	$(5725)=5^2 * 229$
2	4	80289074436443	$107^3 * 4201 * 15601$	$(65539801)=4201*15601$

$m = 1$ に平方因子 5^2

4.4.6 $P = 131$

表 4.28: $P = 131$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	1124111	$131*8581$	$(8581)=8581$
2	4	A	B	C
3	8	D	E	F

$$A = 331031312074451$$

$$B = 113 * 131^3 * 1303097$$

$$C = (147249961) = 113 * 1303097$$

$$D = 28710412953340543080499631931131$$

$$E = 17^2 * 131^7 * 7841 * 19136877329$$

$$F = (43365101734503121) = 17^2 * 7841 * 19136877329$$

$m = 3$ に平方因子 17^2

4.4.7 $P = 157$

表 4.29: $P = 157$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	1935025	$5^2 * 17 * 29 * 157$	$(12325)=5^2 * 17 * 29$
2	4	A	B	C
3	8	D	E	F

$$A = 1175621640703693$$

$$B = 113 * 157^3 * 2688377$$

$$C = (303786601) = 113 * 2688377$$

$$D = 433975078587972309446276265685093$$

$$E = 157^7 * 1297 * 142307322503233$$

$$F = (184572597286693201) = 1297 * 142307322503233$$

$$m = 1 \text{ に平方因子 } 5^2$$

4.4.8 $P = 179$ 表 4.30: $P = 179$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	2867759	$(2867759) = 37 * 179 * 433$	$(16021) = 37 * 433$
2	4	2944023156188099	$17^2 * 179^3 * 1776169$	$(513312841) = 17^2 * 1776169$

4.4.9 $P = 193$ 表 4.31: $P = 193$

m	2^m	a	素因数分解	(L_m) =素因数分解
1	2	3594625	$(3594625) = 5^3 * 149 * 193$	$(18625) = 5^3 * 149$
2	4	4987365166597057	$193^3 * 257 * 2699393$	$(693744001) = 257 * 2699393$

第5章 フェルマの完全数の方程式の解

以下奇素数 P を底として考える. $e = 2^m - 1$ とおき, $L_m = \frac{P^{e+1}-1}{2}$ は素数とする. $a = P^e L_m$ は P を底とするフェルマの完全数である.

$q = L_m$ としてこれの満たす方程式を求める.

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

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

よって,

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

q は a の最大素因子なので $q = \text{Maxp}(a)$ と書ける. そこで $\bar{P}\sigma(a) - aP = \text{Maxp}(a) - 2$ が P を底とするフェルマの完全数の方程式と言う.

$P, \text{Maxp}(a)$ は奇数なので, a も奇数である.

この方程式は見かけは簡明で美しい方程式である. この方程式の解の研究は高い価値がありそうである.

しかしながらフェルマの弱完全数の方程式はきれいになることはない.

5.1 $s(a) = 2$ の場合

a は奇数なので素因数分解し $a = p^e q^f$ ($2 < p < q$) とおく. $X = p^e, Y = q^f$ とおくと $a = XY$ となる. そこで $\bar{p} = p - 1, \bar{q} = q - 1$ を使うと

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

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

$\overline{P}\sigma(a) - aP = q - 2$ を書き直して

$$\frac{\overline{P}AB}{\overline{p}q} = \frac{\overline{P}AB}{\rho'} = XY\rho' + q - 2.$$

分母を払って

$$\overline{P}AB = P\rho'XY + \rho'(q - 2).$$

$\overline{P}AB - P\rho'XY$ の XY の係数を R とおけば

$$R = \overline{P}pq - P\rho'.$$

変形して $\Delta = p + q$ とおくと

$$R = P(\Delta - 1) - pq.$$

$C = pX + qY - 1$ とおくと, $AB = pqXY - C$ によって次の基本方程式をえる:

$$RXY = C\overline{P} + (q - 2)\rho'.$$

これによって $R > 0$.

