Contents

書泉グランデでの講義 第 3 期 資料 1
高校生も十分わかる新しい数論研究 , 2015 年 6 月 12 日

飯高 茂

第３期をはじめるにあたって

1. 開講の辞　3

4,5月を休んで 6.7月に第３期をすることになった.

2ヶ月の休みはありがたかった.

弱弱完全数、フェルマーの弱完全数の理論がこのような形をとってきたのは大きな収穫であり, この講座がなければこのような発展は無かったであろう.

参加者および書店に深甚なる謝意を表したい.

2015 年6月12日

2. はじめに

自然数 a の約数の和を $\sigma(a)$ で表す．これを a の関数と見てユークリッド関数という.

$\sigma(a)-2a=0$ を満たす自然数 a を完全数(perfect number)という.

完全数の概念は2300年昔に遡り,多くの研究が行われたが,完全数が無限にあるかどうかも未解決で、これは最古のそして未だに解決がされていない数学界最大の難問の1つである.

完全数の概念を究極の形に一般化して研究することがこの講座の目的である.ここで語られ説明される主要な結果はすべて新しい研究の成果である. 講座の参加者も一緒になってこの研究に加わってほしい.

次の2つの結果がこの研究の出発点であり,実に古めかしい.

$\sigma(2^e)$ が素数のとき $2^e\sigma(2^e)$ は完全数になる.(ユークリッド)

完全数が偶数なら上の形になる.(オイラー)

2.1. 研究目標. 目標 究極の完全数の探究

P を素数とし $\sigma(P^e)$ が素数 q のとき $a = P^e q$ を底が P の(究極の) 完全数.

究極の完全数を整数 m だけ平行移動する. $q = \frac{P^{e+1}-1}{\overline{P}} + m$ は素数とし $a = P^e q$ を m だけ平行移動した底が P の完全数と呼ぶ. ただし $q > P$. ($\overline{P} = P - 1$)

これより a の最大素因子 $\mathrm{Maxp}(a)$ を用いると $q = \mathrm{Maxp}(a)$ になるので

$$\overline{P}\sigma(a) - Pa = (P-2)\mathrm{Maxp}(a) - m(P-1). \tag{1}$$

m 平行移動した究極の完全数の基本方程式という. 基本方程式を解くことこそ究極の課題である.

弱完全数

3. 完全数

2 のべき $2^{e+1}-1$ が素数になるとき$q=2^{e+1}-1$ とおく. このとき$a=2^eq$ は完全数になる.

すなわち自然数 a に対して $\sigma(a)$　を a の約数の和とするとき$\sigma(a)=2a$ を満たす. この形の$a=2^eq$ は完全数をとくにユークリッドの完全数という.

3.1. 完全数の数表. 数値例をみて見よう.

Table 1. 完全数

p	$(2p+1)=$	$2^p-1=$ 素因数分解	a:完全数
2	(5)=5	(3)=3	6
3	(7)=7	(7)=7	28
5	(11)=11	(31)=31	496
7	(15)=3*5	(127)=127	8128
13	$(27)=3^3$	(8191)=8191	33550336
17	(35)=5*7	(131071)=131071	8589869056
19	(39)=3*13	(524287)=524287	137438691328
31(Euler)	$(63)=3^2*7$	(2147483647)=2147483647	2305843008139952128
61	(123)=4*41	A	B

$$A=(2305843009213693951)=2305843009213693951$$
$$B=2658455991569831744654692615953842176$$

3.2. **末尾の数は.** 完全数 a の末尾の数は 6 か 8. 言い換えると $a \equiv 6$ または $8 \mod 10$. これは完全数の持つ周知の性質のひとつ.

完全数の歴史的経緯によると, 古代ギリシャの数学者が 最初の完全数４個 6,28,496,8128 を発見し, 末尾の数は 6, 8, 6, 8 となることを見出し, 以後も6,8 が交互に繰り返されることを期待した. しかし, 次々と完全数を求めると33550336 の次に 8589869056 がでてきて末尾の 6 がダブることがわかり, 甘い期待は消え去った.

$e = p - 1$ とする. 数表を観察すると次の結果がわかる. ただし, ここで $e > 1$ の場合しか扱わない. ($e = 1$ は例外の場合として考える.)

