書泉グランデでの講義 第 3期 資料2
高校生も十分わかる新しい数論研究 , 2015 年6月26日

飯高 茂

平成 27 年6 月 24 日

目 次

第３期はじまる

0.1　開講の辞　4

担当者から, 受講希望者が７名という報告があった. 小学生は積極的なのだが大人の参加が厳しくなった. しかし, これは連絡ミスで, 第三期の案内を数学セミナ６月号 (販売は５月中旬) に載せ損なったことが一因であることがわかった. 数学セミナ７月号には掲載されたが第三期の開催当日と重なった. １２名の正式の参加者があり, そのほかの傍聴者を加えて 15 名なので何とか書店に対して面目がたってほっとした.

2015 年 6 月 26 日

第1章　前回の訂正と補充

1.1　古典的な完全数の数表

表 1.1: $\sigma(2^e) = 2^{e+1} - 1$, $e + 1$:素数

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

1.2　フェルマーとオイラーの結果;$(P = 2)$ の場合

補題 1 p が素数のとき $2^p - 1$ の素因数 Q については $Q - 1 = 2Lp$ と書ける.
さらに $Q \equiv \pm 1 \bmod 8$.

```
24 ?- all_factor_qq(2,3=<30).

p=3     [2,3]
N_p=[7]
6=[2,3]
p=5     [2,5]
N_p=[31]
30=[2,3,5]
p=7     [2,7]
N_p=[127]
126=[2,3^2,7]
p=11    [2,11]
N_p=[23,89]
22=[2,11]       88=[2^3,11]
p=13    [2,13]
N_p=[8191]
8190=[2,3^2,5,7,13]
p=17    [2,17]
N_p=[131071]
131070=[2,3,5,17,257]
p=19    [2,19]
N_p=[524287]
524286=[2,3^3,7,19,73]
p=23    [2,23]
N_p=[47,178481]
46=[2,23]       178480=[2^4,5,23,97]
p=29    [2,29]
N_p=[233,1103,2089]
232=[2^3,29]    1102=[2,19,29]  2088=[2^3,3^2,29]
```

1.3　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 2 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 $Q \equiv \pm 1 \bmod 12$.

Proof.
条件より,

$$3^p \equiv 1 \mod Q.$$

p は素数なので 3 の mod$p$ での位数は p.
フェルマーの小定理によると $3^{Q-1} \equiv 1 \mod Q$. よって, $Q-1 = kp$ と書ける. $Q-1$ は偶数なので k も偶数. よって $k = 2L$ と表せることによって $Q-1 = 2Lp$ と書ける.

$$3^{\frac{Q-1}{2}} \equiv 3^{Lp} \equiv 1 \bmod Q.$$

ルジャンドルの記号を用いるとオイラーの基準によって

$$3^{\frac{Q-1}{2}} \equiv \left(\frac{3}{Q}\right)$$

$3^{\frac{Q-1}{2}} \equiv 1$ なので $\left(\frac{3}{Q}\right) = 1$. 平方剰余の補充法則から $Q \equiv \pm 1 \bmod 12$.

```
p=3     [3,3]
N_p=[13]
12=[2^2,3]
p=5     [3,5]
N_p=[11,11]
10=[2,5]        10=[2,5]
p=7     [3,7]
N_p=[1093]
1092=[2^2,3,7,13]
p=11    [3,11]
N_p=[23,3851]
22=[2,11]       3850=[2,5^2,7,11]
p=13    [3,13]
N_p=[797161]
797160=[2^3,3,5,7,13,73]
p=17    [3,17]
N_p=[1871,34511]
1870=[2,5,11,17]        34510=[2,5,7,17,29]
p=19    [3,19]
N_p=[1597,363889]
1596=[2^2,3,7,19]       363888=[2^4,3^2,7,19^2]
p=23    [3,23]
N_p=[47,1001523179]
46=[2,23]       1001523178=[2,23,29,37,103,197]
p=29    [3,29]
N_p=[59,28537,20381027]
58=[2,29]       28536=[2^3,3,29,41]     20381026=[2,29,351397]
```

