書泉グランデでの講義 第 3期 資料3
高校生も十分わかる新しい数論研究 , 2015 年7月10日

飯高 茂

平成 27 年 6 月 30 日

目 次

第３期はじまる

0.1　開講の辞　6

担当者から, 受講希望者が 10 名を超えたという報告があった.
2015 年 7 月 10 日

第1章　前回の訂正と補充

1.1　フェルマーとオイラーの結果;$(P=2)$ の場合

$p>2$ が素数のとき 2^p-1 をメルセンヌ数, もしこれ自身が素数ならメルセンヌ素数という.

2^p-1 がメルセンヌ素数のとき,$2^{p-1}(2^p-1)$ は完全数となる. メルセンヌ数が素数でないとき, 各素因子の持つ著しい特徴をあげる.

補題 1 $p>2$ が素数のとき 2^p-1 の素因数 Q は $Q-1=2Lp$ と書ける. さらに $Q\equiv\pm1 \bmod 8$.

$Q=1+2Lp$ なので $2p+1$ が最小になる. そこで $Q=1+2p$ の場合を調べる. このように $p, 2p+1$ がともに素数になる場合, p を Sophie Germain 素数という. $p=2,3,5,11,23$ らがその例で, 数多くありそうだが無限にあるかどうかは分かっていない.

次の結果はオイラーが予想し 25 年後ラグランジュが証明した.

補題 2 $p>2$ が奇素数のとき, $M_p=2^p-1$ とおく.

$Q=2p+1$ が素数, かつ $Q\equiv\pm1 \bmod 8$ 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, $Q\equiv\pm1 \bmod 8$ のとき, $Q\equiv1 \bmod 8$ の場合はおきない.

$Q\equiv -1 \bmod 8$ の場合は $Q=2p+1=-1+8L$ と書けるので $p=-1+4L$ すなわち, $p\equiv 3 \mod 4$. このような Q は $Q\equiv 7 \mod 8$ $Q=7,47$ などである.

次の表は $M_p=2^p-1$ の各素因数 Q について $Q-1$ を素因数分解したものである. $[2,p,\cdots]$ の形になっていることを味わうべきである.

次の見方を説明する.

− −

P=2 p=3

N_p =7 = [7]

6=[2, 3]

− −

$P = 2$ なので [2,3] は 2^3 を意味し, $N_p = 2^3 - 1 = 7$.

N_p の各素因子 Q について $Q - 1$ を素因数分解している.

$Q - 1 = 6$ の素因数分解は [2,3] (2*3 をこのように list で表現している.

− −

P=2 p=5

N_p =31 = [31]

30=[2, 3, 5]

− −

P=2 p=7

N_p =127 = [127]

126=[2, 3^2, 7]

− −

P=2 p=11

N_p =2047 = [23, 89]

22=[2, 11] 88=[2^3, 11]

− −

P=2 p=13

N_p =8191 = [8191]

8190=[2, 3^2, 5, 7, 13]

− −

P=2 p=17

N_p =131071 = [131071]

131070=[2, 3, 5, 17, 257]

− −

P=2 p=19

N_p =524287 = [524287]

524286=[2, 3^3, 7, 19, 73]

− −

P=2 p=23

N_p =8388607 = [47, 178481]

46=[2, 23] 178480=[2^4, 5, 23, 97]

$p = 11, 23$ の場合は N_p は素数にならない. したがって, 完全数ではない. しかし, N_p の各素因子のもつ性質は興味あるものである. これらの性質は, フェルマ, オイラー, ラグランジュという泰西の巨匠の見出したものでその後の追加研究がなされたことは特に聞いていない.

ここでは $p = 23, Q = 47$ が $Q = 2p + 1$ を満たす.

数の大きい例をあげておく.

$P = 2, p = 29$ なので [2,29] は 2^{29} を意味している.

$N_p = 2^{29} - 1$ の素因数分解が [233,1103,2089].

