第1章　素数べき と完全数

1.1　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.

さて, 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が, これを a の関数と見てユークリッド関数と言いたい.

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 $S = \frac{p^4-1}{p-1}$.

これから 一般に $a = p^e$ のとき $\sigma(p^e) = \dfrac{p^{e+1} - 1}{p - 1}$.

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

$$\sigma(a) = \sigma(p^e)\sigma(q^f). \tag{1.1}$$

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.

1.1.1　$\sigma(a)$ の表

$\sigma(a)$ に親しむため a とその素因数分解 , $\sigma(a)$ を横に $\sigma(a)$ にしたがって 並べてみた.

素因数分解がわかれば $\sigma(a)$ は直ちに計算できる.

表 1.1: $\sigma(a)$ の順

a	素因数分解	$\sigma(a)$	a	素因数分解	$\sigma(a)$
2	$[2]$	3	33	$[3,11]$	48
3	$[3]$	4	35	$[5,7]$	48
5	$[5]$	6	47	$[47]$	48
4	$[2^2]$	7	34	$[2,17]$	54
7	$[7]$	8	53	$[53]$	54
6	$[2,3]$	12	28	$[2^2,7]$	56
11	$[11]$	12	39	$[3,13]$	56
9	$[3^2]$	13	49	$[7^2]$	57
13	$[13]$	14	24	$[2^3,3]$	60
8	$[2^3]$	15	38	$[2,19]$	60
10	$[2,5]$	18	59	$[59]$	60
17	$[17]$	18	61	$[61]$	62
19	$[19]$	20	32	$[2^5]$	63
14	$[2,7]$	24	67	$[67]$	68
15	$[3,5]$	24	30	$[2,3,5]$	72
23	$[23]$	24	46	$[2,23]$	72
12	$[2^2,3]$	28	51	$[3,17]$	72
29	$[29]$	30	55	$[5,11]$	72
16	$[2^4]$	31	71	$[71]$	72
25	$[5^2]$	31	73	$[73]$	74
21	$[3,7]$	32	45	$[3^2,5]$	78
31	$[31]$	32	57	$[3,19]$	80
22	$[2,11]$	36	79	$[79]$	80
37	$[37]$	38	44	$[2^2,11]$	84
18	$[2,3^2]$	39	65	$[5,13]$	84
27	$[3^3]$	40	83	$[83]$	84
20	$[2^2,5]$	42	40	$[2^3,5]$	90
26	$[2,13]$	42	58	$[2,29]$	90
41	$[41]$	42	89	$[89]$	90
43	$[43]$	44	36	$[2^2,3^2]$	91

$\sigma(a)$ にしたがって並べた上の表を観察して次のことがわかった.
$\sigma(a)$ に出てこない数として 9,10,11 があり,$\sigma(a)=121$ なる数 a として 6,11 があげられる.
$\sigma(a)=121$ なる数 a として 24,38,59.　こられ数学的に証明してみよう.

1.1.2　$\sigma(a)$ のグラフ

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

図 1.1: $\sigma(a)$

$x = a, y = \sigma(a)$ とおいた.
$a = p > 1$ 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.
$m(\neq p)$ を素数とすると, $a = mp$ 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

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

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

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

の上にある.

$m = 2$ に対して直線 $y = \frac{3a}{2} + 3$,
$m = 3$, に対して直線 $y = \frac{4a}{3} + 4$,
$m = 5$, に対して直線 $y = \frac{6a}{5} + 6$,$\cdots$ などが対応する.

1.1.3　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.

そこで数学の世界ではよくあることだが, 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 $\sigma(a) - 2a = -1$ を満たす自然数を概完全数 (almost perfect number) と呼ぶそうだ.

1.2　完全数

$\sigma(a) = 2a$ を満たす自然数 a を完全数と古代ギリシャの数学者は定義した.

1.2.1　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

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

であり, 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 Nichomchus 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.

完全数は稀少性があり, 6,28,496,8128, などであり, 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が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.

Cardano (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, と述べた.

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.

実際, $q = 2^{e+1} - 1$ 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になることは容易に示されるがこれは不思議で美しい性質である.

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.

P.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 $2n$ で割れることを示した.

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, と述べた.

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.(次項で証明する)

このように偶数の完全数はオイラーによってその形が決められ. しかし, 偶数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依然として未解決の大難問である.

