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 5 月 22 日

目 次

第1章　第３期をはじめるにあたって

1.1　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い. 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.

1.2　はじめに

自然数 a の約数の和を $\sigma(a)$ で表す.

a の関数と見て**ユークリッド関数**という.

$\sigma(a)-2a=0$ を満たす自然数を完全数という.

完全数の概念は 2300 年昔に遡り, 最古のそして未だに解決がされていない数学界最大の懸案の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狙いである. 主要な結果はすべて新しい研究の成果である.

この講座の参加者も一緒になって研究に加わってほしい.

$\sigma(2^e)$ 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)

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 $a=P^eq$ 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 $a=P^eq$ を m だけ平行移動した底が P の完全数と呼ぶ. ただし $q>P$. $(\overline{P}=P-1)$

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

$$\overline{P}\sigma(a)-Pa=(P-2)\mathrm{Maxp}(a)-m(P-1). \tag{1.1}$$

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 $a=P^eQ$ を弱完全数という.
$e+1$ が奇数のとき $Q=\sigma(P^e)$ として $a=P^eQ$ 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 が素数の場合なら, a_m を P が**底のフェルマの完全数**と呼ぶ.
弱完全数と P が底の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.

第2章　オイラーとフェルマの古典的結果

2.1　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,$\cdots$ となって意外に多い.

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

表 2.1: $\sigma(2^e) = 2^{e+1} - 1$, $e+1$:素数

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

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

2.1.1　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 $Q \equiv \pm 1 \bmod 8$.

Proof.

条件より,

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

p は素数なので 2 の mod$Q$ での位数は p. ゆえに

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

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

ルジャンドルの記号を用いるとオイラーの基準によって

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

$2^{\frac{Q-1}{2}} \equiv 1$ 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 $Q \equiv \pm 1 \bmod 8$.

例

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

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

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

$q = 2p + 1$ が素数, かつ $q \equiv \pm 1 \bmod 8$ のとき,*($q = 2p + 1$ 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,$q \equiv 1 \bmod 8$ は成立しない.

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

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

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

表 2.2:

$2/q$ のルジャンドル	p	$q=2p+1$	M_p の素因数分解
$(+)$	3	7	7
$(+)$	11	23	23*89
$(+)$	23	47	47*178481
$(+)$	83	167	167*57912614113275649087721
$(+)$	131	263	263*1035079443105516238671861923746823456 9
$(-)$	5	11	31
$(-)$	29	59	233*1103*2089
$(-)$	41	83	13367*164511353
$(-)$	53	107	6361*69431*20394401
$(-)$	89	179	6.1897E+26
$(-)$	113	227	3391*23279*65993*1868569*1066818132868207

2.2　3 のべきとそのユークリッド関数の値

3 のべき $a=3^e$ について $e+1$ が素数 p の場合 $N_p=\sigma(a)=\frac{3^{e+1}-1}{2}$ の素因数分解を行う.

表 2.3: $3^e=a$

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

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 奇素数 のときにも, フェルマとオイラーの結果, および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 q はすべて $q + 1 = 12L$ を満たし結果としてすべて q は すべて N_p の因子となっていた. これは感動の結果である.

表 2.4: $q = 2p + 1$: 素数

p	$q = 2p + 1$	$q + 1$	$q + 1 \bmod 12$	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

$A = 167 * 12119 * 1036745531 * 950996059627210897943351$
$B = 179 * 1611479891519807 * 5042939439565996049162197$
$C = 227 * 1583 * 2172539 * 526256453012063980796131127321354599535039$
$D = 263 * 60519958859114400310088130657440685166028842774039488582817 1$
$E = 347 * 762239 * 2125048865543 * 309854287003880455089590180543928107 62$
$- - 033149280306907746766819$
$F = 359 * 56207 * 100957 * 19510643 * 291066066130451 * 6779963644378513811*$
$- - 161868664744491655705858963594331$
$G = 383 * 311713 * 9593931911 * 589086859176036543433200507492971040054890$
$- - 9181468214858888800348369500317$

2.2.1　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 mod12 で分類すると $q \equiv 1, 5, 7, 11 \mod 12$ である.
(1).$q \equiv 1 \mod 12$ 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). $q \equiv 5 \mod 12$ とすると $q = 5 + 12k = 2p + 1$. よって $p = 4 + 6k$. 矛盾.
(3). $q \equiv 7 \mod 12$ とすると $q = 7 + 12k = 2p + 1$. よって $p = 3 + 6k$. 矛盾.
$q \equiv 11 \mod 12$ のみ生き残り, このとき q を法として 3 は平方剰余.

一方, フェルマ数には平方因子が無い. という予想がある.
底が 3 のとき $p = 5$ の場合 $N_5 = 11^2$. これは反例.
(しかし, これが唯一の反例であることを期待)

第3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 $a=p^eN_p$ 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. $a=2^eq$ を P を底とする**弱完全数**という.

数値例

3.0.2　$P=2$

表 3.1: $P=2$, 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	3868562622766373554408652 8
47	(95)=5*19	(140737488355327)=2351*4513*13264529	9903520314282971830448816128
53	(107)=107	(9007199254740991)=6361*69431*20394401	4056481920730333634429487520 1536

$A=166153499473114483824745506383331328$

$B=265845599156983174465469261595384217 6$

$C=10889035741470030830754200461521744560128$

表 3.2: $P = 2$

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	$C1$	$D1$

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

$E = 2787593149816327892690784192460327776944128$

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

$G = 4460149039706124628306671417881385336674713 6$

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

$J = 18268770466636286477546030185808047379969789 1328$

$K = (9671406556917033397649407) = 167 * 57912614113275649087721$

$L = 467680523945888933825179098112177781704731425 50528$

$M = (6189700196426901374495621 11) = 618970019642690137449562111$

$N = 191561942608236107294793378084303638130997321548169216$

$O = (158456325028528675187087900671) = 11447 * 13842607235828485645766393$

$P = 125542034707733615276715788463361046696904465513345250754 56$

$Q = (2535301200456458802993406410751) = 7432339208719 * 341117531003194129$

$R = 32138760885179805510839241846810575544441777581640889673973 76$

$S = (10141204801825835211973625643007) = 2550183799 * 3976656429941438590393$

$T = 5142201741628768881734278695491213267830958288344338391682252 8$

$U = (16225927682921336339157801028 8127) = 162259276829213363391578010288127$

$V = 131640364585696483372397534604587229102234723183869431177837281 28$

$W = (64903710731685345356631204115251 1) = 745988807 * 87003598609872098733287 3$

$X = 21062458333711437339583605536734054011923653237437143935260137881 6$
$Y = (10384593717069655257060992658440191) = 3391*23279*65993*1868569*1066818132868207$
$Z = 53919893334301279589334030174039256154977430310253516431710891278336$
$A1 = (17014118346046923173168730371588410572 7) = 17014118346046923173168730371588410572 7$
$B1 = 14474011154664524427946373126085988481573677491474835889066354349131199152128$
$C1 = (27222589353675077077069968594541456916 47) = 263*10350794431055162386718619237468234569$
$D1 = 37053468555941182535542715202780130513032783798328142954087891898234930756321 28$

3.0.3　末尾１桁の数

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

Proof.
弱完全数でこの結果を示す. $e+1=p$ は素数, という性質を用いる. q は素数という性質は使えない.

