1　素数べき

2 を公比とし初項1の等比数列 $1, 2, 2^2 = 4, 2^3 = 8, \cdots$ は数学において基本的で大切な数列である.

3 を公比とする等比数列 $1, 3, 3^2 = 9, 3^3 = 27, \cdots$ も大切である.

自然数 a の約数の和を $\sigma(a)$ で表すことは現在ほぼ確定した記号である

たとえば, $a = p^3 (p : \text{素数})$ ならその約数は $1, p, p^2, p^3$. この和 $1 + p + p^2 + p^3$ が $\sigma(a)$ である.

$S = 1+p+p^2+p^3$ とおくと, $pS = p+p^2+p^3+p^4$. $pS-S$ を作るとうまく消し合って $pS-S = p^4-1$.

$p > 1$ なので $S = \frac{p^4-1}{p-1}$.

一般に $a = p^e$ のとき$\sigma(p^e) = \frac{p^{e+1}-1}{p-1}$ がわかる.

2個以上の素因子を持つときは次のように考えるとよい.

$a = p^2q^2$ の約数は $1, p, p^2, q, pq, p^2q, q^2, pq^2, p^2q^2$.
これらの和は

$$(1+p+p^2)+(1+p+p^2)q+(1+p+p^2)q^2 = (1+p+p^2)(1+q+q^2) = \sigma(p^2)\sigma(q^2).$$

$a = p^eq^f$ の約数は素因子分解の一意性より $p^rq^s, (r \leq e, s \leq f)$ と書ける. したがって

$$\sigma(a) = \sigma(p^e)\sigma(q^f). \tag{1}$$

一般には a, b が互いに素ならば

$$\sigma(ab) = \sigma(a)\sigma(b)$$

が成り立つ. これを $\sigma(a)$ は乗法性を持つと言う.

素因数分解の一意性によって乗法性が成り立つことが証明される.

素因数分解の一意性は割り算による互除法によって古代ギリシャで証明されていた.

$\sigma(a)$ は奇数になるのは少ない.

$\sigma(a)$ にしたがって並べてみた.

$\sigma(a)$ に出てこない数として9,10,11 があり,12になる数として6,11 があげられる. これを表によらないで数学的に証明するにはどうしたらよいか.

1.1 $\sigma(a)$ のグラフ

ユークリッド関数$\sigma(a)$のグラフを描いて見た．きわめて複雑な形をしている．

図 1: $\sigma(a)$

$x = a, y = \sigma(a)$ とおく.

$a = p > 1$ が素数なら$\sigma(a) = a + 1$ なので $y = x + 1$: これが素数の直線.

$a = p > 1$ が素数でないなら$\sigma(a) \geq a + 2$ なので $y \geq x + 2$. 素数の直線の上側になる.

$m(\neq p)$ を素数として$a = mp$ について

$b = \sigma(a) = \sigma(m)\sigma(p) = \widetilde{m}\widetilde{p}$ となるので$p = \frac{a}{m}$ を用いて

$$b = \widetilde{m}(\frac{a}{m} + 1) = \frac{\widetilde{m}x}{m} + \widetilde{m}$$

したがって, 素数 m に対して $a=mp, b=\sigma(a)$ とおけば (a,b) は直線

$$y=\frac{\widetilde{m}x}{m}+\widetilde{m}$$

の上にある.

$m=2$ に対して直線 $y=\frac{3x}{2}+3$,

$m=3$, に対して直線 $y=\frac{4x}{3}+4$,

$m=5$,に対して直線 $y=\frac{6x}{5}+6$,$\cdots$ などが対応する.

1.2 等比数列の和

$a = 2^e$ とし, 等比数列の和の公式を用いると

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

と書けるから $a = 2^e$ なら $\sigma(a) = 2a - 1$ を満たす.

これはごく初等的なことであるが, 等比数列の和の公式が用いられていることに注意を払いたい.

そこで数学の世界によくあることだが, この逆を問題として考える.

$\sigma(a) = 2a - 1$ を満たす自然数 a は $a = 2^e$ に限るか?

ごく自然な発想で生まれた問題である．一般に $\sigma(a)-2a=-1$ を満たす自然数 a を概完全数(almost perfect number) と呼ぶそうだ．そこで200 までの範囲で概完全数をパソコン君に探してもらうと次の表ができた．

表 1:

a	$\sigma(a)$	素因数分解
2	3	[2]
4	7	[2^2]
8	15	[2^3]
16	31	[2^4]
32	63	[2^5]
64	127	[2^6]
128	255	[2^7]

概完全数の数表として2のべきがでてきた.しかし2のべき以外に概完全数があるかは,未だに解決されることなく,一見やさしそうで意外に難しい問題として残されている.