$p_0 = p - P, q_0 = q - P, D = P(P - 1)$ とおけば $R = D - p_0q_0$ をえる.

5.1.1 $P = 3$ に挑む

$P = 3$ のとき $2\sigma(a) - 3P = Maxp(a) - 2$ が 3 を底とするフェルマの完全数の方程式である.

この方程式の完全な解を得たいのだが. これは過大な期待であろう.

$s(a) = 2$ の仮定のもとで $D = P(P - 1) = 6, R = 6 - (p - 3)(q - 3)$, により $p = 3, R = 6. C = 3X + qY - 1, q'' = (q - 1)(q - 2)$ とおくと基本方程式は

$$3XY = 3X + qY - 1 + q''.$$

1) $Y = q$.

$3Xq = 3X + q^2 - 1 + q''$ を変形し, $q - 1$ で両辺を約すと

$3X = 3^{e+1} = 2q - 1$ なので

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

これは $P = 3$ のときのフェルマ素数である. これはすでに計算している.

2) $Y = q^2$.

$3Xq^2 = 3X + q^3 - 1 + q''$ を変形し, $q - 1$ で両辺を約すと

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

$$3X = q + 1 - \frac{2}{q+1}.$$

$q+1$ は2の約数となり矛盾.

3) $Y \geq q^3.$

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

これを变形して

$$3X = q + \frac{\bar{q}^2}{Y-1}.$$

$\frac{\bar{q}^2}{Y-1}$ は整数になり

$$1 \leq \frac{\bar{q}^2}{Y-1} < \frac{\bar{q}^2}{q^3-1} < 1.$$

これは矛盾.

ところで $s(a) = 2$ の条件をはずして $a \leq 1000000$ の範囲で方程式の解を探してみた結果は次の通り.

表 5.1: $P = 3$

a	素因数分解
15	$3 * 5$
741	$3 * 13 * 19$
1107	$3^3 * 41$
14883	$3 * 11^2 * 41$
38781	$3^2 * 31 * 139$

$s(a) = 2$ に限ると, $a = 15 = 3 * 5, a = 1107 = 3^3 * 41$ の2例はすでに $P = 3$ のフェルマの完全数で登場している. さらに多くの解を得るため

$a = 3^e q r$ の解を探すことが策のひとつだがこの条件を満たさないが類似した解 $a = 14883 = 3 * 11^2 * 41$ がある. 事態は複雑怪奇なのだ.

5.1.2 難関 $P = 5$ に挑む

$P = 5$ のとき $4\sigma(a) - 5P = Maxp(a) - 2$ が5を底とするフェルマの完全数の方程式である.

表 5.2: $P = 5$

a	素因数分解
65	$5 * 13$
14861	$7 * 11 * 193$
39125	$5^3 * 313$

$s(a) = 2$ に限る. $a = 65 = 5 * 13, a = 39125 = 5^3 * 313$ の 2 例のみ解があるがこれを以下で証明する. 長く辛抱の必要な証明である.

$s(a) = 2$ の仮定のもとで $P = 5$ と仮定したので次の基本方程式をえる:

$$RXY = C\bar{P} + (q-2)\rho'.$$

これによって $R > 0$.

$D = P(P-1) = 20, R = 20 - (p-5)(q-5)$, により次の 3 つの場合がある.

i. $p = 3, q \geq 5, R = 2R_1, R_1 = 5 + q$.

ii. $p = 5, q \geq 7, R = 20$.

iii. $p = 7, q = 11, 13, R = 8, 4$.

i. $p = 3, R = 20 + 2(q-5) = 10 + 2q = 2R_1$. ここで $R_1 = 5 + q, C = 3X + qY - 1$ とおくと基本方程式は

$$RXY = 4C + 4(q-2)\bar{q}.$$

よって

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

これより移項して

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

1). $X = 3$ と仮定する.

$$(3R_1 - 2q)Y = 16 + 2(q-2)\bar{q}.$$

$3R_1 - 2q = 3(q+5) - 2q = q + 15 = \bar{q} + 16$ を用いて

$$(\bar{q} + 16)Y = 16 + 2(q-2)\bar{q} = 16 + 2(\bar{q}-1)\bar{q}.$$

$Q = \bar{q} + 16 = q + 15$ とおけば, $Q \geq 20$.

$$QY = 16 + 2(\bar{q}-1)\bar{q} = 16 + 2(Q-16)(Q=17) = 2Q^2 - 66Q + 16 * 35.$$

$Y = \frac{16*35}{Q} + 2Q - 66$ により Q は $16*35$ の約数.