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

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

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

3.0.4　$P = 3$

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

表 3.3: $P = 3$

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	635867374128242023258756024 77
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

3.0.5　偶然にも

$p = 5$ 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.

3.0.6　$P = 3$ 続き

表 3.4: $P = 3$

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	$M1$	$N1$

$A = 337925993174087615427129041636594 01$
$B = 221713244121518884968045982580046482001$
$C = (164128483697268538813) = 431 * 380808546861411923$
$D = 1795877277384302968284940054550981447 8917$
$E = (13294407179478751643893) = 1223 * 21997 * 5112661 * 96656723$
$F = 11782750816918411774952943450387599284 0011597$
$G = (9691622833840009948398361) = 107 * 24169 * 3747607031112307667$
$H = 626183687689393767209300240359820400199694144570 01$
$I = (706519304586936725238240 5533) = 14425532687 * 489769993189671059$
$J = 33277968516933911303947774618193177127885685499906811237$
$K = (635867374128243052714416498 01) = 603901 * 10529331366039186103590 1$
$L = 269551544987164681561976974424321198045960533954962944 3001$
$M = (463547315739489185428809627052 93) = 221101 * 441019876741 * 475384700124973$
$N = 143250742619523785533978605266160556630271139215533373443437 8997$
$O = (375473325748986240197335797912877 3) = 375473325748986240197335797912877 3$
$P = 939868122326695556888433629151289424673228917359519725450340403327 7$
$Q = (337925993174087616177602218121589 61) = 11243*20149*15768033143*9460375336977361$
$R = 761293179084623401079631239612544524098913602817908624975367225786001$

$S = (2463480490239098721934720170106388293 3)$
$= 432853009 * 392038110671 * 145171177264407947$

$T = 4045824083859113448931603056109302804096 9$
$- - 6733642031742793788413297107082637$
$U = (19954191970936699647671233377861745176 13)$
$= 167 * 12119 * 1036745531 * 950996059627210897943351$
$V = 265446518141996433384402476511331356982123144801453479686383573531661755631771 7$
$W = (14546605946812854043152329132461212233402 41)$
$= 179 * 1611479891519807 * 5042939439565996049162197$
$X = 14106916304790072655424023651965844768597180596019350455715608901993462761639077388 01$
$Y = (95440281617039135377122431438078013463353244 81)$
$= 76631 * 2549755542947 * 488459628280284211557312283 33$
$Z = 607256490342649221167767082843574821283112603199541158927322029723$
$61234658808964021817054401$
$A1 = (77306628109801699655469169464843190905316128300 1)$
$= 33034273 * 465092326319 * 503167756680197593062029640 23$
$B1 = 39842098331381215400817198305366944024385017897983405520149643694312$
$05057870704638552259948050 01$
$C1 = (69575965298821529689922252518358871814784515470 13)$
$= 6957596529882152968992225251835887181478451547013$
$D1 = 32272099648418784474661930627347224659751864497385112062067563800310$
$07356942426993809058144999711 7$
$E1 = (56356531892045439048837024539870686169975457530809 3) =$
$50077 * 229837 * 489650285050451239934212504065160365715 57$
$F1 = 21173724579327564493825692684 6[42digits]8955366005801242983487726337 97$
$G1 = (50720878702840895143953322085883617552977911777728 41)$
$= 1091 * 521402591 * 3499901929 * 239789806103 * 10624346875389299603$
$H1 = 17150716909255327239998811074 5[44digits]4243542159547489603603907318 01$
$I1 = (41083911749301125066602190889565730217912108539960016 1)$
$= 227 * 1583 * 2172539 * 52625645301206398079613112732135459953503 9$
$J1 = 11252585364162420202163219945 9[48digits]7585617404993721534675806840 01$
$K1 = (19650307629564305285868121435687531109463685987126401848494 93)$
$= 5843 * 681229 * 21520151 * 76082653 * 3015153157523008742365642355913576 73$
$L1 = 25742305995767543104618479035 1[61digits]9732150460588312724634365211 97$
$M1 = (15916749179947087281553178362906900198665585649572385497280897 3)$
$= 263 * 60519958859114400310088130657440685166028842774039488582817 1$
$N1 = 16889526963823085030940184094 9[65digits]9835613481651979354062904794 77$

3.0.7　末尾の数

2 が底の弱完全数でも末尾の数が 6, 8 となる事実は成立する.

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.

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

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

1. $e = 4k+2$ のとき

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

よって $q \equiv 3 \mod 5$. $q = 3 + 5L$ となる.

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

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

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

a は奇数なので L は奇数. よって $a \equiv 7 \mod 10$.

2. $e = 4k$ のとき

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

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

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

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.

$q = Q_1 Q_2 Q_3$ 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:

- $e \equiv 2 \mod 4$ のとき $q \equiv 13, 33, 73, 93 \mod 100$.

表 3.5: 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

- $e \equiv 0 \mod 4$ のとき $q \equiv 01, 41, 61, 81 \mod 100$.

3.0.8　$P = 5$

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

表 3.6: $P = 5$

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 3.7: $P = 5$

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

$A = 1818989403545761108398437 5$
$B = (2980232238769531) = 8971 * 332207361361$
$C = 710542735760100126266479492 1875$
$D = (46566128730773925781) = 59 * 35671 * 22125996444329$
$E = 1734723475976807094402611255645751953125$

$F = (1164153218269348144531) = 1861 * 625552508473588471$
$G = 10842021724855044340072199702262878417968 75$
$H = (1818989403545856475830078 1) = 149 * 13971969971 * 8737481256739$
$I = 26469779601696885595885077782440930604934692382 8125$
$J = (113686837721616029739379882 81) = 2238236249 * 5079304643216687969$
$K = 10339757656912845935892608650647161994129419326782226 5625$
$L = (28421709430404007434844970703 1) = 1644512641 * 172827552198815888791$
$M = 64623485355705287099328804067909004515968263149261474609375$
$N = (17763568394002504646778106689453 1)$
$= 1776356839400250464677810668945 31$
$O = 252435489670723777731753140890491238224058179184794425964355468 75$
$P = (27755575615628913510590791702270507 81)$
$= 5960555749 * 17154094481 * 27145365052629449$
$Q = 6162975822039154729779129416271767418766813761976663954555988311767578125$
$R = (43368086899420177360298112034797668457031) = 21180247636732981*204757223065733875157505 1$
$S = 150463276905252801019998276764447446760788323905089214349573012441396713256835937 5$
$T = (10842021724855044340074528008699417114257 81) = 8419*918585913061*140194179307171898833699259$
$U = 940395480657830006374989229777796542254932228577235520106114563532173633575439453125$
$V = (16940658945086006781366450013592839241027832031)$
$= 269 * 1609 * 26399 * 2454335007529 * 604088623657497125653141$
$W = 22958874039497802890014385492621985894895811655366021225566086627623008098453283309936523437 5$
$X = (10587911840678754238354031258495524525642395019531)$
$= 569 * 18607929421228039083223253529869111644362732899$
$Y = 8968310171678829253911869333055463240193676428009489181008423441809895848564337939023971557617 18$
$Z = (26469779601696885595885078146238811314105987548828 1)$
$= 4853479 * 5729041 * 95195241517703499147262005767140272 79$
$A1 = 560519385729926828369491833315[41 digits]5372781315818428993225097656 25$
$B1 = (41359030627651383743570434603498142678290605545043945 31)$
$= 205367807127911 * 58523123221688392679 * 344120456368919234899$
$C1 = 13684555315672041708239546711 8[50 digits]7443229882046580314636230468 75$

3.0.9　末尾の数

$a \equiv 25, 75 \mod 100$ は成り立つ.
より詳しく,

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

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.

