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

$\sigma(a) - 2a = 0$ を満たす自然数を完全数という.

$\sigma(2^e)$ 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)

目標 究極の完全数の探究

- 完全数の平行移動
- 底が3以上の素数について完全数を定義しまたその平行移動も研究する.
- 概完全数の一般化
- 亜完全数
- 疑似完全数
- φ 完全数を導入しその平行移動,底の一般化を研究する.

パラメータ m に対して $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ**平行移動した完全数**という.

平行移動した完全数 は方程式 $\sigma(a) = 2a - m$ を満たす.
逆に方程式 $\sigma(a) = 2a - m$ を満たす解を求める.

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 $q > P$.

これより $q = \mathrm{Maxp}(a)$ を用いて

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

m 平行移動した究極の完全数の基本方程式という.
$\overline{P} = P - 1$.

逆にこの方程式を解くという問題を建てる.

0.1. **素数べきの約数の和.** $\sigma(2^e) = 2^{e+1} - 1$ が素数になるとき, $e+1$ も素数である. ここでは $e+1$ が素数になる場合に限って ,$\sigma(2^e)$ の素因数分解をしている.

$\sigma(2^e)$ が素数になる場合は 7,31,127,8191, 131071,524287,$\cdots$ となって意外に多い.

これらを (2を底とする) **メルセンヌ素数**という. ($e+1$ は素数と限定した効果である)

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

$2^e = a$	$\sigma(a)$	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	$[2147483647]$

$\sigma(2^e)$ が素数のとき $2^e\sigma(2^e)$ は完全数になる. 例えば

$$2 * 3 = 6, 4 * 7 = 28, 16 * 31 = 496, 64 * 127 = 8128, \cdots$$

となり, これらは古代人が発見した4つの完全数である.

実際, $a = 2^e$ に対して $\sigma(a)$ が素数 q のとき $\alpha = aq$ とおき $q = \sigma(2^e) = 2^{e+1} - 1$ より $q + 1 = 2^{e+1} = 2a$ なので

$$\sigma(\alpha) = \sigma(a)\sigma(q) = q(q+1) = 2aq = 2\alpha.$$

したがって α は完全数になる.

0.2. **平方剰余の意味.** a(p で割れないとする) は p を法とするとき平方数 x^2 と合同とする. (a は 平方数を p で割った余り, と見る)

(2) $$a \equiv x^2 \bmod p$$

a は p を法とするとき平方剰余という.
このように書けないとき平方非剰余という.

5 を法とするとき, 1,4 は平方剰余. 2,3 は平方非剰余.

7 を法とするとき, 1,2,4 は平方剰余. 3,5,6 は平方非剰余.

a は p を法とするとき平方剰余なら $\left(\frac{a}{p}\right) = 1$ と書き,

平方非剰余なら $\left(\frac{a}{p}\right) = -1$ と書く. (ルジャンドルの平方剰余記号)

a, b がp で割れないとき

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$a \equiv a' \mod p$ なら

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$$

(3) $$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right).$$

これをオイラーの基準という.

相異なる奇素数 p, q に対して

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

平方剰余の相互法則という.
これによって計算できる.

0.3. フェルマーとオイラーの結果.

補題 1. q が素数のとき 2^q-1 の素因数 p については $p-1=2Lq$ と書ける.

さらに $p \equiv \pm 1 \bmod 8$.

Proof.

条件より,

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

q は素数なので 2 の $\bmod p$ での位数は素数 q.

フェルマーの小定理: $2^{p-1} \equiv 1 \mod p$. よって, $p-1=kq$ と書ける.

$p-1$ は偶数なので k も偶数. よって $k=2L$ と表せる. $p-1=2Lq$ により

$$2^{\frac{p-1}{2}} \equiv 2^{Lq} \equiv 1 \bmod p.$$

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

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

ゆえに $p \equiv \pm 1 \bmod 8$.

例

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

$$23 - 1 = 22 = 2 * 11 = 2q, 89 - 1 = 88 = 4 * 11 = 4q.$$

$q = 23$

$2^{22} = 4194304$, 8388607 , $[47, 178481]$

0.4. オイラーとラグランジュの結果.

補題 2. $p > 3$ 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.

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

このとき $q = 2p + 1$ を法として 2 が平方剰余なら M_p の素因子になる.

実例
より詳しい例

Table 2

$(\frac{2}{q})$	p	$q=2p+1$	$M_p=2^p-1$ の素因数分解
$(+)$	3	7	7
$(+)$	11	23	$23*89$
$(+)$	23	47	$47*178481$
$(+)$	83	167	$167*57912614113275649087721$
$(+)$	131	263	$263*1035079443105516238671861923746823456 9$
$(-)$	5	11	31
$(-)$	29	59	$233*1103*2089$
$(-)$	41	83	$13367*164511353$
$(-)$	53	107	$6361*69431*20394401$
$(-)$	89	179	$6.1897E+26$
$(-)$	113	227	$3391*23279*65993*1868569*1066818132868207$

1. 完全数の数表

TABLE 3. 完全数の場合

$e \bmod 4$	e	$e+1$	$2^e * q$	a	$a \bmod 10$
1	1	2	$2 * 3$	6	6
2	2	3	$2^2 * 7$	28	8
0	4	5	$2^4 * 31$	496	6
2	6	7	$2^6 * 127$	8128	8
0	12	13	$2^{12} * 8191$	33550336 (1456)	6
0	16	17	$2^{16} * 131071$	8589869056 (Cataldi,1588)	6
2	18	19	$2^{18} * 524287$	137438691328 (Cataldi,1588)	8
2	30	31	A	B (Euler, 1772)	8
0	60	61	C	D (Pervushin, 1883)	6
0	88	89	E	F (Powers, 1911)	6
0	106	107	G	H (Powers, 1914)	8
2	126	127	I	J (Lucas, 1876)	8
0	520	521	K	$--$ (Robinson, 1952)	6
2	606	607	L	$--$ (Robinson, 1952)	8
2	1278	1279	M	$--$ (Robinson, 1952)	8

$A = 2^{30} * 2147483647$
$B = 23058430081399521 28$
$C = 2^{60} * 2305843009213693951$
$D = 265845599156983174465469261595384217 6$
$E = 2^{88} * 6189700196426901374495621 11$
$F = 191561942608236107294793378084303638130997321548169216$
$G = 2^{106} * 162259276829213363391578010288127$
$H = 131640364585696483372397534604587229102234723183869431177837281 28$
$I = 2^{126} * 170141183460469231731687303715884105727$
$J = 144740111546645244279463731260859884815736774914748358890663534349131199152128.$
$K = 2^{520} * 6864797660130609714981900799081393217269435300143$
$- - 305409394463459185543183397656052122559640661454554977296$
$- - 311391480858037121987999716643812574028291115057151.$
$L = 2^{606} * 5311379928167670986895882065524686273295931$
$- - 177270319231994441382004035598608522427391625$
$- - 022652292856688932948624650101534657933765 27$
$- - 072394095199787665873519438312708353932190317$

$- - 28127.$
$M = 2^{1278} * 1040793219466439908192524032736408553861 52$
$- - 622472667048053191123504036080596733602980$
$- - 122394417323241848424216139542810077913 83$
$- - 566248323464908139906605677320762924129509$
$- - 389220345773183349661583550472959420547689 8$
$- - 112116936771475484788669625013844382602917 32$

2. m だけ並行移動した場合の数表

2.1. $m = 2$. 2 だけ並行移動した場合を見てみよう. $q = 2^{e+1} + 1$ が素数の場合になる.

TABLE 4. $q = 2^{e+1} + 1$ が素数

e	$e+1$	$e \bmod 4$	$2^e * q$	a
0	1	0	3	3
1	2	1	$2 * 5$	10
3	4	3	$2^3 * 17$	136
7	8	3	$2^7 * 257$	32896
15	16	3	$2^{15} * 65537$	2147516416

3,5,17,257,65537 らは5個のフェルマー素数である.

2だけ平行移動した 3,10,136,32896,2147516416 をフェルマーの完全数と呼んでやりたい.

2.2. **オイラーの結果.** $2^{e+1}+1$ が素数になるとき, $e+1=2^m$ と書ける.

一般に $F_m=2^{2^m}+1$ とおきこれをフェルマー数,素数のときフェルマー素数という.

$m=0,1,2,3,4$ のとき F_m はフェルマー素数になる.

フェルマーの期待に反して, $m\geq 5$ のときフェルマー素数は発見されていない.

オイラーは,次の結果を証明しこれを用いて F_5 の素因数 641 を発見した.

補題 **3.** F_m の素因数 Q は $1+2^{m+1}K$ と書ける.

Proof

$2^{2^m}+1 \equiv 0 \mod Q$ なので$2^{2^m} \equiv -1 \mod Q$.

$\mathrm{mod}Q$ での 2の位数 u は 2^{m+1} の約数である.

$u=2^s$ とおくと $s \leq 2^{m+1}$ だが $2^{2^m} \equiv -1$ により $s=2^{m+1}$.