1.3.1　$P = 5$

表 1.2: $P = 5$:弱完全数

p	$(2p+1)$	$Q = N_p =$ 素因数分解	a:弱完全数
2	(5)=5	(6)=2*3	30
3	(7)=7	(31)=31	775
5	(11)=11	(781)=11*71	488125
7	(15)=3*5	(19531)=19531	305171875
11	(23)=23	(12207031)=12207031	119209287109375
13	$(27) = 3^3$	(305175781)=305175781	74505805908203125
17	(35)=5*7	(190734863281)=409*466344409	29103830456695556640625
19	(39)=3*13	(4768371582031)=191*6271*3981071	1818989403545761l083984375

1.3.2　末尾の数

$p > 2$ のとき $p = e + 1$ は奇数なので $e \equiv 0, 2 \mod 4$. そこで $a \equiv 25, 75 \mod 100$ は成り立つ.
より詳しく,

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

が成り立つ事を高嶋耕司さんが詳しく証明した.
多分, 弱完全数でも証明は通用する.

```
p=3     [5,3]
N_p=[31]
30=[2,3,5]
p=5     [5,5]
N_p=[11,71]
10=[2,5]        70=[2,5,7]
p=7     [5,7]
N_p=[19531]
19530=[2,3^2,5,7,31]
p=11    [5,11]
N_p=[12207031]
12207030=[2,3,5,11,71,521]
p=13    [5,13]
N_p=[305175781]
305175780=[2^2,3^2,5,7,13,31,601]
p=17    [5,17]
N_p=[409,466344409]
408=[2^3,3,17]  466344408=[2^3,3,17,31,36871]
p=19    [5,19]
N_p=[191,6271,3981071]
190=[2,5,19]    6270=[2,3,5,11,19]      3981070=[2,5,19,23,911]
p=23    [5,23]
N_p=[8971,332207361361]
8970=[2,3,5,13,23]      332207361360=[2^4,3^2,5,7,23,293,9781]
p=29    [5,29]
N_p=[59,35671,22125996444329]
58=[2,29]       35670=[2,3,5,29,41]     22125996444328=[2^3,7,29,13624382047]
```

1.3.3　$P = 7$

予稿にはミスプリントが多かったので訂正版をここに載せる.

表 1.3: $P = 7$:弱完全数

p	$(2p+1)$	$Q = N_p =$ 素因数分解	a:弱完全数
2	(5)=5	$(8) = 2^3$	56
3	(7)=7	(57)=3*19	2793
5	(11)=11	(2801)=2801	6725201
7	(15)=3*5	(137257)=29*4733	16148148793
11	(23)=23	(329554457)=1123*29345	93090977300134793
13	$(27) = 3^3$	(16148168401)=16148168401	223511436608353935601
17	(35)=5*7	(38771752331201)=14009*2767631689	1288498953284568548534420801
19	(39)=3*13	(1899815864228857)=419*4534166740403	309368598683626211233992762679 3

1.3.4　末尾の数

$p = e + 1$ は素数を仮定しているので, $e \equiv 0, 2 \mod 4$ の場合のみおきる.

- $e \equiv 0 \mod 4$ なら $Q \equiv 01, a \equiv 01 \mod 100$.
- $e \equiv 2 \mod 4$ なら $Q \equiv 57, a \equiv 93 \mod 100$.

証明.
$7^2 = 49 \equiv -1 \mod 50, 7^4 = 2401 \equiv 1 \mod 600$ に注意する.