3.0.10　$P = 7$

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

表 3.8: $P = 7$

p	$(2p+1)$=	(N_p) = 分解	a
2	(5)=5	(8)=2^3	56
3	(7)=7	(57)=3*19	2793
5	(11)=11	(2801)=2801	6725201
7	(15)=3*5	(137257)=29*4733	16148148793
11	(23)=23	(329554457)=1123*293459	93090977300134793
13	(27)=3^3	(16148168401)=16148168401	223511436608353935601
17	(35)=5*7	(38771752331201)=14009*2767631689	1288498953284568548534420801
19	(39)=3*13	(1899815864228857)=419*4534166740403	309368598683626211233992762679 3

表 3.9: $P = 7$

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

$A = 178344840705996722254077465560591327 93$
$B = 24685221610282962357735084542120236488174339 6401$
$C = (26295897005807634435840457) = 311 * 21143 * 3999088279399464409$
$D = 592692170862893926209219560171029203619130597664793$
$E = (309368598683626238374219394 5201) = 223 * 2887 * 4805345109492315767981401$
$F = 8203622558697478826660309198389254312666780494848270305646801$
$G = (74279400543938659833650076624280 01) = 83 * 20515909 * 436213936229068656094783$
$H = 472922515300017846374101771271861183732201324746761000803186736520 01$
$I = (36396906266529943318488537545897 2057)$
$= 166003607842448777 * 2192537062271178641$
$J = 113548695923534284914421835282373872709889396348036286703487710014262793$
$K = (87388971945938393907690978647699190 9257)$
$= 13722816749522711 * 63681511996418550459487$
$L = 654585635808686369208943910457664184071462434342630427022 3$
50295255757960808793
$M = (10281225160467706104845935946923162113219 6401)$
$= 8269 * 319591 * 389042760170351880563720518398412 19$
$N = 906030778287721792675491584254455732334616901264420867062879727505 1$
070279034171965187601
$O = (12095758589038651555290195182195630994581774400857)$
$= 459257 * 134927809 * 550413361 * 354639323684545612988577649$
$P = 125406322152259123444080572115244112551842147850386779280007493 2$
$275853246452545538134636728154867 93$
$Q = (59269217086289392620921956392758591873450694564200 1)$
$= 367 * 4759 * 177237331 * 191466244981372766068053032606459190 7$
$R = 30110057948757415538923745364 8[42digits]9788374014381404579061824780 01$
$S = (69729641209848607524588472476516555753196007647835795257)$
$= 228337 * 147300841 * 206244761 * 1005201175737082903354093202182516 1$
$T = 41676195970750432955274375403 3[52digits]9886541206862524704665111387 93$
$U = (16742086854484650666653692241611625036342361436245374441245 7)$
$= 990643452963163 * 16900214506446855676567697524741375654214573 9$
$V = 24025497620837806665099867459 9[59digits]6922822598814935123060807247 93$
$W = (82036225586974788266603091983896962678077571037602334762104 01)$
$= 439 * 3675989 * 359390389 * 1958423494433591 * 722260522810553620275760696 9$
$X = 57685219787631573802904781771 4[62digits]2298280858003488313579428136 01$

3.0.11　末尾の数

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

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

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

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

$$6N_p = 7^p - 1 \equiv 342 = 6 \times 57 \mod 600$$

ゆえに

$$N_p \equiv 57 \mod 100.$$

よって

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

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

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

ゆえに

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

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).

3.0.12　$P = 11$

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

表 3.10: $P = 11$

e	p	$(2p+1)$	(N_p) = 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

$A0 = 232251544198878080950520379327369 7$
$A = 340039485861577398986846964992269755 49$
$B = (89543024325523737224653) = 829 * 28878847 * 3740221981231$
$C = 728904836851030521429027853850124525396790261 3$
$D = (158630929717149157441443670489) = 523 * 303309617049998388989376043$
$E = 228761562390246506066453264733348483256258951604954126056 09$
$F = (191943424957750480504146841291 81) = 50159 * 2428541 * 157571957584602258799$
$G = 33492980349555990953189422489630490716271536793263604160376698 1$
$H = (340039485861577398992406882305761986 97) = 2591*36855109*136151713*2615418118891695851$
$I = 10511531995000535984031884072175901907045798792322646350775223148922564706 17$
$J = (49785181124993546986478291638386612512424 1)$
$= 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$
$K = 22532402360440124879373085380333495679667293998886148220552925184518462352208939864 1$
$L = (60240069161242191853638732882447801140033173)$
$= 1416258521793067 * 42534656091583268045915654719$
$M = 32989690295920386835890134305346271024600891715413118108859739977787976996901960495011 33$

$N = (881974852589746930929124688131918256491225687357)$
$= 2069 * 22666879066355177 * 1880632704182469059574711388 9$
$O = 707163309637005298722853982863373897435617063145640 9943$
$- - 1850055646826732718108113320818748383107 7$

3.0.13　末尾の数

表を観察してもきれいな結果が見えてこない.
$e \equiv 0 \mod 4$ のとき $q \equiv 1, 3, 5, 7, 9 \mod 10$
$e \equiv 2 \mod 4$ のとき $q \equiv 1, 3, 7, 9 \mod 10$

$P = 11$ 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, ということもできる.

3.0.14　$P = 13$

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

表 3.11: $P = 13$

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	(1218266908646205092 23)=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

$A = 47967753575824408977422124072925 2401$
$B = 13700070098791209449615908553795581328767$

$C = (347949211778442636392048 3) = 1381 * 2519545342349331183143$
$D = 1117556805943749451280484243418726939907951748922 7$
$E = (167948438695509292332086630309 81) = 1973 * 2843 * 3539 * 846041103974872866961$
$F = 260369335940854550834324579101958487505450742744381795527146101$
$G = (283832861395410704041226405223580 3) = 311 * 1117 * 817050901143136340856815036 9$
$H = 74364086038067468263791443037310730415821897627517337897708794533 47$
$I = (13700070098791209449625279837708244444861) = 1481 * 67495678093 * 4287755796749 *$
$31964044249933\ J = 17325408065703967333731570425733633541601502212368638138050285732520948469816590 1$
$K = (39128770209157573309074761744478516958967740 1)$
$= 6740847065723 * 58047259977349384372529747126587$
$L = 14132867613055912645705301563845973842840462857276808424623988436014205081844591327623500 1$
$M = (66127621653476298892336347348168693660655480783)$
$= 119627 * 55278174369896677917473770426549770253082 9$
$N = 40364883189648992107398911796500485892536645975214015955248 58$
$73828020990992504453946640330752 7$
$O = (18886710020449365726640184166110460596419811866456 43)$
$= 183959 * 19216136497 * 53428034448190923485367106932639174 1$
$P = 32926875267373152068691823754 3[43digits]85284098240245558553275363438 7$

3.0.15　末尾の数

表を観察すると,

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

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

3.0.16　$P = 17$ の弱完全数

表 3.12: $P = 17$

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= 25159060694329964487063216164112815210 41
E=(14942027230321957802947)=229*1103*202607147*291973723
F= 21013099082511329639265382324442386296870 3523
G=(124797305630372023765994 1607)=47*26552618219228090162977481
H= 14658228228329868069790994964526039642568537952974012 23