$Q_1 = 233, Q_2 = 1103, Q_3 = 2089$ について

$Q_1 - 1, Q_2 - 1, Q_3 - 1$ を素因数分解した結果が

$$Q_1 - 1 = 232 = [2^3, 29], Q_2 - 1 = 1102 = [2, 19, 29], Q_3 - 1 = 2088 = [2^3, 3^2, 29]$$

どれも $2 * 29 = 2 * p$ が因子として入っている.

これが定理の主張なので当然だが数値計算の結果が鮮やかで感動してしまう.

以下では, 底が一般の素数の場合もこめて N_p の各素因子の素因数分解を行っている. この数値例から意味のある結果を発見していただければうれしい.

表 1.1: $P = 2$:弱メルセンヌ数 (非素数)

p	$(2p+1)$	素因数分解	N_p	素因数分解
11	23	23	(2047)	23*89
23	47	47	(8388607)	47*178481
29	59	59	(536870911)	233*1103*2089
37	75	$3 * 5^2$	(137438953471)	223*616318177
41	83	83	(2199023255551)	13367*164511353
43	87	3*29	(8796093022207)	431*9719*2099863
47	95	5*19	(140737488355327)	2351*4513*13264529
53	107	107	(9007199254740991)	6361*69431*20394401
59	119	7*17	(576460752303423487)	179951*3203431780337
67	135	$3^3 * 5$	(147573952589676412927)	193707721*761838257287
71	143	11*13	(2361183241434822606847)	228479*48544121*212885833
73	147	$3 * 7^2$	(9444732965739290427391)	439*2298041*9361973132609
79	159	3*53	(604462909807314587353087)	2687*202029703*1113491139767
83	167	167	(967140655691703339764940 7)	167*57912614113275649087721
97	195	3*5*13	(158456325028528675187087900671)	11447*13842607235828485645766393
101	203	7*29	(2535301200456458802993406410751)	7432339208719*341117531003194129

1.2　フェルマーとオイラーの結果;$(P=3)$ の場合

3 を底としたメルセンヌ素数についてもフェルマーとオイラーの結果は成立する.

補題 3 p が素数のとき $\frac{3^p-1}{2}$ の奇数素因数 Q については $Q-1=2Lp$ と書ける.
さらに $Q \equiv \pm 1 \bmod 12$.

次の表は $3^{\frac{Q-1}{2}}$ の各素因数 Q について $Q-1$ を素因数分解したものである. $[2, p, \cdots]$ の形になっていることを味わうべきである.

P=3 p=3
N_p =13 = $[13]$
12=$[2^2, 3]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=5
N_p =121 = $[11, 11]$
10=$[2, 5]$ 10=$[2, 5]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=7
N_p =1093 = $[1093]$
1092=$[2^2, 3, 7, 13]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=11
N_p =88573 = $[23, 3851]$
22=$[2, 11]$ 3850=$[2, 5^2, 7, 11]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=13
N_p =797161 = $[797161]$
797160=$[2^3, 3, 5, 7, 13, 73]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=17
N_p =64570081 = $[1871, 34511]$
1870=$[2, 5, 11, 17]$ 34510=$[2, 5, 7, 17, 29]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=19
N_p =581130733 = $[1597, 363889]$
1596=$[2^2, 3, 7, 19]$ 363888=$[2^4, 3^2, 7, 19^2]$
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
P=3 p=23
N_p =47071589413 = $[47, 1001523179]$
46=$[2, 23]$ 1001523178=$[2, 23, 29, 37, 103, 197]$

1.3　一般の弱完全数でのフェルマとオイラーの結果

フェルマとオイラーの結果が一般化された究極の完全数でも成立するという著しい結果を紹介する.

定理 1 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 $P-1 \not\equiv 0 \bmod Q$ ならば,

(1) N_p の素因子 *(*奇数*)* Q について $Q-1 = kp$ と書ける. $p > 2$ のとき,k は偶数になり,$Q-1 = 2Lp$ と書ける. これより $\left(\frac{P}{Q}\right) = 1$.

(2) *(*$L = 1$ のとき, 逆が成り立つことを主張*)* 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.