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

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

ゆえに

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

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

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

ゆえに

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

よって

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

```
p=3     [7,3]
N_p=[3,19]
2=[2]   18=[2,3^2]
p=5     [7,5]
N_p=[2801]
2800=[2^4,5^2,7]
p=7     [7,7]
N_p=[29,4733]
28=[2^2,7]      4732=[2^2,7,13^2]
p=11    [7,11]
N_p=[1123,293459]
1122=[2,3,11,17]        293458=[2,11,13339]
p=13    [7,13]
N_p=[16148168401]
16148168400=[2^4,3,5^2,7,13,19,43,181]
p=17    [7,17]
N_p=[14009,2767631689]
14008=[2^3,17,103]      2767631688=[2^3,3^2,17,71,31847]
p=19    [7,19]
N_p=[419,4534166740403]
418=[2,11,19]   4534166740402=[2,13,19,15913,576791]
p=23    [7,23]
N_p=[47,3083,31479823396757]
46=[2,23]       3082=[2,23,67]  31479823396756=[2^2,7^2,23,1811,3855937]
```

1.4　一般の弱完全数

$e+1$ が素数になるとき, $Q=\frac{P^{e+1}-1}{P}$ と ($N_p=\frac{P^{e+1}-1}{P}$ も使われる) おき, $a=P^eQ$ を (P を底とする) 弱い完全数, または弱完全数 (weak perfect number with respect to P) ということにしこれを研究しよう. 総称して一般の弱完全数とも言う.

1.5　フェルマとオイラーの結果 (一般の場合):完成版

(ここからが本体部分になる.)

フェルマとオイラーの結果は $P=2$ で成り立つのだ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.

1) $P-1\not\equiv 0 \bmod Q$ のときと 2) $P-1\equiv 0 \bmod Q$ のときで区別する必要があることにだんだんと気づいたが定理として明確に述べてはいなかった. それが反省点である.

奇素数 P を底とするとき $N_p=\frac{P^p-1}{P}$ の素数因子 (奇数) Q について

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

になる.

1) $P-1\not\equiv 0 \bmod Q$ ならば mod$Q$ で P の位数は素数 p である. $P\neq Q$ により, フェルマの小定理によれば $P^{Q-1}\equiv 1 \bmod Q$ なので $Q-1$ は位数 p で割れる. よって $Q-1=kp$ と書ける.

1-a) $p>2$ を仮定する. Q,p はともに奇数なので k は偶数. したがって, $Q=1+2k'p$ と書ける. オイラーの基準によって

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

$P^{\frac{Q-1}{2}}=P^{pk'}\equiv 1 \mod Q$. ゆえに

$$\left(\frac{P}{Q}\right)=1.$$

逆に $Q=2p+1$ が素数 (p : Sophie Germain 素数) とする. さらに $\left(\frac{P}{Q}\right)=1$ を仮定すると, $P\equiv n^2 \mod Q$ を満たす n がある.

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

これより, 素因子 Q は P^p-1 の素因子になる. $P-1\not\equiv 0 \bmod Q$ なので Q は $N_p=\frac{P^p-1}{P}$ の素因子.

1-b) $p=2$ のときは, $Q-1=2k$. $p=2$ なので $N_2=P+1$ となりこの素因数分解から奇数素因子 Q を求める.

2) $P \equiv 1 \bmod Q$ ならば次の場合がおこる.
$P^j \equiv 1 \bmod Q$ によって

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

Q は N_p の素因子なので $N_p \equiv 0 \bmod Q$. ゆえに $p \equiv 0 \bmod Q$. p, Q は素数なので $p = Q$.
$P \equiv 1 \bmod Q$ によれば $\left(\frac{P}{Q}\right) = \left(\frac{1}{Q}\right) = 1$.
したがって次の結果が証明できた.

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 $\left(\frac{P}{Q}\right) = 1$.

(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.

$P \equiv 1 \bmod Q$ 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.

