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 12 月 15 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 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

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

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

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.

4.5 素因数分解

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

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

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

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

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

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

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

P=3

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=3 ee=4

L_p =41 = [41]

40=$[2^3, 5]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=3 ee=8

L_p =3281 = [17, 193]

16=$[2^4]$ 192=$[2^6, 3]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=3 ee=16

L_p =21523361 = [21523361]

21523360=$[2^5, 5, 17, 41, 193]$

4.6 一般の場合

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

これらを表計算を用いて計算する.

4.7 素因数分解

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

```
?- A is 257-1,factorize(A,B), exps(B,C).
A = 256,
C = [2^8].

 ?- A is 275201-1,factorize(A,B), exps(B,C).
A = 275200,
C = [2^8, 5^2, 43].

 ?- A is 138424618868737-1,factorize(A,B), exps(B,C).
A = 138424618868736,
C = [2^13, 3, 2131, 2643131].
```

見所は 2 の指数が $m+1$ を超えるところ.

```
?- A is 3913786281514524929-1,factorize(A,B), exps(B,C).
A = 3913786281514524928,
C = [2^8, 31, 787, 3919, 159898891].

?- A is 153849834853910661121-1,factorize(A,B), exps(B,C).
A = 153849834853910661120,
C = [2^11, 3, 5, 433, 19801, 584118287].
```

これらは数値例とはいえ, 実に見事な美しい結果である.

4.8 末尾２桁

L_m, a_m の末尾を調べるため, 次の数列を導入する.

$h_m = 3^{2^m}, L_m = \frac{1+h_m}{2}, h_{m+1} = h_m^2, K_m = 3^{2^m-1}$ 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 11: $P = 3$

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 12: $P = 3$

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

4.9 $P = 5$

表 13: $P = 5$; 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 となり変化しない. a_m の末尾 3 桁も 125 で変化しない.

4.10 素因数分解

$P = 5, m = 3$

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

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

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

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

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

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

4.11 $P = 7$

表 14: $P = 7$; Fermat 弱完全数

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

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

$B = (16616465284801) = 353 * 47072139617$

$C = (87125749116845407152755275976242821071395424316895543) = 7^31 * 7699649 * 134818753 * 531968664833$

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

$E = (10627254622840083542216519155 2[48digits]63301555209876316061428773 3943) = 7^{63} * 35969 * 1110623386241 * 152668481967935560980850003328886343 69$

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

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.

4.12 $P = 11$

表 15: $P = 11$; Fermat 弱完全数

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

$A = (95971712478875242340697505353731) = 11^15 * 51329 * 447600088289$
$B = (22974864931786081) = 51329 * 447600088289$
$C = (202632531114813745266796006062265620493992544102127830051326774371) =$
$11^{31} * 193 * 257 * 212836200332176295391787993 61$
$D = (105568883726762764272807627104961) = 193 * 257 * 212836200332176295391787993 61$
$E = (90331873865191113335801469288 8[72digits]3181993573086176804036725916 51) =$
$11^{63} * 316955440822738177 * 703240126270470764951876770375638576157606206 0673$
$F = (22289578422629511979347560666849207697450807174957633577569674131 21) =$
$316955440822738177 * 703240126270470764951876770375638576157606206 0673$
驚くべきはことに $m \geq 2$ について L_m の末尾桁は 1 となりで変化しない. a_m の末尾 1 桁も 1 で変化しない.

4.13 末尾 3 桁

表 16: $P = 5$

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, $L_m \equiv 313; a_m \equiv 125 \mod 1000$

4.14 $P = 7$

$A = 125749116845407152755275976242821071395424316895543$
$B = (55221383712196032315264960 1) = 7699649 * 134818753 * 531968664833$
$C = 10627254622840083542216519155 2[48digits]6330155520987631606142877339 43$
$D = (60988024381791785006928693128148591037780764706561920 1)$
$= 35969 * 1110623386241 * 1526684819679355609808500033288863436 9$

表 17: $P = 7$

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

$P = 7, m = 1$ 平方因子 5^2 あり.

4.15 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?

4.16 末尾 2 桁

表 18: $P = 7$

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

4.17 末尾 3 桁

表 19: $P = 7$

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

4.18 $P = 11$

表 20: $P = 11$

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].
```

4.19 末尾２桁

表 21: $P = 11$

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

周期 4 である.

4.20 末尾３桁

表 22: $P = 11$

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

周期 20 である.

4.21 $P = 13$

表 23: $P = 13$

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

$A = 170299716837246422680665308204601 97$

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

$C = 754051832426004128194845232398330830258394399157524945745785215350 1317$

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

$E = 1478344831561037988057253427 14[82digits]0669729785585885555890851839557$

$F = (980267382153805366653298802117830077122016400020578937947954819211244 81)$

$= 257 * 3230593 * 36713826768408543617 * 3215877717636198473712500018174097551256193$

```
18 ?-  B= [2657,441281,283763713],fer_euler_list(B).
2657=[2^5,83]   441281=[2^6,5,7,197]    283763713=[2^10,3,71,1301]
B = [2657, 441281, 283763713] .

19 ?- B=[193,1601,10433] ,fer_euler_list(B).
193=[2^6,3]     1601=[2^6,5^2]  10433=[2^6,163]
B = [193, 1601, 10433] .
```

4.22　末尾２桁

表 24: $P = 13$

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

周期４である.

4.23 末尾 3 桁

表 25: $P = 13$

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.

5　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.

5.1　P を底とする Wieferich 素数

Q は P を底とする Wieferich 素数とする.

$Q-1$ の 2 の指数を s とおく.

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

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

66 ?- fer_wief3(7,5).
2^1=2   ok
2^2=4   n0
```

5.2 一般の Wieferich 素数

表 26: 一般の Wieferich 素数の例

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

```
72 ?- fer_wief3(19,43).
```

```
73 ?- fer_wief3(19,137).
2^1=2   n0
2^2=4   n0
2^3=8   n0
```

```
74 ?- fer_wief3(23,13).
2^1=2   n0
2^2=4   n0


75 ?- fer_wief3(31,7).


76 ?- fer_wief3(31,79).


77 ?- fer_wief3(37,3).


78 ?- fer_wief3(41,29).
2^1=2   ok
2^2=4   n0
```

表 27: $m = 1$ 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 28: $m = 2$ の場合

P	L_2 素因数分解
179	$[17^2, 1776169]$

表 29: $m = 3$ の場合

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

5.3 $P = 41$

表 30: $P = 41$

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

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

5.4 $P = 43$

表 31: $P = 43$

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

5.5 $P = 107$

表 32: $P = 107$

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

5.6 $P = 131$

表 33: $P = 131$

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

5.7 $P = 157$

表 34: $P = 157$

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

5.8 $P = 179$

表 35: $P = 179$

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

5.9 $P = 193$

表 36: $P = 193$

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

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.

6 $s(a)=2$ 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.

6.1 $P = 3$ 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 37: $P = 3$

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.

6.2 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 38: $P = 5$

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.

6.3 $P = 7$ 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 39: $p = 7$

a	素因数分解
411943	$7^3 * 1201$

6.4 $P = 11$ 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 40: $P = 11$

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

6.5 $P = 19$ のとき

表 41: $p = 19$

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.

7　$a = P^e qr$ 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

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

$\widetilde{q}_0 = \widetilde{q} - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + 2$ 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 42: $P = 3$

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

$P = 11$ のときの

表 43: $P = 11$

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

$P = 17$ のときの

表 44: $P = 17$

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 45: $P = 23$

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
```