$2^{Q-1} \equiv 1 \mod Q$ によれば $Q-1$ は2^{m+1} の倍数なので $Q=1+2^{m+1}k$.

$m=5$ なら $Q=1+64k$. $k=10$ のとき $Q=641$.

$F_5=641*6700417$ が素因数分解. $6700417-1=6700416=2^7*3*17449$.

3. 3のべきとそのユークリッド関数の値

3のべき 3^e について $e+1$ が素数の場合 $\sigma(a)$ の素因数分解を行う.

TABLE 5. $3^e = a$

$3^e = a$	$\sigma(a)$	の素因数分解
$3^2 = 9$	13	$[13]$
$3^4 = 81$	121	$[11^2]$
$3^6 = 729$	1093	$[1093]$
$3^{10} = 59049$	88573	$[23, 3851]$
$3^{12} = 531441$	797161	$[797161]$
$3^{16} = 43046721$	64570081	$[1871, 34511]$
$3^{18} = 387420489$	581130733	$[1597, 363889]$
$3^{22} = 31381059609$	47071589413	$[47, 1001523179]$
$3^{28} = 22876792454961$	34315188682441	$[59, 28537, 20381027]$
$3^{30} = 2058911320946 49$	3088366981419 73	$[683, 102673, 4404047]$

$\sigma(3^e)$ が素数になるのは 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.

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

補題 4. q が素数のとき $\frac{3^q-1}{2}$ の奇数素因数 p については $p-1=2Lq$ と書ける.

さらに $p \equiv \pm 1 \bmod 12$ を満たす.

Proof.

条件より,

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

q は素数なので 3 の $\mathrm{mod}p$ での位数は q.

フェルマーの小定理によると $3^{p-1} \equiv 1 \mod p$.

よって, $p-1 = kq$ と書ける. $p-1$ は偶数なので k も偶数. $k = 2L$ と表せるから $p-1 = 2Lq$.

$$3^{\frac{p-1}{2}} \equiv 3^{Lq} \equiv 1 \bmod p.$$

オイラーの基準によって

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

$3^{\frac{p-1}{2}} \equiv 1$ なので $\left(\frac{3}{p}\right) = 1$.

平方剰余の法則から $p \equiv \pm 1 \bmod 12$.

例$q = 17$ 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 $[2, 5, 7, 17, 29]$.

3.2. **オイラーとラグランジュの結果.** オイラーとラグランジュの結果は底が3でも成り立つ. しかも具体例で計算すると, 底が2のときより結果が断然良い. これは驚くべき結果であった.

補題 5. p を素数とし, $q = 2p + 1$ も素数とする.
$N_p = 3^p - 1$ とおくとき, q を法として 3 が平方剰余とする.
このとき q は N_p の素因子である.

Proof.

仮定から$3 \equiv n^2 \mod q$ を満たす整数 n がある. フェルマーの小定理を用いて

$$3^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \mod q$$

ゆえに $N_p = 3^p - 1 = qk$ と書けるので, q はN_p の素因子.

注意

q を法として3 が平方剰余とするとき (平方剰余の相互法則から)

$q \equiv \pm 1 \mod 12$.

この逆も成立する.

補題 6. p を素数とし, $q = 2p + 1$ が 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 $q_0 \neq 3$.

$$3^p = N_p + 1 \equiv 1 \mod q_0.$$

p は素数なので q_0 を法とした3の位数である. フェルマーの小定理を用いて

$$3^{q_0-1} \equiv 1 \mod q_0.$$

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

TABLE 6. p : Germain 素数

p	$q=2p+1$	$q+1$	$(q+1)/12$	$q-1$	N_p 素因数分解
5	11	12	1	10	$2*11^2$
11	23	24	2	22	$2*23*3851$
23	47	48	4	46	$2*47*1001523179$
29	59	60	5	58	$2*59*28537*20381027$
41	83	84	7	82	$2*83*2526913*86950696619$
53	107	108	9	106	$2*107*24169*3747607031112307667$
83	167	168	14	166	A
89	179	180	15	178	B

$$A = 2*167*12119*1036745531*95099605962721089794335 1$$

$$B = 2*179*1611479891519807*5042939439565996049162197$$

p : Sophie Germain 素数について, q はすべて $q+1=12L$ を満たし結果としてすべて q は N_p の因子となっていた. これは感動の結果である.

フェルマー数には平方因子が無い.

という予想がある. 底が3のとき

$p=5$ の場合 $N_5=2*11^2$. これは反例.

3.3. **3を底とする完全数の公式.**

$q = \sigma(3^e) = \dfrac{3^{e+1}-1}{2}$ より $q+1 = \dfrac{3^{e+1}+1}{2}$ なので

$$\begin{aligned} 2\sigma(a) &= 2\sigma(3^e)\sigma(q) \\ &= (3^{e+1}-1)(q+1) \\ &= q(3^{e+1}+1) \\ &= 3a+q \end{aligned}$$

ここから q を消すことができないので a の最大素因子 $\mathrm{Maxp}(a)$ と書くことにすると次の公式の形にまとめられた.

$$2\sigma(a) = 3a + \mathrm{Maxp}(a).$$

次の問題はこの公式を満たす a は $\sigma(3^e)$ が素数 q になるのを用いて $a = 3^e q$ と書くことができるか, である.

この問題を**3を底とする完全数の基本問題**と呼ぶ. これは難しそうな問題だが逆に反例をつくりやすいかもしれない.

3.4. $s(a) = 1$ **のときの証明.** 3を底とする完全数の基本問題を $s(a) = 1$ の場合だけ扱う.

$a = q^f$ が $2\sigma(a) = 3a + \mathrm{Maxp}(a)$ を満たすと仮定する.

$Y = q^f$ とおくと

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

これより

$$Y(2q - 3\overline{q}) = 2 + q\overline{q}.$$

$2q - 3\overline{q} > 0$ により, $q = 2$.

$Y(2q - 3\overline{q}) = 2 + q\overline{q}$ に $q = 2$ を代入すると $Y = 4$. よって $a = 4$.

このような解を**微小解**という.

3.5. $s(a) = 2$ のときの証明. $2\sigma(a) = 3a + \mathrm{Maxp}(a)$ を満たすと仮定する.

$s(a) = 2$ の場合だけ扱う.

結果的には$q = \sigma(3^e) = \dfrac{3^{e+1} - 1}{2}$ を満たす素数により$a = 3^e q$ と書けることになる.

ここで a は奇数である. なぜなら$\mathrm{Maxp}(a)$ は奇数で,$2\sigma(a)$ は偶数だから.

a を素因数分解し $a = p^e q^f (2 < p < q)$ とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる.すると $\overline{p} = p - 1, \overline{q} = q - 1$ を使うと

$$\sigma(a) = \frac{(pX - 1)(qY - 1)}{\overline{pq}}$$

であり,$A = pX - 1, B = qY - 1, \rho' = \overline{pq}$ とおけば

$\mathrm{Maxp}(a) = q$ なので

$$\frac{2AB}{\rho'} = 3XY + q.$$

書き直して

$$2AB = 3\rho' XY + q\rho'.$$

$2AB - 3\rho' XY$ の XY の係数を R とおけば

$$R = 2pq - 3\rho' = 6 - (p-3)(q-3).$$

$q\rho' = RXY - (pX + qY - 1)$ によって $R > 0$.

$0 < R = 6 - (p-3)(q-3)$ により,a は奇数になるので $p = 3, R = 6$. $\rho' = 2\overline{q}$.

$$2\overline{q}q = RXY - 2(3X + qY - 1)$$

を2で割って

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

$3X > q$ かつ $Y \geq q$ によって

$$\overline{q}q \geq (3X - q)q - 3X + 1 = 3X\overline{q} - \widetilde{q}\overline{q}.$$

$\overline{q}q \geq 3X\overline{q} - \widetilde{q}\overline{q}$ から $\overline{q}$ を消すと

$$q \geq 3X - \widetilde{q} = 3X - q - 1.$$

よって

$$2q+1 \geq 3X.$$

ここで $Y = q$ を仮定すると $2q+1 = 3X$ が成り立ち $q = \frac{3^{e+1}-1}{2} = \sigma(3^e)$ は素数. $a = 3^e q$ は3 を底とした完全数になる.

$Y > q$ のとき $Y \geq q^2$ になる.

$$\begin{aligned}
\overline{q}q &= (3X-q)Y - 3X + 1 \\
&= (3X-q)Y - 3X + q + 1 - q \\
&= (3X-q)(Y-1) + 1 - q \\
&\geq (3X-q)(q^2-1) + 1 - q \\
&\geq (3X-q)\overline{q}\widetilde{q} - \overline{q}.
\end{aligned}$$

よって

$$q \geq (3X - q)\widetilde{q} - 1 > 3X - q - 1.$$

1 を移項すると $\widetilde{q} \geq (3X - q)\widetilde{q}$ になるので $\widetilde{q}$ で割ると

$$1 \geq (3X - q) > 0.$$

ゆえに $3X - q = 1$. しかし $q = 3X - 1 = 3^{e+1} - 1 = 2\sigma(3^e)$ の右端は素数ではない. これは矛盾.