- $e \equiv 0 \mod 4$ なら $q \equiv 1 \mod 10$. $a \equiv 6 \mod 10$.
- $e \equiv 2 \mod 4$ なら $q \equiv 7 \mod 10$. $a \equiv 8 \mod 10$.

3.3. **弱完全数.** しかし, $2^{e+1}-1$ が素数になるとき $e+1$ は素数になるので $2^{e+1}-1$ が素数になるという条件をはずして,

$e+1=p$ が素数になるという条件をつける.

このとき, $Q=2^{e+1}-1$ とおき, $a=2^eQ$ を弱い完全数, または弱完全数 ということにしこれを研究しよう.

数値例

TABLE 2. $P = 2$:弱完全数

p	$(2p+1)$	$Q =$ 素因数分解	a:弱完全数
2	(5)=5	(3)=3	6
3	(7)=7	(7)=7	28
5	(11)=11	(31)=31	496
7	(15)=3*5	(127)=127	8128
11	(23)=23	(2047)=23*89	2096128
13	$(27) = 3^3$	(8191)=8191	33550336
17	(35)=5*7	(131071)=131071	8589869056
19	(39)=3*13	(524287)=524287	137438691328
23	(47)=47	(8388607)=47*178481	35184367894528
29	(59)=59	(536870911)=233*1103*2089	144115187807420416
31	$(63)=3^2*7$	(2147483647)=2147483647	2305843008139952128

この表を観察するとQ と a の末尾の数は $Q \equiv 1$ または $7 \mod 10$; $a \equiv 6$ または $8 \mod 10$

- $p \equiv 1 \mod 4$ なら $Q \equiv 1 \mod 10$. $a \equiv 6 \mod 10$.
- $p \equiv 3 \mod 4$ なら $Q \equiv 7 \mod 10$. $a \equiv 8 \mod 10$.

という性質は相変わらず成立していることがわかる.

そこで実際に弱完全数でこの結果が成り立つことを示す.

$e+1=p$ は素数,という性質を用いる. Q は素数という性質は使えない.

$2^4 = 16 \equiv 1 \mod 5$ を以下用いる.

1). $e = 4k$ のとき.

$Q = 2^{e+1} - 1 \equiv 1 \mod 5$ によって $Q = 1 + 5L$とかけて Q は奇数なので L は偶数. $Q \equiv 1 \mod 10$.

$a = 2^e q \equiv Q \equiv 1 \mod 5$; $a = 1 + 5L$. a は偶数なので $L = 2m + 1$. $a = 1 + 5(2m + 1) \equiv 6 \mod 10$.

2). $e = 4k + 1$ のとき.

$p = e + 1 = 4k + 2$ が素数なので, $Q = 3, k = 0, e = 1$. $a = 2 * Q = 6$. これは例外的な場合.

3). $e = 4k + 2.$のとき.

$Q = 2^{e+1} - 1 = 2^{4k+3} - 1 \equiv 8 - 1 = 7 \equiv 2 \mod 5$ によって $Q = 2 + 5L$ とかけてQ は奇数なのでL は奇数になり, $Q \equiv 7 \mod 10$.

4). $e = 4k + 3$. $e = 4k + 2$.のとき.
$p = e + 1 = 4(k + 1)$ は素数ではない.
このように証明は簡単にできる.

完全数の発見の歴史では, 完全数の末尾 1 桁が 6 または 8 という事実は強烈なインパクトをもたらした.しかし,その性質は弱完全数も持っている. これはやや意外な結果である.

4. フェルマとオイラーの結果

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 $Q \equiv \pm 1 \bmod 8$.

Proof.

条件より,

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

p は素数なので 2 の mod$Q$ での位数は p. フェルマの小定理によると $2^{Q-1} \equiv 1 \mod Q$. 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. $Q-1=2Lp$ により

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

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

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

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

$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$$

が成り立つゆえに $Q \equiv \pm 1 \bmod 8$.