1.3 概完全数問題の $s(a)=1,2$ での解決

$\sigma(a)-2a=-1$ を条件 $s(a)=1,2$ の下で解いてみよう. ただし $s(a)$ は a の相異なる素因子の数.

$s(a)=1$ のとき. $a=p^e$ とかける. $\overline{p}=p-1$ とおくと$\sigma(a)=\frac{pa-1}{\overline{p}}$ となるので,

$$\frac{pa-1}{\overline{p}}=2a-1.$$

よって

$$pa-1=(2a-1)\overline{p}.$$

$$a(p-2\overline{p})=1-\overline{p}=2-p.$$

$p-2\overline{p}=2-p$ により

$$2-p=a(2-p).$$

$a>1$ により, $p=2$. よって $a=2^e$.

$s(a) = 2$ のとき．概完全数はないことを背理法で示す．

$a = p^e q^f (p < q)$,$\overline{p} = p - 1, \overline{q} = p - 1$ とおく．

$X = p^e, Y = q^f$, $A = pX - 1 - 1, B = qY - 1$, $\rho' = \overline{pq}$ とおくと

$\sigma(a) = \frac{AB}{\rho'}, a = XY$ と書けるので,

$$\frac{AB}{\rho'} = 2XY - 1.$$

これを整理して

$$AB - 2\rho' XY = -\rho'.$$

左辺の XY の係数を R とおくと $R = pq - 2\rho' = 2 - (p-2)(q-2)$.

$$RXY - (pX + qY - 1) = -\rho'. \qquad (2)$$

式 (2) より

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

これを変形して

$$0=2XY-(2X+qY)+1+\overline{q}=2XY-(2X+qY)+q.$$

一方 $2XY-(2X+qY)+q=(2X-q)(Y-1)$ により

$0=(2X-q)(Y-1)$. $Y\neq 1$ なので $q=2X=2^{e+1}$,矛盾.

$s(a)\geq 3$ の場合は複雑になりなかなかできない.

2　3点セット

関連して次の問題を合わせ考え,$a=2^e$ に関しての3点セットと言う.

1. $\sigma(a)-2a=0$ を満たす自然数は何か,(これは完全数で次項でふれる)
2. $\sigma(a)-2a=-1$ を満たす自然数は何か, (概完全数)
3. $\sigma(a)-2a=1$ を満たす自然数は何か.

$\sigma(a)-2a; a<100$ の順に並べた表をみて見よう.

表 2:

a	素因数分解	$\sigma(a)$	$\sigma(a)-2a$
7	$[7]$	8	-6
15	$[3,5]$	24	-6
9	$[3^2]$	13	-5
5	$[5]$	6	-4
14	$[2,7]$	24	-4
44	$[2^2,11]$	84	-4
3	$[3]$	4	-2
10	$[2,5]$	18	-2
2	$[2]$	3	-1 (2のべき)
4	$[2^2]$	7	-1
8	$[2^3]$	15	-1
16	$[2^4]$	31	-1
32	$[2^5]$	63	-1
6	$[2,3]$	12	0 (完全数)
28	$[2^2,7]$	56	0
20	$[2^2,5]$	42	2
18	$[2,3^2]$	39	3
12	$[2^2,3]$	28	4

3 完全数

完全数(perfect number)とは $\sigma(a) - 2a = 0$ を満たす 自然数 a のことである.

偶数の完全数はオイラーによってその形が決められたが,完全数は無限にあるか, あるいは奇数の完全数は存在するかなどは大難問である.

4 完全数の歴史

L.E.Dickson 著の Theory of Numbers I,1919/20(Chelsea Publishing Company 版 1992) の第1章を参考にして完全数の歴史について書いて簡単にふれる.

ユークリッドは原論 IX,prop.36 において $p = 1 + 2 + 2^2 + \cdots + 2^n$ が素数なら $a = 2^n p$ は完全数になることを示した.

a の約数は

$$1, 2, 2^2, \cdots, 2^n, 1 \cdot p, 2 \cdot p, 2^2 \cdot p, \cdots, 2^n \cdot p$$

であってこれらの和は等比数列の和の公式を使うと $2a$ になる.

AD 100 年の頃 Nichomachus はすべての偶数を 過剰数 $(\sigma(a) - a > a)$,不足数$(\sigma(a) - a < a)$,完全数$(\sigma(a) - a = a)$に分類した.

完全数には稀少性があり, 6,28,496,8128, などでこれらの末尾の数が 6 または8 であることに注目が集まった. (6,8 は交互にきて、さらに桁が上がる度に 1 つずつあることを観察した. しかしこれらは正しくなかったことが後にわかった).