3.0.17　$P = 19$ の弱完全数

表 3.13: $P = 19$

p	$(2p+1)=$	$(N_p) =$ 分解	a
2	(5)=5	(20)=2^2*5	380
3	(7)=7	(381)=3*127	137541
5	(11)=11	(137561)=151*911	17927087081
7	(15)=3*5	(49659541)=701*70841	2336276856400621
11	(23)=23	(6471681049901)=104281*62060021	396783053162981708115277 01
13	(27)=3^3	A	B
17	(35)=5*7	C	D
19	(39)=3*13	E	F

A=(2336276859014281)=599*29251*133338869
B= 5170916427125338184627482845241
C=(304465936543600121441)=3044803*99995282631947
D= 878205851198256655553811862328 73824348321
E=(109912203092239643840221)=1099122030922396438402 21
F= 1144486647340080056084491411806030788772819786 1

3.0.18　$P = 23$ の弱完全数

表 3.14: $P = 23$

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

A=(43309534450633)=11*3937230404603
B= 17941629145770656573062898 17
C=(22910743724384881)=47691619*480393499
D= 5020803441781611565572358171668 01
E=(6411365434575589496641)=103*62246266355102810647
F= 3931840644281539245080643519965766304764000 1

G=(33916123148904868437231 13)=2129*63877469*24939218613613
H= 1100290217736390223882620149232923757087347272869 7

以上から次の推察が可能:
N_p は $p=2$, $P \equiv -1 \mod 4$(P=3,7,11,19,23, $\cdots$) のとき $p^2=4$ で割れる.
$p>2$ は奇数.

3.1　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 $P-1 \not\equiv 0 \bmod Q$ かつ

$$P^p \equiv 1 \bmod Q$$

になる. よって mod$Q$ 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
$P^{Q-1} \equiv 1 \bmod Q$ 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

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

$P^{\frac{Q-1}{2}} = P^{pk'} \equiv 1 \mod Q$. 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 $P-1 \not\equiv 0 \bmod Q$ かつ $\left(\frac{P}{Q}\right)=1$ を仮定すると, $P \equiv n^2 \mod Q$ を満たす n がある.

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

これより, 素因子 Q は P^p-1 の素因子になる. $P-1 \not\equiv 0 \bmod Q$ 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 $N_p = \frac{P^p-1}{P}$ の素数因子 *(奇数) Q* について $\left(\frac{P}{Q}\right)=1$.
素数 Q は $2p+1$ とする.
$\left(\frac{P}{Q}\right)=1$ を仮定すると, Q は N_p の素数因子.

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 でも同じく成立することがわかった.

次は Lagrange の結果の一般化.

補題 4 p を素数とし, $N_p = \frac{P^p-1}{\overline{P}}$ 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 $q_0 \neq P$.

$$P^p = \overline{P}N_p + 1 \equiv 1 \mod q_0.$$

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

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

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

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

これで矛盾した.

3.1.1　実例

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

$p = 73$, $W = 439 * 3675989 * 359390389 * 1958423494433591 * 722260522810553620275760696 9$ について

```
 1 ?-  B=439, A is B-1, factorize(A,S),exps(S,SX).
 SX = [2, 3, 73].

2 ?- B=3675989, A is B-1, factorize(A,S),exps(S,SX).
SX = [2^2, 73, 12589].

3 ?- B=3675989, A is B-1, factorize(A,S),exps(S,SX).
SX = [2^2, 73, 12589].

4 ?- B=359390389, A is B-1, factorize(A,S),exps(S,SX).
SX = [2^2, 3, 7, 29, 43, 47, 73].

5 ?- B=1958423494433591, A is B-1, factorize(A,S),exps(S,SX).
 SX = [2, 5, 73, 2682771910183].
```

3.2　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.

3.2.1　$P = 3$

表 3.15: $P = 3, q = 2p+1$ 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	$C = D$

$A = (19954191970936699647671233377861745176 13)$
$B = 167 * 12119 * 1036745531 * 950996059627210897943351$
$C = (14546605946812854043152329132461212233402 41)$
$D = 179 * 1611479891519807 * 50429394395659960491621 97$

$q = 2p+1$ が N_p の最小素因子となる.

3.2.2　$P = 5$

$A = (46566128730773925781) = 59 * 35671 * 22125996444329$
$B = (113686837721616029739379882 81) = 2238236249 * 5079304643216687969$
$C = (27755575615628913510590791702270507 81) = 960555749*17154094481*27145365052629449$
$D = (25849394142282114839731521627186339173931628465656246582031)$
$E = 20515111 * 14311857070701868962383741 * 88040095945103834627376781$
$F = (40389678347315804437080502542478654959268169477581977844238281)$
$G = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 * 231669654363683130095909$
$H = (24074124304840448163199724282311591481726270602692352440499234944581985473632 81)$
$I = 2939 * 6329 * 129499 * 308491 * 304247586761 * 2084303944451$

表 3.16: $P = 5, q = 2p + 1$ 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	$J = K$

– $*620216264269531 * 8237123176890810696379$

$J = 9183549615799121156005754197048794357958324662281 93$

–

$37617871227053001348394900560379028320 31)$

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

$25080566643341653267842952512497709031897599900179635412 4089$

$q = 2p + 1$ 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.

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

3 ?- A=332207361361,B is A-1, factorize(B,BB),exps(BB,J).
A = 332207361361,
B = 332207361360,
BB = [2, 2, 2, 2, 3, 3, 5, 7, 23|...],
J = [2^4, 3^2, 5, 7, 23, 293, 9781].
```

B がどれも 2×23 を因数に持つ.

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

```
4 ?- A=59,B is A-1, factorize(B,BB),exps(BB,J).
```

```
A = 59,
B = 58,
BB = J, J = [2, 29].

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

6 ?- A=22125996444329,B is A-1, factorize(B,BB),exps(BB,J).
A = 22125996444329,
B = 22125996444328,
BB = [2, 2, 2, 7, 29, 13624382047],
J = [2^3, 7, 29, 13624382047].
```

B はどれも 2×29 を因数に持つ.

3.2.3　$P = 7$

表 3.17: $P = 7, q = 2p + 1$ 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	$D = E$

$A = (74279400543938659833650076624280 01) = 83 * 20515909 * 436213933622906865609 4783$
$B = (10281225160467706104845935946923162113219 6401)$
$C = 8269 * 319591 * 89042760170351880563720518398412 19$
$D = (23173203249700874472330986792321198522833668720161907874906686459440 57)$
$E = 167*66733*76066181*7685542369*62911130477521*303567967057423*18624275418445601$

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

- $e \equiv 1 \mod 4$ なら $q \equiv 01, a \equiv 93 \mod 100$.

- $e \equiv 3 \mod 4$ なら $q \equiv 57, a \equiv 01 \mod 100$.

が成立していることを確認.

3.2.4　$P = 11$

表 3.18: $P = 11, q = 2p + 1$ 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	(1586309297171491574414436704 89)=523*303309617049998388989376043
41	83	$X = Y$
53	107	$A = B$
83	167	$C = D$

$X = (4978518112499354698647829163838661251242 41)$
$Y = 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$
$A = (1562472251828744662703731061631669238387852269920031433)$
$B = 107 * 351497 * 6005113 * 691808237490131385512539766532597713 5579$
$C = (2726420685613255110404143331020352977239743121502216309 6159$
$- - 207985879419668700193602213)$
$D = 167 * 12119 * 178057577 * 52447614013*$
$1442525225996981034595894901431683672700025887063977893738081$
$q = 2p + 1$ が N_p の最小素因子となるのは $q = 7, 83, 107, 167$

3.2.5　$P = 13$

$A = (74279400543938659833650076624280 01) = 83 * 20515909 * 4362139336229068656094783$
$B = (1028122516046770610484593594692316211321961 401)$
$C = 8269 * 319591 * 389042760170351880563720518398412 19$
$D = (2317320324970087447233098679232119852283366872016190787490668645944057)$
$E = 167*66733*76066181*7685542369*62911130477521*303567967057423*18624275418445601$
$F = (2726304189124058180795268265129796685012858291258328299574896755266723816 01)$
$G = 1805633*184896053147409877659 13*816614687584787676285911901514700476265645056 9$
$q = 2p + 1$ が N_p の最小素因子となるのは $q = 47, 59, 83, 167$

表 3.19: $P = 13, q = 2p + 1$ 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	$F = G$

$p = 89$ のときの G = 1805633∗184896053147409877659 13∗816614687584787676285911901514700476265645056 9の各素因数について