例

$p = 11$ とする. $A = 2^{11} - 1$ の素因数分解は $23 * 89$. このとき

$$23 - 1 = 22 = 2 * 11 = 2q, 89 - 1 = 88 = 8 * 11 = 8p.$$

$p = 23$ とする. $A = 2^{23} - 1$ の素因数分解は $47, 178481$. このとき

$$47 - 1 = 46 = 2 * 23 = 2p, 178480 = 178481 - 1 = 2^4 * 5 * 23 * 97 = 2^4 * 5 * 97 * p.$$

4.1. **ラグランジュの結果.** 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$Q \equiv \pm 1 \bmod 8$ のとき,
$Q = 2p + 1$ 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.

$Q = 2p + 1$ が素数なので,$Q \equiv 1 \bmod 8$ は成立しない. (By Mizutani)

$Q = 2p + 1$ が素数になる素数 p をSophie Germain の素数という.

[注] $Q \equiv -1 \bmod 8$ かつ $Q = 2p+1$ によって $p \equiv 3 \bmod 4$, なのでこれを条件にしてもよい.

$p \equiv 1 \bmod 4$, $Q = 2p+1$: 素数のとき $\left(\dfrac{2}{Q}\right) = -1$.

Table 3. $Q=2p+1$ が素数とする

$\left(\frac{2}{Q}\right)$	p	$Q=2p+1$	M_p の素因数分解
$(+)$	3	7	7
$(+)$	11	23	23*89
$(+)$	23	47	47*178481
$(+)$	83	167	167*57912614113275649087721
$(+)$	131	263	Z
$(-)$	5	11	31
$(-)$	29	59	233*1103*2089
$(-)$	41	83	13367*164511353
$(-)$	53	107	6361*69431*20394401
$(-)$	89	179	A
$(-)$	113	227	3391*23279*65993*1868569*1066818132868207

$$Z = 263 * 1035079443105516238671861923746823 4569$$

$$A = 6189700196426901374495621111$$

$\left(\frac{2}{Q}\right) = 1$ のとき $p \equiv 3 \mod 4$. このとき, $Q = 2p + 1$ が M_p の最小素因子として出ている.実に壮観である.

$\left(\frac{2}{Q}\right) = -1$ のとき $p \equiv 1 \mod 4$. このとき, M_p の最小素因子がどうなるか誰も分からない.悲しい限り.

5. 一般の弱完全数

$e+1$ が素数 p になるとき, $Q=\frac{P^{e+1}-1}{P-1}$ と($N_p=\frac{P^{e+1}-1}{P-1}$ 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.

5.1. $P=3$. $N_p=\frac{P^p-1}{P}=\frac{3^p-1}{2}$ とおく. $p\geq 2$ を仮定する. $p=e+1$ は素数と仮定している.

$P=3$ のとき弱完全数の数表は次の通り.

TABLE 4. $P=3$; 弱完全数の数表

p	$(2p+1)=$	$N_p=$ 分解	a
2	(5)=5	$(4)=2^2$	12
3	(7)=7	(13)=13	117
5	(11)=11	$(121)=11^2$	9801
7	(15)=3*5	(1093)=1093	796797
11	(23)=23	(88573)=23*3851	5230147077
13	$(27)=3^3$	(797161)=797161	423644039001
17	(35)=5*7	(64570081)=1871*34511	27795302617544011
19	(39)=3*13	(581130733)=1597*363889	225141952751788437
23	(47)=47	(47071589413)=47*1001523179	1477156353259726319517
29	(59)=59	(34315188682441)=59*28537*20381027	785021449541029367424039801
31	$(63)=3^2*7$	(308836698141973)=683*102673*4404047	63586737412824202325875602477
37	$(75)=3*5^2$	(225141952945498681)=13097927*17189128703	A
41	(83)=83	(18236498188585393201)=83*2526913*86950696619	B
43	(87)=3*29	C	D
47	(95)=5*19	E	F

$A = 33792599317408761542712904163659401$
$B = 22171324412151888496804598258004648200\,1$
$C = (16412848369726853881\,3) = 431 * 38080854686141192\,3$
$D = 179587727738430296828494005455098144789\,17$
$E = (13294407179478751643893) = 1223 * 21997 * 5112661 * 96656723$
$F = 1178275081691841177495294345038759928400115\,97$

$p = 5$ のときの　$a = 9801 = 3^4 \times 11^2$. 昔懐かしきパソコンの番号 9801 が登場.