Proof.
$Q = 2p+1$ は素数でないとする. その最小の素因子をとり Q_0 とする. $2p+1 \geq N_0^2$ を満たす. Q_0 も N_p の素因子なので $Q_0 \neq P$.

$$P^p = \overline{P}N_p + 1 \equiv 1 \mod Q_0.$$

p は素数なので Q_0 を法とした P の位数である. フェルマの小定理を用いて

$$P^{Q_0-1} \equiv 1 \mod Q_0.$$

ゆえに, $Q_0 - 1$ は p の倍数. とくに $Q_0 - 1 > p$ になり

$$2p+1 \geq Q_0^2 > p^2 + 2p + 1 > 2(p+1) + 1.$$

これで矛盾した.

1.5.1　$P = 5$ 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.

1.5.2　$P = 5$ のときの弱完全数の数表

$N_p = \frac{P^p-1}{P} = \frac{5^p-1}{4}$

表 1.4: $P = 5$

p	$(2p+1)$	$N_p =$ 分解	a
2	(5)=5	(6)=2*3	30
3	(7)=7	(31)=31	775
5	(11)=11	(781)=11*71	488125
7	(15)=3*5	(19531)=19531	305171875
11	(23)=23	(12207031)=12207031	119209287109375
13	(27)=3^3	(305175781)=305175781	74505805908203125
17	(35)=5*7	(190734863281)=409*466344409	29103830456695556640625
19	(39)=3*13	(4768371582031)=191*6271*3981071	A
23	(47)=47	B	C
29	(59)=59	D	E
31	(63)=$3^2 * 7$	F	G

表 1.5: $P = 5$ 続き

p	$(2p+1)$	$N_p =$ 分解	a
37	(75)=$3 * 5^2$	H	I
41	(83)=83	J	K
43	(87)=3*29	L	M
47	(95)=5*19	N	O

$A = 1818989403545761108398437 5$
$B = (2980232238769531) = 8971 * 332207361361$
$C = 710542735760100126266479492 1875$
$D = (46566128730773925781) = 59 * 35671 * 22125996444329$
$E = 1734723475976807094402611255645751953125$
$F = (1164153218269348144531) = 1861 * 625552508473588471$
$G = 10842021724855044340072199702262878417968 75$
$H = (1818989403545856475830078 1) = 149 * 13971969971 * 8737481256739$
$I = 2646977960169688559588507778244093060493469238281 25$
$J = (1136868377216160297393798828 1) = 2238236249 * 5079304643216687969$
$K = 1033975765691284593589260865064716199412941932678222656 25$
$L = (2842170943040400743484497070 31) = 1644512641 * 172827552198815888791$
$M = 6462348535570528709932880406790900451596826314926147460937 5$
$N = (1776356839400250464677810668945 31)$
$= 177635683940025046467781066894531$
$O = 2524354896707237777317531408904912382240581791847944259643554687 5$

1.5.3　$P = 5, Q = 2p + 1$ 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

1.5.4　$P = 7$

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.

1.6　$P = 7;\ p$: 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	(45614578900134860 57)=47*3083*31479823396757
29	59	(53665095930219662113 9601)=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 $p=23, 29, p=83=13+5*14, 167=13+11*14$.

1.6.1　$P = 11$

$P = 11, P - 1 = 10 = 2 * 5$. $Q = p = 5$ 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

$A0 = 232251544198878080950520379327369 7$
$A = 340039485861577398986846964992269755 49$
$B = (89543024325523737224653) = 829 * 28878847 * 3740221981231$
$C = 728904836851030521429027853850124525396790261 3$
$D = (158630929717149157441443670489) = 523 * 303309617049998388989376043$
$E = 228761562390246506066453264733348483256258951604954126056 09$
$F = (191943424957750480504146841291 81) = 50159 * 2428541 * 157571957584602258799$
$G = 33492980349555990953189422489630490716271536793263604160376698 1$
$H = (34003948586157739899240688230576198697) = 2591*36855109*136151713*2615418118891695851$
$I = 10511531995000535984031884072175901907045798792322646350775223148922564706 17$
$J = (49785181124993546986478291638386612512424 1)$
$= 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$
$K = 225324023604401248793730853803334956796672939988861482205529251845184623522089398641$
$L = (60240069161242191853638732882447801140033173)$

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

1.6.2　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.

