数学の研究を始めよう (V)

オイラーをモデルに数論研究

第7章 フェルマ 完全数とは何か

飯高 茂

平成 30 年 3 月 5 日

1　フェルマ 完全数

完全数の定義を参考にして

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

を満たす a を調べよう. a を偶数と仮定して $a = 2^e q, (q = 2^{e+1} + 1 : \text{素数})$ の形になることを示したい. しかしこれが難しい.

実際, $a = 2^e L, (L{:}\text{奇数})$ と表し $\sigma(a) = (2^{e+1} - 1)\sigma(L)$ と書き, $N = 2^{e+1} - 1$ とおくと, $\sigma(a) = N\sigma(L)$, $2a - 2 = 2^{e+1}L - 2 = (N + 1)L - 2$.

$$\sigma(a) = N\sigma(L) = (N + 1)L - 2$$

ゆえに, $N(\sigma(L) - L) = L - 2$.

完全数の場合なら, $\sigma(a) = 2a$ を満たすので $N(\sigma(L) - L) = L$ になる. よって, $d = \sigma(L) - L$ が L の約数になり, 議論が進む.

しかし今の場合は $N(\sigma(L) - L) = L - 2$ を満たすので d が $L - 2$ の約数になるだけでこれ以上議論が進まない. いわゆるデッドロックである.

そこで $\sigma(a) = 2a - 2$ を満たすとき ,$a = 2^e q, (q : \text{素数})$ の形をしていると仮定しよう.

定義から

$$\sigma(a) = (2^{e+1} - 1)(q + 1) = 2a - 2 = 2^{e+1}q - 2$$

となりこれより $q = 2^{e+1} + 1$ をえる.

$q = 2^{e+1} + 1$ が素数のとき $e + 1$ は 2 のべき, すなわち 2^m とかける.

そこで $F_m = 2^{2^m} + 1$ と書ける数 F_m を フェルマ 数. とくに素数になるときフェルマ 素数という.

$m = 0, 1, 2, 3, 4$ のとき F_m は素数になる. これら以外のフェルマ 素数は知られていない. 6 番目のフェルマ 素数はあるかどうかまったく分からない. もし見つかれば, ニューヨークタイムズのトップ記事になったとしても不思議ではない.

そこでユークリッドの完全数にならって,$e = 2^m - 1$ とするとき

- F_m がフェルマ 素数のとき $2^e F_m$ をフェルマ 完全数

- F_m がフェルマ 数のとき $2^e F_m$ をフェルマ 弱完全数

と言うことにする.

フェルマ 完全数は 5 個しか知られていないが, フェルマ 弱完全数なら無限にある. したがって研究しやすい.

1.1 数値例

表 1: $P = 2$; フェルマ 弱完全数

m	2^m	$e = 2^m - 1$	$a_m = 2^e F_m$	(F_m)=素因数分解
0	1	0	3	(3)=3
1	2	1	10	(5)=5
2	4	3	136	(17)=17
3	8	7	32896	(257)=257
4	16	15	2147516416	(65537)=65537
5	32	31	9223372039002259456	(4294967297)=641*6700417
6	64	63	A	B
7	128	127	C	D

A= 170141183460469231740910675752738881536

B= (18446744073709551617)=274177*67280421310721

C= 57896044618658097711785492504343953926805133516280751251460479307672448925696

D= (340282366920938463463374607431768211457)=59649589127497217*5704689200685129054721

1.2　フェルマ の弱完全数

普通の完全数 (ユークリッドの完全数) の最初の 4 つは 6,28,496,8128 であり, その末尾 1 桁の数は 6 または 8. この性質はユークリッドの発見による.

フェルマ の弱完全数ではどうか.

最初の 4 つは 3,10,136,32896 であり, その末尾 1 桁の数は (1,2 番を無視して)3 番目からに限ると, 6 である. フェルマ数の末尾 1 桁の数は 3 番目からに限ると, 7 である.

何となく 完全数に近い性質を持っているではないか.

フェルマ の完全数という言い方がすでにあるかどうかわからないが, 新しい用語フェルマ の完全数 をここで提案する次第である. そこで読者もフェルマ の完全数 の宣伝, 広報の仕事に参加してほしい.

10 を街で見かけたら, フェルマ の完全数を見つけた, と叫ぼう.