1456 年の文書に5番目の完全数 33550336 が記載された.

Luca Paciuolo (1494 年 ?) は $1 + 2 + 2^2 + \cdots + 2^n$ が素数になることは実行して初めてわかることだが無限にあるだろう, と述べた.

Cardan (1501–1576) は完全数はユークリッドが与えた方法ですべて構成されるだろう.

Tartaglia (1506–1559) $1 + 2 + 4, 1 + 2 + 4 + 8, 1 + 2 + 4 + 8 + 16, \cdots$ は交互に素数か合成数になる, と述べた.

F.Maurolucus (1494– 1575) は完全数は三角数になることを注意した.

$q = 2^{e+1} - 1$ とおくと $q + 1 = 2 * 2^e$ によって

$$1 + 2 + 3 + \cdots + q = \frac{q(q+1)}{2} = 2^e q = a$$

等比数列の和で定義された完全数が等差数列の和としての三角数であった.

R.Descartes は 1638 年の Mersenne への手紙で偶数完全数はユークリッドが与えた形になることは証明できたと思う. しかし奇数完全数は ps^2 の形になると述べた.

Fermat は 1640 年の Mersenne への手紙で n が合成数なら $2^n - 1$ も合成数. n が素数なら $2^n - 2$ は $2n$ で割れる.

L.Euler は1752 年の Goldbacher への手紙で7個の完全数は$2^{p-1}(2^p-1), p = 2, 3, 5, 7, 13, 17, 19$ であるが $p = 31$ のときは分からない,と述べた.

L.Euler は Bernoulli への手紙で$p = 31$ のときは完全数であることを確認した.

L.Euler は死後出された論文で 偶数完全数は$2^{p-1}(2^p-1)$ と表せることの証明を与えた.

Sylvester はオイラーの証明を確認した.

Servaias とともに奇数の完全数は 4 個以上の素因子を持つ事を示した.

4.1　オイラーによる証明

a を偶数の完全数とし, $a = 2^e L(L:$ 奇数$)$ の形に書く.

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

となるので $N = 2^{e+1} - 1$ とおけば$N\sigma(L) = (N + 1)L$ となるので

$$N(\sigma(L) - L) = L.$$

$d = \sigma(L) - L$ とおくとき $Nd = L$. したがって d は L の約数である. つぎの3つの場合がある.

(1) $d=1$. $N=L.d=1=\sigma(L)-L$ により L は素数 p であり, $p=L=N=2^{e+1}-1$. $p=2^{e+1}-1$ は素数で $a=2^e p$. これはユークリッドの与えた完全数の形となっている.

(2) $d=L$. $N=1=2^{e+1}-1$ になるので $e=0$. a が奇数になり仮定に反す.

(3) $1<d<L$. d は $1, L$ 以外の約数なので$\sigma(L)>1+L+d$. よって $d=\sigma(L)-L>1+d$. これは矛盾.

Dickson にある完全数の証明:

$(2^{e+1}-1)\sigma(L)=2^{e+1}L$ により

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

左辺は既約分数だから $L=c(2^{e+1}-1), \sigma(L)=2^{e+1}c$ を満たす自然数 c がある.

$c=1$ なら $\sigma(L)=L+1$ になるので L は素数.

$c>1$ なら c は $1, L$ 以外の L の約数 になり $\sigma(L)\geq 1+L+c$ を満たすから

$$2^{e+1}c=\sigma(L)\geq 1+L+c=1+c(2^{e+1}-1)+c=1+2^{e+1}c$$

となってしまい矛盾.

4.2 $\sigma(a)-a=1$

オイラーの証明では $\sigma(a)-a=1$ なら a は素数ということが有効に使われている.

$\sigma(a)=a+1$ と書き換えればこれは a の約数は $1, a$ だけということだから定義によって, a は素数.

したがってこのことは当たり前なのだ.

私は高校生への課題として $a=2p; p>2$ (素数の2倍)になることを$\sigma(a)$ で判定したらどうか.

を出してみた.しかし事前に自分でして見た.

$$\sigma(a) = 3(p+1) = 3(\frac{a}{2}+1)$$

とすると$2\sigma(a) = 3a+6$ になる．この逆問題を考えた.

$2\sigma(a) = 3a+6$ を満たすとき, $a = 2p$, および 8.

が証明できた．$a = 2p$ の特徴づけは,8 を例外としてうまくできた．しかし, $a = 6p$, $28p$ などの特徴づけは難しい.

高校生でも解ける問題や,数学者でも絶対に解けない数多くの問題がでてきたので,好都合な問題設定であった.

