書泉グランデでの講義 第 3期　資料 4
高校生も十分わかる新しい数論研究 , 2015 年 7月 24 日

飯高 茂

平成 27 年 7 月 21 日

フェルマの (弱) 完全数について

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 $L_m=\frac{P^E+1}{2}$ とする. $F_m(P)$ と書く流儀もある;[1]

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

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

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.

L_m を P が**底のフェルマ素数**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.

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

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}.

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

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

$$P^{\frac{Q-1}{2}} = P^{2^m K}.$$

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 1 Q を L_E の 素因子とすると $Q = 1 + 2^{m+1}K$ と書ける.

$Q = 1 + 2^{m+1}K$ 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.

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.

定理 2 $Q_0 = 1 + 2^{m+2}$ は素数で $\left(\frac{P}{Q_0}\right) = 1$ とする.

Q_0 は $P^{2^{m'}} + 1$ の約数になる.

$\left(\frac{P}{Q_0}\right) = -1$ とする. $Q_0 = 1 + 2^{m+1}$. $1 + P^{2^m} \equiv 0 \mod Q_0$.

Proof.

$Q_0 = 1 + 2^{m+2}$ は素数で $\left(\frac{P}{Q_0}\right) = 1$ とする.

オイラーの基準によって $\left(\frac{P}{Q_0}\right) = P^{\frac{Q_0-1}{2}}$.

仮定により $1 = P^{\frac{Q_0-1}{2}} = P^{2^{m+1}}$. よって

$$P^{2^m} \equiv \pm 1 \mod Q_0.$$

したがって Q_0 は $P^{2^m} - 1$ または $P^{2^m} + 1$ の因子になる.

Q_0 が $P^{2^m}+1$ の因子になれば良し.
Q_0 が $P^{2^m}-1$ の因子になる場合は.

$$P^{2^m}-1=(P^{2^{m-1}}-1)(P^{2^{m-1}}+1)$$

と分解する. 必要ならくり返す.

$\left(\frac{P}{Q_0}\right)=-1$ とすると $Q_0=1+2^{m+1}$.
オイラーの基準によって

$$-1=\left(\frac{P}{Q_0}\right)=P^{\frac{Q_0-1}{2}}=P^{2^m}$$

よって $1+P^{2^m}\equiv 0 \mod Q_0$.

3 共鳴原理

一般化されたユークリッドの完全数に関する結果から一般化されたフェルマの完全数に関する結果を推理してその結果新しい事実がわかることが多い.
定理 1,2 の元の定理はフェルマとオイラーによる次の結果である.

定理 3 奇素数 P が底のとき $N_p=\frac{P^p-1}{P}$ の素因子 *(*奇数*)* Q について $P-1\not\equiv 0 \mod Q$ ならば,

⟨*1*⟩ N_p の素因子 *(*奇数*)* Q について $\left(\frac{P}{Q}\right)=1$.

⟨*2*⟩ 一般に $2p+1$ が素数 Q のとき $\left(\frac{P}{Q}\right)=1$ を仮定すると, Q は N_p の素数因子.

$P\equiv 1 \mod Q$ ならば, $p=Q$.

共鳴原理の例
一般に $2p+1$ が素数 Q のとき に共鳴してできた定理は素数 $Q=1+2^{m+1}$ に対して考えるが, これはフェルマー素数なので 5 種類しかない上に一番大きな 65537 は例の計算に使えないから, 257 を代表的に扱うにとどめた.

表 1: 平方剰余; (P/Q)=1

P/Q
11/257
13/257
17/257
23/257
29/257
31/257
59/257
61/257
67/257
73/257
79/257
89/257
113/257
137/257
139/257
157/257
173/257
193/257
197/257
199/257
211/257
223/257
227/257
239/257
241/257

後半の定理の例.

$Q_0 = 257$, 素数 P に対して ルジャンドル記号 $\pm 1 = [P/257]$ の値を書く. $MM = 2^M$ とし $P^M M$ を Q_0 で割った余り K を $P = K$ の形で書く.

$M = 7$ のとき 平方剰余なら $K = 1$.