```
?- A=1805633,B is A-1, factorize(B,BB),exps(BB,J).
A = 1805633,
B = 1805632,
J = [2^6, 89, 317].

?- A=1848960531474098776591 3,B is A-1, factorize(B,BB),exps(BB,J).
A = 1848960531474098776591 3,
B = 1848960531474098776591 2,
J = [2^3, 3, 7, 89, 89839, 13764595178129].
```

B はどちらも 2×89 を因数に持つ.

第4章　弱弱完全数

4.1　条件を弱め

条件をさらに弱めて, $\varepsilon+1$ を奇数 ($\varepsilon+1=2$ は付加する) 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) と呼んでみたい.

表 4.1: $P=2$

$2\varepsilon-1$	$Q=2^{2\varepsilon-1}-1$	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 $6,8,6,8,\cdots$ 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 $7,1,7,1,\cdots$ となり正確に繰り返されている.

の繰り返しになりそうだ.

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 4.2: $P = 2$

$2\varepsilon - 1$	$Q = 2^{2\varepsilon-1} - 1$	素因数分解	Q の下 2 桁	a	Q 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. これは第 2 の完全数.

完全数の下 2 桁 の数を研究した結果はあるそうだが私は知らない.

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ずらくなっている.

4.1.1　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.

$2^{10} = 1024 \equiv 24 \mod 100$ 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

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

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

$20 + 3 = 23$ 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

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

$L = 1, 2, 3, 4$ 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.

$\xi = 20m + 3 + 2L$ とおくとき

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

$a_\xi = 2^{\xi-1}Q_\xi$ が成り立つ.

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

が成り立つことを以下で示す.

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

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

4.1.2　$P = 2$; 弱弱完全数の p, Q, a 変化

表 4.3: $P = 2$

$p = 2e - 1$	$Q = 2^p - 1$	$a = 2^{p-1}Q$
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.

4.2　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**という.

表 4.4: $P = 3$

$2\varepsilon - 1$	$(3^{2\varepsilon-1} - 1)/2$ = 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*757	64566801
11	(88573)=23*3851	5230147077
13	(797161)=79716	423644039001
15	$(7174453)=11^2 * 13 * 4561$	34315186290957
17	(64570081)=1871*34511	2779530261754401
19	(581130733)=1597*363889	225141952751788437
21	(5230176601)=13*1093*368089	18236498186842001001
23	(47071589413)=47*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

$A = (423644304721) = 11^2 * 8951 * 391151$
$B = 119649664615167550026801$
$C = (3812798742493) = 13 * 109 * 433 * 757 * 8209$
$D = 96916228338387390154841 97$
E=(34315188682441)=59*28537*20381027
F= 785021449541029367424039801
G= 308836698141973 = 683*102673*4404047
H=635867374128242023258756024 77
I= 2779530283277761 = 13*23*3851*2413941289
J= 515052573043876780047667920 8001

$K = 25015772549499853 = 11^2 * 71 * 1093 * 2664097031$
L= 417192584165540258547337814514357
M=225141952945498681 = 13097927*17189128703
N= 337925993174087615427129041636594 01
$O = 2026277576509488133 = 13^2 * 313 * 6553 * 7333 * 797161$

P= 27372005447101096903631521079483798 37

表 4.5: $P = 3$

$2\varepsilon - 1$	$Q = (3^{2\varepsilon-1} - 1)/2$	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=96916228338387390154841 97
G=78502144954102936742403 9801

4.3　$P = 3$

表 4.6: $P = 3$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 ?- B is 3^5.
B = 243.

 ?- C is 43^4.
C = 3418801.
```

これより

$$3^5 \equiv 43 \mod 200, 43^4 - 1 \equiv 0 \mod 200.$$

よって $3^{20} - 1 \equiv 0 \mod 200$.

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

4.3.1　$P = 5$

表 4.7: $P = 5$

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

周期 は 2

4.3.2　$P = 7$

表 4.8: $P = 7$

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

4.3.3　$P = 11$

表 4.9: $P = 11$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $(53 - 3)/2 = 25$

```
10 ?- A is 11^10.
A = 25937424601.

11 ?- B is 4601^5.
B = 2061869461571623001.
```

これより

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

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

4.3.4　$P = 11$ 弱弱完全数

表 4.10: $P = 11$

$2e+1$	$(11^{2e+1}-1)/10$	分解	a
3	133	7*19	16093
5	16105	5*3221	235793305
7	1948717	43*45319	3452271037237
9	235794769	7*19*1772893	U
11	28531167061	15797*1806113	V
13	3452271214393	1093*3158528101	W
15	417724816941565	5*7*19*3221*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= 232251544198878080950520379327369 7
Z=340039485861577398986846964992269755 49
$A = 7^2 * 19 * 43 * 1723 * 8527 * 27763 * 45319$
B= 4978518112499354698647156413843728691233 21
C=829*28878847*3740221981231
D= 728904836851030521429027853850124525396790 2613
$E = 5^2 * 3001 * 3221 * 24151 * 1856458657451$
F= 106718957163359378642424086278988841454677198699025
$G = 7 * 19 * 1772893 * 5559917315850179173$
H= 156247225182874466270373106151248747301058017567401 8157

4.3.5　$P = 13$

表 4.11: $P = 13$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $(23 - 3)/2 = 10$

4.3.6　$P = 13$

表 4.12: $P = 13$

$2e+1$	$Q = (13^{2e+1}-1)/12$	分解	a
3	183	3*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	99377774376041001379932917343	S	T
29	167948438695509292332086630309 81	U	V
31	283832861395410704041226405223 5803	W	X
33	47967753575824408982967262482785 0721	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= 167948438695509289050939642227 07
$I = 103 * 443 * 15798461357509$
J= 47967753575824408977422124072925 2401
$K = 12865927 * 9468940004449$
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= 911625419070951825336383806945630217591167918481033654408 7

$U = 1973 * 2843 * 3539 * 846041103974872866961$

V= 260369335940854550834324579101958487505450742744381795527146101

$W = 311 * 1117 * 817050901143136340856815036 9$

X= 74364086038067468263791443037310730415821897627517337897708794533 47

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

Z=212391266133324496108214740458863183339538614689722045030030778150037601

```
2 ?- A is (13^20-1)/12.
A = 1583746981240066619900
```