例

$a > b$ は互いに素な 2以上の数.

$q = a^{e+1} - b$ が素数になる e はあるか?

4.3 疑似完全数

$\sigma(a)-2a=1$ を満たす自然数はpseudo perfect number (疑似完全数) と呼ばれることがある．これは果たして存在するかどうかが問われている.

$\sigma(a)-2a=-1,0,1$ を満たす自然数 a を求める問題はどれも未解決の難問である．完全数の問題は2300年かかっても解けない難問だが,その前後の問題(3点セット)も未だに解けない. 実は,これらの問題は解けないで残されている点に価値がある,

1995年にフェルマーの大定理の証明が確認されて,350年におよぶ数論の難問が解けた.そのため目標を失った人は数知れない.しかし3点セット問題が手つかずに残されていることは大きな励みにな

私がこの連続講義で意図していることは3点セット問題を解くことでは無い. 3点セット問題をさらに一般にして考えてみることによりこの問題の本質を理解することである.

いろいろ一般化すると, 中には解ける問題がみつかって解決できることもある.

さらに解決不可能な多くの興味深い問題も出てくる.

このようにして数学の広く発展する様を体験できる.

4.4 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)

表 3: $\sigma(2^e) = 2^{e+1} - 1$, $e + 1$: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.

完全数の定義には約数の和が必要である. 素因数分解の一意性と約数の和の公式には, 等比数列の和の公式が不可欠である. ともに,ユークリッドに代表される古代ギリシャの数学者が見いだしたモノである.

日本の高校生なら誰でも知っている等比数列の和の公式は2500年も前に発見され完全数の理論に使われた. 日本がようやく弥生式の稲作を始めたころ(BC300年頃) 等比数列の和の公式(ユークリッド BC300–)がすでにできていた.

しかし, 完全数 a は$\sigma(2^e)$ が素数 q になる $a = 2^e$ を用いて必ず $a = 2^e q$ と書けるか ?

という問いは依然として解けていない.

ここでは完全数 a に対しその素因子の個数が2の場合に限って解くことにする.

4.5 $s(a) = 2$ のときの完全数の証明

$s(a) = 2$ のとき a を素因数分解し $a = p^e q^f$ とする. $X = p^e, Y = q^f$ とおくと $a = XY$ となる.

$\overline{p} = p - 1, \overline{q} = q - 1$ 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

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

書き直して

$$AB = 2\rho' XY.$$

$AB - 2\rho' XY$ の XY の係数を R とおくとき $R = pq - 2\rho'$ となり

$$RXY = pX + qY - 1.$$

この式を基本等式という.

$R = pq - 2\rho' = 2 - (p-2)(q-2)$ であり基本等式から $R > 0$ なので $p = 2$ かつ $R = 2$. したがって $2XY = 2X + qY - 1$ が成り立ち, $Y \geq q$ によって,

$$\begin{aligned} 0 = 2XY - (2X + qY - 1) &= (2X - q)Y - (2X - 1) \\ &\geq (2X - q)q - (2X - 1) \\ &= 2X(q-1) - (q^2 - 1) \\ &= \overline{q}(2X - q - 1) \end{aligned}$$

よって

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

一方, $(2X-q)Y = (2X-1)$ によれば $2X-q \geq 1$. すなわち $2X \geq q+1$. よって $2X = q+1.q = 2^{e+1} - 1, a = XY = 2^e q$. したがって,完全数.

5 完全数の平行移動

$q=2^{e+1}-1$ が素数のとき $2^e q$ は完全数になる.
完全数の平行移動とは次の意味である.

別のパラメータ 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. ただし m は偶数の整数.

6　完全数の数表

表 4: 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	6
0	16	17	$2^{16} * 131071$	8589869056	6
2	18	19	$2^{18} * 524287$	137438691328	8
2	30	31	A	B	8
0	60	61	C	D	6
0	88	89	E	F	6

$$A = 2^{30} * 2147483647$$

$$B = 2305843008139952128$$

$$C = 2^{60} * 2305843009213693951$$

$$D = 26584559915698317446546926159538 42176$$

$$E = 2^{88} * 618970019642690137449562111$$

$$F = 191561942608236107294793378084303638130997321548169216$$

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 $q \equiv 7 \mod 10$. $a \equiv 8 \mod 10$.

Proof. (金子元さんの援助による)

$2^4 = 16 \equiv 1 \mod 5$ を以下用いる.

1). $e = 4k$. $q = 2^{e+1} - 1 \equiv 1 \mod 5$ によって $q = 1 + 5L$. 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). $e=4k+1$. $c=2^{2k+1}$ とおくとき

$q=2^{e+1}-1=2^{4k+2}-1=c^2-1=(c-1)(c+1)$ は素数なので $c-1=1$. ゆえに $q=3, k=0, e=1$. $a=2*q=6$. これは例外的な場合.