1.6.3　$P = 13$

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

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

$A = 479677535758244089774221240729252401$
$B = 13700070098791209449615908553795581328767$

1.6.4　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.

1.6.5　$P = 17$ 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

1.6.6　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 $q \equiv 7, a \equiv 3 \mod 10$.

1.6.7　$P = 31$ 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 1.11: $P = 31$

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 $Q = 5$.

1.6.8　$P = 47$ の弱完全数

表 1.12: $P = 47$

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 $Q = 7$.

1.6.9　$P = 19$ の弱完全数

1.6.10　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 $q \equiv 1, a \equiv 1 \mod 10$.

1.6.11　$P = 23$ の弱完全数

1.6.12　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 $q \equiv 3, a \equiv 7 \mod 10$.

第2章　弱弱完全数

2.1　条件を弱める

弱完全数の条件をさらに弱めて, $e+1$ を奇数 $2\varepsilon-1$($e+1=2$ はあえて付加する) だけにしてみよう. 意外にも次からわかるように 末尾1桁が 6 または 8 という性質はやはり成立している.

$e+1$ を奇数と仮定している場合, 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 2.1: $P=2$

$2\varepsilon-1$	$Q=2^{2\varepsilon-1}-1$	素因数分解	a: 弱弱完全数
2	3	3	6
3	7	7	28
5	31	31	496
7	127	127	8128
9	511	7*73	130816
11	2047	23*89	2096128
13	8191	8191	33550336
15	32767	7*31*151	536854528
17	131071	131071	8589869056
19	524287	524287	137438691328
21	2097151	$7^2*127*337$	2199022206976
23	8388607	47*178481	35184367894528
25	33554431	31*601*1801	562949936644096
27	134217727	7*73*262657	9007199187632128
29	536870911	233*1103*2089	144115187807420416
31	2147483647	2147483647	2305843008139952128
33	8589934591	7*23*89*599479	36893488143124135936
35	34359738367	31*71*127*122921	590295810341525782528
37	137438953471	223*616318177	9444732965670570950656
39	549755813887	7*79*8191*121369	151115727451553768931328

弱弱完全数 a の末尾の数は $6,8,6,8,\cdots$ が正確に繰り返され, $Q=2^{2\varepsilon-1}-1$ の末尾の数は 最初を飛ばすと $7,1,7,1,\cdots$ となり正確に繰り返されている.

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 2.2: $P = 2$

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

弱弱完全数については, 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なったその結果, 下 2 桁の数が周期 10 で正しく変化することが分かった.

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.

2.1.1　周期性の証明

以下ではこの周期性の結果を証明する.

$Q = 2^{2\varepsilon-1} - 1$ となる Q を $Q_{2\varepsilon-1}$ と書き, 弱弱完全数 $a = 2^{2\varepsilon-2}Q_{2\varepsilon-1}$ 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 $Q_{20m+3} - Q_3 \equiv 0$. $L = \varepsilon - 1$ とおき 2^{2L} を掛けると

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

$L = 1, 2, 3, 4, \cdots$ に応じて $Q_{3+2L} = Q_5 = 2^5 - 1 = 31, Q_7 = 2^7 - 1 = 32 \times 4 - 1 \equiv 287$ と計算した結果, Q_{3+2L}　はそれぞれ

$$27, 11, 47, 91, 67, 71, 87, 51, 7, 31, 27, \cdots$$

これから 周期が 10 もわかった.

$\xi = 20m + 3 + 2L$ とおくとき $a_\xi = 2^{\xi-1}Q_\xi$ が成り立つ.