1.2.2　オイラーによる証明

a を偶数完全数とし, $a = 2^e L(e > 0, L :$ 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.

1.2.3　$\sigma(a)-a=1$

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.

私は高校生への研究課題として $a=2p,(p>2$ 素数の 2 倍) になることを $\sigma(a)$ で判定したらどうか. という問題をを出してみた. しかし高校生に聞かれたら適切に答える必要があると反省して事前に自分でして見た.

$a=2p,(p>2$: 素数) のとき

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

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, $a=2p$ の他に 8 も出てくることが証明できた.

$a=2p$ の特徴づけは,8 を例外としてうまくできた. しかし, $a=6p,\ 28p$ の特徴づけは極端に難しいらしく証明できない.

これに関連した問題は高校生でも解け場合があり, また絶対に解けそうもない数多くの問題があるので, 好都合であった.

1.2.4　3 点セット

$\sigma(a)-2a=1$ 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 (3 点セット) はどれも未解決である. 完全数の問題が 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) も解けていない.

ありていに言うと, 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, ということである.

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て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のは大きな励みになる.

1.2.5　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. 次の表では $e+1$ が素数になる場合に限り ,$\sigma(2^e)$ の素因数分解をしている.

素数になる $\sigma(2^e)$ は 7,31,127,8191, 131071,524287,$\cdots$ などであり意外に多い.

これらを メルセンヌ素数という.

$e+1$ は素数とした場合の $\sigma(2^e)$ を メルセンヌ数という.

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

表 1.2: $\sigma(2^e) = 2^{e+1} - 1$:メルセンヌ数数

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

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の証明には, 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.

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 は必ず $\sigma(2^e)$ が素数 q になる $a = 2^e$ を用いて $a = 2^e q$ 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.

ところで a の素因子の個数を $s(a)$ とおくと, 先ほどの奇数完全数の非存在問題は $s(a) < 8$ なら解けているらしい.

1.3　$s(a) = 2$ のときの完全数の証明

ここでは $s(a) = 2$ のときだけ扱う.

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. 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

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

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.

1.4　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. 完全数を m だけ平行移動するとは次の意味である.

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 (狭義の) 完全数という. 結果として m は偶数.

1.5　完全数の数表

表 1.3: 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	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

$A = 2^{30} * 2147483647$

$B = 2305843008139952128$

$C = 2^{60} * 2305843009213693951$

$D = 2658455991569831744654692615953842176$

$E = 2^{88} * 618970019642690137449562111$

$F = 191561942608236107294793378084303638130997321548169216$

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

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. q の末尾の 1 桁は 1 (最初だけ 3), または 7 になるという性質は完全数の歴史では取り上げられていなかった.

1.5.1　$m = 2$

2 だけ平行移動した場合を見てみよう. $q = 2^{e+1} + 1$ が素数の場合

表 1.4: $q = 2^{e+1} + 1$ 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.

$e \geq 3$ のとき $q \equiv 7, a \equiv 6 \mod 10$.
とくに a の末尾の数は 6.
Proof. $e + 1 = 2^r$ により $r \geq 2$ なら $e + 1 = 4N$ と書けるので
$q = 2^{e+1} + 1 \equiv 2 \bmod 5$. 一方, q は奇数なので $2^e \equiv 3 \times 2^{e+1}$ なので $q \equiv 7 \mod 10$.
$a = 2^e * q \equiv 3 * q \equiv 6 \bmod 5$, a は偶数なので $a \equiv 6 \mod 10$.

1.5.2　$m = 4$

$q = 2^{e+1} + 3$ が素数の場合

表 1.5:

$e \bmod 4$	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

$A = 2^{27} * 268435459, B = 36028797421617152$
$C = 2^{29} * 1073741827, D = 576460753914036224$
$E = 2^{54} * 36028797018963971, F = 576460753914036224$
$G = 2^{66} * 147573952589676412931$
$H = 649037107316853507609507569598464$
$I = 2^{83} * 193428131138340667952988 19$
$J = 187072209578355573530071687601903897267059558449152$
$K = 2^{98} * 633825300114114700748351602691$
$L = 2008672555323737844427452615435960632654465462739716318 16704$

表を見ると

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

Proof.

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

$e = 4k + 2$ 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,
$q \equiv 1 + 3 \equiv 4 \bmod 5$, $q \equiv 9 \mod 10$.
$a = 2^e q \equiv 3 * 4 = 12 \equiv 2 \bmod 5$, $a \equiv 2 \mod 10$.