3). $e=4k+2$. $q=2^{e+1}-1\equiv 2 \mod 5$ によって $q=2+5L$. L は奇数になり, $q\equiv 7 \mod 10$.

$a=2^e q\equiv -q\equiv 3 \mod 5$; $a=3+5L$. a は偶数なので $L=2m+1$. $a=3+5(2m+1)\equiv 8 \mod 10$.

4). $e=4k+3$. $q=2^{e+1}-1\equiv 0 \mod 5$ によって $q=5$. $q=2^{e+1}-1=5$ とは矛盾する.

偶数完全数の末尾の1桁は6,または8になるという結果は完全数の中でもやさしいが美しい性質である.

6.1 $m=2$

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.

表 5: $q=2^{e+1}+1$ 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.

6.2 $m = 4$

$q = 2^{e+1} + 3$ が素数の場合

表 6:

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
1	5	$2^5 * 67$	2144	4
2	6	$2^6 * 131$	8384	4
3	11	$2^{11} * 4099$	8394752	2
2	14	$2^{14} * 32771$	536920064	4
3	15	$2^{15} * 65539$	2147581952	2
1	17	$2^{17} * 262147$	34360131584	4
3	27	A	B	2
1	29	C	D	4
2	54	E	F	4
2	66	G	H	4
3	83	I	J	1
2	98	K	L	4

$$A = 2^{27} * 268435459, B = 36028797421617152$$

$$C = 2^{29} * 1073741827, D = 576460753914036224$$

$$E = 2^{54} * 36028797018963971, F = 576460753914036224$$

$$G = 2^{66} * 147573952589676412931$$

$$H = 6490371073168535076095075695 98464$$

$$I = 2^{83} * 19342813113834066795298819$$

$$J = 187072209578355573530071687601903897267059558449152$$

$$K = 2^{98} * 633825300114114700748351602691$$

$$L = 200867255532373784442745261543596063265446546273971631816704$$

表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 7, a \equiv 4 \pmod{10}$.
- $e \equiv 2 \bmod 4$ なら $q \equiv 1, a \equiv 8 \pmod{10}$.
- $e \equiv 3 \bmod 4$ なら $q \equiv 4, a \equiv 2 \pmod{10}$.

Proof.

$e = 4k + 1$ のとき,
$q \equiv 4 + 3 \equiv 7 \bmod 5$, $q \equiv 7 \pmod{10}$.
$a = 2^e q \equiv 2 * 7 = 14 \equiv 4 \bmod 5$, $a \equiv 4 \pmod{10}$.

$e = 4k + 2$ のとき,

$q \equiv -2 + 3 \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.

$a = 2^e q \equiv 4 * q \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 3$ のとき,

$q \equiv 1 + 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.

$a = 2^e q \equiv 3 * 4 = 12 \equiv 2 \bmod 5$, $a \equiv 2 \mod 10$.

6.3 $m = -2$

$q = 2^{e+1} - 3$ が素数の場合これらは指数 e の擬素数 $\mathbf{p}_e$ である. 完全数のときと比べると素数の数が断然多い.

表 7: $q = 2^{e+1} - 3$ が素数

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
2	2	$2^2 * 5$	20	0
3	3	$2^3 * 13$	104	4
0	4	$2^4 * 29$	464	4
1	5	$2^5 * 61$	1952	2
0	8	$2^8 * 509$	130304	4
1	9	$2^9 * 1021$	522752	2
3	11	$2^{11} * 4093$	8382464	4
1	13	$2^{13} * 16381$	134193152	2
3	19	A	B	4
1	21	C	D	2
3	23	E	F	4
0	28	G	H	4

$A = 2^{19} * 1048573, B = 549754241024$
$C = 2^{21} * 4194301, D = 8796086730752$
$E = 2^{23} * 16777213, F = 140737463189504$
$G = 2^{28} * 536870909, H = 144115187270549504$
$I = 2^{93} * 19807040628566084398385987581$
$J = 1961594292308337738698684194455290145603494810419220971\!52$
表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 1, a \equiv 2 \mod 10.$
- $e \equiv 0 \bmod 4$ なら $q \equiv 9, a \equiv 4 \mod 10.$
- $e \equiv 3 \bmod 4$ なら $q \equiv 3, a \equiv 4 \mod 10.$

Proof.

$e = 4k + 1$ のとき,

$q \equiv 4 - 3 \equiv 1 \bmod 5$, $q \equiv 1 \mod 10$.