$Q = 5Q_1$ のとき $5Q_1 = Q = q + 15$ により q は 5 の倍数だから $q = 5$. $Q_1 = 4, Q = 20$.
 $QY = 16 + 2(Q - 16)(Q - 17)$ により

$$20Y = 16 + 2 * 12 = 40.$$

$Y = 2$ がでて矛盾.

$Q = 7Q_1$ のとき Q_1 は 16 の約数.

$7Q_1Y = 16 + 2(7Q_1 - 16)(7Q_1 - 17)$ により

A. $Q_1 = 4$ のとき,

$28Y = 16 + 2 * 12 * 11$ から $7Y = 4 + 66 = 70$. $Y = 10$ となり矛盾.

B. $Q_1 = 8$ のとき,

$56Y = 16 + 2 * 40 * 39$ なので $7Y = 2 + 2 * 5 * 39 = 392$ により $Y = 56$ となり矛盾.

C. $Q_1 = 16$ のとき,

$7Y = 1 + 12 * (7 * 16 - 17) = 1141$ により $Y = 163$ となり矛盾.

Q は 5 や 7 で割れないので 16 の約数. $Q \leq 16$.

$20Y \leq QY = 16 + 2(Q - 16)(Q - 17) \leq 16$ となり矛盾.

ii. $p = 5, q \geq 7, R = 20$.

$C = 5X + qY - 1, q'' = (q - 1)(q - 2)$ とおくと基本方程式は

$$5XY = C = 5X + qY - 1 + q''.$$

1) $Y = q$.

$5Xq = 5X + q^2 - 1 + q''$ を変形し, $q - 1$ で両辺を約すと

$5X = 5^{e+1} = 2q - 1$ なので

$$q = \frac{5^{e+1} + 1}{2}$$

これは $P = 5$ のときのフェルマ素数である.

2) $Y = q^2$.

$C = 5X + q^3 - 1$ によって $5Xq^2 = 5X + q^3 - 1 + q''$ を変形し, $q - 1$ で両辺を約すと

$$5X(q + 1) = q^2 + 2q - 1.$$

$$5X = q - 1 + \frac{2}{q + 1}.$$

これは矛盾.

$$3) Y \geq q^3.$$

$$5X(Y-1) = q(Y-1) + (q-1)^2.$$

これを变形して

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

$\frac{(q-1)^2}{Y-1}$ は整数になり

$$1 \leq \frac{(q-1)^2}{Y-1} \leq \frac{(q-1)^2}{q^3-1} = \frac{q-1}{q^2+q+1} < 1.$$

これは矛盾.

$$\text{iiia. } p = 7, q = 11, R = 8. \rho' = 6 * 10 = 60.$$

$$RXY = C\bar{P} + (q-2)\rho'$$

によって

$$8XY = 4C + (q-2)\rho' = 4(7X + 11Y - 1) + 9 * 60.$$

$$2XY = 7X + 11Y - 1 + 9 * 15.$$

これより

$$(2X - 11)Y = 7X + 134.$$

$Z = 2X$ とおけば

$$2(Z - 11)Y = 7Z + 134 * 2 = 7Z + 268.$$

$$(Z - 11)(2Y - 7) = 77 + 134 * 2 = 345 = 3 * 5 * 23.$$

$$Y = 11, 121.$$

$Y = 11$ のとき $2Y - 7 = 15$. $15 * (Z - 11) = 3 * 5 * 23$ により $Z = 23 + 11 = 34$. $X = 17$ となり $X = 7^e$ に矛盾.