Windows 10 という命名の背後に 10 は 2 番目のフェルマ の完全数だからこの名前がついた, と勝手に思い込むことにしよう.

2　オイラーの結果

フェルマ 数 F_m の素因子を Q とおく.$E = 2^m$ を用いると

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

$E = 2^m$ によって

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

ゆえに

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

Q を法とすると 2 の位数は 2^{m+1} の約数であるが $2^E = 2^{2^m} \equiv -1$ によって Q を法とする 2 の位数は 2^{m+1}.

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

$2^{Q-1} \equiv 1 \mod Q$. $Q_1 = Q - 1$ は位数 2^{m+1} の倍数なので, $Q_1 = 2^{m+1}K$ と整数 K で表せる.

ここで $K = 1$ なら $Q = Q_1 + 1 = 2^{m+1} + 1$ これもフェルマ素数. この結果はオイラーによる.

$\frac{Q-1}{2} = 2^m K$ によれば

$$2^{\frac{Q_1}{2}} = 2^{2^m K} \equiv (-1)^K \mod Q.$$

オイラーの基準にしたがい $\left(\frac{2}{Q}\right) = 2^{\frac{Q-1}{2}} \mod Q$.

$$\left(\frac{2}{Q_1}\right) = 2^{\frac{Q_1}{2}} \equiv (-1)^K \mod Q.$$

次のようにまとめる.

定理 1 $Q = 1 + 2^{m+1}K$ において

- K が奇数なら *($Q-1$ の 2 の指数は $m+1$ のとき)* $\left(\frac{2}{Q}\right) = -1$. すなわち, Q を法とするとき 2 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)* $\left(\frac{2}{Q}\right) = 1$. すなわち, Q を法とするとき 2 は平方剰余.

$m = 5, 6, 7$ のフェルマ数について各素因子 Q について $Q_1 = Q - 1$ を素因数分解した結果を次に述べる. これは美しい性質をもっている. Q_1 の素因数 2 の指数 e は m 以上である.

表 2: 素因子 Q

m	Q	$Q_1 = Q - 1$	Q_1 の素因数分解
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

ここで $A = [2^9, 116503103764643]$

そこで $m = 5$ のとき素因子の 1 つは $Q = 641$ という例外的に小さい値を持っていることに注意しよう. このため F_5 の素因数として 641 が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. しかも $Q_1 = Q - 1 = 640 = 2^7 * 5$ という美しい構造を持っている.

3　フェルマ の弱完全数の末尾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 3: $P = 2;$, 法は 100

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
7	128				96

m と 2^m には周期性がないが, この表により 100 を法とすると f_m , F_m , B_m , a_m には周期 4 の周期性があることがこの表により分かる.

- $m \equiv 2 \mod 4$ ならば $F_m \equiv 17, a_m \equiv 36 \mod 100$.
- $m \equiv 3 \mod 4$ ならば $F_m \equiv 57, a_m \equiv 96 \mod 100$.
- $m \equiv 0 \mod 4$ ならば $F_m \equiv 37, a_m \equiv 16 \mod 100$.
- $m \equiv 1 \mod 4$ ならば $F_m \equiv 97, a_m \equiv 56 \mod 100$.

3.1　フェルマ の弱完全数の末尾３桁

表 4: $P = 2$ 法は 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	128	456	457	728	696
8	256	936	937	968	16
9	512	96	97	48	656
10	1024	216	217	608	936
11	2048	656	657	328	496
12	4096	336	337	168	616
13	8192	896	897	448	856
14	16384	816	817	408	336
15	32768	856	857	928	296
16	65536	736	737	368	216
17	131072	696	697	848	56
18	262144	416	417	208	736
19	524288	56	57	528	96
20	1948576	136	137	568	816
21	2097152	496	497	248	256
22	4194304	16	17	8	136

$m = 2$ 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　P を底とするフェルマの弱完全数

フェルマ 完全数の概念を一般化しよう.

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 1　$e>1$ 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.

5　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.

5.1 $P = 3$

$P = 3$ のときのフェルマ 弱完全数を計算してみよう.
ここで面白い例が出なければ, 底を一般化する試みは失敗したとも言える.