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

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

2.1.2　$P = 2$; 弱弱完全数の p, Q, a 変化

表 2.3: $P = 2$

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

2.2　P を底とする弱弱完全数

一般に P を奇素数とし, $p = e+1$ が奇数のとき, $Q_p = \frac{P^p-1}{\overline{P}}$ に関して $a_p = P^e Q_p$ を P を**底とする弱弱完全数** (ww-perfect number) という.

$Q_p = \frac{P^p-1}{\overline{P}}$ を変形する

$$\begin{aligned}\overline{P}Q_{p+2} &= P^2P^p - 1\\ &= P^2(\overline{P}Q_p + 1) - 1\\ &= P^2\overline{P}Q_p + P^2 - 1.\end{aligned}$$

これより

$$Q_{p+2} = P^2Q_p + P + 1.$$

これより

$$\begin{aligned}a_{p+2} &= P^2P^p - 1(P^2Q_p + P + 1)\\ &= P^4a_p + P^{p+1}(P+1)\\ &= P^4a_p + P(P+1)(\overline{P}Q_p + 1).\end{aligned}$$

これより

$$a_{p+2} = P^4a_p + P(P^2-1)Q_p + P(P+1).$$

数列 (p : 奇数のみ) $\{Q_p\}, \{a_p\}$ は連立漸化式で定まるがこれを 10,100,1000 を法としてエクセルで計算すると容易にそれぞれの下 1 桁,2 桁,3 桁が求められる.

2.2.1　$P = 3$; 弱弱完全数の表

表 2.4: $P = 3$;

$2\varepsilon - 1$	$(3^{2\varepsilon-1} - 1)/2 =$ 素因数分解	a: 弱弱完全数
3	(13)=13	117
5	$(121) = 11^2$	9801
7	(1093)=1093	796797
9	(9841)=13*757	64566801
11	(88573)=23*3851	5230147077
13	(797161)=79716	423644039001
15	$(7174453)=11^2 * 13 * 4561$	34315186290957
17	(64570081)=1871*34511	2779530261754401
19	(581130733)=1597*363889	225141952751788437
21	(5230176601)=13*1093*368089	18236498186842001001
23	(47071589413)=47*1001523179	1477156353259726319517
25	A	B
27	C	D
29	E	F
31	G	H
33	I	J
35	K	L
37	M	N
39	O	P

$A = (423644304721) = 11^2 * 8951 * 391151$
$B = 119649664615167550026801$
$C = (3812798742493) = 13 * 109 * 433 * 757 * 8209$
$D = 96916228338387390154841 97$
$E = (34315188682441) = 59 * 28537 * 20381027$
$F = 78502144954102936742403 9801$
$G = 308836698141973 = 683 * 102673 * 4404047$
$H = 63586737412824202325875602477$
$I = 2779530283277761 = 13 * 23 * 3851 * 2413941289$
$J = 515052573043876780047667920 8001$
$K = 25015772549499853 = 11^2 * 71 * 1093 * 2664097031$
$L = 41719258416554025854733781451 4357$
$M = 225141952945498681 = 13097927 * 17189128703$
$N = 337925993174087615427129041636 59401$

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

$P = 27372005447101096903631521079483798 37$

弱弱完全数の Q 下 2 桁 と a 下 2 桁 を書き出した.

表 2.5: $P = 3$

$2\varepsilon - 1$	$Q = (3^{2\varepsilon-1} - 1)/2$	Q の素因数分解	a : 弱弱完全数	Q 下 2 桁	a 下 2 桁
3	13	13	117	13	17
5	121	11^2	9801	21	1
7	1093	1093	796797	93	97
9	9841	13*757	64566801	41	1
11	88573	23*3851	5230147077	73	77
13	797161	79716	423644039001	61	1
15	7174453	$11^2 * 13 * 4561$	34315186290957	53	57
17	64570081	1871*34511	A	81	1
19	581130733	1597*363889	B	33	37
21	5230176601	13*1093*368089	C	1	1
23	47071589413	47*1001523179	D	13	17
25	423644304721	$11^2 * 8951 * 391151$	E	21	1
27	3812798742493	13*109*433*757*8209	F	93	97
29	34315188682441	59*28537*20381027	G	41	1