4. 3を底とする完全数の平行移動

定義によれば$\sigma(3^e) = \frac{3^{e+1}-1}{2}$ が素数 q のとき $a = 3^e q$ が3を底とする完全数である. これを m だけ 平行移動することを考える.

$q = \frac{3^{e+1}-1}{2} + m$ が素数 q のとき$a = 3^e q$ をm だけ **平行移動した3を底とする完全数**という.

4.1. $p = 3.m = 1$. $p = 3.m = 1$ のとき $q = \frac{3^{e+1}+1}{2}$ は素数になる場合を調べる.

TABLE 7. $m = 1$

$e \bmod 4$	e	素因数分解	$q \bmod 10$	a	$a \bmod 10$
1	1	$3 * 5$	5	15	7
3	3	$3^3 * 41$	1	1107	7
3	15	$3^{15} * 21523361$	1	308836705316427	7
3	31	$3^{31} * 926510094425921$	1	X	7
3	63	A	1	B	7

$X = 57228063671541905627967299018 7$

$A = 3^{63} * 1716841910146256242328924544641$

$B = 19650307629564305285868121435693253915830840174600831596977 07$

q の末尾の数は 1, a の末尾の数は 7.

4.2. **オイラーの結果.** $3^{e+1}+1=2N_{e+1}$ とおくとき N_{e+1} が素数になるとき, $e+1=2^m$ と書ける.

一般に $G_m=(3^{2^m}+1)/2$ とおき

これを底が3のフェルマー数;

素数のときフェルマー素数という.

オイラーの結果と類似した結果が成り立つ.

補題 **7.** G_m の素因数 Q は $1+2^{m+1}K$ と書ける.

$3^{2^m}+1 \equiv 0 \mod Q$ なので $3^{2^m} \equiv -1 \mod Q$.
$\mathrm{mod} Q$ での 3の位数 u は 2^{m+1} の約数である.

$u=2^s$ とおくと $s \leq 2^{m+1}$ だが $3^{2^m} \equiv -1$ により $s=2^{m+1}$.
$3^{Q-1} \equiv 1 \mod Q$ によれば $Q-1$ は 2^{m+1} の倍数なので $Q=1+2^{m+1}k$.

$G_m=(3^{2^m}+1)/2;\ m=1,2,3,4,5,6$
$m=7$ のとき $2^m=128$. よって $Q=1+256K$.

TABLE 8. $P = 3$

m	2^m	$2G_m$	素因数分解
1	2	10	$2 * 5$
2	4	82	$2 * 41$
3	8	6562	$2 * 17 * 193$
4	16	43046722	$2 * 21523361$
5	32	1853020188851842	$2 * 926510094425921$
6	64	3433683820292512484657849089282	$2 * 1716841910146256242328924544641$
7	128	−	A