$P \equiv 1 \bmod Q$ ならば, $p = Q$.

次は Lagrange の結果の一般化.

定理 2 p を素数とし, $N_p = \frac{P^p-1}{P}$ とおく. $Q = 2p+1$ は N_p の因子とする.
このとき $Q = 2p+1$ も素数.

Lagrange の結果は面白いが役に立たないようだ.

1.3.1 $P = 5$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=3

N_p =31 = [31]

30=$[2, 3, 5]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=5

N_p =781 = $[11, 71]$

10=$[2, 5]$ 70=$[2, 5, 7]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=7

N_p =19531 = [19531]

19530=$[2, 3^2, 5, 7, 31]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=11

N_p =12207031 = [12207031]

12207030=$[2, 3, 5, 11, 71, 521]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=13

N_p =305175781 = [305175781]

305175780=$[2^2, 3^2, 5, 7, 13, 31, 601]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=17

N_p =190734863281 = $[409, 466344409]$

408=$[2^3, 3, 17]$ 466344408=$[2^3, 3, 17, 31, 36871]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=19

N_p =4768371582031 = $[191, 6271, 3981071]$

190=$[2, 5, 19]$ 6270=$[2, 3, 5, 11, 19]$ 3981070=$[2, 5, 19, 23, 911]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=5 p=23

N_p =2980232238769531 = $[8971, 332207361361]$

8970=$[2, 3, 5, 13, 23]$ 332207361360=$[2^4, 3^2, 5, 7, 23, 293, 9781]$

1.3.2　$P = 7$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=3

N_p =57 = $[3, 19]$

2=[2] 18=$[2, 3^2]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=5

N_p =2801 = [2801]

2800=$[2^4, 5^2, 7]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=7

N_p =137257 = $[29, 4733]$

28=$[2^2, 7]$ 4732=$[2^2, 7, 13^2]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=11

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=11

N_p =329554457 = $[1123, 293459]$

1122=$[2, 3, 11, 17]$ 293458=$[2, 11, 13339]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=13

N_p =16148168401 = [16148168401]

16148168400=$[2^4, 3, 5^2, 7, 13, 19, 43, 181]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− P=7 p=17

N_p =38771752331201 = $[14009, 2767631689]$

14008=$[2^3, 17, 103]$ 2767631688=$[2^3, 3^2, 17, 71, 31847]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=19

N_p =1899815864228857 = $[419, 4534166740403]$

418=$[2, 11, 19]$ 4534166740402=$[2, 13, 19, 15913, 576791]$

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

P=7 p=23

N_p =4561457890013486057 = $[47, 3083, 31479823396757]$

46=$[2, 23]$ 3082=$[2, 23, 67]$ 31479823396756=$[2^2, 7^2, 23, 1811, 3855937]$

1.3.3　$P \equiv 1 \bmod Q$ の例

表 1.2: $P-1$ の素因数分解

P	$P-1$ の素因数分解
3	$[2]$
5	$[2^2]$
7	$[2, 3]$
11	$[2, 5]$
13	$[2^2, 3]$
17	$[2^4]$
19	$[2, 3^2]$
23	$[2, 11]$
29	$[2^2, 7]$
31	$[2, 3, 5]$
37	$[2^2, 3^2]$
41	$[2^3, 5]$
43	$[2, 3, 7]$
47	$[2, 23]$
53	$[2^2, 13]$
59	$[2, 29]$
61	$[2^2, 3, 5]$
67	$[2, 3, 11]$
71	$[2, 5, 7]$
73	$[2^3, 3^2]$
79	$[2, 3, 13]$
83	$[2, 41]$
89	$[2^3, 11]$
97	$[2^5, 3]$
101	$[2^2, 5^2]$

1.3.4　$P = 31$ の弱完全数

$P - 1$ が 2 個以上の奇数素因子を含む場合を計算した.