表 5: $P = 3$; フェルマ 弱完全数

m	2^m	a_m	(L_m)=素因数分解
1	2	15	(5)=5
2	4	1107	(41)=41
3	8	7175547	(3281)=17*193
4	16	308836705316427	(21523361)=21523361
5	32	A	B
6	64	C	D

$A = 572280636715419056279672990187$
$B = (926510094425921) = 926510094425921$
$C = 196503076295643052858681214356932539158308401746008315969770 7$
$D = (1716841910146256242328924544641) = 171684191014625624232892454464 1$

5.2 新素数 5 兄弟

$L_1 = 5, L_2 = 41, L_3$ は素数ではない, $L_4 = 21523361$
$L_5 = 926510094425921, L_6 = 171684191014625624232892454464 1$
は新しい素数 5 兄弟である.
フェルマ 素数がフェルマ自身により 5 つ発見された. しかもフェルマ 数はすべて 素数 に違いないとフェルマは死ぬまで思い込んでいたそうである.
皮肉なことに彼の見出した 5 つのフェルマ 素数のほかにフェルマ 素数は発見されていない.
ガウス が素数 $p > 2$ について正 p 角形の作図可能ならそれはフェルマ 素数であることを示した.
5 つのフェルマ 素数をまとめて (フェルマ) 素数 5 兄弟と呼ぶ.
似たような美しい性質をもつ素数 5 兄弟がどこかに居てほしい, できたら自分で発見したいと思っていた.
$P = 3$ を底とするフェルマ 素数を定義したら, 新しい素数 5 兄弟がでてきた. これには驚いた.

5.3 素因数 Q について $Q - 1$ の素因数分解

$m = 7$ に出てくる $L_7 = 589509228886929158576043643070625933283910579613792055454848 1$ の素因数 Q について $Q_1 = Q - 1$ の素因数分解をそれぞれ行う.
$Q_1 = 257 - 1 = 256 = 2^8$.
$Q_1 = 275201 - 1 = 275200 = 2^8 * 5^2 * 43$
$Q_1 = 138424618868737 - 1 = 138424618868736 = 2^{13} * 3 * 2131 * 2643131$
$Q_1 = 3913786281514524929 - 1 = 3913786281514524928 = 2^8 * 31 * 787 * 3919 * 159898891$

$Q_1 = 153849834853910661121 - 1 = 153849834853910661120 =$
$2^{11} * 3 * 5 * 433 * 19801 * 584118287.$

この見所は 2 の指数が $m + 1 = 8$ を超えるところである. これらは単なる数値例とはいえ, 見事な美しい結果である.

5.4 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 $L_{m+1} = 2{L_m}^2 - 2L_m + 1$. $a_m = K_m L_m$ に注意して次の表を作る.

表 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.

表 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

$22 - 2 = 20$ が周期なので案外短い.

5.5 $P = 5$

表 8: $P = 5$; フェルマ 弱完全数

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

$A = 542101086242752217003749683499336242675781 25$

$B = (10842021724855044340074993669986724853515625 0) = 641 * 75068993 * 241931001601$

C=2938735877055718769921841343055614194546663897351229666199401435733307152986526489257812 5

D=(271050543121376108501863200217485427856445313)

=769*3666499598977*96132956782643741951225664001

この計算結果によると, $P = 5$ のときのフェルマ 完全数 a は

$a = 65 = 5 * 13, a = 39125 = 5^3 * 313$

だけしか見出せない.

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.

5.6 $P = 7$

表 9: $P = 7$

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

$A = 125749116845407152755275976242821071395424316895543$
$B = (552213837121960323152649601) = 7699649 * 134818753 * 531968664833$

$P = 7, m = 1$ のとき平方因子 5^2 がある. 実際 $7^2 + 1 = 2 * 5^2$.
$P = 7, m = 4$ のとき 7 を底とする フェルマ 素数 1201 がある. 実際 $7^4 + 1 = 2 * 1201$.
これ以外は見つからないので, 1201 を $P = 7$ のときの一人っ子素数と呼ぶ.

5.7 $P = 11$

表 10: $P = 11$

m	2^m	a_m	(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

$A = 95971712478875242340697505353731$

$B = (22974864931786081) = 51329 * 447600088289$

$C = 202632531114813745266796006062265620493992544102127830051326774371$

$D = (10556888372676276427728076271049 61) = 193 * 257 * 212836200332176295391787993 61$

この結果,

$L_1 = 61, L_2 = 7321$ が 11 を底とするフェルマ 素数. $a_1 = 671 = 11 * 61$, $a_2 = 9744251 = 11^3 * 7321$ が 11 を底とするフェルマ 完全数.