1.5.3　$m = -2$

$q = 2^{e+1} - 3$ が素数の場合これらは指数 e の擬素数 $\mathbf{p}_e$ と呼ばれる. 完全数と比べると数が多い.

表 1.6: $q = 2^{e+1} - 3$ 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
1	93	I	J	2

$A = 2^{19} * 1048573, B = 549754241024$
$C = 2^{21} * 4194301, D = 8796086730752$
$E = 2^{23} * 16777213, F = 140737463189504$
$G = 2^{28} * 536870909, H = 144115187270549504$
$I = 2^{93} * 19807040628566084398385987581$
$J = 1961594292308337738698684194455290145603494810419220971 52$
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,
$q \equiv 3 - 3 \equiv 0 \bmod 5$. $q = 5$.
$q = 2^{e+1} - 3 = 5$; $e = 2$. $a = 2^e q = 4 * 5 = 20$.

1.6　m だけ平行移動した完全数の定義式

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 (狭義の) 完全数ということはすでに紹介したとおりである. 次にこれの満たす方程式を求めよう.

$N = 2^{e+1} - 1$ とおく. $q = N + m$ は素数であることに注意.

$$\sigma(a) = 2^e \sigma(2^e q) = (2^{e+1} - 1)(q + 1) = Nq + N, N + m = q$$

に注意して次の式変形を行う.

$Nq = 2^{e+1}q - q = 2a - q.$

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

かくして $\sigma(a) = 2a - m$ がえられた.

方程式 $\sigma(a) = 2a - m$ の解を平行移動 m の広義の完全数という.

広義の平行移動 m の広義の完全数, すなわち方程式 $\sigma(a) = 2a - m$ の解は, $q = 2^{e+1} - 1 + m$ が素数となる e によって $a = 2^e q$,(とくに $s(a) = 2$ となるか, という問題を考えよう.

一般的に言って m が少し大きいと反例が出やすい.

$m = 2$ では反例が見つからない, 次に $m = 4$ の場合を扱う.

1.6.1　$\sigma(a) = 2a - 4$ の場合

$\sigma(a) = 2a - 4$ を満たす解の表を作った.

$a = 110, a = 884, a = 18632$ は解だが $s(a) = 3$.

表 1.7: $\sigma(a) = 2a - 4$

a	素因数分解	$\sigma(a)$
5	$[5]$	6
14	$[2, 7]$	24
44	$[2^2, 11]$	84
110	$[2, 5, 11]$	216
152	$[2^3, 19]$	300
884	$[2^2, 13, 17]$	1764
2144	$[2^5, 67]$	4284
8384	$[2^6, 131]$	16764
18632	$[2^3, 17, 137]$	37260

第2章　底が３の場合

2.1　3^e のとき

完全数では $\sigma(2^e) = 2^{e+1} - 1$ が基本的な役割を演じたので $A = 3^e$ とおき, $\sigma(A) = \sigma(3^e)$ を計算する.

$\sigma(A) = \sigma(3^e) = \frac{3^{e+1}-1}{2}$, なので $2\sigma(A) = 3^{e+1} - 1 = 3A - 1$.

そこで A を a に置き換えた式 $2\sigma(a) - 3a = -1$ を満たす a は何かを問題とする.

これだけを単独で考えるのはもったいないので 3 点セットにして

(1) $2\sigma(a) - 3a = -1$ を満たす自然数は何か,

(2) $2\sigma(a) - 3a = 1$ を満たす自然数は何か,

(3) $2\sigma(a) - 3a = 0$ を満たす自然数は何か

を問題にする.

2.1.1　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 2.1: $2\sigma(a) - 3a = -1$

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]

この場合は期待に応えて 3 のべきが並んで出てきた. 言い換えれば $s(a) = 1$ の解だけである.

$s(a) = 1$ を仮定したとき 3 のべきになることはすぐわかる.

2.1.2　$s(a)=2$ のときの証明

$s(a)=2$ を仮定して $2\sigma(a)=3a-1$ を満たすとき矛盾を導こう.

最初に a は奇数であることを確認する. なぜなら -1 は奇数で,$2\sigma(a)$ は偶数だから.