4.3.7　$P = 17$

表 4.13: $P = 17$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $(23 - 3)/2 = 10$

4.3.8　$P = 19$

表 4.14: $P = 3$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $(23 - 3)/2 = 10$

4.3.9　$P = 23$

表 4.15: $P = 23$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $(23 - 3)/2 = 10$

4.3.10　$P = 31$

表 4.16: $P = 31$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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

4.3.11　$P = 37$

表 4.17: $P = 31$

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $(23 - 3)/2 = 20$

4.3.12　$P = 41$

表 4.18: $P = 41$ 前半分

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 4.19: $P = 41$ 後半分

$p = 2e - 1$	$Q = N_p$	$a = P^{p-1}Q$
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

4.3.13　$P = 43$

表 4.20: $P = 43$

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

第5章　Wieferich の素数

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)
$2^{\frac{p-1}{2}}-1$ 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=<2000).
wieferich = 1093
wieferich = 3511

 ?- wieferich_loop2(2,1=<2000).
wieferich2 = 3511

3 ?- wief2(191,13).
prime=2 146=191^2       (mod)=169       no
prime=3 1=191^3 (mod)=169       1=ok
prime=5 146=191^5       (mod)=169       no
```

この結果, $Q=13, P=191, p=3$

```
4 ?- wief2(197,7).
prime=2 1=197^2 (mod)=49        1=ok
prime=3 1=197^3 (mod)=49        1=ok


5 ?- wief2(199,5).
prime=2 1=199^2 (mod)=25        1=ok
```

この結果, $Q=5, P=199, p=2$

[1] Arthur Wieferich in 1909

完全数については多くの難問があるが

「弱完全数のとき N_p 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 p は強い意味での Wieferich の素数になる.

Wieferich の素数ですら人類はまだ 2 つ発見しただけである. 強い意味での Wieferich の素数は 3511 ただ 1 つしか発見されていない.

ここで, 奇素数を底とする弱完全数に戻る.

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

これはうれしい. そこで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.

表 5.1: $p=e+1$、$N_p=(3^p-1)/2$:素数

e	3^e=素因数分解	N_p	N_p の素因数分解
1	3=3	4	$[2^2]$
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.

5.1　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.

5.1.1　$Q=2$ 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 $P\equiv 1 \mod 4$ 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 N_p は 4 を平方因子に持たない. これを以下で証明する.

一方, p : 奇素数のとき, 各 k について $P^k\equiv 1 \mod 4$ によって

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

N_p は 4 を平方因子に持たない.

一方, $p=2$ とのき,

$$N_2=1+P\equiv 2 \mod 4.$$

N_2 は 4 を平方因子に持たない.

ただし $P=1+4k$.

表 5.2: $p = 2, Q = 2, P = 3 + 4k$

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	$[2^3, 5^2]$

5.1.2　弱完全数と Wieferich の素数

弱完全数に話しを戻す.

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

$$P^p \equiv 1 \mod Q^2.$$

1) $P \equiv 1 \mod Q$ 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

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

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

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

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, $Q = 1 + 2pL \geq 7$.

$Q = 2$, $p \geq 3, P \equiv 1 \mod 4$ のとき

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

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

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

したがって, $Q = 2$ ならば $p = 2$ になる.

$Q = 2$, $p = 2, P \equiv 1 \mod 4$ のとき

$$N_2 = P + 1 \equiv 2 \mod 4.$$

N_2 は平方因子 4 を持たない.

$p = 2, P \equiv -1 \mod 4$ のとき $(P = 3, 7, 11, 19, 23, 31, 43, \cdots)$

$$N_2 = P + 1 \equiv 0 \mod 4.$$

N_2 は平方因子 4 を持つ.

$Q - 1 = pk$ となるが, p が奇数なら k は偶数なので $k = 2L$. $Q - 1 = 2pL \geq 2p$ により $\frac{Q-1}{2} \geq p$.

したがって, $Q \geq 3$ のとき $\frac{Q-1}{2} \geq p$ を満たす p について $N_p = \frac{P^p-1}{\overline{P}}$ 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.

p が偶数なら $p = 2$. $Q = 1 + 2k$.

$k = 1, 2, 3, 5, 6$ 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.

表 5.3: $P = -1 + 9N$

P	$P+1$ 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 5.4: $P = -1 + 5^2N$

P	$P+1$ 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 5.5: $P = -1 + 7^2N$

P	$P+1$ 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 5.6: $P = -1 + 11^2N$

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

表 5.7: $P = -1 + 13^2N$

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

2) $P \equiv 1 \mod Q$ なら, 各 j につき $P^j \equiv 1 \mod Q$ により

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

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

$$P^j = 1 + Qkj + \cdots \equiv 1 + Qkj \mod Q^2.$$

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

このとき $N_p \equiv 0 \mod Q^2$ に矛盾. よってこの場合は起きない.

5.1.3　(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 の整数倍かどうかが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 5.8: 強い意味の Wieferich 素数の例, $Q \geq 7$

P	prime	prime
P=3	prime = 11	
P=19	prime = 3	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 = 3	prime = 5

この表にある P に対して $prime = Q$ で与えられる Q について, 奇素数 p なら, $\frac{Q-1}{2} \geq p$ を満たす. これらの 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. しかし $\frac{Q-1}{2} \geq p \geq 3$ なので $Q \geq 7$.

$p = 2$ については $Q = 2, 3, 5$ が対応するので別途検討する.

5.1.4　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,KK),
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.

表 5.9: Q^2 が N_p の因数

P	prime=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

5.1.5　参考

強い意味の Wieferich 素数 Q はあまりない.

表 5.10: 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

5.1.6　一般の Wieferich 素数

表 5.11: 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 Wiefirech 素数は本来の Wiefirech 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 Wiefirech 素数だった. 半分は強い意味の Wiefirech 素数であるとは意外だった.

5.2　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

5.2.1　$P = 53$

表 5.12: $P = 53$

p	$(2p+1)=$	$N_p =$ 分解	a
2	(5)=5	(54)=2*3^3	2862
3	(7)=7	(2863)=7*409	8042167
5	(11)=11	(8042221)=11*131*5581	63456991998301
7	(15)=3*5	(22590598843)=29*778986167	500706190876621573747
11	(23)=23	(178250690949465223)=178250690949465223	311738124310568242387515485781949 27
13	(27)=3^3	A	B
17	(35)=5*7	C	D
19	(39)=3*13	E	F
23	(47)=47	G	H

$A = (500706190877047811461) = 13 * 3297113 * 11681692691969$
$B = 24597637468481768160273653860668729814050 1$
$C = (39508126856977190924247544 81) = 647 * 4013 * 12479 * 121936356626073149$
$D = 153144129363856840298269545521743533506967830282106204 01$
$E = (11097832834124892930621135337183) = 229 * 32688470798197 * 1482545708952391$
$F = 120838084300705448509353018182383219548095580591429385933186087$
$G = (875672391188386192961003865764712067 63) = 47^2$*4969*21529*16055056483*23080289344401529
$H = 752334171846386320152577501685552265953592059779483528661393037833264739606 7$

$p = 2$ において $N_2 = 54 + 1 = 2 * 3^3$ 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.

5.2.2　$P = 71$

表 5.13: $P = 71$

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

$A = (1664410677979282272187 3) = 3202878953 * 5196608121641$
$B = 27312451175774899273898654531941447400995 3393$
$C = (42295473201803245709778876153 7) = 239 * 3652120847 * 484563667343825089$
$D = 17637111793734078180699022458617462600579284312004106099897 7$
$E = (21321148041029016162299531469080 89) = 1900857799450121 * 1121659287043817009$
$F = 44818865866370819355698391573023779564748172141839760217379732555 29$
$G = (54180621257240427046019992014174494350633) = 47^2$*242329*10121453273837111836563693857035 3
$H = 28941940899639060048490540264976542606198068092929301862261381129262097526594281 53$
$p = 2$ 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.

5.2.3　$P = 79$

表 5.14: $P = 79$

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

5.2.4　$P = 137$

表 5.15: $P = 137$

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)=234632047438371100326 7

B= 5465035682610653717879961178365556122821683

$C = (440380889837078718203184 61) = 864319 * 19805293 * 2572605139183$

D= 1925197417969549460912161511671456536120639693634141

$E = (155135336944858136640444129863296 81) = 17*103*885981364619406834040229182543 1$

F= 2389130143491441285714104851126852602568450957459175013920626680199 21

G=(291173513911804236660449587340421782827)=29117351391180423666044958734042178282 7

H= 84163168377442927933524042922256325776247704876773687945116498292399482547483

$I = (102573254726919359630889312802648113437647615807)$

$= 1381 * 143235060131 * 518550578298278365204966204101137$

$J = 104444749751619994641076050602515305522087006896962812$

$- - 24738478203470769145406043274426557803983$

$K = (67819961541149092335018708592760553688023207495468775836654 1)$

$= 59^2 * 616367 * 3160924605365392930438533910600424447165692844394 83$

$L = 4565973846337519033465476544 83[60digits]475472486261488580834605020461$

$p = 23$ で $K = 59^2 * 616367 * 3160924605365392930438533910600424447165692844394 83$ において平方因子 59^2.

5.2.5　$P = 197$

表 5.16: $P = 197$

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

5.2.6　$P = 199$

表 5.17: $P = 199$

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

第6章　フェルマの (弱) 完全数について

6.1　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

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

ゆえに, $P^E\equiv -1$.

一方, $P=2k+1$ とおくとき

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

これで前の式に矛盾した.

以上を踏まえて, $E=2^m$ 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.

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

補題 5 $e>1$ 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, 弱完全数は無限にあるので研究材料として有利である.

6.2　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

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

$E=2^m$ によって

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

ゆえに

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

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

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

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

この結果は $P = 2$ のときオイラーによる.

$\frac{Q-1}{2} = 2^m K$ によれば

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

オイラーの基準にしたがい

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

次のようにまとめる.

定理 2 $Q = 1 + 2^{m+1}K$ 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.

6.3　例

6.3.1　$P = 2$

$F_m = 2^{2^m} + 1$ 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 6.1: $P = 2$; フェルマ完全数

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= 170141183460469231731687303715884105728
B= (18446744073709551617)=274177*67280421310721
C= 57896044618658097711785492504343953926805133516280751251460479307672448925696
D= (340282366920938463463374607431768211457)=59649589127497217*5704689200685129054721
E= 670390396497129854978701249910[94 digits]761687993013765220781067862016
F= (115792089237316195423570985008687907853269984665640564039457584007913129639937)
= 1238926361552897∗93461639715357977769163558199606896584051237541638188580280321.

$m = 5, 6$ 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 6.2: 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. このためオイラーによって発見されたのである. まさに僥倖としかいいようがない.

6.3.2　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 を法として計算すると次の表ができる.

表 6.3: $P = 2$

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.

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

表 6.4: $P = 2, \mathrm{mod} = 1000$

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

6.3.3　末尾３桁

$m = 2$ 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おこる.

$22 - 2 = 20$ なので周期 20 である.

6.3.4　$P = 3$

表 6.5: $P = 3$; フェルマ完全数

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

$A = 572280636715419056279672990187 = 3^{31} * 926510094425921$
$B = (926510094425921) = 926510094425921$
$C = 196503076295643052858681214356932539158308401746008 3159697707$
$D = (171684191014625624232892454 4641) = 171684191014625624232892454 4641$
$E = 231680753961907887941566311316[62digits]771379200003876302731668088747$
$F = (589509228886929158576043643070625933283910579613792055454 8481)$
$= 257 * 275201 * 138424618868737 * 3913786281514524929 * 153849834853910661121$

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

6.3.5　素因数分解