このほかにあるかどうかは不明.

私は 素数の国に行って, 61 と 7321 を対面させ, 「君たちは 11 を底とするフェルマ 素数の兄弟だ. 今後仲良くしてほしい.」と言って励ましてやりたい.

5.8 $P = 13$

表 11: $P = 13$

m	2^m	a_m	(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

$A = 170299716837246422680665308204601 97$

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

$C = 754051832426004128194845232398330830258394399157524945745785215350 1317$

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

$L_2 = 14281, L_3 = 407865361$ という素数兄弟が見つかった.

6　フェルマの弱完全数の平方因子

p が奇素数のとき, 2^p-1 をメルセンヌ数という. これは平方因子をもたないだろう, という予想がある.

同様に $2^{2^m}+1$ は素数でないとき平方因子をもたないであろう.

ここではこの予想を踏まえて, 一般に底を P とするときフェルマの弱完全数の平方因子について考える. 結論を言うと, この場合は平方因子を持つことがある.

$E=2^m$ のとき $L_m=\frac{P^E+1}{2}$ に素数の平方 Q^2 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.

$P\not\equiv 1 \mod Q$ なので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 を底とする Wieferich 素数である.

以前扱った完全数では P を底とする強い意味での Wieferich 素数 であったからフェルマの弱完全数の場合は条件が少し弱くなっている.

$P^{\frac{Q-1}{2}}-1$ が Q^2 の倍数のとき Q は P を底とする 強い意味での Wieferich 素数と定義したのである.

表 12: P: 底, Wieferich 素数 Q, $Q < 5000$

P	$Q_1, Q_2, \cdots$	P	$Q_1, Q_2, \cdots$
3	11	101	5
7	5	107	3 , 5 , 97
11	71	109	3
13	863	127	3 , 19 ,907
17	3	131	17 , 29
19	3 , 7, 13, 43, 137	137	59 , 6733
23	13	149	5
31	7 , 79 , 6451	151	5 , 2251
37	3	157	5
41	29	163	3
43	5 , 103	173	3079
53	3 , 47 , 59, 97	179	3 , 17
59	2777	181	3 , 101
67	7 , 47	191	13
71	3 , 47 , 331	193	5, 4877
73	3	197	3 , 7 , 653
79	7 , 263, 3037	199	3 , 5
83	4871		
89	3 , 13		
97	7		

6.1 P を底とする Wieferich 素数

Q は P を底とする Wieferich 素数とする.

$Q-1=2^{m+1}k$ の関係を利用する. $Q-1$ の 2 の指数を s とおくとき $2^{m+1}\leq s$ 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パソコンを使って丹念に探す.

その結果

$P=7, Q=5, L_1=(P^2+1)/2=5^2$.

$P=41, Q=29, L_1=(41^2+1)/2=29^2$ などがが発見された.

6.2 $P = 41$ の場合

表 13: $P = 41$

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

$A = 777549157495866332581241$
$B = 17 * 41^7 * 234850742033$
$C = (3992462614561) = 17 * 234850742033$
$m = 1$ のとき平方因子 29^2
さらに平方因子を探す.

6.3 $P = 43$ の場合

表 14: $P = 43$

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

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

6.4 $P = 107$ の場合

表 15: $P = 107$

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

$m = 1$ のとき平方因子 5^2

6.5 $P = 131$ の場合

表 16: $P = 131$

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

$A = 331031312074451$
$B = 113 * 131^3 * 1303097$
$C = (147249961) = 113 * 1303097$
$D = 28710412953340543080499631931131$
$E = 17^2 * 131^7 * 7841 * 19136877329$
$F = (43365101734503121) = 17^2 * 7841 * 19136877329$
$m = 3$ のとき平方因子 17^2

6.6 $P = 157$ の場合

表 17: $P = 157$

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

$A = 1175621640703693$
$B = 113 * 157^3 * 2688377$
$C = (303786601) = 113 * 2688377$

$D = 433975078587972309446276265685093$
$E = 157^7 * 1297 * 142307322503233$
$F = (184572597286693201) = 1297 * 142307322503233$
$m = 1$ のとき平方因子 5^2

6.7 $P = 179$ の場合

表 18: $P = 179$

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

$m = 2$ に平方因子 17^2
このようにして, ときどき平方因子が見つかりその度に珍しい Wieferich 素数と出会う.
こんなことをして何が楽しいか? と言われかねない.
しかし, 素数をネタにした旅をすることがこんなにも楽しいことかと思う.