$M = 7$ のとき 平方非剰余なら $Q_0 = 1 + 2^{m+1} = 257.m = 7.\ 2L_m = 1 + P^{2^7} \equiv 0 \mod Q_0$.

```
5 ?- p2mm_all(257,7,2=<100).
5=256   -1=[5/257]
7=256   -1=[7/257]
11=1    1=[11/257]
13=1    1=[13/257]
17=1    1=[17/257]
19=256  -1=[19/257]
```

```
23=1     1=[23/257]
29=1     1=[29/257]
31=1     1=[31/257]
37=256   -1=[37/257]
41=256   -1=[41/257]
43=256   -1=[43/257]
47=256   -1=[47/257]
53=256   -1=[53/257]
59=1     1=[59/257]
61=1     1=[61/257]
67=1     1=[67/257]
71=256   -1=[71/257]
73=1     1=[73/257]
79=1     1=[79/257]
83=256   -1=[83/257]
89=1     1=[89/257]
97=256   -1=[97/257]

101=256 -1=[101/257]
103=256 -1=[103/257]
107=256 -1=[107/257]
109=256 -1=[109/257]
113=1    1=[113/257]
127=256 -1=[127/257]
131=256 -1=[131/257]
137=1    1=[137/257]
139=1    1=[139/257]
149=256 -1=[149/257]
151=256 -1=[151/257]
157=1    1=[157/257]
163=256 -1=[163/257]
167=256 -1=[167/257]
173=1    1=[173/257]
179=256 -1=[179/257]
181=256 -1=[181/257]
191=256 -1=[191/257]
193=1    1=[193/257]
197=1    1=[197/257]
199=1    1=[199/257]
```

$M = 6$ のとき平方剰余なら $K = 1$ または $K = -1$. (P=13,29,31,59,61,)

```
6 ?- p2mm_all(257,6,2=<100).
5=16     -1=[5/257]
```

```
7=241   -1=[7/257]
11=1    1=[11/257]
13=256  1=[13/257]
17=1    1=[17/257]
19=241  -1=[19/257]
23=1    1=[23/257]
29=256  1=[29/257]
31=256  1=[31/257]
37=16   -1=[37/257]
41=16   -1=[41/257]
43=16   -1=[43/257]
47=241  -1=[47/257]
53=241  -1=[53/257]
59=256  1=[59/257]
61=256  1=[61/257]
67=1    1=[67/257]
71=16   -1=[71/257]
73=1    1=[73/257]
79=256  1=[79/257]
83=16   -1=[83/257]
89=256  1=[89/257]
97=16   -1=[97/257]

101=16  -1=[101/257]
103=241 -1=[103/257]
107=16  -1=[107/257]
109=16  -1=[109/257]
113=256 1=[113/257]
127=241 -1=[127/257]
131=16  -1=[131/257]
137=1   1=[137/257]
139=256 1=[139/257]
149=16  -1=[149/257]
151=241 -1=[151/257]
157=256 1=[157/257]
163=241 -1=[163/257]
167=241 -1=[167/257]
173=256 1=[173/257]
179=16  -1=[179/257]
181=241 -1=[181/257]
191=241 -1=[191/257]
193=1   1=[193/257]
197=1   1=[197/257]
```

```
199=256 1=[199/257]
```

$M = 5$ のとき平方剰余なら $K = -1(K = 256)$ (P=11,23,67,73,)

```
7 ?- p2mm_all(257,5,2=<100).
5=253   -1=[5/257]
7=193   -1=[7/257]
11=256  1=[11/257]
13=241  1=[13/257]
17=1    1=[17/257]
19=193  -1=[19/257]
23=256  1=[23/257]
29=16   1=[29/257]
31=241  1=[31/257]
37=4    -1=[37/257]
41=4    -1=[41/257]
43=253  -1=[43/257]
47=193  -1=[47/257]
53=64   -1=[53/257]
59=16   1=[59/257]
61=241  1=[61/257]
67=256  1=[67/257]
71=4    -1=[71/257]
73=256  1=[73/257]
79=16   1=[79/257]
83=253  -1=[83/257]
89=16   1=[89/257]
97=253  -1=[97/257]

101=4   -1=[101/257]
103=64  -1=[103/257]
107=253 -1=[107/257]
109=4   -1=[109/257]
113=241 1=[113/257]
127=64  -1=[127/257]
131=253 -1=[131/257]
137=1   1=[137/257]
139=16  1=[139/257]
149=4   -1=[149/257]
151=64  -1=[151/257]
157=16  1=[157/257]
163=193 -1=[163/257]
167=64  -1=[167/257]
173=16  1=[173/257]
```

```
179=4   -1=[179/257]
181=193 -1=[181/257]
191=193 -1=[191/257]
193=1   1=[193/257]
197=1   1=[197/257]
199=16  1=[199/257]
```