表 1.3: $P = 31$

p	(N_p)	分解
3	(993)	3*331
5	(954305)	5*11*17351
7	(917087137)	917087137
11	(846949229880161)	23*397*617*150332843
13	(813918209914834753)	42407*2426789*7908811
17	(751670559138758105956097)	751670559138758105956097
19	(722355407332346539823809249)	571*14251*88770666332610762169
23	(667110388134976008804624141476513)	1509997*61562537*7176374761323733117

$P - 1 = 30 = 2 * 3 * 5$ なので $Q = 3, 5$ に注目.
$p = 3$ での素因数分解 $3 * 331$ で $Q = 3$.
$p = 5$ での素因数分解 $5 * 11 * 17351$ で $Q = 5$.

1.3.5　$P = 43$ の弱完全数

表 1.4: $P = 43$

p	(N_p)	分解
3	(1893)	3*631
5	(3500201)	3500201
7	(6471871693)	7*5839*158341
11	(22126041415981493)	6038099*3664405207
13	(40911050578149780601)	40911050578149780601
17	(139866740627629048068560801)	647*56770350869*3807926835707
19	(258613603420486109878768921093)	229*2699*4219*46399*2137444528747943

$P - 1 = 46 = 2 * 3 * 7$ なので $Q = 3, 7$ に注目.
$p = 3$ での素因数分解 $3 * 631$ で $Q = 3$.
$p = 7$ での素因数分解 $7 * 5839 * 158341$ で $Q = 7$.
これで結果は正しいが,6/26 に配布資料が $P = 43$ と書くべきところを $P = 47$ と誤記.

そこで $P = 47$ の弱完全数も今回は載せた. これは面白い.

1.3.6　$P = 47$ の弱完全数

表 1.5: $P = 47$

p	(N_p)	分解			
2	(5)	5	(48)	$2^4 * 3$	2256
3	(7)	7	(2257)	$37 * 61$	4985713
5	(11)	11	(4985761)	$11 * 31 * 14621$	24328923222241
7	(15)	$3 * 5$	(11013546097)	$43 * 256128979$	118717384915430520913
23	(47)	47	P	Q	R

$P = (624443142787099110314358719090439345 7)$
$Q = 23 * 6630274723 * 409480798225872502360103 33$
$R = 381632871795662863647395849602843186459035609325206057716193555256141977 13$
ただし $p = 11, 13, 17, 19$ は省略
$P - 1 = 47 - 46 = 2 * 23$, $p = Q = 23$ があることを確認できた.

1.3.7　$P = 5$ の場合

フェルマとオイラーの結果 (一般の場合) を $P = 5$ で使うと
$P - 1 = 4 = 2^2$ なので $p = Q = 2.N_2 = P + 1 = 5 + 1 = 2 * 3$. $Q = 3, p = 2$.

定理 3　*(1)* $N_p = \frac{5^p-1}{4}$ の素因子 *(*奇数*)* Q について $\left(\frac{5}{Q}\right) = 1$.

(2) 素数 Q は $2p + 1$ と書けるとき $\left(\frac{5}{Q}\right) = 1$ を仮定すると, Q は N_p の素数因子.

$\left(\frac{5}{Q}\right) = 1$ の条件は 平方剰余の相互法則から容易にもとまり $Q \equiv \pm 1 \mod 5$ がその条件になる.

$Q \equiv 1 \mod 5$ のとき $Q = 2p + 1$ と素数でかけるとすると $2p + 1 = 1 + 5L$. これより $2p = 5L$.
$p = 5, L = 2, Q = 11$. したがって, $(5^5 - 1)/4 = 11 * 71$.

$Q \equiv -1 \mod 5$ のとき $Q = 19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239, 269 \cdots$
このとき $Q = 2p + 1$ と素数 p でかけることはありうる.