$p = 7$ のとき $N_p = 1093$. これは Wieferich 素数のひとつ. Wieferich 素数は 2 つしかないから貴重な素数.

5.2. **末尾の数.** 3が底の弱完全数 の場合, $Q=\frac{3^p-1}{2}$ は素数でなくても $p=e+1$ が素数を仮定するときQ の末尾の数が 3 または 1, も同様に成立する. また, 3を底とする弱完全数では末尾の数が 7 または 1 になる.

Proof.

$e>1$ とする. $p=e+1$ が素数は使える. しかし$Q=\frac{3^p-1}{2}$ が素数とは言えない.

$3^2=9\equiv -1 \mod 5$ により$3^4\equiv 1 \mod 5$. これを以下使う.

$2Q=3^{e+1}-1$ となるQ についてその末尾の数は 3 または 1 を示す.

1. $e=4k+2$ のとき

$$2Q=3^{e+1}-1=3^{4k+3}-1\equiv 27-1\equiv -3-1\equiv 1\equiv 6 \mod 5.$$

よって $Q\equiv 3 \mod 5$. $Q=3+5L$ となる.

$$Q=\frac{3^p-1}{2}=1+3+\cdots+3^{p-1}\equiv p \mod 2$$

2. $e=4k$ のとき

$$2q=3^{e+1}-1=3^{4k+1}-1\equiv 3-1\equiv 2 \mod 5.$$

よって $Q\equiv 1 \mod 5$. $Q=1+5L$ となるが Q は奇数. L は偶数になるので$Q\equiv 1 \mod 10$.

$a=3^e q\equiv Q\equiv 1 \mod 5$ により a は奇数なので $a\equiv 1 \mod 10$.

3. $e=4k+3$ のとき $e+1=4(k+1)$ は素数ではない.

4. $e=4k$+1 のとき e+1 $=4k$+2 は素数なので $k=0, e=1$.

$e=1$

しかし,$Q = 2^p-1$ が合成数のとき,各素因子の末尾の数はさまざまである. Q の素因子の数が2個の場合, Q_1, Q_2 とおく.

$Q=Q_1Q_2$ の末尾の数が 1,3 なら可能性は絞られる.

$Q = Q_1Q_2Q_3$ の末尾の数が 1,3 ならどんな可能性があるか例と対応させて調べるとよい.

Table 5. mod10 での乗算表

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$Q = Q_1Q_2Q_3$ の末尾の数が 1,7 ならどんな可能性があるか例と対応させて良く調べるとよい.

次は課題:

- $e \equiv 2 \mod 4$ のとき $Q \equiv 13, 33, 73, 93 \mod 100$.
- $e \equiv 0 \mod 4$ のとき $Q \equiv 01, 41, 61, 81 \mod 100$.

N_p が素数になるのは $p=13,1093,797161$ であり数少ない．これらを **3を底としたメルセンヌ素数**という．

底が 3，一般には奇素数 P のときにもオイラーとラグランジュの結果が成立する．これは弱完全数に関して後に取り上げて証明する．

ここでは,$P=3$ の場合を取り上げる．

6. 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 $Q \equiv \pm 1 \bmod 12$.

Proof.

条件より,

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

p は素数なので 3 の $\mathrm{mod} p$ 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.

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

例 $p = 17$ のとき $A = 3^{17} - 1 = 129140162$. この 素因子分解 [2, 1871, 34511].

$p_1 = 1871$ とおくと $p_1 - 1$ の 素因子分解 [2, 5, 11, 17].

$p_2 = 34511$ とおくと $p_2 - 1$ の 素因子分解 $[2, 5, 7, 17, 29]$.

$P = 3$ のとき p がSophie Germain 素数ならば 素数 $Q = 2p + 1$ は $Q + 1 \equiv 0 \mod 12$ を満たし Q は すべて N_p の因子となる. これは意外な結果である.