表 2: P=7 平方非剰余

m	2^m	$2L_m$	素因数分解
1	2	(50)	2*5^2
2	4	(2402)	2*1201
3	8	(5764802)	2*17*169553
4	16	(33232930569602)	2*353*47072139617
5	32	(1104427674243920646305299202)	2*7699649*134818753*531968664833
6	64	X	Y

$X = (1219760487635835700138573862562971820755615294131238402)$

$Y = 2 * 35969 * 1110623386241 * 152668481967935560980850003328886343 69$

P=11

表 3: P=11　平方剰余

m	2^m	$2L_m$	素因数分解
1	2	(122)	2*61
2	4	(14642)	2*7321
3	8	(214358882)	2*17*6304673
4	16	(45949729863572162)	2*51329*447600088289
5	32	E	F

$E = (211137767453525528554561525420992 2)$
$F = 2 * 193 * 257 * 21283620033217629539178799361$

表 4: P=13;　平方剰余

m	2^m	$2L_m$	素因数分解
1	2	(170)	2*5*17
2	4	(28562)	2*14281
3	8	(815730722)	2*407865361
4	16	(665416609183179842)	2*2657*441281*283763713
5	32	A	B
6	64	C	D

$A = (44277926377684069830431319214878528 2)$

$B = 2 * 193 * 1601 * 10433 * 68675120456139881482562689$

$C = (196053476430761073330659760423566015424403280004115787589590963842248962)$

$D = 2*257*3230593*3671382676840854361 7*3215877717636198473712500018174097551256193$

表 5: Fermat 弱完全数

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

4 例

4.1 $P = 2$

$F_m = 2^{2^m} + 1$ とおきこれをフェルマ数という.
$a_m = 2^{2^m-1} * F_m$ 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: Fermat 弱完全数

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= 170141183460469231740910675752738881536
B= (18446744073709551617)=274177*67280421310721
C= 57896044618658097711785492504343953926805133516280751251460479307672448925696
D= (340282366920938463463374607431768211457)=59649589127497217*5704689200685129054721
E= 67039039649712985497870124991 0[94 digits]76168799301376522078106786 2016
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 7: 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. 彼にとって僥倖としかいいようがない.

4.2 末尾２桁

$f_m = 2^{2^m}, F_m = f_m + 1, B_m = 2^{2^m - 1}$ とおくと, $B_{m+1} = B_m \times f_m, a_m = B_m \times F_m$.

これは数列の漸化式になるので, 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 8: $P = 2$

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 $F_m = 97, a_m = 56$.

4.3 末尾３桁

表 9: $P = 2, \mathrm{mod} = 1000$

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

$m = 2$ 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.

4.4 $P = 3$

表 10: $P = 3$; 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

$A = 57228063671541905627967299 0187 = 3^{31} * 926510094425921$
$B = (926510094425921) = 926510094425921$
$C = 196503076295643052858681214356932539158308401746008 3159697707$
$D = (1716841910146256242328924544641) = 171684191014625624232892454464 1$
$E = 231680753961907887941566311316[62digits]771379200003876302731668088747$
$F = (589509228886929158576043643070625933283910579613792055454848 1)$
$= 257 * 275201 * 138424618868737 * 3913786281514524929 * 1538498348539106611 21$

$L_1 = 5, L_2 = 41, L_4 = 21523361, L_5, L_6$ 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.

5 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 11: $P=2$

$2\varepsilon-1$	$Q=2^{2\varepsilon-1}-1$	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.

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 12: $P = 2$

$2\varepsilon - 1$	$Q = 2^{2\varepsilon-1} - 1$	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そうだ.

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ずらくなっている.

5.1 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

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

5.2 $P = 2$; 弱弱完全数の p, Q, a 変化

表 13: $P = 2$

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

6 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.