$$\text{iiib. } p = 7, q = 13, R = 4. \rho' = 6 * 12 = 72.$$

$$RXY = C\bar{P} + (q-2)\rho'$$

によって

$$4XY = 4C + (q - 2)\rho' = 4(7X + 13Y - 1) + 11 * 72.$$

これより

$$XY = 7X + 13Y - 1 + 11 * 18.$$

$$X(Y - 7) = 13(Y - 7) + 13 * 7 + 11 * 18, 289 = 17^2 \text{ により}$$

$$X = 13 + \frac{17^2}{Y-7} \text{ により } Y - 7 = 1, 17, 17^2. Y \text{ は偶数. しかし } Y = 13^f \text{ なので奇数となり矛盾.}$$

5.1.3 $P = 7$ のとき

$a < 1000000$ で解を探すと $s(a) = 2$ が1つ.

$P = 3, 5$ のときの議論をそのまま繰り返すことはできない. ならばどうするか.

表 5.3: $p = 7$

a	素因数分解
411943	$7^3 * 1201$

5.1.4 $P = 11$ のとき

$a < 1000000$ で解を探すと $s(a) = 2, 3$ の解が1つずつあった.

表 5.4: $P = 11$

a	素因数分解
671	$11 * 61$
861773	$11 * 157 * 499$

5.1.5 $P = 19$ のとき表 5.5: $p = 19$

a	素因数分解
3439	$19 * 181$

$a < 1000000$ で解を探すと $s(a) = 2$ の解が1つあった.

5.2 $a = P^e qr$ の解

$s(a) = 3$ の解を $a = P^e qr$ の形に限定して探す. すなわち $\bar{P}\sigma(a) - aP = \text{Maxp}(a) - 2$ の解 $a = P^e qr$ があるとする.

$$(P^{e+1} - 1)\tilde{q}\tilde{r} - P^{e+1}qr = r - 2$$

を得るので $\Gamma = P^{e+1} - 1, \Delta = q + r$ を用いると

$$\Gamma(qr + \Delta + 1) - (\Gamma + 1)qr = r - 2.$$

これより, $\Delta' = \tilde{q} + r = \Delta + 1$ によって

$$\Gamma\Delta' = \tilde{q}r - 2.$$

$\tilde{q}_0 = \tilde{q} - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + 2$ によれば

$$\tilde{q}_0 r_0 = D.$$

これによって, 与えられた $\Gamma = P^{e+1} - 1$ について, D の因子分解 $\tilde{q}_0 r_0$ を求め $q = \tilde{q}_0 - 1 + \Gamma, r = r_0 + \Gamma$ がともに素数なら $a = P^e qr$ が解である.

その結果, 得られた解は $P = 3$ のときの

表 5.6: $P = 3$

a	素因数分解
741	$3 * 13 * 19$
38781	$3^2 * 31 * 139$
4954286665155815901	$3^{11} * 536917 * 52088299$

$P = 11$ のときの

表 5.7: $P = 11$

a	素因数分解
861773	$11 * 157 * 499$
18850718310561181	$11^4 * 164431 * 7830211$

$P = 17$ のときの

表 5.8: $P = 17$

a	素因数分解
6491399	$17^1 * 421 * 907$
446613443803097	$17^3 * 91153 * 997273$
6897168	
474526784103120	

$P = 23$ のときの だけだった. 少し残念である.

表 5.9: $P = 23$

a	素因数分解
25222533274109	$23^2 * 12203 * 3907207$
26369012236896	

7 ?- all_pq_3e(11,1,1=<5).

e=1 n=14402

861773 \$a=11^1*157*499\$ sigma=948000

e=2 n=1768902

e=3 n=214329602

e=4 n=25937102502

18850718310561181 $a=11^4*164431*7830211$ sigma=20735790142400320

e=5 n=3138424833602