```
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].
```

6.3.6　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.

6.3.7　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.
$h_m = 3^{2^m}, L_m = \frac{1+h_m}{2}, h_{m+1} = h_m^2, K_m = 3^{2^m-1}$ とおく.
$h_m = 2L_m - 1, (h_m)^2 + 1 = 4{L_m}^2 - 4L_m + 1$. ゆえに $L_{m+1} = 2{L_m}^2 - 2L_m + 1$. $a_m = K_m L_m$ に注して次の表を作る.

表 6.6: $P = 3$

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 6.7: $P = 3$

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

6.3.8　$P = 5$

表 6.8: $P = 5$; 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

$A = (5421010862427522170037496834993362426757812 5) = 5^{31}$*641*75068993*241931001601

$B = (11641532182693481445313) = 641 * 75068993 * 241931001601$
$C = (29387358770557187699218413430556141945466638973512296661994014357333071529865264892578125) =$
$5^{63} * 769 * 3666499598977 * 961329567826437419512256640 01$
$D = (27105054312137610850186320021748542785644 5313) =$
$769 * 3666499598977 * 961329567826437419512256640 01$

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

6.3.9　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].
```

6.3.10　$P = 7$

表 6.9: $P = 7$; 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

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

$B = (16616465284801) = 353 * 47072139617$

$C = (871257491168454071527552759762428210713954243168955 43) = 7^31*7699649*134818753*$
531968664833

$D = (55221383712196032315264960 1) = 7699649 * 134818753 * 531968664833$

$E = (106272546228400835422165191552[48digits]6330155520987631606142877339 43) =$
$7^63 * 35969 * 1110623386241 * 152668481967935560980850003328886343 69$

$F = (60988024381791785006928693128148591037780764706561920 1) =$
$35969 * 1110623386241 * 152668481967935560980850003328886343 69$

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.

6.3.11　$P = 11$

表 6.10: $P = 11$; 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

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

$B = (22974864931786081) = 51329 * 447600088289$

$C = (20263253111481374526679600606226562049399254410212783005132677437 1) =$
$11^{31} * 193 * 257 * 212836200332176295391787993 61$
$D = (10556888372676276427728076271049 61) = 193 * 257 * 212836200332176295391787993 61$
$E = (90331873865191113335801469288 8[72digits]3181993573086176804036725916 51) =$
$11^{63} * 316955440822738177 * 703240126270470764951876770375638576156760620606 73$
$F = (22289578422629511979347560666849207697450807174957633577569674131 21) =$
$316955440822738177 * 703240126270470764951876770375638576156760620606 73$
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.

6.3.12　一般の場合

奇素数 P について $h_m = P^{2^m}$, $B_m = P^{2^m-1}, L_m = \frac{h_m+1}{2}$ とおくとき, $h_{m+1} = {h_m}^2, h_m = 2L_m - 1, N_{m+1} = 2L_m - 2L_m + 1$ が成り立つ.
これらを表計算にいれて計算する.