6.1 $P = 3$ 弱弱完全数の表

表 14: $P = 3$

$2\varepsilon - 1$	$(3^{2\varepsilon-1} - 1)/2 =$ 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

$A = (423644304721) = 11^2 * 8951 * 391151$
$B = 119649664615167550026801$
$C = (3812798742493) = 13 * 109 * 433 * 757 * 8209$
$D = 96916228338387390154841 97$
$E = (34315188682441) = 59 * 28537 * 20381027$
$F = 78502144954102936742403 9801$
$G = 308836698141973 = 683 * 102673 * 4404047$
$H = 63586737412824202325875602477$
$I = 2779530283277761 = 13 * 23 * 3851 * 2413941289$
$J = 515052573043876780047667920 8001$
$K = 25015772549499853 = 11^2 * 71 * 1093 * 2664097031$
$L = 41719258416554025854733781451 4357$

$M = 225141952945498681 = 13097927 * 17189128703$

$N = 337925993174087615427129041636594 01$

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

$P = 27372005447101096903631521079483798 37$

弱弱完全数の Q 下 2 桁 と a 下 2 桁 を書き出した.

表 15: $P = 3$

$2\varepsilon - 1$	$Q = (3^{2\varepsilon-1} - 1)/2$	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

$A = 2779530261754401$
$B = 225141952751788437$
$C = 18236498186842001001$
$D = 1477156353259726319517$
$E = 119649664615167550026801$
$F = 9691622833838739015484197$
$G = 785021449541029367424039801$

7　$P = 3$; 弱弱完全数の p, Q, a 変化

表 16: $P = 3$

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

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

よって $3^{20} - 1 \equiv 0 \mod 200$.

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

表 17: $P = 5$

ε	$Q = N_\varepsilon$	素因数分解	$a = P^{\varepsilon-1}Q$
3	(31)	31	775
5	(781)	11*71	488125
7	(19531)	19531	305171875
9	(488281)	19*31*829	190734765625
11	(12207031)	12207031	119209287109375
13	(305175781)	305175781	74505805908203125
15	(7629394531)	11*31*71*181*1741	46566128729248046875
17	(190734863281)	409*466344409	29103830456695556640625
19	(4768371582031)	191*6271*3981071	1818989403545761l083984375
21	(119209289550781)	31*379*19531*519499	113686837721615791320800781 25
23	(2980232238769531)	8971*332207361361	710542735760100126266479492l875
25	(74505805969238281)	11*71*101*251*401*9384251	444089209850062614679336547851 5625

7.1 $P = 5$ の弱弱完全数の p, Q, a 変化

表 18: $P = 5$

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

周期 は 2

7.2 $P = 7$; 弱弱完全数の p, Q, a 変化

表 19: $P = 7$

ε	$Q = N_\varepsilon$	素因数分解	$a = P^{\varepsilon-1}Q$
3	(57)	3*19	2793
5	(2801)	2801	6725201
7	(137257)	29*4733	16148148793
9	(6725601)	$3^2 * 19 * 37 * 1063$	38771751370401
11	(329554457)	1123*293459	93090977300134793
13	(16148168401)	16148168401	223511436608353935601
15	(791260251657)	3*19*31*2801*159871	536650959302083583960793
17	(38771752331201)	14009*2767631689	1288498953284568548534420801
19	(1899815864228857)	419*4534166740403	309368598683626211233992762679 3
21	(93090977347214001)	3*19*29*4733*11898664849	74279400543938659700662966128260 01
23	(4561457890013486057)	47*3083*31479823396757	17834484070599672225407746556059132793
25	(2235114366106608 16801)	2551*2801*31280679788951	42820596253509813014736649332142509151201

表 20: $P = 7$

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

7.3 $P = 11$; 弱弱完全数の p, Q, a 変化

表 21: $P = 11$

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

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

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

7.4 $P = 11$ 弱弱完全数の表

表 22: $P = 11$

$2e+1$	$(11^{2e+1} - 1)/10$	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