$A = 2779530261754401$
$B = 225141952751788437$
$C = 18236498186842001001$
$D = 1477156353259726319517$
$E = 119649664615167550026801$
$F = 96916228333838739015484197$
$G = 78502144954102936742403980 1$

2.3　$P = 3$; 弱弱完全数の p, Q, a 変化

表 2.6: $P = 3$

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
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 $3^{20} - 1 \equiv 0 \mod 200$.

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

2.3.1　$P = 5$ の弱弱完全数の p, Q, a 変化

表 2.7: $P = 5$

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

周期 は 2

2.3.2　$P = 7$; 弱弱完全数の p, Q, a 変化

表 2.8: $P = 7$

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

2.3.3　$P = 11$; 弱弱完全数の p, Q, a 変化

表 2.9: $P = 11$

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

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

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

2.3.4　$P = 11$ 弱弱完全数の表

表 2.10: $P = 11$

$2e+1$	$(11^{2e+1} - 1)/10$	分解	a
3	133	7*19	16093
5	16105	5*3221	235793305
7	1948717	43*45319	3452271037237
9	235794769	7*19*1772893	U
11	28531167061	15797*1806113	V
13	3452271214393	1093*3158528101	W
15	417724816941565	5*7*19*3221*195019441	X
17	50544702849929377	50544702849929377	Y
19	6115909044841454629	6115909044841454629	Z
21	740024994425816010121	A	B
23	89543024325523737224653	C	D
25	10834705943388372204183025	E	F
27	1310999419149993036706146037	G	H

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

2.3.5　$P = 13$; 弱弱完全数の p, Q, a 変化

表 2.11: $P = 13$

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

2.3.6　$P = 13$ のときの弱弱完全数

表 2.12: $P = 13$

$2e+1$	$Q = (13^{2e+1} - 1)/12$	分解	a
3	183	3*61	30927
5	30941	30941	883705901
7	5229043	5229043	25239591813787
9	883708281	A	B
11	149346699503	C	D
13	25239592216021	E	F
15	4265491084507563	G	H
17	720867993281778161	I	J
19	121826690864620509223	K	L
21	20588710756120866058701	M	N
23	3479492117784426363920483	O	P
25	588034167905568055502561641	Q	R
27	99377774376041001379932917343	S	T
29	16794843869550929233208663030981	U	V
31	2838328613954107040412264052235803	W	X
33	479677535758244089829672624827850721	Y	Z

$A = 3^2 * 61 * 1609669$
$B = 720867993213800601$
$C = 23 * 419 * 859 * 18041$
$D = 20588710756109377851047$
$E = 53 * 264031 * 1803647$
$F = 588034167905566113995468101$
$G = 3 * 61 * 4651 * 30941 * 161971$
$H = 16794843869550928905093964222707$
$I = 103 * 443 * 15798461357509$
$J = 479677535758244089774221240729252401$
$K = 12865927 * 9468940004449$
$L = 13700070098791209449615908553795581328767$
$M = 3 * 43 * 61 * 337 * 547 * 2714377 * 5229043$
$N = 391287702091575733090746033697803929523057501$
$O = 1381 * 2519545342349331183143$
$P = 11175568059437494512804842434187269399079517489227$
$Q = 701 * 9851 * 30941 * 2752135920929651$

$R = 319185399345594280780219112362033386548297277812147401$
$S = 3^3 * 61 * 650971 * 1609669 * 57583418699431$
$T = 91162541907095182533638380694563021759116791848103365440 87$
$U = 1973 * 2843 * 3539 * 846041103974872866961$
$V = 260369335940854550834324579101958487505450742744381795527146101$
$W = 311 * 1117 * 817050901143136340856815036 9$
$X = 7436408603806746826379144303731073041582189762751733789770879453347$
$Y = 3 * 23 * 61 * 419 * 859 * 18041 * 17551032119981679046729$
$Z = 212391266133324496108214740458863183339538614689722045030030778150037601$

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

2.3.7　$P = 41$; 弱弱完全数の p, Q, a 変化

$P = 41$ のとき弱弱完全数の周期は 50. 本当だろか.