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

$$\frac{2AB}{\rho'}=3XY-1.$$

書き直して

$$2AB=3\rho'XY-\rho'.$$

$2AB-3\rho'XY$ の XY の係数を R とおけば

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

$-\rho'+pX+qY-1=RXY$ によって $R>0$.

$q>p\geq 3$ と $0<R=6-(p-3)(q-3)$ により $p=3, R=6$. $\rho'=2\overline{q}$ となり

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

を 2 で割って

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

移項して $(3X-q)Y-3X+1+\overline{q}=0$ により

$$(3X-q)Y-3X+q=(3X-q)(Y-1)=0.$$

$3X=q$ となり矛盾.

$s(a)\geq 3$ のときも矛盾が導けるとよいのだが, 難しそうである.

2.2　$2\sigma(a)-3a=0$ の場合

表 2.2: $2\sigma(a)-3a$ を順に並べる

a	素因数分解	$\sigma(a)$	$\sigma(a)-2a$	$2\sigma(a)-3a$
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
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.
実はこのことを簡単に証明できた.

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 $N = 2^{e+1} - 1$ とおくと

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

$L > 1$ なら $\sigma(L) > L$ なので

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

これより $3L > NL + 4N$, $N \geq 3$ 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. これは大変うれしい.

2.3　$2\sigma(a)-3a=1$ 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.

表 2.3: $2\sigma(a)-3a=1$

a	$\sigma(a)$	素因数分解
21	32	$[3,7]$
2133	3200	$[3^3,79]$
19521	29282	$[3^4,241]$
176661	264992	$[3^5,727]$
129127041	193690562	$[3^8,19681]$

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

$a=3^e*q,(q>3:$ 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

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

$(3^{e+1}-1)q+3^{e+1}-1\quad=3^{e+1}q+1$ となるので $3^{e+1}q$ が消えて

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

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.

2.4　亜完全数

このような $a=3^e*q$ 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.

2.5　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.

与えられた W は適当に小さいとして $W=2\sigma(a)-3a$ を満たす a を仮定 $s(a)=2$ の下でこれを求めよう.

$s(a)=2$ と仮定したので a を素因数分解し $a=p^eq^f$ とする.

2.5.1　亜完全度が奇数の場合

W は奇数と仮定する.
$W = 2\sigma(a) - 3a$ によって a は奇数. したがって $2 < p < q$ となる.
$X = p^e, Y = q^f$ とおくと $a = XY$ となる. すると

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

であり,$A = pX - 1, B = qY - 1, \rho' = \overline{pq}$ とおけば $2\sigma(a) = W + 3a$ に注意すると,

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

書き直して

$$2AB = \rho'(3XY + W)$$

$2AB - 3\rho' XY$ の XY の係数を R とおくとき $R = 2pq - 3\rho'$ になりさらに

$$\begin{aligned} R &= 2pq - 3\rho' \\ &= -pq + 3(p + q - 1) \\ &= -(p-3)(q-3) + 6. \end{aligned}$$

それから $\rho' W = 2AB - 3\rho' XY$ により

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

$\rho' W + 2(pX + qY - 1) = RXY$ によって $RXY > \rho' W + 2(p^2 + q^2 - 1) > 0$ により $R > 0$ なので $p \geq 3$ に注意し $p = 3, R = 6$.
このとき $\rho' = 2\overline{q}$ になり

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

移項し 2 で割って

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

(1) $Y = q$ と仮定すると

$$\overline{q} W = (3X - q)q - 3X + 1 = 3X\overline{q} - \overline{q}(q + 1)$$

により, $\overline{q}$ を払うことによって

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

ここで話を逆転させる. $3X - W - 1$ が素数のときこれを q とおいて $a = 3^e q$ を定めれば亜完全度 W の数 a を得るのである.

とくに $W = -1$ なら $3X = q$ が素数なので $X = 1, q3$. この場合は起きない.
$W = 1$ なら $q = 3^{e+1} - 2$ が素数なので,$a = 3^e q$ は亜完全数.
(2) $Y > q$ とすると $Y \geq q^2$. ページ数の関係でここまで.

2.6　3 のべきとそのユークリッド関数の値

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

表 2.4: $3^e = a$

$3^e = a$	$\sigma(a)$	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 q になるのは $q = 13, 1093, 797161$ 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.

$a = 3^e q = 9 * 13 = 117, 729 * 1093 = 796797$ などは完全数の類似とみなすことができる.