$$A = 3^{128}+1 = 2*257*275201*1384246188687 37*391378628151452 4929*153849834853910661121$$

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

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

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

```
 ?- A is 39137862815145249 29-1,factorize(A,B), exps(B,C).
A = 3913786281514524928,
C = [2^8, 31, 787, 3919, 159898891].

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

これらは数値例とはいえ,実に見事な美しい結果である.

5. m だけ平行移動した完全数の公式

$q = \frac{3^{e+1}-1}{2} + m$ が素数 q のとき $a = 3^e q$ とおく. これが満たす形式を決定しよう.

$q + 1 = \frac{3^{e+1}+1}{2} + m$ に注意して,

$$\sigma(a) = \sigma(3^e q) = (3^{e+1} - 1)/2 * (q + 1)$$

によって

$$\begin{aligned} 2\sigma(a) &= (3^{e+1}-1)(q+1) \\ &= 2(q-m)(q+1) \\ &= q(3^{e+1}+1+2m) - 2mq - 2m \\ &= 3a + q - 2m \end{aligned}$$

かくして $q = \mathrm{Maxp}(a)$ を使うと方程式

$$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2m$$

がえられた.

この方程式を満たす解を探す. 一種の逆問題を考えることになる.

6. 方程式を満たす解

6.1. $m = 0$ のとき. $m = 0$ のとき $2\sigma(a) = 3a + \mathrm{Maxp}(a)$.

TABLE 9. $[p = 3, m = 0]$

a	素因数分解	$\sigma(a)$
4	$[2^2]$	7
117	$[3^2, 13]$	182
796797	$[3^6, 1093]$	$--$

117 は最も小さい 3 を底とする完全数であるがさらに小さい解 4 が出てきた.

6.2. $m = 1$ のとき．$m = 1$ のとき $2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2$.

3 を底とするフェルマーの完全数(拡張版)

TABLE 10. $[p = 3, m = 1]$

a	素因数分解	$\sigma(a)$
2	$[2]$	3
15	$[3, 5]$	24
741	$[3, 13, 19]$	1120
1107	$[3^3, 41]$	1680
14883	$[3, 11^2, 41]$	22344
38781	$[3^2, 31, 139]$	58240

6.3. $m = -2$ のとき. $2\sigma(a) = 3a + \mathrm{Maxp}(a) + 4$

TABLE 11. $[p = 3, m = -2]$

a	素因数分解	$\sigma(a)$
8	$[2^3]$	15
99	$[3^2, 11]$	156
759	$[3, 11, 23]$	1152

6.4. $m = 2$ のとき. $m = 2$ のとき

$$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 4.$$

$a = 3^f$ はこの式を満たす.

実際に $2\sigma(a) = 3 * 3^f - 1, 3a + \mathrm{Maxp}(a) - 4 = 3 * 3^f + 3 - 4.$

TABLE 12. $[p = 3, m = 2]$

a	素因数分解	$\sigma(a)$
3	$[3]$	4
9	$[3^2]$	13
27	$[3^3]$	40
81	$[3^4]$	121
243	$[3^5]$	364
729	$[3^6]$	1093
2187	$[3^7]$	3280
6561	$[3^8]$	9841
19683	$[3^9]$	29524
59049	$[3^{10}]$	88573
99807	$[3, 17, 19, 103]$	149760
177147	$[3^{11}]$	265720

$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 4$ のエイリアン解として99807([3, 17, 19, 103]) が出た.

実は $m = 2$ を選ぶのは違反行為である.

本来は $q = \frac{3^{e+1}-1}{2} + m$ が素数になるはずなので $m = 2$ は出てこない.

しかし,公式が$2\sigma(a) = 3a + \mathrm{Maxp}(a)$ が得られたら $m = 2$ も代入してパソコンで結果を出してもらうと,非常に面白い例が出てきた.

$m = -1$ も違反であり,解がないようなのだが $s(a) = 4$ の例を出してきた. 私は困惑させられた.このような異常な例をとりこむ理論ができそうにないからである.

TABLE 13. $[p = 3, m = -1]$

a	素因数分解	$\sigma(a)$
27755	$[5, 7, 13, 61]$	41664

6.5. $m = -1$ のとき.

7. 解 $3^e qr$ のとき

解 a の素因数分解で$3^e qr$ となる解を探す.

$a = 3^e qr (3 < q < r : \text{素数})$とおくと $\mathrm{Maxp}(a) = r$ になるので$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2m$ に代入して

$$(3^{e+1} - 1)(q + 1)(r + 1) = 3^{e+1} qr + r - 2m.$$

$\Gamma = 3^{e+1} - 1, \Delta = q + r$ とすると

$$\Gamma(qr + \Delta + 1) = (\Gamma + 1)qr + r - 2m.$$

よって

$$\Gamma(\Delta + 1) = qr + r - 2m.$$
$$qr = \Gamma(\Delta + 1) - r + 2m.$$

$q' = q + 1, \Delta' = q' + r = \Delta + 1$ とすると

$$q'r = \Gamma\Delta' + 2m.$$

よって $q_0 = q' - \Gamma, r_0 = q - \Gamma$ は次式を満たす.

$$q_0 r_0 = \Gamma^2 + 2m.$$

そこで,与えられた e に対して, $\Gamma = 3^{e+1} - 1, U = \Gamma^2 + 2m$ を求め2因数分解: $q_0 r_0 = U, q_0 < r_0$ を行い, $q = q_0 + \Gamma - 1, r = r_0 + \Gamma$ がともに素数になるもの探すと次の結果をえた.

$e = 1, 2, 11$ について解が発見された.

TABLE 14. $[p = 3, m = 1; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
741	$a = 3 * 13 * 19$	1120
38781	$a = 3^2 * 31 * 139$	58240
A	$a = 3^{11} * 536917 * 52088299$	B

$A = 49542866651558159 01$

$B = 743142999775976 8000$

TABLE 15. $[p = 3, m = -2; a = 3^e qr]$

a	素因数分解	$\sigma(a)$
759	$3^1 * 11 * 23$	1152
19184931	$3^4 * 433 * 547$	28777672
8061750261	$3^5 * 739 * 44893$	12092647840
721889577	$3^5 * 947 * 3137$	1082835936
629690031	$3^5 * 1019 * 2543$	944536320
998897581791	$3^7 * 7331 * 62303$	1498346403840
156372861294706304709	$3^{12} * 1608337 * 182948677$	234559291942150931404
247361549705402839 11	$3^{12} * 1692433 * 27502087$	371042324558241769 12
436123392252707027348851 59	$3^{13} * 4782971 * 5719200505223$	654185088379089137025803 5

7.1. $[p = 3, m = -2; a = 3^e qr]$.

8. $s(a)=2$ のときの証明

$$2\sigma(a)=3a+\mathrm{Maxp}(a)-2m$$

を満たすと仮定する.

$s(a)=2, q\geq 2m>0$ の場合だけ扱う.

ここで a は奇数である. なぜなら $\mathrm{Maxp}(a)$ は奇数で,$2\sigma(a)$ は偶数だから.

$q\geq 2m>0$ を仮定する.

a を素因数分解し $a=p^eq^f(2<p<q)$ とする.

$X=p^e, Y=q^f$ とおくと $a=XY$ となる.すると $\overline{p}=p-1, \overline{q}=q-1$ を使うと

$$\sigma(a)=\frac{(pX-1)(qY-1)}{\overline{pq}}$$

であり,$A=pX-1, B=qY-1, \rho'=\overline{pq}$ とおけば

$\mathrm{Maxp}(a) = q$ なので

$$\frac{2AB}{\rho'} = 3XY + q - 2m.$$

書き直して

$$2AB = 3\rho' XY + (q - 2m)\rho'.$$

$2AB - 3\rho' XY$ の XY の係数を R とおけば

$$R = 2pq - 3\rho' = 6 - (p-3)(q-3).$$

$(q - 2m)\rho' = RXY - 2(pX + qY - 1)$ によって $R > 0$.

$0 < R = 6 - (p-3)(q-3)$ により,a は奇数になるので $p = 3, R = 6$. $\rho' = 2\overline{q}$.

$$2\overline{q}(q - 2m) = 6XY - 2(3X + qY - 1)$$

を2で割って

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

$3X > q$ かつ $Y \geq q$ によって

$$\overline{q}(q-2m) \geq (3X-q)q - 3X + 1 = 3X\overline{q} - \widetilde{q}\overline{q}.$$

$\overline{q}(q-2m) \geq 3X\overline{q} - \widetilde{q}\overline{q}$ から $\overline{q}$ を消すと

$$q - 2m \geq 3X - \widetilde{q}.$$

よって

$$2q+1-2m \geq 3X.$$

ここで $Y=q$ を仮定すると $2q+1-2m=3X$ が成り立ち $q=\frac{3^{e+1}-1}{2}+m=\sigma(3^e)+m$ は素数. $a=3^e q$ は3 を底とした平行移動は m の完全数になる.

$Y>q$ のとき $Y \geq q^2$ になる.

$$\begin{aligned}
\overline{q}(q-2m) &= (3X-q)Y-3X+1 \\
&= (3X-q)Y-3X+q+1-q \\
&= (3X-q)(Y-1)+1-q \\
&\geq (3X-q)(q^2-1)+1-q \\
&\geq (3X-q)\overline{q}\widetilde{q}-\overline{q}.
\end{aligned}$$

$$1 - \frac{2m}{\widetilde{q}} \geq 3X - q.$$

$$0 \geq 3X - q.$$

$3X - q > 0$ に矛盾.

9. $2\sigma(a) - 3a$ の値

$2\sigma(a) - 3a = Maxp(a) - 2m$ が出てきたのでパソコンに $2\sigma(a) - 3a$ の値を調べて表をつくってもらった.

興味ある結果が見えたら証明してみよう. うまく行けば自分の定理が見つかるかもしれない.

TABLE 16. $2\sigma(a) - 3a$ の値

a	素因数分解	$\sigma(a)$	$\sigma(a) - 2a$	$2\sigma(a) - 3a$(亜完全度)
51	$[3, 17]$	72	-30	-9
35	$[5, 7]$	48	-22	-9
11	$[11]$	12	-10	-9
39	$[3, 13]$	56	-22	-5
7	$[7]$	8	-6	-5
33	$[3, 11]$	48	-18	-3
5	$[5]$	6	-4	-3

TABLE 17. $2\sigma(a)-3a$ の値

a	素因数分解	$\sigma(a)$	$\sigma(a)-2a$	$2\sigma(a)-3a$(亜完全度)
27	$[3^3]$	40	-14	-1(3のべき)
9	$[3^2]$	13	-5	-1
3	$[3]$	4	-2	-1
2	$[2]$	3	-1	0
21	$[3,7]$	32	-10	1
4	$[2^2]$	7	-1	2
15	$[3,5]$	24	-6	3
46	$[2,23]$	72	-20	6 ($a=2p$)
38	$[2,19]$	60	-16	6
34	$[2,17]$	54	-14	6
26	$[2,13]$	42	-10	6
22	$[2,11]$	36	-8	6
14	$[2,7]$	24	-4	6
10	$[2,5]$	18	-2	6

表によれば $2\sigma(a) = 3a$ を満たす a は2だけらしい.
やってみたら簡単に証明できた. そこで定理とした.

定理 1. $2\sigma(a) = 3a$ を満たすとき $a = 2$.

Proof.

$2\sigma(a) = 3a$ により a は偶数なので $a = 2^e L$ とおき L は奇数とする.

$$2\sigma(a) = 2(2^{e+1} - 1)\sigma(L) = 3 * 2^e L$$

これより $N = 2^{e+1} - 1$ とおき両辺を2倍する.

$$4N\sigma(L) = 3 * 2^{e+1} L = 3(N + 1)L$$

$L > 1$ なら $\sigma(L) > L$ なので

$$3(N + 1)L = 4N\sigma(L) > 4N(L + 1)$$

$3L > NL + 4N$, $N \geq 3$ なので矛盾.