$a = 2^e q \equiv 2 * 1 = 2 \bmod 5$, $a \equiv 2 \mod 10$.

$e = 4k$ のとき,

$q \equiv 2 - 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.

$a = 2^e q \equiv 9 \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 3$ のとき,

$q \equiv 1 - 3 \equiv 3 \bmod 5$, $q \equiv 3 \mod 10$.

$a = 2^e q \equiv 9 \equiv 4 \bmod 5$, $a \equiv 4 \mod 10$.

$e = 4k + 2$ のとき,

$q \equiv 3 - 3 \equiv 0 \bmod 5$. $q = 5$.

$q = 2^{e+1} - 3 = 5$; $e = 2$. $a = 2^e q = 4 * 5 = 20$.

6.4 $m = -4$

$q = 2^{e+1} - 5$ が素数の場合

表 8: $q = 2^{e+1} - 5$

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
3	3	$2^3 * 11$	88	8
1	5	$2^5 * 59$	1888	8
3	7	$2^7 * 251$	32128	8
1	9	$2^9 * 1019$	521728	8
3	11	$2^{11} * 4091$	8378368	8
1	17	$2^{17} * 262139$	34359083008	8
3	19	$2^{19} * 1048571$	549753192448	8
1	25	$2^{25} * 67108859$	2251799645913088	8
3	31	$2^{31} * 4294967291$	9223372026117357568	8
3	35	$2^{35} * 68719476731$	2361183241263023915008	8

指数 e が奇数になることの証明

偶数になる, すなわち $e = 2N$ と仮定して矛盾を導く.

$q = 2^{2N+1} - 5$ が素数とする. 3 を法としてみる. $2^{2N+1} = 4^N \times 2 \equiv 2, 5 \equiv 2 \mod 3$.

これらにより $q = 2^{2N+1} - 5 \equiv 0 \mod 3$ したがって q が3の倍数,が導かれた.

表を見ると

- $e \equiv 1 \bmod 4$ なら $q \equiv 9, a \equiv 8 \mod 10$.
- $e \equiv 3 \bmod 4$ なら $q \equiv 1, a \equiv 4 \mod 10$.

Proof.

$e = 4k + 1$ のとき,

$q \equiv 4 \bmod 5$, $q \equiv 9 \pmod{10}$.

$a = 2^e q \equiv 2 * 9 \equiv 3 \bmod 5$, $a \equiv 8 \pmod{10}$.

$e = 4k + 3$ のとき,

$q \equiv 1 \bmod 5$, $q \equiv 1 \pmod{10}$.

$a = 2^e q \equiv 3 * 1 \bmod 5$, $a \equiv 8 \pmod{10}$.

6.5 $m = -6$

$q = 2^{e+1} - 7$ が素数の場合

表 9: $q = 2^{e+1} - 7$ が素数

$e \bmod 4$	e	$2^e * q$	a	$a \bmod 10$
2	2	$2^2 * 1$	4	4
2	38	$2^{38} * 549755813881$	151115727449904501489664	4

$a = 4$ のとき, $\widetilde{\sigma}(4) = \frac{7}{2}$ なので $4 - 2\widetilde{\sigma}(4) = -3$.
$q = 2^{e+1} - 7$ が素数になる場合がきわめて少ない.
a の末尾の数は 4.

e が偶数の証明
$e = 2k + 1$ として矛盾を導く.
$q = 2^{e+1} - 7 = (2^2)^{k+1} - 7 \equiv 1 - 1 = 0 \bmod 3$ なので矛盾.

$e = 4k + 2$ の証明
$e = 4k$ として矛盾を導く.

$q = 2^{e+1} - 7$ が素数となる場合を探すには e が公差 4の等差数列となることを使えば,効率の向上が期待できる.

- $N = 2^{42+1} - 7$ の最小素因子 107
- $N = 2^{46+1} - 7$ の最小素因子 11
- $N = 2^{50+1} - 7$ の最小素因子 17174671
- $N = 2^{54+1} - 7$ の最小素因子 896723
- $N = 2^{58+1} - 7$ の最小素因子 13
- $N = 2^{62+1} - 7$ の最小素因子 157

$e = 122$ まで試みたが$q = 2^{e+1} - 7$ が素数となる場合は見つからなかった.

6.6 数値計算例

$2\sigma(a) - 3a = -1$ を満たす自然数についてパソコン君に計算してもらう.