2.7　3 を底とする完全数

$\sigma(3^e)$ が素数 q になったとする. このとき $\alpha = 3^e q$ を 3 を底とする完全数と言う.

2.7.1　3 を底とする完全数の数表

表 2.5: 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

$A = 3^{70} * 375473325748986240197335797912877 3$

$B = 939868122326695556888433629151289424673228917359519725450340403327 7$

$C = 3^{102} * 695759652988215296899222525183588718147845154701 3$

$D = 3227209964841878447466193062734722465975186449738511$

$- - 2062067563800310073569424269938090581449997117$

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.

言い換えると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 a は奇数. L は偶数になるので $a \equiv 1 \mod 10$.
$a = 3^e q \equiv -q \equiv 2 \mod 5$ により $a = 2 + 5L$. L は奇数になるので $a \equiv 7 \mod 10$.

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.

2.7.2　3 を底とする完全数の公式

普通の完全数では $\sigma(a) - 2a = 0$ を満たす数 a を完全数という.

a が偶数の場合, オイラーにより $a = 2^e\sigma(2^e)$;(ただし,$\sigma(2^e)$ は素数) と書けることが証明された.

ここではオイラーの与えた形から出発し $A = 3^e$ とおき $\sigma(A)$ が素数 q になったとき $\alpha = Aq = 3^eq$ を 3 を底とする (狭義の) 完全数と呼ぶことにした. ここが少しずるい.

そこで $\sigma(\alpha)$ を計算する.

$$\sigma(\alpha) = \sigma(A)\sigma(q) = \sigma(3^e)\sigma(q) = \sigma(q)(q+1)$$

になる. $q = \sigma(A) = \underline{\underline{3A}}12$ より

$$q + 1 = \frac{3A+1}{2}.$$

なので

$$\sigma(\alpha) = \sigma(A)(q+1) = \frac{\sigma(A)(3A+1)}{2} = \frac{(3\alpha+q)}{2}.$$

これから

$$2\sigma(\alpha) = 3\alpha + q.$$

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.

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

すると次の大きな問題はこの公式を満たす上の市 k を満たす α は $\sigma(3^e)$ が素数 q になるのを用いて $\alpha = 3^eq$ 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案外反例をつくりやすい.

2.7.3　$s(a) = 1$ 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 $Y = 8$. よって $a = 8$.
このように素因子が 1 つ, 言い換えれば $a = p^e$ と書ける解を微小解という.

2.7.4　$s(a)=2$ 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 $a=p^eq^f(2<p<q)$ 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

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

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. $a=3^eq$ 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.

2.8　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.

2.8.1　$m=1$

$m=1$ のとき

表 2.6: $m=1$

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

$X=57228063671541905627967299 0187$

$A=3^{63}*1716841910146256242328924544641$

$B=19650307629564305285868121435693253915830840174600831596977 07$

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 $q\equiv 1 \mod 10$.

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

$a=2+5L'$ 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.

2.8.2　$m = 3$

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

表 2.7: $m = 3$

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

$A = 3^{59} * 211955791376081017571472166 03$

$B = 2995017166524052017355299716202601385179261075182205454 01$

2.8.3　m だけ平行移動した完全数の公式

$q = \dfrac{3^{e+1}-1}{2} + m$ が素数 q のとき $a = 3^e q$ とおく. これの満たす方程式を決定しよう.

$N = 3^{e+1} - 1$ とおく. $q = \dfrac{N}{2} + m$ により, $N = 2(q-m)$.

$\sigma(a) = \sigma(3^e)\sigma(q) = \dfrac{N(q+1)}{2}$, $Nq = 3a - q$ により

$$2\sigma(a) = Nq + N = 3a - q + N = 3a - q + 2(q-m) = 3a + q - 2m.$$

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.

この式を満たす解を　3 のべきを基本とした (広義の)m だけ平行移動した完全数という　.

2.8.4　広義の完全数

$m = 0$ のときの方程式は簡単である.

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

表 2.8: $2\sigma(a) = 3a + \mathrm{Maxp}(a)$

a	$\sigma(a)$	素因数分解
4	$[2^2]$	7
117	$[3^2, 13]$	182
796797	$3^6 * 1093$	1195742

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.

Wieferch 素数

3 番目に出たの素数 1093 は Wieferch 素数である.