7　フェルマの完全数の方程式

以下奇素数 P を底として考える. $e=2^m-1$ とおき, $L_m=\dfrac{P^{e+1}+1}{2}$ 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 $\sigma(a)=\dfrac{P^{e+1}-1}{\overline{P}}(q+1)$ 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 $q=\mathrm{Maxp}(a)$ と書ける. そこで $\overline{P}\sigma(a)-aP=\mathrm{Maxp}(a)-2$ を P を底とするフェルマの完全数の方程式と言う.

P と $\mathrm{Maxp}(a)$ は奇数なので, a も奇数.

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

8　$s(a)=2$ の場合

$s(a)=2$ の仮定をおいて計算する.

a は奇数なので素因数分解し $a=p^eq^f(2<p<q)$ とおく. $X=p^e, Y=q^f$ と書けば $a=XY$ 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

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

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:

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

$p_0 = p - P, q_0 = q - P, D = P(P-1)$ とおけば $R = D - p_0q_0$ をえる.
よって $R > 0$.

8.1 $P = 3$ 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. これは無理な話であろう.

(i). $s(a) = 2$ 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) $Y = q$ の場合.
$3Xq = 3X + q^2 - 1 + q''$ を変形し, $q-1$ で両辺を 割ると
$3X = 3^{e+1} = 2q - 1$ なので

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

例
$e = 1, q = \dfrac{3^2+1}{2} = 5, a = 5 * 3 = 15,$
$e = 3, q = \dfrac{3^4+1}{2} = 41, a = 5^3 * 41 = 1107$
これらの q は $P = 3$ のときのフェルマ素数である. これはすでに計算されていて次の結果が得られている.

表 19: $P = 3$; フェルマ完全数

m	2^m	a	(L_m)=素因数分解
1	2	15	(5)=5
2	4	1107	(41)=41
4	16	308836705316427	(21523361)=21523361

$Y \geq q^2$ の場合は矛盾が出ることを示す.

2) $Y = q^f, f \geq 2$ の場合.

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

これを変形して

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

$\dfrac{\overline{q}^2}{Y-1}$ は整数になるが

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

これは矛盾.

(ii). $s(a) > 2$ の仮定のもとで
一般に $a \leq 1000000$ の範囲で方程式の解を探してみた. その結果は次の通り.

表 20: $P = 3$

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

$s(a) = 2$ に限ると, $a = 15 = 3 * 5$,$a = 1107 = 3^3 * 41$ の 2 例がある.
$s(a) = 3$ の解が 3 個でてきた.
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. この場合は後でふれる.

9　$P=5$ のときもあえて挑む

$P=5$ のとき $s(a)=2$ の仮定のもとで $D=P(P-1)=20, p_0=p-5<q_0=q-5$, $R=20-(p-5)(q-5)$ により

$p=3$ の場合.
$R=20+2(q-5)=10+2q$.
$C=3X+qY-1, \rho'=\overline{pq}=2\overline{q}.q''=(q-1)(q-2)$ とおくと基本方程式は

$$RXY=4(3X+qY-1)+2q''.$$

$(RX-4q)Y=12X-2q''-4, Y\geq q$ によれば

$$12X-2q''-4=(RX-4q)Y\geq (RX-4q)q$$

なので X で整理して

$$(12-Rq)X\geq 2q''-4q^2+4.$$

$12-Rq=12-(10+2q)q<0$ なので

$$(-12+Rq)X\leq -2q''+4q^2-2.$$

$$3\leq X\leq \frac{4q^2-2q''-2}{-12+Rq}.$$

$$3(-12+Rq)\leq 4q^2-2q''-2=2(q^2+3q-3).$$

この式は矛盾. この場合は起きない.