Table 6. $P = 3, Q = 2p + 1$: 素数

p	$Q = 2p + 1$	$Q + 1$	$Q + 1 \bmod 12$	N_p の素因数分解
5	11	12	0	11^2
11	23	24	0	$23 * 3851$
23	47	48	0	$47 * 1001523179$
29	59	60	0	$59 * 28537 * 20381027$
41	83	84	0	$83 * 2526913 * 86950696619$
53	107	108	0	$107 * 24169 * 3747607031112307667$
83	167	168	0	A
89	179	180	0	B
113	227	228	0	C
131	263	264	0	D
173	347	348	0	E
178	359	360	0	F
190	383	384	0	G

$A = 167 * 12119 * 1036745531 * 9509960596272108979 43351$

$B = 179 * 1611479891519807 * 504293943956599604916 2197$

$C = 227*1583*2172539*526256453012063980796131127321354599535039$

$D = 263*6051995885911440031008813065744068516602884277403948858 2$

$E = 347*762239*212504886554 3*309854287003880455089590180543928 10$

$- - 03314928030690774676 6819$

$F = 359 * 56207 * 100957 * 19510643 * 291066066130451 *$

$6779963644378513811*$

$- - 16186866474449165570585896359 4331$

$G = 383*311713*9593931911*58908685917603654343320050749297104005$

$- - 91814682148588888003483695003 17$

6.1. **証明.** 参加者の水谷氏の指摘により, 次の結果を証明する.

補題 4. *p を素数とし, $Q = 2p + 1$ も素数とする. このとき Q を法として 3 は平方剰余である.*

3 より大きい素数 Q を mod 12 で分類すると $Q \equiv 1, 5, 7, 11 \mod 12$ である.

(1).$Q \equiv 1 \mod 12$ とすると $Q = 1 + 12k$. $Q = 2p + 1$ なので$1 + 12k = 2p + 1$. よって $p = 6k$. 矛盾.

(2). $Q \equiv 5 \mod 12$ とすると $Q = 5 + 12k = 2p + 1$. よって $p = 4 + 6k$. 矛盾.

(3). $Q \equiv 7 \mod 12$ とすると $Q = 7 + 12k = 2p + 1$. よって $p = 3 + 6k$. 矛盾.

$Q \equiv 11 \mod 12$ のみ生き残り, このときQ を法として3 は平方剰余.

一方,メルセンヌ数 $M_p = 2^p - 1$ には平方因子が無い. という予想がある.

しかし 底が3のとき$p = 5$ の場合 $N_5 = 11^2$. これは平方因子なので反例.

これは Wieferich の素数の一般化としてのちにとりあげる.

Table 7. $P = 5$: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	745058059082031
17	(35)=5*7	(190734863281)=409*466344409	29103830456695556
19	(39)=3*13	(4768371582031)=191*6271*3981071	181898940354576110839

6.2. $P = 5$.

6.3. **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.

TABLE 8. $P = 7$:弱完全数

p	$(2p+1)=$	$N_p=$ 素因数分解	a:弱完
2	(5)=5	$(8) = 2^3$	56
3	(7)=7	(57)=3*19	279
5	(11)=11	(2801)=2801	6725
7	(15)=3*5	(137257)=29*4733	161481
11	(23)=23	(329554457)=1123*29345	930909773
13	$(27) = 3^3$	(16148168401)=16148168401	22351143660
17	(35)=5*7	(38771752331201)=14009*2767631689	12884989532845
19	(39)=3*13	(1899815864228857)=419*4534166740403	30936859868362

6.4. $P = 7$.

6.5. **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

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

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

よって

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

7. 一般の弱完全数

$e+1$ が素数になるとき, $Q=\frac{P^{e+1}-1}{P-1}$ と$(N_p=\frac{P^{e+1}-1}{P-1}$ 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.

8. フェルマとオイラーの結果(一般の場合)

底が奇素数 P で, $N_p = \frac{P^p-1}{P}$ 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 $Q-1 = kp$ と書けるが 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

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

逆に素数 $Q = 2p + 1$ が素数(p : Sophie Germain)とする. さらに$\left(\dfrac{P}{Q}\right) = 1$ 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.

2)
$P - 1 \equiv 0 \bmod Q$ 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 $p = Q$.

したがって次の結果が証明できた.

定理 1. 底が奇素数 P 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, $p = Q$.