表 10: $2\sigma(a) - 3a = -1$

a	$\sigma(a)$	素因数分解
3	4	$[3]$
9	13	$[3^2]$
27	40	$[3^3]$
81	121	$[3^4]$
243	364	$[3^5]$
729	1093	$[3^6]$
2187	3280	$[3^7]$
6561	9841	$[3^8]$
19683	29524	$[3^9]$

7　3 のべきとそのユークリッド関数の値

表 11: $3^e = a$

$3^e = a$	$\sigma(a)$	$\sigma(a)$ 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	$[47, 1001523179]$
$3^{30} = 205891132094649$	308836698141973	$[683, 102673, 4404047]$

$\sigma(3^e)$ 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．

$9 * 13 = 117, 729 * 1093 = 796797$ などは完全数の類似とみ

8 $\mathbf{3}$ を底とする完全数

$a=3^e$ に対して $\sigma(3^e)=\dfrac{3^{e+1}-1}{2}$ が素数 q になったとする.
このとき $\alpha=aq$ を**$\mathbf{3}$ を底とする完全数**と言うことにする.

8.1 3を底とする完全数の数表

表 12: 3 を底とする完全数

$e \bmod 4$	e	素因数分解	$q \bmod 10$	a	$a \bmod 10$
2	2	$3^2 * 13$	3	117	7
2	6	$3^6 * 1093$	3	796797	7
0	12	$3^{12} * 797161$	1	423644039001	1
2	70	A	3	B	7
2	102	C	3	D	7

$$A = 3^{70} * 3754733257489862401973357979128773$$

$$B = 9398681223266955568884336291512894246732289173595197254503404033277$$

$$C = 3^{102} * 6957596529882152968992225251835887181478451547013$$

$$D = 322720996484187844746619306273472246597518644973851$$

$$- - 206206756380031007356942426993809058144999711 7$$

これらから次の結論を導くことができる.

- $e \equiv 2 \mod 4$ のとき q の末尾の数は 3, a の末尾の数は 7.
- $e \equiv 0 \mod 4$ のとき q の末尾の数は 1, a の末尾の数は 1.

普通の完全数では末尾の数が4 または 6 であったが3を底とする完全数では末尾の数が 7 または 1 になる.

Proof.

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

$2q = 3^{e+1} - 1$ となる素数 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

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

よって $q \equiv 3 \mod 5$. $q = 3 + 5L$ となるが q は素数なので奇数. L は偶数になるので $q \equiv 3 \mod 10$.

$a = 3^e q \equiv -q \equiv 2 \mod 5$ により $a = 2 + 5L$. L は奇数になるので $a \equiv 7 \mod 10$.

2. $e = 4k$ のとき

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

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 1 は奇数なので $a \equiv 1 \mod 10$.

3. $e = 4k + 3$ のとき $A = 3^{k+1}$ とおくとき

$2q = 3^{e+1}-1 = 2q = 3^{4k+4}-1 = A^4-1 = (A-1)(A^3+A^2+A+1)$.

$A - 1 = 3^{k+1} - 1 = 2(3^k + 3^{k-1} + \cdots 1)$ なので $k > 0$ なら $\frac{A-1}{2} > 1$. よって q が素数に矛盾.

$k = 0$ なら $e = 3$ なので $2q = 3^4 - 1 = 80. q = 40$; これは矛盾.

4. $e=4k+1$ のとき $A=3^{2k+1}$ とおくとき

$2q=3^{e+1}-1=2q=3^{4k+2}-1=A^2-1=(A-1)(A+1).$

$A-1=3^{2k+1}-1=2(3^{2k}+3^{2k-1}+\cdots+1)$

$q=(A^2-1)/2=(A-1)/2(A+1)=(3^{2k}+3^{2k-1}+\cdots 1)(A+1).$

q が素数に矛盾.

8.2　3を底とする完全数の公式

普通の完全数の定義では $\sigma(a)-2a=0$ を満たす数のことでこれが偶数の場合はオイラーにより $a=2^e\sigma(2^e)$;(ただし,$\sigma(2^e)$ は素数)が証明された．ここではオイラーの与えた形から出発し $\sigma(3^e)$ が素数 q のとき $a=3^e q$ を**3を底とする完全数**と呼ぶことにした.ここが少しずるい.

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

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

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

とりあえず, 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.

8.3 $s(a)=1$ 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.

8.4 $s(a)=2$ のときの証明

3を底とする完全数の基本問題を $s(a)=2$ の場合だけ扱う.

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

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

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

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

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

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.

9　3を底とする完全数の平行移動

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

これらが存在しなければ意味がないのでパソコンで確認する．

9.1 $p = 3.m = 1$

$p = 3.m = 1$ のとき

表 13: $m = 1$

$e \bmod 4$	e	素因数分解	$q \bmod 10$	a	$a \bmod 10$
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

$$X = 57228063671541905627967299 0187$$

$$A = 3^{63} * 1716841910146256242328924544641$$

$$B = 196503076295643052858681214356932539158308401746008315969770 7$$

a の末尾の数は 7 になることを証明したい.