$p=5$ の場合.
$R=20-(p-5)(q-5)=20, q\geq 7$ により
$C=5X+qY-1, \rho'=\overline{pq}=2\overline{q}.q''=(q-1)(q-2)$ とおくと基本方程式は

$$20XY=RXY=4(5X+qY-1)+2q''=4(5X+qY-1)+4q''.$$

4 で割って,

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

1) $Y=q$ の場合

$$5Xq=5X+q^2-1+q''.$$

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

$5X = 2q - 1$ になって

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

$e = 1, q = \dfrac{25 + 1}{2} = 13,$
$e = 3, q = \dfrac{625 + 1}{2} = 313.$
これがもっとも簡単な場合である.

2) $Y \geq q^2$ の場合.

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

これを変形して

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

以前と同じ論法でこれから矛盾が出る.

表 21: $P = 5$; コンピュータによる計算結果

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

$s(a) = 3$ の例が発見された.

$p \geq 7$ の場合.
$D = P(P-1) = 20, R = 20 - (p-5)(q-5) \leq 20 - 2(q-5)$ により $p = 7, q = 11$, または $q = 13$
1) $p = 7, q = 11, R = 8, \rho' = 60$

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

これより $2XY = 7X + 11Y - 1 + 9 * 15$ をえるので

$$Y = \frac{7X - 1 + 9 * 15}{2X - 11}$$

$Y = 3 + \dfrac{X + 9 * 15 + 32}{2X - 11}$ と変形し, $Y = 11, Y \geq 121$ の場合にわけて計算するとそれぞれ矛盾が出る.

2) $p = 7, q = 13, R = 4, \rho' = 72$
$(X - 13)(Y - 7) = 288$ を得るが $X = 7^e, Y = 13^f$ を満たす解はない.

9.1 輝く方程式の解

数式処理系 wxmaxima で輝く方程式の解を探索する.

表 22: 輝く方程式の解

$P = 7$	
a	素因数分解
411943	$7^3 * 1201$
$P = 11$	
a	素因数分解
671	$11 * 61$
861773	$11 * 157 * 499$
$P = 19$	
a	素因数分解
3439	$19 * 181$

10 $a = P^e qr$ の解

$\overline{P}\sigma(a) - aP = Maxp(a) - 2$ の解として D 型 $a = P^e qr$ 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 $P = 3$ と $P = 11$ のときだけだった. 少し残念である.

表 23: $P = 3$

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

表 24: $P = 11$

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

11　フェルマの完全数の平行移動方程式

奇素数 P を底としたフェルマの完全数は数が少ないので思い切って平行移動を考えよう.

以下奇素数 P を底として考える. 整数 k について $e=2^m-1$ とおき, $L_m=\dfrac{P^{e+1}+1}{2}+k$ は素数とする. $a=P^eL_m$ は P を**底とするフェルマの k だけ平行移動した完全数**ということにする.

$q=L_m$ としてこれの満たす方程式を求める.

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

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

よって,

$$\overline{P}\sigma(a)=Pa+q-2k-2.$$

したがって $\overline{P}\sigma(a)-aP=\mathrm{Maxp}(a)-2-2k$ を P を**底とするフェルマの k だけ平行移動した完全数の方程式**と言う.

$P=2$ のときのフェルマの完全数は $q=2^{2^m}+1$ が素数の場合で, $a=2^{2^m-1}q$ と書かれたものである.

これを k だけ平行移動する: $q=2^{2^m}+1+k$ が素数の場合,$a=2^{2^m-1}q$ を k だけ平行移動したフェルマの完全数という.

これの満たす方程式を考えてみよう.

$$\sigma(a)=\sigma(2^{2^m-1}q)=(2^{2^m}-1)\sigma(q)=(2^{2^m}-1)(q+1)=2^{2^m}q+2^{2^m}-(q+1).$$

$q=2^{2^m}+1+k$ により $2^{2^m}=q-k-1$ なのでこれを代入する.

$$\sigma(a)=2^{2^m}q+(2^{2^m})-(q+1)=2a+q-k-1-q-1=2a-2-k.$$

これよりえられた式

$$\sigma(a)=2a-2-k$$

が k だけ平行移動したフェルマの完全数の方程式である.

底が奇数の場合と比べて q がなく, $-2-2k$ が $-2-k$ に変化しているだけである.