第1章で示したようこの結果は $P = 2$ のとき, フェルマとオイラーにより示された.

底が P でも同じ証明が成立することがわかった.

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. $2p+1 \geq Q_0^2$ 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.

8.1. $P=5$**.** フェルマとオイラーの結果(一般の場合)を$P=5$で使うと

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 $11, 21, 31, 41, 51, 61, 71, 81, 91, 101$ と公差10の数列をまず書いてここから合成数を除く.

$Q = 11, 31, 41, 61, 71, 91, 101, \cdots$

$Q \equiv 1 \mod 5$ のとき $Q = 2p+1$ と素数でかけることはない.

$Q \equiv -1 \mod 5$ のとき $9, 19, 29, 39, 49, 59, 69, 79, 89, 99, 109, 119, 129, 139,$ 公差10の数列をまず書いてここから合成数を除く.

$Q = 19, 29, 59, 79, 89, 109, 119, 139, 149, 159, 169, 179 \cdots$

$Q = 2p+1$ と素数でかけることはおきる.

Table 9. $P=5, Q=2p+1$ 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	(298023223876953 1)=8971*332207361361
29	59	A
41	83	B
53	107	C
83	167	$D=E$
89	179	$F=G$
113	(227)=227	$H=I$
131	(263)=263	$J=K$

8.2. $P=5$.

$A = (465661287307739257 81) = 59 * 35671 * 22125996444329$

$B = (11368683772161602973937988281) = 2238236249*5079304643216687$

$C = (277555756156289135105907917022705 0781) = 960555749*$
$17154094481 * 27145365052629449$

$D = (2584939414228211483973152162718633917393162846565246582031)$

$E = 20515111*1431185706701868962383741*880400959451038346273767 8$

$F = (4038967834731580443708050254247865495926816947758197784423 8$

$G = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 *$
$23166965436368313009 5909$

$H = (24074124304840448163199724282311591481726270602692352440499$

$I = 2939*6329*129499*308491*304247586761*2084303944451$

$- *620216264269531 * 8237123176890810696379$

$J = 9183549615799121156005754197048794357958324662 28193$

$-$

$3761787122705300134839490056037902832031)$

$K = 2621 * 23928199 * 34720241 * 1681564261186 1* -$

$Q \equiv 1 \mod 5$ のとき $Q = 2p+1$ と素数でかけることはない.

$Q \equiv -1 \mod 5$ のとき$Q = 19, 29, 59, 79, 89, 109, \cdots$

$Q = 59, Q = 179$ の 2 例ができたことがわかる.

8.3. $P = 7$.

定理 4. 底が奇素数 $P = 7$ のとき, 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.

9. $P=7$; p : Sophie Germain 素数

$\left(\frac{7}{Q}\right)=1$ を解くと $Q=\pm1,\pm3,\pm9 \mod 28$

$p, Q=2p+1$ も素数のときの数表.

Table 10. $P=7, Q=2p+1$ 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	(5366509593021966211396O1)=59*127540261*7131692298499
41	83	A
53	107	$B=C$
83	167	$D=E$

$A = (742794005439386598336500766242800 1) = 83*20515909*$
$4362139336229068656094783$

$B = (1028122516046770610484593594692316211321964 01)$

$C = 8269 * 319591 * 890427601703518805637205183984121 9$

$D = (23173203249700874472330986792321198522833668720161907874906 6$

$E = 167 * 66733 * 76066181 * 7685542369 * 62911130477521 *$
$303567967057423 * 18624275418445601$

$Q = 2p+1$ が N_p の最小素因子となるのは$Q = 47, 59, 83, 167.$

9.1. $P = 11$. $N_p = \frac{P^p - 1}{\overline{P}}$

Table 11. $P = 11$

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	23579330
6	7	(15)=3*5	(1948717)=43*45319	34522710
10	11	(23)=23	(28531167061)=15797*1806113	74002499
12	13	(27)=3^3	(3452271214393)=1093*3158528101	10834705
16	17	(35)=5*7	(505447028499293771)=505447028499293771	$A0$
18	19	(39)=3*13	(61159090448414546291)=61159090448414546291	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