6.3.13　末尾 3 桁

表 6.11: $P = 5$

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

$m \geq 2$ のとき, $L_m \equiv 313; a_m \equiv 125 \mod 1000$

6.3.14　$P = 7$

表 6.12: $P = 7$

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

$A = 125749116845407152755275976242821071395424316895543$
$B = (552213837121960323152649601) = 7699649 * 134818753 * 531968664833$
$C = 10627254622840083542216519155 2[48digits]6330155520987631606142877339 43$
$D = (60988024381791785006928693128148591037780764706561920 1)$
$= 35969 * 1110623386241 * 152668481967935560980850003328886343 69$

$P = 7, m = 1$ 平方因子 5^2 あり.

6.3.15　素因分解

```
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
$q \equiv 1, a \equiv 43 \mod 100.$ を以下で証明する.
$7^3 = 343 \equiv 43 \mod 100.$
$7^4 = 2401 = 1 + 200 \times 12 \equiv 1 \mod 200.$
$(7^{2^e})^{2^f} = 7^{2^{e+f}}$ を使う.
$(7^{2^{m-2}})^4 = 7^{2^m} \equiv 1 \mod 200$ と変形すると

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

$m \geq 3$ のとき,

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

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

$m = 2$ $2^m - 1 = 3$ なので $a = 7^3 q \equiv 343 \equiv 43 \mod 100.$

[課題]

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

6.3.16　末尾 2 桁

表 6.13: $P = 7$

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

6.3.17　末尾 3 桁

表 6.14: $P = 7$

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

6.3.18　$P = 11$

表 6.15: $P = 11$

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

$A = 95971712478875242340697505353731$
$B = (22974864931786081) = 51329 * 447600088289$
$C = 202632531114813745266796006062265620493992544102127830051326774371$
$D = (10556888372676276427728076271049 61) = 193 * 257 * 212836200332176295391787993 61$
$E = 90331873865191113335801469288 8[72digits]3181993573086176804036725916 51$
$F = (22289578422629511979347560666849207697450807174957633577569674131 21)$
$= 316955440822738177 * 703240126270470764951876770375638576157606206067 3$

```
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].
```

6.3.19　末尾２桁

表 6.16: $P = 11$

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.

6.3.20　末尾３桁

周期 20 である.

表 6.17: $P = 11$

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

6.3.21　$P = 13$

表 6.18: $P = 13$

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

$A = 170299716837246422680665308204601 97$

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

$C = 754051832426004128194845232398330830258394399157524945745785215350131 7$

$D = (221389631888420349152156596074392641) = 193*1601*10433*6867512045613988148256268 9$

$E = 14783448315610379880572534271 4[82 digits]0669729785585885558908518395 57$

$F = (98026738215380536665329880211783007712201640002057893794795481921124481)$

$= 257 * 3230593 * 36713826768408543617 * 3215877717636198473712500018174097551256193$

```
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] .
```

6.3.22　末尾２桁

表 6.19: $P = 13$

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.

6.3.23　末尾 3 桁

表 6.20: $P = 13$

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.

第7章　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.

$$P^E+1\equiv 0 \mod Q^2.$$

$P^E\equiv -1 \mod Q$ により $(P^E)^2\equiv 1 \mod Q$ なので Q を法としてみるとき 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 $P^{Q-1}\equiv 1 \mod Q$ が成り立つので $Q-1$ は 2^{m+1} の倍数. よって $Q-1=2^{m+1}k$.

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

$P^{Q-1}-1$ 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 $P^{2^{m+1}k}-1\equiv 0 \mod 4$ 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.

7.0.24　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
```

7.0.25　一般の Wieferich 素数

```
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 7.1: 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				

7.0.26　$P = 41$

$A = 777549157495866332581241$
$B = 17 * 41^7 * 234850742033$
$C = (3992462614561) = 17 * 234850742033$
$m = 1$ に平方因子 29^2

表 7.2: $m = 1$ 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 7.3: $m = 2$ の場合

P	L_2 素因数分解
179	$[17^2, 1776169]$

表 7.4: $m = 3$ の場合

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

表 7.5: $P = 41$

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

7.0.27　$P = 43$

表 7.6: $P = 43$

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

$A = 135909345307$
$B = 17 * 43^3 * 193 * 521$
$C = (1709401) = 17 * 193 * 521$
$m = 1$ に平方因子 5^2

7.0.28　$P = 107$

表 7.7: $P = 107$

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

7.0.29　$P = 131$

表 7.8: $P = 131$

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

7.0.30　$P = 157$

表 7.9: $P = 157$

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

$A = 1175621640703693$

$B = 113 * 157^3 * 2688377$
$C = (303786601) = 113 * 2688377$
$D = 433975078587972309446276265685093$
$E = 157^7 * 1297 * 142307322503233$
$F = (184572597286693201) = 1297 * 142307322503233$
$m = 1$ に平方因子 5^2

7.0.31　$P = 179$

表 7.10: $P = 179$

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	$17^2 * 179^3 * 1776169$	$(513312841) = 17^2 * 1776169$

7.0.32　$P = 193$

表 7.11: $P = 193$

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8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. $a=P^eL_m$ 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 $\sigma(a)=\frac{P^{e+1}1}{\overline{P}}(q+1)$ によって

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

よって,

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

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

$P, Maxp(a)$ 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ることはない.

8.1　$s(a)=2$ の場合

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

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

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

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

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

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 $\Delta = p + q$ とおくとき

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

$C = pX + qY - 1$ 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 $R = D - p_0 q_0$ をえる.

8.1.1　$P = 3$ 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) $Y \geq q^3$.

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

これを変形して

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

$\frac{\overline{q}^2}{Y-1}$ は整数になり

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

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 8.1: $P = 3$

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

$a = 3^e qr$ 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.

8.1.2　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 8.2: $P = 5$

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:

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

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

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

よって

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

これより移項して

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

1). $X = 3$ と仮定する．

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

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

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

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

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

$Y = \frac{16*35}{Q} + 2Q - 66$ 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. $Q \leq 16$.
$20Y \leq QY = 16 + 2(Q - 16)(Q3517) \leq 16$ 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) $Y \geq q^3$.

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

これを変形して

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

$\frac{(q-1)^2}{Y-1}$ 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.

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

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

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.

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

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

によって

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

これより

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

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

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

8.1.3　$P = 7$ 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 8.3: $p = 7$

a	素因数分解
411943	$7^3 * 1201$

8.1.4　$P = 11$ 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 8.4: $P = 11$

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

8.1.5　$P = 19$ のとき

表 8.5: $p = 19$

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.

8.2　$a = P^e qr$ 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 $\overline{P}\sigma(a) - aP = Maxp(a) - 2$ の解 $a = P^e qr$ があるとする.

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

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, $\Delta' = \widetilde{q} + r = \Delta + 1$ によって

$$\Gamma\Delta' = \widetilde{qr} - 2.$$

$\widetilde{q_0} = \widetilde{q} - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + 2$ によれば

$$\widetilde{q_0}r_0 = D.$$

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 $\widetilde{q_0}r_0$ を求め $q = \widetilde{q_0} - 1 + \Gamma, r = r_0 + \Gamma$ 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 8.6: $P = 3$

a	素因数分解
741	$3 * 13 * 19$
38781	$3^2 * 31 * 139$
49542866651558159O1	$3^{11} * 536917 * 52088299$

$P = 11$ のときの

表 8.7: $P = 11$

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

$P = 17$ のときの

表 8.8: $P = 17$

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

$P = 23$ のときの だけだった. 少し残念である.

表 8.9: $P = 23$

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
```