よって $L = 1$. $a = 2^e$ になって $4N = 3(N + 1)$. ゆえに $N = 3, e = 1$. したがって $a = 2$.

3 点セットのうち 1 つは解けてしまった. これはうれしい.

10. $2\sigma(a) - 3a = 1$ の場合

パソコン君に数値例をだしてもらい次の表ができた.

Table 18. $2\sigma(a) - 3a = 1$

a	$\sigma(a)$	素因数分解
21	32	$[3, 7]$
2133	3200	$[3^3, 79]$
19521	29282	$[3^4, 241]$
176661	264992	$[3^5, 727]$

この解の素因数分解は $3^e * q$ の形になっているのでこのような解があるとしてそれを決めよう.

$a = 3^e * q, (q > 3 : \text{素数})$ として代入すると

$$2\sigma(a) = (3^{e+1} - 1)(q + 1) = 3a + 1 = 3^{e+1}q + 1.$$

これより

$$(3^{e+1} - 1)(q + 1) = (3^{e+1} - 1)q + 3^{e+1} - 1 = 3^{e+1}q + 1.$$

$3^{e+1}q$ が両辺から消えて

$$-q + 3^{e+1} - 1 = 1.$$

書き直して $q = 3^{e+1} - 2.$ そこで $3^{e+1} - 2$ が素数になるときそれを q とおき $a = 3^e * q$ と定義すると $2\sigma(a) - 3a = 1$ を満たす.

11. 亜完全数

$q = 3^{e+1} - 2$ が素数になるとき $a = 3^e * q$ を(3 を底とする)**亜完全数**とよぼう. 亜完全数は $2\sigma(a) - 3a = 1$ を満たす.

逆に $2\sigma(a) - 3a = 1$ を満たすときそれは亜完全数か, という問題を考える. これは難しい問題であろう.

12. 亜完全度

$W = 2\sigma(a) - 3a$ とおき W を 亜完全度とよぶ. 亜完全数の亜完全度は1である.

ここでは,亜完全度は偶数 $2m$ の場合を扱う.

$2\sigma(a) - 3a = 2m$ を満たすので a は偶数である. a の素因数分解で 2 の指数部分を e とし奇数 L により $a = 2^e L$ と表す.

$2\sigma(a) - 3a = 2(2^{e+1} - 1)\sigma(L) - 3 \cdot 2^e L$ により

$$(2^{e+1} - 1)\sigma(L) - 3 \cdot 2^{e-1} L = m. \tag{4}$$

移項して

$$(2^{e+1} - 1)\sigma(L) = 3 \cdot 2^{e-1} L + m.$$

12.1. **亜完全度が2,6の場合.** 亜完全度が4,6; $m \leq 3$ と仮定する.

$L = 1$ の場合.

$$2^{e+1} - 1 - 3 \cdot 2^{e-1} = 2^{e-1} - 1 = m \leq 3$$

により $2^{e-1} \leq 4$. したがって $e - 1 \leq 2$.

$e = 3$ なら $a = 8$. このとき $2\sigma(a) - 3a = 6$.
$e = 2$ なら $a = 4$. このとき $2\sigma(a) - 3a = 2$.

$L > 1$ の場合. $\sigma(L) \geq L + 1$ によって

$$3 \cdot 2^{e-1} L + m = (2^{e+1} - 1)\sigma(L) \geq (2^{e+1} - 1)(L + 1).$$

$3 \cdot 2^{e-1} L$ を右辺に移して

$$3 \geq m \geq (2^{e+1} - 1)(L+1) - 3 \cdot 2^{e-1} L = (2^{e-1} - 1)L + 2^{e+1} - 1.$$

$L \geq 3$ により

$$3 \geq (2^{e-1} - 1)L + 2^{e+1} - 1 \geq (2^{e-1} - 1)3 + 2^{e+1} - 1 = 2^{e-1} - 4.$$

かくして $7 \geq 2^{e-1}$. よって $e - 1 \leq 2$. かくて $e = 1, 2, 3$.

式 (4) に $e = 1$ を代入すると,

$$3\sigma(L) = 3 \cdot L + m \leq 3(L + 1).$$

ゆえに $\sigma(L) = L + 1$. L は素数pで $a = 2L = 2p$.

式 (4) に $e = 2$ を代入すると

$$7(L + 1) \leq 7\sigma(L) = 3 \cdot 2L + m = 6L + m \leq 6L + 3.$$

これは矛盾.

$e = 3$ を代入.

$$15\sigma(L) - 3 \cdot 4L = m \leq 3.$$

矛盾.

以上によって亜完全度 $W = 6$ なら $a = 2p, (p : \text{奇素数})$ または $a = 8$.

13. 5べき の場合

一般に P を素数とし $E > 0$ について $a = P^E$ とおくと $\sigma(a) = \sigma(P^E) = \frac{aP-1}{P}$ によって

$$\overline{P}\sigma(a) - Pa = -1.$$

これが $a = P^E$ に関しての方程式である.

$P = 5$ については $4\sigma(a) - 5a = -1$ となる. とりあえず,$a \leq 20000$ についてパソコンで計算して表を作る.

TABLE 19. $4\sigma(a) - 5a = -1$

a	$\sigma(a)$	素因数分解
5	6	$[5]$
25	31	$[5^2]$
77	96	$[7, 11]$
125	156	$[5^3]$
625	781	$[5^4]$
3125	3906	$[5^5]$
15625	19531	$[5^6]$

驚いたことに 5のべきでない数 $77 = 7 * 11$ が登場した. 懐かしの昭和歌謡曲を聞いていたら,そこにAKBが出てきたような衝撃である.

$s(a) = 1$ を期待していたところに $s(a) = 2$ の例が出てきたのだから驚かざるを得ない.

13.1. $s(a)=2$ **のときの証明.** 方程式 $4\sigma(a)-5a=-1$ の解を $s(a)=2$ のときに求めよう.

$[s(a)=1$ のときに求めるのは良い演習問題である.$]$

a を素因数分解し $a=p^eq^f(2<p<q)$ とする. $X=p^e, Y=q^f$ とおくと $a=XY$ となる.すると $\overline{p}=p-1, \overline{q}=q-1$ を使うと

$$\sigma(a)=\frac{(pX-1)(qY-1)}{\overline{pq}}$$

であり,$A=pX-1, B=qY-1, \rho'=\overline{pq}$ とおけば

$$\frac{4AB}{\rho'}=5XY-1.$$

書き直して

$$4AB=5\rho' XY-\rho'.$$

$4AB-5\rho' XY$ の XY の係数を R とおけば

$$R=4pq-5\rho'=20-(p-5)(q-5)$$

$-\rho' + 4(pX + qY - 1) = RXY$ によって $R > 0$. $0 < R = 20 - (p-5)(q-5)$ により 次の場合がある.

(1) $p = 5, R = 20$. $\rho' = 4\overline{q}$,

(2) $p = 3, R = 30 + 2q$. $\rho' = 2\overline{q}$,

(3) $p = 7, R = 30 - 2q; q = 11, 13$. $\rho' = 6\overline{q}$.

次の基本等式

$$RXY - 4(pX + qY - 1) = -\rho'$$

を各場合ごとに調べる.

1. $p = 5, R = 20$. $\rho' = 4\overline{q}$ の場合.

基本等式を 4 で割って

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

$(5X - q)Y - 5X = -\overline{q} - 1 = q$ により

$$(5X - q)(Y - 1) = 0.$$

よって $5X = 5^{f+1} = q$ となり矛盾.

2. $p = 3, R = 30 + 2q$. $\rho' = 2\overline{q}$.
$R_1 = R/2 = 5 + q$ とおくと

$$R_1XY - 2(3X + qY - 1) = -\overline{q}.$$

変形して

$$(R_1X - 2q)Y = 6X - q - 1.$$

$Y = q$ のとき,
$(R_1X - 2q)q = 6X - q - 1$ によって $X \geq 3$ により
$(R_1q-6)X = 2q^2-q-1 \geq 3(5+q)q-6q = 3q^2+15q-6q = 3q^2+9q.$
これから矛盾が出る.

$Y \geq q^2$ のとき,

$$(R_1X-2q)Y = 6X-q-1 \geq (R_1X-2q)q^2 = ((5+q)X-2q)q^2 = (5+q)Xq^2-$$

$$2q^3 - q - 1 \geq 3((5+q)q^2 - 6) = 3q^3 + 15q^2 - 18.$$

これから矛盾が出る.

3. $p = 7, R = 30 - 2q; q = 11, 13;\ \rho' = 6\overline{q}$.

$$R_1XY - 2(7X + qY - 1) = -3\overline{q}.$$

$q = 11$ のとき, $R_1 = 4$.

$$4XY - 2(7X + 11Y - 1) = -30.$$

$4XY - 2(7X + 11Y) = -32$ を変形して

$2(2X-11)Y = 14X-32 = 7(2X-11)-32 = 7(2X-11)+45.$

$(2X-11)(2Y-7) = 45$ の解として $2X-11 = 3, 2Y-7 = 15$ があり, $X = 7, Y = 11$. ここで $a = 77$. かくして 5のべきでない解が発見された.

$q = 13$ のとき, $R_1 = 2$.

$$XY - (7X + 13Y) = -25.$$

$(X - 7)(Y - 13) = 91 - 25 = 65.$

しかし, X, Y は奇数なので$X - 7$,$Y - 13$ はともに偶数で矛盾.

したがって $s(a) = 2$ のとき $a = 77$.

証明は適当に難しい. しかしながら $s(a) = 3$ の解がある可能性が残る.

14. $\sigma(5^e)$ が素数になる場合

TABLE 20. $5^e a$ の $\sigma(a)$

$5^e = a$	$\sigma(a)$	素因数分解
$5^2 = 25$	31	[31]
$5^4 = 625$	781	[11, 71]
$5^6 = 15625$	19531	[19531]
$5^{10} = 9765625$	12207031	[12207031]
$5^{12} = 244140625$	305175781	[305175781]
$5^{16} = 152587890625$	190734863281	[409, 466344409]
$5^{18} = 3814697265625$	4768371582031	[191, 6271, 3981071]
$5^{22} = 2384185791015625$	298023223876953 1	[8971, 332207361361]

$\sigma(5^e)$ が素数になるのは 31,19531, 12207031,305175781 であり少ない.

14.1. **フェルマーとオイラーの結果.** 5を底としたメルセンヌ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 8. q が素数のとき $\frac{5^q-1}{2}$ の奇数素因数 p については $p-1=2Lq$ と書ける.

さらに $p \equiv \pm 1 \bmod 5$.

Proof.

条件より,

$$5^q \equiv 1 \mod p.$$

q は素数なので 5 の $\mathrm{mod}p$ での位数は q.

フェルマーの小定理によると $5^{p-1} \equiv 1 \mod p$. よって, $p-1=kq$ と書ける. $p-1$ 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 $p-1=2Lq$ と書ける.

$$5^{\frac{p-1}{2}} \equiv 5^{Lq} \equiv 1 \bmod q.$$

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

$$5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right)$$

14.2. **オイラーとラグランジュの結果.** オイラーとラグランジュの結果は底が5でも成り立つ.

補題 9. p を素数とし, $q = 2p+1$ も素数とする. $L_p = 5^p - 1$ とおくとき, q を法として 5 が平方剰余とする. このとき q は L_p の素因子である.

Proof.

仮定から $5 \equiv n^2 \mod q$ を満たす整数 n がある. フェルマーの小定理を用いて

$$5^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \mod q$$

ゆえに $L_p = 5^p - 1 = qk$ と書けるので, q は L_p の素因子.

(平方剰余の相互法則から $q \equiv \pm 1 \mod 5$)

この逆も成立する.

補題 10. p を素数とし, $q = 2p + 1$ が $L_p = 5^p - 1$ 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 $q_0 \neq 5$.

$$5^p - 1 = N_p \equiv 0 \mod q_0.$$

p は素数なので q_0 を法とした5の位数である. フェルマーの小定理を用いて

$$5^{q_0-1} \equiv 1 \mod q_0.$$

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.

TABLE 21. q : 素数

p	$q=2p+1$	$q-1$	$q+1$	L_p 素因数分解
11	23	22	24	$2^2 * 12207031$
23	47	46	48	$2^2 * 8971 * 332207361361$
29	59	58	60	$2^2 * 59 * 35671 * 2212599644432962555250847358847 1$
41	83	82	84	A
53	107	106	108	$2^2 * 5960555749 * 17154094481 * 27145365052629449$
89	179	108	180	$2^2 * B$

$A = 2^2$*2238236249*5079304643216687969512641*17282755219881588879