1.3.8　$P = 5, Q = 2p + 1$ も素数の数表

表 1.6: $P = 5, Q = 2p + 1$ 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	$H = I$
131	263	$J = K$

$A = (46566128730773925781) = 59 * 35671 * 22125996444329$
$B = (113686837721616029739379882 81) = 2238236249 * 5079304643216687969$
$C = (27755575615628913510590791702270 50781) = 960555749*17154094481*27145365052629449$
$D = (25849394142282114839731521627186339173931628465652465820 31)$
$E = 20515111 * 14311857067018689623837 41 * 880400959451038346273767 81$
$F = (40389678347315804437080502542478654959268169477581977844238281)$
$G = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 * 231669654363683130095909$
$H = (240741243048404481631997242823115914817262706026923524404992349445819854736328 1)$
$I = 2939 * 6329 * 129499 * 308491 * 304247586761 * 2084303944451$
$- *620216264269531 * 8237123176890810696379$
$J = 91835496157991211560057541970487943575958324662281 93$
$-$
$37617871227053001348394900560379028320 31)$
$K = 2621 * 23928199 * 34720241 * 16815642611861* -$
$25080566643341653267842952512497709031897599900179635412 4089$

$Q \equiv 1 \mod 5$ のとき $Q = 2p + 1$ と素数でかけるときは $2p + 1 = 1 + 5L$. これより
$2p = 5L$. $p = 5, L = 2, Q = 11$. したがって, $(5^5 - 1)/4 = 11 * 71$.
$Q \equiv -1 \mod 5$ のとき $Q = 9 + 10L$ と書ける.

$Q \equiv -1 \mod 5$ のとき $Q = 19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239, 269 \cdots$ のうちから $Q = 59, Q = 179$ の 2 例ができたことがわかる.
$p = 5, N_p$ の素因子 $Q = 11$ に対し, $(Q, Q - 1,$ 素因数分解 $)(11, 10, [2, 5])$ を表示
$p = 29, N_p$ の素因子 $Q =$ に対し, $(Q, Q - 1,$ 素因数分解 $)$　$(59, 58, [2, 29])$ を表示
$p = 41, N_p$ の素因子 $Q = 2238236249$ に対し, $(Q, Q-1,$ 素因数分解 $)(2238236249, 2238236248, [2^3, 41, 6823891])$ を表示
$p = 83, N_p$ の素因子 $Q = 20515111$ に対し, $(Q, Q-1,$ 素因数分解 $)(20515111, 20515110, [2, 3, 5, 7, 11, 83, 107])$ を表示
$p = 89, N_p$ の素因子 $Q = 179$ に対し, $(Q, Q - 1,$ 素因数分解 $)(179, 178, [2, 89])$ を表示
$p = 113, N_p$ の素因子 $Q = 2939$ に対し, $(Q, Q - 1,$ 素因数分解 $)(2939, 2938, [2, 13, 113])$ を表示

1.3.9　$P = 7$

奇素数 $P = 7$ が底のとき,

定理 4 奇素数 $p \neq 7$ について

(1) $N_p = \frac{7^p - 1}{6}$ の素因子 *(*奇数*)* Q について $\left(\frac{7}{Q}\right) = 1$.

(2) 素数 Q は $2p + 1$ と書けるとき $\left(\frac{7}{Q}\right) = 1$ を仮定すると, Q は N_p の素数因子.

$P - 1 = 6 = 2 * 3$. したがって $Q = 3 = p$ となり $\frac{7^3 - 1}{6} = 3 * 19$ を満たす.

1.4　$P = 7$; p : Sophie Germain 素数

1) 最初にすること:2, 7 と異なる素数 Q について $\left(\frac{7}{Q}\right) = 1$ を解く.
相互法則により

$$\left(\frac{7}{Q}\right)\left(\frac{Q}{7}\right) = (-1)^{\frac{Q-1}{2}*3} = (-1)^{\frac{Q-1}{2}}.$$

$Q \equiv 1 \mod 4$ のとき $(-1)^{\frac{Q-1}{2}} = 1$. この場合,

$$\left(\frac{7}{Q}\right) = \left(\frac{Q}{7}\right)$$

$\left(\frac{Q}{7}\right)$ の計算は簡単にできる.
$2^2 = 4, 3^2 = 9 \equiv 2 \mod 7$ により $Q \equiv 1, 2, 4 \mod 7$ なら $\left(\frac{Q}{7}\right) = 1$.
$Q \equiv 3, 5, 6 \mod 7$ なら $\left(\frac{Q}{7}\right) = -1$.
組み合わせると $Q \equiv 1 \mod 4$ かつ $Q \equiv 1, 2, 4 \mod 7$ なら $\left(\frac{7}{Q}\right) = 1$