$A0 = 232251544198878080950520379327369\,7$

$A = 3400394858615773989868469649922697554\,9$

$B = (8954302432552373722465\,3) = 829*28878847*3740221981231$

$C = 72890483685103052142902785385012452539679026\,13$

$D = (15863092971714915744144367048\,9) = 523*303309617049998388989$

$E = 22876156239024650606645326473334848325625895160495412605609$

$F = (19194342495775048050414684129181) = 50159*2428541*$
157571957584602258799

$G = 33492980349555990953189422489630490716271536793263604160376$

$H = (3400394858615773989924068823057619869\,7) = 2591*$
$36855109*136151713*2615418118891695851$

$I = 1051153199500053598403188407217590190704579879232264635077522$

$J = (4978518112499354698647829163838661251242\,41)$
$= 83*1231*27061*509221*14092193*29866451*840139875599$

$K = 2253240236044012487937308538033349567966729399888614822055\,29$

$L = (602400691612421918536387328824478011400331\,73)$

9.2. **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になるのである.

9.3. $P = 13$. $N_p = \frac{P^p - 1}{\overline{P}}$

Table 12. $P = 13$

p	$(2p+1)=$	$(N_p)=$ 分解	
2	(5)=5	(14)=2*7	
3	(7)=7	(183)=3*61	
5	(11)=11	(30941)=30941	
7	(15)=3*5	(5229043)=5229043	
11	(23)=23	(149346699503)=23*419*859*18041	20588
13	(27)=3^3	(25239592216021)=53*264031*1803647	5880341
17	(35)=5*7	(720867993281778161)=103*443*15798461357509	
19	(39)=3*13	(121826690864620509223)=12865927*9468940004449	

$A = 479677535758244089774221240729252401$

$B = 1370007009879120944961590855379558132876 7$

9.4. **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.

TABLE 13. $P = 17$

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

9.5. $P = 17$ の弱完全数.

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

9.7. $P = 19$ の弱完全数.

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

9.9. $P = 23$ の弱完全数.

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

弱弱完全数

10. 条件を弱める

条件をさらに弱めて, $\varepsilon+1$ を奇数($\varepsilon+1=2$ はあえて付加する)だけにしても次からわかるように 末尾 1 桁が 6 または 8, はやはり成立している.

$\varepsilon+1$ を奇数とだけ仮定している場合, 弱々しいが完全な数,(弱々完全数; ww-perfect number) と呼んでみたい.

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.

Table 14. $P = 2$

$2\varepsilon - 1$	$Q = 2^{2\varepsilon-1} - 1$	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
[illegible]	[illegible]	[illegible]	[illegible]

Table 15. $P = 2$

$2\varepsilon - 1$	$Q = 2^{2\varepsilon-1} - 1$	素因数分解	Q の下 2 桁	a	a の下
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

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.

10.1. **周期性の証明.** 以下ではこの周期性の結果を証明する.

$Q = 2^{2\varepsilon-1} - 1$ となる Q を $Q_{2\varepsilon-1}$ と書き, 弱弱完全数 a を $a_{2\varepsilon-1}$ と書くことにする.

$Q_3 = 2^3 - 1 = 7, Q_{23} = 2^{23} - 1$ なので $Q_{23} - Q_3 = 2^{23} - 2^3 = 2^3(2^{20} - 1)$. この数が 100 の倍数であることを確認しよう.

$2^{10} = 1024 \equiv 24 \mod 100$ を利用すると $2^{20} \equiv 24^2 = 576 \equiv 76$ により $2^{20} - 1 \equiv 75$.

4 倍すると

$$4(2^{20} - 1) \equiv 300 \equiv 0 \mod 100$$

$$Q_{23} - Q_3 = 2^3(2^{20} - 1) \equiv 0 \mod 100$$

$20+3=23$ を一般にして $20m+3$ を考えると $Q_{20m+3}-Q_3 \equiv 0$. これに 2^{2L} を掛けると

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

$L = 1,2,3,4$ に応じて $Q_{3+2L} = Q_5 = 2^5 - 1 = 31, Q_7 = 2^7 - 1 = 32 \times 4 - 1 \equiv 17$, と計算した結果,

27,11,47,67,71,87,37,7.