$p = 29, q = 59 \equiv -1 \mod 5$ なので q を法として 5 は平方剰余.

$q = 59$ は L_p の素因子.

$B = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 *$ 231669654363683130095909

$p = 89, q = 179 \equiv +1 \mod 5$ なので q を法として 5 は平方剰余.

$q = 179$ は L_p の素因子.

15. 5を底とする完全数

$a = 5^e$ に対して $\sigma(5^e)$ が素数 q になったとする. $\alpha = aq$ とおき$\sigma(\alpha)$ を計算する.

$$\sigma(\alpha) = \sigma(aq) = \sigma(a)\sigma(q) = \sigma(q)(q+1)$$

になる. $q = \sigma(5^e) = \frac{5^{e+1}-1}{4}$ より

$$q + 1 = \frac{5^{e+1}+3}{2} = \frac{5a+3}{4}$$

なので

$$\sigma(\alpha) = \sigma(a)(q+1) = \frac{\sigma(a)(5a+3)}{4} = \frac{(5\alpha+3q)}{4}.$$

これから

$$4\sigma(\alpha) = 5\alpha + 3q.$$

ここから q を消すことができないので a の最大素因子を $\mathrm{Maxp}(a)$ と書きこれを使う. すると

$$4\sigma(\alpha) = 5\alpha + 3\mathrm{Maxp}(\alpha)$$

を満たす.

15.1. $s(a)=2$ **の場合.** $4\sigma(\alpha)=5\alpha+3\mathrm{Maxp}(\alpha)$ の解を $s(a)=2$ の場合に求めよう.

a を素因数分解し $a=p^eq^f(2<p<q)$ とする. $X=p^e, Y=q^f$ とおくと $a=XY$ となる.すると $\overline{p}=p-1, \overline{q}=q-1$ を使えば

$$\sigma(a)=\frac{(pX-1)(qY-1)}{\overline{pq}}$$

であり,$A=pX-1, B=qY-1, \rho'=\overline{pq}$ とおけば

$$\frac{4AB}{\rho'}=5XY+3q$$

書き直して

$$4AB=5\rho'XY+3\rho'q.$$

$4AB - 5\rho' XY$ の XY の係数を R とおけば

$$R = 4pq - 5\rho' = 20 - (p-5)(q-5).$$

$3q\rho' + 4(pX + qY - 1) = RXY$ によって $R > 0$. $0 < R = 20 - (p-5)(q-5)$ により 次なる解がある.

(1) $p = 5, R = 20$. $\rho' = 4\overline{q}$,
(2) $p = 3, R = 30 + 2q$. $\rho' = 2\overline{q}$,
(3) $p = 7, R = 30 - 2q; q = 11, 13$ $\rho' = 6\overline{q}$.

$$RXY - 4(pX + qY - 1) = 3q\rho'.$$

1. $p = 5, R = 20$. $\rho' = 4\overline{q}$.

$$(20X - 4q)Y - 20X = 12q\overline{q} - 4.$$

4 で割って

$$(5X - q)Y - 5X = (5X - q)Y - (5X - q) - q = 3q\overline{q} - 1.$$

変形して

$$(5X - q)(Y - 1) = 3q\overline{q} + \overline{q}.$$

$Y - 1 \geq \overline{q}$ により

$$3q\overline{q} + \overline{q} \geq (5X - q)\overline{q}$$

$\overline{q}$ を除して

$$3q+1 \geq (5X-q).$$

i. $Y=q$ なら $3q+1=(5X-q)$. ゆえに $q=\frac{5^{e+1}-1}{4}$.

ここで話を逆転し e を動かして $\frac{5^{e+1}-1}{4}$ が素数のときを探して q とおけばよい.

ii. $Y = q^2$ なら

$$(5X - q)(q^2 - 1) = (5X - q)(Y - 1) = 3q\overline{q} + \overline{q}$$

により,

$$(5X - q)(q + 1) = 3q + 1.$$

$5X = q + \frac{3q+1}{q+1} = q + 4 - \frac{2}{q+1}$. しかるに $\frac{2}{q+1}$ は整数になれないから矛盾.

iii. $Y \geq q^3$ なら

$$(5X-q)(Y-1) = 3q\overline{q}+\overline{q} \geq (5X-q)(q^3-1) = (5X-q)(q^2+q+1)\overline{q}.$$

$\overline{q}$ を除すると $3q + 1 \geq q^2 + q + 1$; 矛盾.

2. $p = 3, R = 30 + 2q$. $\rho' = 2\overline{q}$,
$R_1 = 15 + q$ とおくとき

$$R_1XY - 2(3X + qY - 1) = 3q\overline{q} - 2.$$

$Y \geq q$ により

$$(R_1X - 2q)Y = 6X + 3q\overline{q} - 2 \geq (R_1X - 2q)q.$$

$6X + 3q\overline{q} - 2 \geq (R_1X - 2q)q$ により

$$3q\overline{q} - 2 + 2q^2 \geq (R_1q - 6)X.$$

i. $X \geq 3^2 = 9$ のとき

$$3q\overline{q} - 2 + 2q^2 \geq 9(R_1 q - 6) = 9(q^2 + 15q - 6).$$

これから矛盾が出る.

ii. $X = 3$ のとき

$$3R_1 Y - 2(9 + qY - 1) = 3q\overline{q} - 2.$$

これより

$$Y(3R_1 - 2q) = 3q\overline{q} - 4.$$

$3R_1 - 2q = q + 45$ なので $q_1 = q + 45$ とおいて

$$q_1 Y = 3q^2 - 3q - 4 = \overline{q} - 4 = 3q_1^2 - 273q_1 + 6226.$$

$\frac{6226}{q_1}$ は整数で$6226 = 2 * 11 * 283$, $q_1 = q + 45$ は偶数なので $q_1 = q + 45 = 6226, 2 * 283$.

その結果$q = 6226 - 45 = 6161 = 61 * 11, q = 2 * 283 - 45 = 521$. しかし, $a = 3 * 521$ は条件を満たさない.

3. $p = 7, R = 30 - 2q; q = 11, 13$ $\rho' = 6\overline{q}$.
$p = 7$ より $R_1 = 15 - q$ とおくと

$$R_1XY - 2(7X + qY - 1) = 9q\overline{q}$$

i. $q = 11$ なら

$$4XY - 2(7X + 11Y - 1) = 9q\overline{q} = 90 \times 11.$$

$X_1 = 2X, Y_1 = 2Y$ とすると

$$X_1Y_1 - 7X_1 - 11Y_1 = 9q\overline{q} = 90 \times 11 - 2 = 988.$$

$X_1(Y_1-7)-11(Y_1-7) = (X_1-11)(Y_1-7) = 988+77 = 1065 = 3*5*71.$
これより $X_1 = 2X = 11+3, Y_1 = 2Y = 7+5*71.$ $X = 7, 2Y = 362, Y = 81 = 3^4.$ 矛盾

ii. $q = 13$ なら $R_1 = 2$.

$$4XY - 4(7X + 13Y - 1) = 18q\overline{q} = 2808.$$

$$XY - (7X + 13Y) = 3^2 * 6 * 13 - 1 = 701.$$

$$(X - 13)(Y - 7) = 701 + 13 * 7 = 792 = 8 * 9 * 11.$$

$X - 13 = 36, Y - 7 = 22; Y = 29$. 矛盾

16. P を底とするフェルマーの完全数

P を奇素数とし $E > 0$ について $Q = P^E + 1$ とおく. これは偶数なので $L_E = \frac{Q}{2}$ とする. L_E を素数とすると, E は 2 のべきになるので $E = 2^m, m > 0$ とかける.

そこで一般に $E = 2^m$ とかけるときL_E は奇数であることがを証明する.

実際,$L_E = \frac{Q}{2} = 2L'$ とすると$Q = 4L'$ なので

$$Q = P^E + 1 = 4L' \equiv 0 \mod 4.$$

ゆえに, $P^E \equiv -1$.

一方, $P = 2k + 1$ とおくとき

$$P^E = (2k+1)^{2^m} \equiv 1 \mod 4.$$

これで前の式に矛盾した.

$E = 2^m$ のとき $L_m = \frac{P^E+1}{2}$ とおく. これは奇数であり,. P を底とするフェルマー数と理解する.

TABLE 22. $P = 2$

m	2^m	$2^{2^m}+1$	素因数分解
0	1	3	3
1	2	5	5
2	4	17	17
3	8	257	257
4	16	65537	65537
5	32	4294967297	$641 * 6700417$
6	64	18446744073709551617	$274177 * 67280421310721$
7	128	A	B

16.1. 例.

$A = 340282366920938463463374607431768211457$

$B = 59649589127497217 * 5704689200685129054721$

$m = 0, 1, 2, 3, 4$ のときのみ素数(フェルマー素数)

$P = 3$

TABLE 23. $P = 3$

m	2^m	$2L_E$	素因数分解
1	2	10	$2 * 5$
2	4	82	$2 * 41$
3	8	6562	$2 * 17 * 193$
4	16	43046722	$2 * 21523361$
5	32	1853020188851842	$2 * 926510094425921$
6	64	3433683820292512484657849089282	$2 * 1716841910146256242328924544641$
7	128	A	B

$$A = 11790184577738583171520872861412518665678211592275841109096961$$

$$B = 2*257*275201*1384246188687 37*391378628151452492 9*153849834853 9$$

TABLE 24. $P = 5$

m	2^m	$2L_E$	素因数分解
1	2	26	$2 * 13$
2	4	626	$2 * 313$
3	8	390626	$2 * 17 * 11489$
4	16	152587890626	$2 * 2593 * 29423041$
5	32	23283064365386962890626	$2 * 641 * 75068993 * 2419310016 01$

TABLE 25. $P = 7$

m	2^m	$2L_E$	素因数分解
1	2	50	$2 * 5^2$
2	4	2402	$2 * 1201$
3	8	5764802	$2 * 17 * 169553$
4	16	33232930569602	$2 * 353 * 47072139617$
5	32	1104427674243920646305299202	$2 * 7699649 * 134818753 * 53196866$

$m = 2$ のときのみ素数.

TABLE 26. $P = 11$

m	2^m	$2L_E$	素因数分解
1	2	122	$2 * 61$
2	4	14642	$2 * 7321$
3	8	214358882	$2 * 17 * 6304673$
4	16	45949729863572162	$2 * 51329 * 447600088289$

16.2. **オイラーの結果.** L_E は奇数なのでその素因子を ρ とおくと

$$P^E + 1 = 2L_E \equiv 0 \mod \rho.$$

$E = 2^m$ によって

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

ゆえに

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

ρ を法とすると P の位数は 2^{m+1} 以下であるが $P^E = P^{2^m} \equiv -1$ によって 2^m より大なので, P の位数は 2^{m+1}.

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

$P^{\rho-1} \equiv 1 \mod \rho$. $\rho-1$ は位数 2^{m+1} の倍数なので, $\rho-1 = 2^{m+1}K$.

この結果は $P = 2$ のときオイラーによる.

16.3. $P = 5$ のとき. $P = 5$ のとき, L_E が合成数の場合に確認する.

TABLE 27. $P = 5$

m	2^m	$2L_E$	素因数分解
3	8	390626	$2 * 17 * 11489$
4	16	152587890626	$2 * 2593 * 29423041$
5	32	23283064365386962890626	$2 * 641 * 75068993 * 2419310016 01$

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

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

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

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

?- A=29423041,B is A-1,factorize(B,C),exps(C,D).
A = 29423041,
B = 29423040,
D = [2^6, 3, 5, 30649].

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

?- A=75068993,B is A-1,factorize(B,C),exps(C,D).
```

```
B = 241931001600,
D = [2^8, 3^2, 5^2, 23, 182617].
```