これをもとに計算する. $Q = 1 + 4k$ を用いて方程式 $Q = 1 + 4k \equiv 1, 2, 4 \mod 7$ を書き直す.
$Q = 1+4k \equiv 1 \mod 7$ から $k \equiv 0 \mod 7$. ゆえに $k = 7L$ と書けるから $Q = 1+4k = 1+28L$. $Q \equiv 1 \mod 28$.
$1 + 4k \equiv 2 \mod 7$ から $4k \equiv 1 \equiv 8 \mod 7$. $k \equiv 2 \mod 7$
ゆえに $k = 2 + 7L$ と書けるから $Q = 1 + 4k = 9 + 28L$. $Q \equiv 9 \mod 28$.
$1 + 4k \equiv 4 \mod 7$ から $4k \equiv 3 \equiv 3 + 21 = 24 \mod 7$. $k \equiv 6 \mod 7$
ゆえに $k = 6 + 7L$ と書けるから $Q = 1 + 4k = 1 + 24 + 28L = 25 + 28L$. $Q \equiv -3 \mod 28$.

次に $Q \equiv 3 \mod 4$ かつ $Q \equiv 3, 5, 6 \mod 7$ なら $\left(\frac{7}{Q}\right) = 1$ の方の計算.
$Q = 3 + 4k$ を用いて方程式 $Q = 3 + 4k \equiv 3, 5, 6 \mod 7$ を書き直す.
$Q = 3+4k \equiv 3 \mod 7$ から $k \equiv 0 \mod 7$. ゆえに $k = 7L$ と書けるから $Q = 3+4k = 3+28L$. よって, $Q \equiv 3 \mod 28$.
$Q = 3 + 4k \equiv 5 \mod 7$ から $4k \equiv 2 \equiv 2 + 14 = 16 \mod 7$. $k \equiv 4 \mod 7$. ゆえに $k = 4 + 7L$ と書けるから $Q = 3 + 4k = 3 + 4(4 + 7L) = 19 + 28L$. $Q \equiv -9 \mod 28$.
$Q = 3 + 4k \equiv 6 \mod 7$ から $4k \equiv 3 \equiv 3 + 21 = 24 \mod 7$. $k \equiv 6 \mod 7$. ゆえに $k = 6 + 7L$ と書けるから $Q = 3 + 4k = 3 + 4(6 + 7L) = 27 + 28L$. $Q \equiv -1 \mod 28$.
以上により, $\left(\frac{7}{Q}\right) = 1$ のとき $Q = \pm 1, \pm 3, \pm 9 \mod 28$.

2) $Q = 2p + 1$ を仮定するとき, $\left(\frac{7}{Q}\right) = 1$ の場合に限って p を求める.
$2p + 1 = \pm 1 + 28k$ と書けるとき $p = (\pm 1 - 1)/2 + 14k$ により $(\pm 1 - 1)/2$ は奇数. $\pm 1 = -1$ なので $p = -1 + 14k$. 例は $p = 13, 13 + 28 = 41$,
$Q = 2p + 1 = \pm 3 + 28k$ と書けるので $p = (\pm 3 - 1)/2 + 14k$ により $(\pm 3 - 1)/2$ は奇数. $\pm 3 = 3$ なので $p = 1 + 14k$. 例は $p = 29, 43$,

$Q = 2p+1 = \pm 9 + 28k$ と書けるので $p = (\pm 9 - 1)/2 + 14k$ により $(\pm 9 - 1)/2$ は奇数. $\pm 9 = -9$ なので $p = -5 + 14k \equiv 9 \mod 14$. 例は $p = 23, 37, 79$

$P-1=6=2*3$ により $p=Q=3$.
$p, Q=2p+1$ も素数のときの数表.