これから 周期が10 もわかった.

$\xi = 20m + 3 + 2L$ とおくとき

$$Q_\xi \equiv Q_{3+2L} \mod 100.$$

$a_\xi = 2^{\xi-1} Q_\xi$ が成り立つ.

$$a_\xi \equiv a_{3+2L} = 2^{2+2L} Q_{3+2L} \mod 100.$$

が成り立つことを以下で示す.

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

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

Table 16. $P = 2$

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

10.2. $P = 2$**; 弱弱完全数の** p, Q, a **変化.** 周期 は $(21-1)/2 = 10$.

11. P を底とする弱弱完全数

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

Table 17. $P = 3$

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

11.1. $P = 3$ 弱弱完全数の表.

$$A = (423644304721) = 11^2 * 8951 * 391151$$
$$B = 119649664615167550026801$$
$$C = (3812798742493) = 13 * 109 * 433 * 757 * 8209$$
$$D = 9691622833838739015484197$$
$$E = (34315188682441) = 59 * 28537 * 20381027$$
$$F = 78502144954102936742403980 1$$
$$G = 308836698141973 = 683 * 102673 * 4404047$$
$$H = 6358673741282420232587560247 7$$
$$I = 2779530283277761 = 13 * 23 * 3851 * 2413941289$$
$$J = 515052573043876780047667920800 1$$
$$K = 25015772549499853 = 11^2 * 71 * 1093 * 2664097031$$
$$L = 417192584165540258547337814514357$$
$$M = 225141952945498681 = 13097927 * 17189128703$$
$$N = 33792599317408761542712904163659401$$
$$O = 2026277576509488133 = 13^2 * 313 * 6553 * 7333 * 797161$$
$$P = 2737200544710109690363152107948379837$$

弱弱完全数の Q 下2桁 と a 下2桁 を書き出した.

TABLE 18. $P = 3$

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

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

12. $P = 3$; 弱弱完全数の p, Q, a 変化

TABLE 19. $P = 3$

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

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

Table 20. $P = 5$

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

12.1. $P = 5$ の弱弱完全数の p, Q, a 変化. 周期 は 2

Table 21. $P = 7$

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

12.2. $P = 7$; 弱弱完全数の p, Q, a 変化.

Table 22. $P = 11$

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

12.3. $P = 11$：弱弱完全数の p, Q, a 変化.

Table 23. $P = 11$ 続き

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

$A = 11^10 = 25937424601$, $B = 4601^5 = 2061869461571623001$.
これより

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

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

Table 24. $P = 11$

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

12.4. $P = 11$ 弱弱完全数の表.

$$U = 5054470282849348 9$$

Table 25. $P = 13$

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

12.5. $P = 13$; 弱弱完全数の p, Q, a 変化. 周期は $(23-3)/2 = 10$

R

TABLE 26. $P = 13$

$2e+1$	$Q = (13^{2e+1}-1)/12$	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

$$A = 3^2 * 61 * 1609669$$
$$B = 720867993213800601$$
$$C = 23 * 419 * 859 * 18041$$
$$D = 2058871075610937785 1047$$
$$E = 53 * 264031 * 1803647$$
$$F = 5880341679055661139954 68101$$
$$G = 3 * 61 * 4651 * 30941 * 161971$$
$$H = 16794843869550928905093964222707$$
$$I = 103 * 443 * 15798461357509$$
$$J = 4796775357582440897742212407292524 01$$
$$K = 12865927 * 9468940004449$$
$$L = 13700070098791209449615908553795581328767$$
$$M = 3 * 43 * 61 * 337 * 547 * 2714377 * 5229043$$
$$N = 391287702091575733090746033697803929523057501$$
$$O = 1381 * 25195453423493311831 43$$
$$P = 1117556805943749451280484243418726939907951748922 7$$

$$
\begin{aligned}
W &= 311 * 1117 * 81705090114313634085681503690 \\
X &= 743640860380674682637914430373107304158218976275173378977087 \\
Y &= 3 * 23 * 61 * 419 * 859 * 18041 * 17551032119981679046729 \\
Z &= 2123912661333244961082147404588631833395386146897220450300307
\end{aligned}
$$

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