17. フェルマーの完全数の方程式

$e = 2^m - 1$ とおき, $q = \frac{P^{e+1}-1}{2}$ は素数とする. $a = P^e q$ は P を底とするフェルマーの完全数である.

これの満たす方程式を求める.

$P^{e+1} - 1 = 2q$ により,$2q + 2 = P^{e+1} + 3$. さらに $\sigma(a) = \frac{P^{e+1}-1}{P}(q+1)$ によって

$$\begin{aligned}\overline{P}\sigma(a) &= (P^{e+1}-1)(q+1)\\ &= (2q-2)(q+1)\\ &= 2q(q+1)-2(q+1)\\ &= q(P^{e+1}+3)-2(q+1)\\ &= qP^{e+1}+q-2\\ &= aP+q-2.\end{aligned}$$

よって,

$$\overline{P}\sigma(a) - aP = \mathrm{Maxp}(a) - 2.$$

これがP を底とするフェルマーの完全数の方程式である.

18. 究極の完全数

19. 究極の完全数とその平行移動

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**と呼ぼう.

このとき $q = \frac{P^{e+1}-1}{P}$ となる. 言葉ができると諒解しやすくまた研究したくなるという効果がある.

究極の完全数を整数 m だけ平行移動する.

$q = \frac{P^{e+1}-1}{P} + m$ は素数として $a = P^e q$ を m だけ平行移動した底が P の完全数と呼ぶ.

19.1. 例.

TABLE 28. $P = 5, m = 0$

e	素因数分解	a
2	$5^2 * 31$	775
6	$5^6 * 19531$	305171875
10	$5^{10} * 12207031$	119209287109375
12	$5^{12} * 305175781$	74505805908203125
46	$5^{46} * 177635683940025046467781066894531$	A

19.1.1. $[p = 5, m = 0]$. $A = 252435489670723777731753140890491238224058$

この表によると q の下 2 桁は, 31 または 81.

$4q = 5^{e+1} - 1$ を利用して, $q \equiv 31 \mod 50$ を証明する.

$e \geq 2$ により

$$4q = 5^{e+1} - 1 \equiv -1 \mod 25$$

6倍して

$$24q \equiv -6 \mod 25$$

$24q \equiv -q$ により

$$q \equiv 6 \equiv 31 \mod 25$$

q は奇数なので $q \equiv 31 \mod 50$.

$e \geq 3$ を仮定する. $a = 5^e * q = 625 * 5^{e-3} * (31 + 50k) = 625K$, K は奇数.

$$a = 625(2s + 1) \equiv 625 \equiv 625 + 50 = 675 \equiv 5 \mod 25.$$

よって $q \equiv 31, q \equiv 25 \mod 50$

TABLE 29. $P = 5, m = 1$

e	素因数分解	a
3	$5^3 * 157$	19625
5	$5^5 * 3907$	12209375
9	$5^9 * 2441407$	4768373046875
11	$5^{11} * 61035157$	2980232275390625
27	$5^{27} * 9313225746154785157$	693889390390722837820649147033691406 25

19.1.2. $[p = 5, m = 1]$. $q \equiv 7, 32 \mod 50$ を以下で証明する.

$q = \frac{5^{e+1}-1}{4} + 1 = \frac{5^{e+1}+3}{4}$ により
$e \geq 2, 5^2 \equiv 0 \mod 25$ を用いて

$$4q = 5^{e+1} + 3 \equiv 3 \mod 25.$$

6倍して

$$24q \equiv -q \equiv 18 \mod 25$$

$q \equiv 7$ により

$$q \equiv 7 \mod 25.$$

$q = 7 + 25k$. q は奇数なので k は偶数になり,

$$q \equiv 7 \mod 50.$$

TABLE 30. $P = 5, m = -2$

e	素因数分解	a
2	$5^2 * 29$	725
10	$5^{10} * 12207029$	119209267578125
14	$5^{14} * 7629394529$	4656612871704101562 5
26	$5^{26} * 186264514923095702 9$	A
32	$5^{32} * 291038304567337036 13279$	B
42	$5^{42} * 284217094304040074348449707029$	C

19.1.3. $[p = 5, m = -2]$. $A = 27755575615628913477063179016113281 25$
$B = 67762635780344027125460561364889144897460937 5$
$C = 64623485355705287099328804067454257165081799030303955078125$

以下で, $q \equiv 9 \mod 10$ を示す.
$q = \frac{5^{e+1}-1}{4} - 2 = \frac{5^{e+1}-9}{4}$ により
$4q = 5^{e+1} - 9$ により
6倍して

$$24q \equiv -q \equiv -54 \equiv -4 \mod 25.$$

$$q \equiv 4 \equiv 29 \mod 25.$$

$q = 19 + 25k$ となるが, q は奇数なので k は偶数. ゆえに

$$q \equiv 29 \mod 50.$$

TABLE 31. $P = 7, m = 0$

e	素因数分解	a
4	$7^4 * 2801$	6725201
12	$7^{12} * 16148168401$	22351143660835393560 1

19.2. $[p = 7, m = 0]$. a, q は末尾が1. 証明できるか?

TABLE 32. $P = 7, m = 1$

e	素因数分解	a
3	$7^3 * 401$	137543
5	$7^5 * 19609$	A
11	$7^{11} * 2306881201$	B
35	$7^{35} * 44195514097660891196317056360 1$	C

19.2.1. $[p = 7, m = 1]$. $A = 329568463$,
$B = 4561457891661258343$,
$C = 16742086854484650666653692241643193260697833501385600910074 3$
q の末尾は 1,9 ;a の末尾は 3 .
証明できるか?