表 1.7: $P=7, Q=2p+1$ 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 $Q=47, 59, 83, 167$.
対応して $p=23, 29, p=83=13+5*14, 167=13+11*14$.

1.4.1　$P = 11$

$P = 11, P - 1 = 10 = 2 * 5$. $Q = p = 5$ がある.
このとき $N_5 = \frac{5^5-1}{4} = (16105) = 5 * 3221$.
$N_p = \frac{P^p-1}{P} = \frac{11^p-1}{10}$.

表 1.8: $P = 11$

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

$A0 = 232251544198878080950520379327369 7$
$A = 340039485861577398986846964992269755 49$
$B = (89543024325523737224653) = 829 * 28878847 * 3740221981231$
$C = 728904836851030521429027853850124525396790261 3$
$D = (158630929717149157441443670489) = 523 * 303309617049998388989376043$
$E = 228761562390246506066453264733348483256258951604954126056 09$
$F = (191943424957750480504146841291 81) = 50159 * 2428541 * 157571957584602258799$
$G = 33492980349555990953189422489630490716271536793263604160376698 1$
$H = (34003948586157739899240688230576198697) = 2591*36855109*136151713*2615418118891695851$
$I = 10511531995000535984031884072175901907045798792322646350775223148922564706 17$
$J = (49785181124993546986478291638386612512424 1)$
$= 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$
$K = 22532402360440124879373085380333495679667293998886148220552925184518462352208939864 1$
$L = (60240069161242191853638732882447801140033173)$

$= 1416258521793067 * 42534656091583268045915654719$
$M = 32989690295920386835890134305346271024600891715413118108859739977787976996901960495011 33$
$N = (881974852589746930929124688131918256491225687357)$
$= 2069 * 22666879066355177 * 188063270418246905957471138 89$
$O = 70716330963700529872285398286337389743561706314564099 43$
$- - 18500556468267327181081133208187483831077$

1.4.2　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.

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

[研究課題] 2, 11 と異なる素数 Q について $\left(\frac{11}{Q}\right) = 1$ を解く.

1.4.3　$P = 13$

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

表 1.9: $P = 13$

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	(12182669086462050922 3)=12865927*9468940004449	B

$A = 479677535758244089774221240729252401$
$B = 13700070098791209449615908553795581328767$

1.4.4　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.

1.4.5　$P = 17$ の弱完全数

表 1.10: $P = 17$

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	43182458695629198054329 23

1.4.6　末尾の数

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

1.4.7　$P = 19$ の弱完全数

表 1.11: $P = 19$

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

1.4.8　$P = 23$ の弱完全数

表 1.12: $P = 23$

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.

第2章　Wieferich の素数とその一般化

2.1　Wieferich の素数の定義

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

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

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

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

Wieferich 素数は 2 個しか見つからない現在, 非 Wieferich 素数は無限にあることは肯定しやすい結果と言ってよい. このようなごく理解しやすい結果でも,abc-予想が解けないと示すことができない. これはまさに数学の奥深さを示唆している.

ここでは $2^{\frac{p-1}{2}}-1$ が p^2 の倍数になる場合の素数 p を 強い意味での Wieferich の素数という.

計算機での実行例:

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

これは Wieferich の素数 は 1093,3511.

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

強い意味での Wieferich の素数は 3511.

2.1.1　Wieferich の素数と完全数の関係

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

素数 p に対して 2^p-1 が素数の平方 Q^2 で割れるとき

$$2^p-1 \quad \equiv 0 \mod Q^2$$

[1] Arthur Wieferich in 1909

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

これより

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

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

$Q=3511$ に対して $Q-1=2pk'$ によって p が定まる.

$3511-1=3510$ の素因数分解は $2*3^3*5*13$.

$p=5$ または 13.

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

これらはともに素数. したがって平方因子を持たない.

$1093-1=1092$ の素因数分解は $2^2*3*7*13$.

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

2.1.2　P を底とする弱完全数

ここで, 奇素数 P を底とする弱完全数に戻る.