表 2.13: $P = 41$ 前半分

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
3	23	63
5	5	5
7	47	27
9	49	29
11	11	11
13	33	73
15	15	15
17	57	37
19	59	39
21	21	21
23	43	83
25	25	25
27	67	47
29	69	49
31	31	31
33	53	93
35	35	35
37	77	57
39	79	59
41	41	41
43	63	3
45	45	45

周期は $(103 - 3)/2 = 50$

表 2.14: $P = 41$ 後半分

$p = 2\varepsilon - 1$	$Q = N_p$	$a = P^{p-1}Q$
47	87	67
49	89	69
51	51	51
53	73	13
55	55	55
57	97	77
59	99	79
61	61	61
63	83	23
65	65	65
67	7	87
69	9	89
71	71	71
73	93	33
75	75	75
77	17	97
79	19	99
81	81	81
83	3	43
85	85	85
87	27	7
89	29	9
91	91	91
93	13	53
95	95	95
97	37	17
99	39	19
101	1	1
103*	23	63
105	5	5

2.3.8　$P = 43$; 弱弱完全数の p, Q, a 変化

表 2.15: $P = 43$

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

2.4　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.

2.4.1　$P = 5$ 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, $T = 2$.

2.4.2　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 2.16: 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 2.17: 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 2.18: 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

第3章　微弱完全数

3.1　弱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 $a_{p^\alpha}=P^eN_{p^\alpha}$ 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.

3.1.1　$P=2,p=3$ 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]
```

3.1.2　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.

3.1.3　$P = 3, p = 5$ 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]
```

3.1.4　$P = 5$ の例

3.1.5　$P = 5, p = 3$

```
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]
```

3.1.6　$P = 7, p = 3$

```
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]
```

3.1.7　$P = 2, p = 3, 5$

```
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]
```

A=(42535295865117307932921825928971026431)

B= 31*601*1801*269089806001*4710883168879506001

C=(179179579374224336844595382445[44 digits]44128756304701994617285692620 7)

D= 127*6073159*1428389887*62228099977*4432676798593*589618044748441647248140959151143380931461182483

E=(21833675143960339206520134928541701232737428874584890942772 1)

F= $11^2 * 251 * 8951 * 391151 * 358291751 * 14781691751 * 391632555001 * 989947158849251$

G=　(587747175411143753984368268611122838909332778386043760754375853139208629727363586425781)

H=11*71*101*251*401*3597751*9384251*28707251*4032808198751*767186663625251*2468704521413923404337560

表 3.1: 弱弱完全数の周期 3

$P=2$		
p	(N_p)	素因数分解
3	(7)	7
9	(511)	7*73
27	(134217727)	7*73*262657
5	(31)	31
25	(33554431)	31*601*1801
125	A	B
7	(127)	127
49	(562949953421311)	127*4432676798593
343	C	D
$P=3$		
p	(N_p)	素因数分解
3	(13)	13
9	(9841)	13*757
27	(3812798742493)	13*109*433*757*8209
5	(121)	11^2
25	(423644304721)	$11^2 * 8951 * 391151$
125	E	F
7	(1093)	1093
49	(119649664615308764795041)	491*1093*4019*8233*51157*131713
$P=5$		
p	(N_p)	素因数分解
3	(31)	31
9	(488281)	19*31*829
27	(1862645149230957031)	19*31*109*271*829*4159*31051
5	(781)	11*71
25	(74505805969238281)	11*71*101*251*401*9384251
125	G	H