ただし, $2^p \equiv 1 \mod p^2$ を満たす素数 p を Wieferch 素数という. 1093,3511 がただ 2 個しか知られていない. (2 個しかないという理論が無い以上もっとあるだろう)

表 2.9: $2\sigma(a) = 3a + \mathrm{Maxp}(a) - 2$

a	素因数分解
15	$3 * 5$
741	$3 * 13 * 19$
1107	$3^3 * 41$
14883	$3 * 11^2 * 41$
38781	$3^2 * 31 * 139$

2.8.5　$m = 1$

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

特色がない解があるのだろうか.
$a = 3^e$　q(q:素数) の形の解を 正規形 $a = 15 = 3 * 5, a = 3^3 * 41$ がその例
$a = 3^e$　rq(r, q:2 素数) の形の解を 第 2 正規形
$a = 74 = 3 * 13 * 19, a = 38781 = 3^2 * 31 * 139$ がその例
$a = 14883 = 3 * 11^2 * 41$ はレアな形で私は ヒトコブ と呼びたい.

2.9　$m = 2$ と素数のべき

$2\sigma(a) = 3a + \mathrm{Maxp}(a) - 4$
ここでは 3 のべき 3^e はみな解になる. 実際, $a = 3^e$ とおくとき,

$$2\sigma(a) - 3a - \mathrm{Maxp}(a) = (3^{e+1} - 1) - 3^{e+1} - 3 = -4.$$

その上,3^e とあまりにも異質な解 (エイリアン解)
$a = 99807 = [3, 17, 19, 103]$,$a = 603681 = 3 * 13 * 23 * 673$
が出たことに, 私は鳩が豆鉄砲をくらったような気がした. ところで, ほかにエイリアン解はあるのだろうか.

表 2.10: $2\sigma(a) = 3a + \mathrm{Maxp}(a) - 4$

a	素因数分解
3	$[3]$
9	$[3^2]$
27	$[3^3]$
81	$[3^4]$
243	$[3^5]$
729	$[3^6]$
2187	$[3^7]$
6561	$[3^8]$
19683	$[3^9]$
59049	$[3^{10}]$
99807	$[3, 17, 19, 103]$
177147	$[3^{11}]$
531441	3^{12}
603681	$[3, 13, 23, 673]$
1594323	3^{13}

第3章　究極の完全数

3.1　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 の完全数と呼ぼう. このとき $q = \frac{P^{e+1}-1}{\overline{P}}$ となる. これを究極の完全数と呼ぶ. 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.

次に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.
究極の完全数の満たす方程式を作る.

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

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.

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

これより

$$\overline{P}\sigma(a) - Pa = (P - 2)\mathrm{Maxp}(a) - m(P - 1). \tag{3.1}$$

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

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

3.1.1　$s(a)=1$ のときの微小解

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. そこで $s(a)=1$ のときの解を求めよう. ($s(a)=1$ のときの解を微小解という.)
$a=q^f$ 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

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

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. $P-1=wq$ なので

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

$\overline{P}=wq$ により 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

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

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

$w=1$ のとき.
$P=1+q$ となり P,q はともに素数だから $q=2,P=3,Y=2^f$.
$2\sigma(a)=3a+2$ なので $a=Y=2^f$. よって $2(2Y-1)=3Y+2$. 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

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

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

$f \geq 3$ のとき.

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

変形して

$$q^3 - q^2 \leq 1 - q.$$

これは矛盾.

$f = 2$ のとき

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

$q^2 - q(q-1) - 1 = q - 1, w\overline{q} = \overline{q}^2$ によって $w = \overline{q}$.

$P - 1 = wq = q(q-1)$ により $P = 1 + q(q-1)$.

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.

3.1.2　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.

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きた. 実に不思議なことである.

表 3.1: P, q が素数

q	P
2	3
3	7
7	43
13	157
67	4423
79	6163
139	19183
151	22651
163	26407
193	37057

3.2　$a = 5^e$ 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
$\sigma(a) = \sigma(P^E) = \frac{aP-1}{\overline{P}}$ 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.

表 3.2: $4\sigma(a) - 5a = -1$

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.

3.2.1　$s(a)=2$ 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,

$$(R_1X - 2q)Y = 6X - q - 1 \geq (R_1X - 2q)q^2 = ((5 + q)X - 2q)q^2 = (5 + q)Xq^2 - 2q^3.$$

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

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.