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

表 2.1: $p=e+1$、$N_p=(3^p-1)/2$:素数

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

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

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

2.2　奇素数 P を底とする Wieferich 素数

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

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

2.2.1　$Q = 2$ の場合

底 が奇素数 P なので $Q = 2$ もある.

$P - 1$ が 4 の倍数になる場合すなわち $P \equiv 1 \mod 4$ 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 奇素数 p について N_p は 4 を平方因子に持たない. これを以下で証明する.

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

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

ゆえに N_p は 4 を平方因子に持たない.

一方, $p = 2$ ならば, $P \equiv 1 \mod 4$ のとき

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

ゆえに N_2 は 4 を平方因子に持たない.

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

表 2.2: $p = 2, Q = 2, P = 3 + 4k$

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	$[2^3, 5^2]$

2.2.2　一般の弱完全数と Wieferich の素数

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

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

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

これは簡単にはできないので後で組織的に行う.

2) p が偶数なら $p = 2$. $Q = 1 + 2k$.

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

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

2.2.3　平方因子を含む例

表 2.3: $P = -1 + 9N$

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

表 2.4: $P = -1 + 5^2N$

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

表 2.5: $P = -1 + 7^2N$

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

表 2.6: $P = -1 + 11^2 N$

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

表 2.7: $P = -1 + 13^2 N$

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

2.2.4　$Q = 2$ の例

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

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

ともに N_p は 4 で割れない. したがって, $Q = 2$ ならば $p = 2$ になる.

4) $Q = 2$, $p = 2, P \equiv 1 \mod 4$ 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.

5) $P \equiv 1 \mod Q$ 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.

2.2.5　(強い意味で)Wieferich の素数の計算

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

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

ここでは, $P^{\frac{Q-1}{2}}-1$ が Q^2 の整数倍かどうか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 2.8: 強い意味の Wieferich 素数 Q の例, $Q \geq 7$

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

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

2.2.6　プログラム

次のプログラムで実行した結果を以下に書く.

```
wief(P,Q,P0,PP):- Q2 is  Q*Q,
power(PP=P^P0 mod Q2),
write(PP=P^P0),put(9),
write(mod=Q2),put(9),
(   PP=1 -> write(PP=ok); write(no)),
nl.
wief2(P,Q):- P0 is (Q-1)//2,
P0 >=2,
for(2=<P0,PW),
factorize(PW,PW0),
PW0=[PP],
write(prime=PP),put(9),
wief(P,Q,PP,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. さらに計算を続けて次の結果をえた.

表 2.9: Q^2 が N_p の因数

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

2.2.7　参考

強い意味の Wieferich 素数 Q はあまりない.

表 2.10: 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

2.2.8　一般の Wieferich 素数

表 2.11: 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.

2.3　平方因子をもつ弱完全数の例

平方因子をもつ弱完全数の例

2.3.1　$P = 53$

表 2.12: $P = 53$

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
$H = 75233417184638632015257750168555226595359205977948352866139303783326473960 67$

$p = 2$ 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.

2.3.2　$P = 71$

表 2.13: $P = 71$

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

2.3.3　$P = 79$

表 2.14: $P = 79$

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

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

2.3.4　$P = 137$

表 2.15: $P = 137$

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

$I = (102573254726919359630889312802648113437647615807)$

$= 1381 * 143235060131 * 518550578298278365204966204101137$

$J = 104444749751619994641076050602515305522087006896962812$

$- - 24738478203470769145406043274426557803983$

$K = (67819961541149092335018708592760553688023207495468775836654 1)$

$= 59^2 * 616367 * 3160924605365392930438533910600424447165692844394 83$

$L = 45659738463375190334654765448 3[60digits]475472486261488580834605020461$

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

2.3.5　$P = 197$

表 2.16: $P = 197$

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

$p = 2$ で 平方因子 3^2.

2.3.6　$P = 199$

表 2.17: $P = 199$

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

$p = 2$ で 平方因子 $2^3 * 5^2$. 2 重の平方因子.