TABLE 33. $P = 11, m = 0$

e	素因数分解	a
16	$11^{16} * 50544702849929377$	A
18	$11^{18} * 6115909044841454629$	B

19.3. $[p = 11, m = 0]$. $A = 232251544198878080950520379327369 7$, $B = 340039485861577398986846964992269755 49$.

TABLE 34. $P = 11, m = 1$

e	素因数分解	a
7	$11^{16} * 21435889$	A

19.3.1. $[p = 11, m = -1]$. $A = 984973308935517986686129$

TABLE 35. $P = 13, m = 0$

e	素因数分解	a
4	$13^4 * 30941$	883705901
6	$13^6 * 5229043$	252395918137 87

19.4. $[p = 13, m = 0]$.

20. 究極の完全数の満たす方程式

平行移動も許した究極の完全数の満たす方程式を作る.

$q = \frac{P^{e+1}-1}{\overline{P}} + m$ であって

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

になり, $q+1 = \frac{P^{e+1}+P-2}{\overline{P}} + m$ を用いて次のように式変形する.

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

これより $q=\mathrm{Maxp}(a)$ を用いて

$$\overline{P}\sigma(a)-Pa=(P-2)\mathrm{Maxp}(a)-m(P-1). \tag{5}$$

これを m 平行移動した究極の完全数の基本方程式という.

例えば $P = 2$ なら

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

$P = 2$に限って不愉快な $\mathrm{Maxp}(a)$ が消えた.

$P = 3$ なら

$$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2m.$$

20.1. **究極の完全数の基本問題.**

(5) を満たすとき

素数 $q = \frac{P^{e+1}-1}{P} + m$ を基にして $a = P^e q$

とかけるか? という問題を

究極の完全数の基本問題と言う.

これが一般に成立するはずはない. とりあえず反例を探す.

21. 諸例

次に方程式を満たす a を表示する.

$a =< 200000$ 程度の範囲で全数検査するので非常に時間がかかる.

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

TABLE 36. $[P = 5, m = 0]$

a	素因数分解	$\sigma(a)$
775	$[5^2, 31]$	992

21.1. $[P = 5, m = 0]$. 微小解は無い.

TABLE 37. $[P = 7, m = 0]$

a	素因数分解	$\sigma(a)$
9	$[3^2]$	13

21.2. $[P = 7, m = 0]$. $a = 3^2$ は微小解.

TABLE 38. $[P = 43, m = 0]$

a	素因数分解	$\sigma(a)$
49	$[7^2]$	57

21.3. $[P = 43, m = 0]$.

22. 微小解

平行移動しない場合を扱う. したがって

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

を満たすので $s(a) = 1$ のときの解を求めよう. $a = q^f$ が上の式を満たすとする.

平行移動しない場合を扱う.したがって

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

を満たす. $s(a) = 1$ のときの解を求めよう. $a = q^f$ が上の式を満たすとする.

$f = 1$ のとき.

$$\overline{P}(q+1) - Pq = (P-2)q.$$

これより,

$$P - q - 1 = (P-2)q.$$

$(P-1)(q-1) = 0$ がでて矛盾.

$f \geq 2$ のとき.

$Y = q^f$ とおけば $a = Y, \overline{q}\sigma(a) = qY - 1$ を満たし $\mathrm{Maxp}(a) = q$ によって

$$\frac{\overline{P}(qY-1)}{\overline{q}} = PY + (P-2)q.$$

整理して

$$Y(\overline{P}q - P\overline{q}) = \overline{P} + (P-2)q\overline{q}.$$

これより

$$\overline{P} = Y(P-q) - (P-2)q\overline{q} = q(q^{f-1}(P-q) - (P-2)\overline{q}).$$

よって $\overline{P} = wq$ を満たす自然数 w がある. q を払って

$$w = (q^{f-1}(P-q) - (P-2)\overline{q}) = P(q^{f-1} - \overline{q}) - q^f + 2\overline{q}.$$

よって $P = 1 + wq$

$$w = (1+wq)(q^{f-1} - \overline{q}) - q^f + 2\overline{q}$$

$2\sigma(a) = 3a + 2$ なので$2(2Y - 1) = 3Y + 2$. これより $a = Y = 4$.

$w \geq 2$ のとき.

$$2(q^f - q\overline{q} - 1) \leq w(q^f - q\overline{q} - 1) = q^f - q^{f-1} - \overline{q}.$$

これより

$$q^f - 2q\overline{q} - 2 \leq -q^{f-1} - \overline{q}.$$

$$q^{f-1}(q+1) \leq 2q^2 - 3q + 3.$$

$f \geq 3$ のとき.

$$q^2(q+1) \leq 2q^2 - 3q + 3.$$

変形して

$$q^3 - q^2 \leq 3 - 3q.$$

これは矛盾.

P, q が素数で $P = 1 + q(q-1)$ を満たすとき方程式で定められた 底が P のとき $a = q^2$ が微小解.

微小解が存在するための素数 P の条件が素数q があって $P = 1 + q(q-1)$ を満たすことである.

このような素数として $P = 7, 43$ がある.

$P = 3$ のとき微小解 $q = 2^2; P = 7$ のとき微小解 $q = 3^2; P = 157$ のとき微小解 $q = 13^2$ などが現れる.

22.1. **微小解の存在する素数.** 微小解の存在する素数はほかにあるだろうか. パソコン君に頼むと次のように意外に多くの解を出してきた.

TABLE 39. P, q が素数

q	P
3	7
7	43
13	157
67	4423
79	6163
139	19183
151	22651
163	26407
193	37057

a, b が互いに素な自然数のとき 等差数列$\{an + b\}$ $(n = 1, 2, 3, \cdots)$ には無限に多くの素数がある. これが有名な Dirichlet の定理である.

しかし, 2次数列たとえば $\{n^2 + 1\}$ には無限に多くの素数があるに違いない. これは有名な数論における期待であるが証明はできるはずがない, と思われているほど難しい.

$\{n^2 - n + 1\}$ は無限に多くの素数があることは確実だが証明はない.

微小解の存在条件では n を素数に限りつつ$\{n^2 - n + 1\}$ には無限に多くの素数があるか問うている.

これは真に難問中の難問である. このような難問が, 微小解の存在問題として登場した. 実に不思議なことである.

22.2. $s(a)=2$ の場合に解く (未完). 与えられた素数 P と整数 m について次式が満たされるとする.

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

これを $m=0$ の条件をつけa の方程式 とみて $s(a)=2$ の場合に解いてみよう.

$a=p^eq^f, p<q$ はいつもの通りで $X=p^e, Y=q^f, A=pX-1, B=qY-1, \rho'=\overline{pq}$ を使う.

$$\frac{\overline{P}AB}{\rho'}-PXY=(P-2)q$$

が基礎方程式になる.ρ' をかけて

$$\overline{P}AB-\rho'PXY=\rho'(P-2)q.$$

左辺の XY の係数を R とおけば

$$R=\overline{P}pq-\rho'P=P(pq-\rho')-pq.$$

$p = P(p' = 0)$ なら $R = P(P-1)$. これが標準的な場合になるが$p > P, p < P$ の場合もあり, ここで一般に考えることは難しい.

実際, $P = 7$ とすると $R = 42 - p'q'$.

- $p = 2$ のとき $R = 7 + 5q$
- $p = 3$ のとき $R = 14 + 4q$
- $p = 5$ のとき $R = 28 + 2q$
- $p = 7$ のとき $q \geq 11, R = 42$
- $p = 11$ のとき $q = 13, 17$.

したがって, ここで小休止.

23. 例

23.1. $[m = p - 1]$ **の解.** $\overline{P}\sigma(a) - Pa = (P-2)\mathrm{Maxp}(a) - m(P-1)$ おいて微小解として $s(a) = 1$ の解 $a = P^e$ があるとする.

$\overline{P}\sigma(a) - Pa = (P^{e+1} - 1) - P^{e+1} = -1$ により

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

よって $m(P-1) = (P-1)^2$. これより $m = P - 1$.

$m = P - 1$ のとき 微小解 P^e 以外の解がどのくらいあるかがわからない

TABLE 40. $[p = 5, m = 1]$

a	素因数分解	$\sigma(a)$
2	$[2]$	3
35	$[5, 7]$	48
3059	$[7, 19, 23]$	3840
7469	$[7, 11, 97]$	9408
19625	$[5^3, 157]$	24648

23.2. $[p = 5, m = 1]$.

TABLE 41. $[p = 5, m = 3]$

a	素因数分解	$\sigma(a)$
847	$[7, 11^2]$	1064

23.3. $[p = 5, m = 3]$.

TABLE 42. $[p = 5, m = 4]$

a	素因数分解	$\sigma(a)$
5	$[5]$	6
25	$[5^2]$	31
125	$[5^3]$	156
625	$[5^4]$	781
3125	$[5^5]$	3906
15625	$[5^6]$	19531
78125	$[5^7]$	97656

23.4. $[p = 5, m = 4]$.