$U = 50544702828493489$
$V = 740024994423222267661$
$W = 10834705943388058361345353$
$X = 158630929717149119466460312165$
$Y = 232251544198878080950520379327 3697$
$Z = 340039485861577398986846964992269755 49$
$A = 7^2 * 19 * 43 * 1723 * 8527 * 27763 * 45319$
$B = 4978518112499354698647156413843728691233 21$
$C = 829 * 28878847 * 3740221981231$
$D = 728904836851030521429027853850124525396790 2613$
$E = 5^2 * 3001 * 3221 * 24151 * 1856458657451$
$F = 106718957163359378642424086278988841454677198699025$
$G = 7 * 19 * 1772893 * 5559917315850179173$
$H = 156247225182874466270373106151248747301058017567401 8157$

7.5 $P = 13$; 弱弱完全数の p, Q, a 変化

表 23: $P = 13$

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

7.6 $P = 13$ のときの弱弱完全数

表 24: $P = 13$

$2e+1$	$Q = (13^{2e+1} - 1)/12$	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	993777743760410013799329173 43	S	T
29	167948438695509292332086630309 81	U	V
31	283832861395410704041226405223 5803	W	X
33	479677535758244089829672624827850721	Y	Z

$A = 3^2 * 61 * 1609669$
$B = 720867993213800601$
$C = 23 * 419 * 859 * 18041$
$D = 20588710756109377851047$
$E = 53 * 264031 * 1803647$
$F = 588034167905566113995468101$
$G = 3 * 61 * 4651 * 30941 * 161971$
$H = 167948438695509289050939642227 07$
$I = 103 * 443 * 15798461357509$
$J = 47967753575824408977422124072925 2401$
$K = 12865927 * 9468940004449$
$L = 13700070098791209449615908553795581328767$
$M = 3 * 43 * 61 * 337 * 547 * 2714377 * 5229043$
$N = 391287702091575733090746033697803929523057501$
$O = 1381 * 2519545342349331183143$
$P = 11175568059437494512804842434187269399079517489227$
$Q = 701 * 9851 * 30941 * 2752135920929651$
$R = 319185399345594280780219112362033386548297277812147401$
$S = 3^3 * 61 * 650971 * 1609669 * 57583418699431$
$T = 91162541907095182533638380694563021759116791848103365440 87$

$U = 1973 * 2843 * 3539 * 846041103974872866961$

$V = 260369335940854550834324579101958487505450742744381795527146101$

$W = 311 * 1117 * 817050901143136340856815036 9$

$X = 7436408603806746826379144303731073041582189762751733789770879453347$

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

$Z = 212391266133324496108214740458863183339538614689722045030030778150037601$

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

7.7 $P = 17$; 弱弱完全数の p, Q, a 変化

表 25: $P = 17$

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

7.8 $P = 19$; 弱弱完全数の p, Q, a 変化

表 26: $P = 3$

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

7.9 $P = 23$; 弱弱完全数の p, Q, a 変化

表 27: $P = 23$

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

7.10 $P = 31$; 弱弱完全数の p, Q, a 変化

表 28: $P = 31$

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

8　弱弱完全数の周期

$p = 2\varepsilon - 1$ を奇数として,$Q = N_p = \frac{P^p-1}{\overline{P}}$, $a = P^{p-1}Q$ とおく. 周期を T とおくとき, 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 の中で最小に選ぶ.

100 を一般化して H とおき $M = \overline{P} \times H$ とする.

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

により

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

故に $P^p(P^{2T}-1) \equiv 0 \mod M$.

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.

8.1　$P = 5$ のときの周期

$P = 5$ のとき $\overline{P} = 4, M = 4H$ になり, $H = 400$ のとき

$5^p(P^{2T}-1) \equiv 0 \mod 400$. $l = 2, p = 3$ のとき

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

これより

$$5^2 \equiv 9, 5^4 \equiv 81 \equiv 1 \mod 16$$

したがって, $T = 2$.

8.2 周期の計算

一般に $H = 100$ について $M = \overline{P} \times H$ とする.
$P^{2T} \equiv 1 \mod M$ を満たす最小の T をパソコンで計算する.

表 29: 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 30: 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 31: 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

9 微弱完全数の因数分解

弱弱完全数の因数分解の性質が見えないので $e+1$ が奇素数のべきに絞ってみた. 案外おもしろいことがわかった.

一般に P を奇素数とし, $e+1$ が奇素数のべき p^α のとき, $N_{p^\alpha} = \frac{P^{p^\alpha}-1}{P}$ に関して $a_{p^\alpha} = P^e N_{p^\alpha}$ を P を**底とする微弱完全数** (little w-perfect number) という.