$m = 1$ なので $2q = 3^{e+1} + 1$ になる.

1. $e = 4k + 3$.

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

$q = 1 + 5L$ となり L は偶数なので $q \equiv 1 \mod 10$.

$$a = 3^e q \equiv 2q \equiv 2 \mod 5.$$

$a = 2 + 5L'$ となるが a は奇数なので L' も奇数. よって $a \equiv 7 \mod 10$.

2. $e = 4k + 1$. $B = 3^{2k+1} = - = (-3)^{2k+1}$.

$2q = 3^{e+1}+1 = 3^{4k+2}+1 = 1-(-3)^{2k+1} = 4D, D = (-3)^{2k}+\cdots+1$.

q は素数に反する.

3. $e = 4k + 2$.

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

今のところここから矛盾が出ない. 計算例が4つしかないので,何とも言えない.

$m = 2$ なら解無し. これは当然である. $q = \frac{3^{e+1}+3}{3}$ の右辺は3 の倍数だから,素数にならない.

9.2 $p = 3.m = 3$

$p = 3.m = 3$ のときは $q = \frac{3^{e+1}+5}{2}$.

表 14: $m = 3$

e	素因数分解	a
3	$3^3 * 43$	1161
5	$3^5 * 367$	89181
9	$3^9 * 29527$	581179941
59	A	B

$A = 3^{59} * 21195579137608101757147216603$

$B = 299501716652405201735529971620260138517926107518220545401$

$q \equiv 3, 7; a \equiv 1 \mod 10$ を示してほしい.

9.3 $p = 3.m = -2$

$p = 3.m = -2$ のときは $q = \frac{3^{e+1}-5}{2}$.

表 15: $m = -2$

e	素因数分解	a
2	$3^2 * 11$	99
6	$3^6 * 1091$	795339
8	$3^8 * 9839$	64553679
30	A	B
44	C	D
48	E	F

$A = 3^{30} * 308836698141971$

$B = 6358673741282379054361 1413179$

$C = 3^{44} * 147715635327541684 9319$

$D = 1454660594681285404312770985990662195258039$

$E = 3^{48} * 1196496646153087647 95039$

$F = 95440281617039135377120437277001091650606 66079$

さて

- q の末尾の数は 1,9.
- a の末尾の数は 9.

正しいか? 証明できるか?

9.4 $p = 3.m = -3$

$p = 3.m = 3$ のときは $q = \frac{3^{e+1}-7}{2}$.

表 16: $m = -3$

e	素因数分解	a
3	$3^3 * 37$	999
11	$3^{11} * 265717$	47070969399
17	$3^{17} * 193710241$	25015772097509283
25	$3^{25} * 1270932914161$	1076846981534813373022323

$2q = 3^{e+1} - 7, a = 3^e q$ が成り立つ.

1. $e = 4k + 3$.

$2q = 3^{e+1} - 7 \equiv 1 - 7 = -6 \equiv 4 \mod 5$ によって $q \equiv 2 \mod 5$. q は奇数なので $q = 2 + 5(2L + 1) = 7 + 10L$. したがって $q \equiv 7 \mod 10$.

$$a = 3^e q \equiv -3 \times 7 = -21 \equiv 4 \mod 5.$$

だから $a = 4 + 5L = 4 + 5(2L' + 1) \equiv 9 \mod 10$.

2. $e = 4k + 1$.

$2q = 3^{e+1} - 7 \equiv -1 - 7 = 2 \equiv 6 \mod 5$ によって $q \equiv 1 \mod 5$. q は偶数なので $q = 1 + 5(2L)$. したがって $q \equiv 1 \mod 10$.

$$a = 3^e q \equiv 3 \mod 5.$$

だから $a = 3 + 5L = 3 + 5(2L') \equiv 3 \mod 10$.

$e = 4k + 1, 4k + 3$ の場合は起きるかどうかわからない

10 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 $a=3^eq$ 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，

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

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 $q=\mathrm{Maxp}(a)$ を使うと公式

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

がえられた．

11 公式を満たす解

11.1 $m = 0$ のとき

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

表 17: $[p = 3, m = 0]$

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

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.

11.2 $m=1$ のとき

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

表 18: $[p=3, m=1]$

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

11.3 $m=-2$ のとき

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

表 19: $[p=3, m=-2]$

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

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

表 20: $[p=3, m=2]$

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

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

11.5　$m = -1$ のとき

表 21: $[p = 3, m = -1]$

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