N_{p^α} の各素因子 Q について $Q-1$ の素因数分解が興味ある対象である.

9.1 $P=2, p=3$ の例

```
1 ?-  factor_qq(2,3^1).
[7]
6=[2,3]

2 ?- factor_qq(2,3^2).
[7,73]
```

```
6=[2,3] 72=[2^3,3^2]
```

```
3 ?- factor_qq(2,3^3).
[7,73,262657]
6=[2,3] 72=[2^3,3^2]    262656=[2^9,3^3,19]

4 ?- factor_qq(2,3^4).
[7,73,2593,71119,262657,97685839]
6=[2,3] 72=[2^3,3^2]    2592=[2^5,3^4]  71118=[2,3^4,439]
262656=[2^9,3^3,19]     97685838=[2,3^4,602999]
```

9.2 証明

$P=2$ に関して $M_{p^\alpha}=2^{p^\alpha}-1$ とおく.

上記の例により気がつくことは N_{p^α} の素因数分解 の一部に $N_{p^(\alpha-1)}$ の素因数分解がそのまま出ていることである. 次にこのことを証明する.

$p^\alpha=p^{(\alpha-1)}\times p$ となるので $E=p^{\alpha-1}, F=p^\alpha$ とおくとき $F=E\times p$.

等比級数の公式を使う.

$$M_{p^\alpha}=2^F-1=2^{Ep}-1=(2^E-1)((2^E)^{p-1}+\cdots+1)=M_{p^{(\alpha-1)}}((2^E)^{p-1}+\cdots+1).$$

M_{p^α} の因子として $M_{p^{\alpha-1)}}$ が出る.

9.3 $P=3, p=5$ の例

```
5 ?- factor_qq(3,5^1).
[11,11]
10=[2,5]        10=[2,5]
```

```
6 ?- factor_qq(3,5^2).
[11,11,8951,391151]
10=[2,5]        10=[2,5]        8950=[2,5^2,179]        391150=[2,5^2,7823]
```

9.4 $P=5$ の例

9.5 $P=5, p=3$

```
1 ?-  factor_qq(5,3).
[31]
```

```
30=[2,3,5]
```

```
8 ?- factor_qq(5,3^2).
[19,31,829]
18=[2,3^2]      30=[2,3,5]      828=[2^2,3^2,23]

9 ?- factor_qq(5,3^3).
[19,31,109,271,829,4159,31051]
18=[2,3^2]      30=[2,3,5]      108=[2^2,3^3]   270=[2,3^3,5]
 828=[2^2,3^2,23]      4158=[2,3^3,7,11]       31050=[2,3^3,5^2,23]
```

9.6 $P = 7, p = 3$

```
10 ?- factor_qq(7,3^1).
[3,19]
2=[2]   18=[2,3^2]

11 ?- factor_qq(7,3^2).
[3,3,19,37,1063]
2=[2]   2=[2]   18=[2,3^2]      36=[2^2,3^2]    1062=[2,3^2,59]

12 ?- factor_qq(7,3^3).
[3,3,3,19,37,109,811,1063,2377,2583253]

2=[2]   2=[2]   2=[2]   18=[2,3^2]      36=[2^2,3^2]    108=[2^2,3^3]
810=[2,3^4,5]   1062=[2,3^2,59] 2376=[2^3,3^3,11]
2583252=[2^2,3^4,7,17,67]
```

9.7 $P = 2, p = 3, 5$

```
1 ?- factor_qq(2,45).
[7,31,73,151,631,23311]

6=[2,3] 30=[2,3,5]      72=[2^3,3^2]    150=[2,3,5^2]   630=[2,3^2,5,7]
23310=[2,3^2,5,7,37]

2 ?- factor_qq(2,5).
```

```
[31]
30=[2,3,5]

4 ?- factor_qq(2,3).
[7]
6=[2,3]


3 ?- factor_qq(2,9).
[7,73]
6=[2,3] 72=[2^3,3^2]


3 ?- factor_qq(2,9).
[7,73]
6=[2,3] 72=[2^3,3^2]

4 ?- factor_qq(2,3).
[7]
6=[2,3]
```