書泉グランデでの講義 Renewal Open 高校生もわかる新しい数論研究 第1期　資料1 予稿1; 完全数の水平展開

飯高 茂

2016 年 10 月 14 日

1　はじめに

神田の老舗である書店: 書泉グランデの７階で 「高校生もわかる新しい数論研究」と題名をつけ金曜日の夜 6:30-8:30 まで一般の方を対象に講義をすることになった.

受講者が集まるかどうか, さらには継続して受講者が来てもらえるかどうか. いろいろ心配の種を抱えて始まった.

8 回続けたいと思いつつ 2014 年 10 月から始めたのだが, 内心では 4 回くらいで参加者がいなくなり打ち切りの事態になるかもしれない, と考えていた.

幸いにして, 20 名前後の熱心な受講者が毎回あり, 彼らと彼女らに励まされて１年 12 回の講義ができた．これを一応の区切りと考え,2015 年 10 月から新たに New Series 「高校生もわかる新しい数論研究」として始めた．それまでの講義内容はご破算にし最初から話すことにし新しく始めた. その結果２年目から入る受講生が多, 継続の受講生も私自身も大いに励まされた.

第 2,4 金曜の講義を２ヶ月続け, 次の２ヶ月はお休みにした. こうして 4ヶ月で 4 回を１クールにして１年間で３クール, 計 12 回の講義が定着した.

2016 年 10 月は 3 年目のスタートになるので模様替え開店のスーパーのように Renewal Open としてはじめることとした.

2　素因数分解の定理

自然数の世界で素因数分解の一意性定理が成り立つことはユークリッドらが証明込みで知っていたことであるが１８世紀の終わりごろガウスがこの定理の証明が不完全であることを嘆いて次の結果を D.A. で証明している.

補題 1 p が素数で a, b 自然数のとき $ab \equiv 0 \mod p$ なら $a \equiv 0$ または $b \equiv 0 \mod p$.

Proof.

背理法で示す:

$ab \equiv 0 \mod p$ のとき $a \not\equiv 0$ かつ $b \not\equiv 0 \mod p$ を仮定する.

ここで, a, p を固定して考える. 上記を満たす b の中で最小に選ぶ. p を b で割るときその商とあまりを 自然数 Q と r で示すと $p = bQ + r, r < b$.

$ab = pm$ と書いてから $p = bQ + r, r < b$ を a 倍すると

$$ap = abQ + ar = pmQ + ar.$$

$p(a - mQ) = ar$ なので $m' = a - mQ$ とおくとき $ar = pm', 0 \leq r < b$.

b は最小値なので $r = 0$.

ゆえに $p = bQ$. p は素数なので $Q = 1; p = b$. 仮定:$b \not\equiv 0 \mod p$ に反する.

$R = Z$ を整数環とする. 環論のことばを使うと $J = pR$ を p の倍数イデアルとすると, J が素イデアルになる.

これがガウスの補題の意味である.

ユークリッド以来の伝統的な証明法は素数 p に対し, イデアル $J = pZ$ が極大イデアルになることを示す.

a が $J = pZ$ に属さないとき p で割れない. a と p の最大公約数は 1 なので互除法によって $1 = am + pn$ を満たす整数 n, m がある.

これは a と J の生成するイデアルが全体になることを意味する.

したがって, J は極大イデアル. よって J は素イデアル.

素因数分解の一意性定理

定理 1 自然数 n を素数の積で表す.

$$n = p_1 p_2 \cdots p_s (p_1 \leq p_2 \leq \cdots \leq p_s), p_j : \text{素数}$$

さて別の方法で n を素数の積で表す.

$$n = q_1 q_2 \cdots q_t (q_1 \leq q_2 \leq \cdots \leq q_t), q_j : \text{素数}$$

このとき

$$s = t, p_1 = q_1, \cdots, p_s = q_s$$

Proof

これを s についての帰納法で示す.

$s=1$. n は素数なのでさらに分解できないから $n=q_1$.

$s>1$ のとき $s-1$ の場合を仮定する.

$p=p_1, m=p_2\cdots p_s$ とおくと $n=pm$.

$q=q_1, k=q_2\cdots q_t$ $n=qk$.

$pm=qk$ なので $qk\equiv 0 \mod p$ なので 1) $q\equiv 0$ または 2) $k\equiv 0 \mod p$.

1) $q\equiv 0 \mod p$ なら p,q : 素数により,$p=q$. したがって $p_1=q_1$. さらに $m=k$. m の素因子の個数は $s-1$.

したがって帰納法の仮定が使えて, $s-1=t-1, p_j=q_j (j>1)$.

2) $k\equiv 0 \mod p$. p は k の素因子なので $p=q_j (j>1)$. ここで $j=2$ と仮におくと

$$p=q_2, p_2\cdots p_s=q_1q_3\cdots q_t$$

$s-1=t-1$ なので $s=t$. $p_2=q_1, p_3=q_3, \cdots$.

$p_1\leq p_2=q_1, q_1\leq q_2=p_1$. よって $p=p_1=q_1=q$. これは矛盾.

最近は高校数学でも整数の性質を扱い数の合同関係も触れられている. しかし素因数分解の一意性定理に言及はあるもののその証明は載っていない. そこで, 簡単に証明を述べた.

3 完全数

a を自然数とするときその約数の和を $\sigma(a)$ と書く. これを a の関数とみてユークリッド関数という.

a,b が互いに素なら

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

が成り立つ. これをユークリッド関数の乗法性という.

$\sigma(a)=2a$ を満たす数 a を 完全数 (perfect numbers) という.

$6, 28, 496, 8128$ などがあり古代の数学者ユークリッドによって考えられた.

これらの数は末尾が 6 , または 8 でこれが交互に繰り返される.

これらを素因数分解すると

$$6=2*(2^2-1), 28=2^2*(2^3-1), 496=2^4*(2^5-1), 8128=2^6*(2^7-1)$$

などとなる. 5 番目の完全数が 15 世紀に発見された. 33550336 という 8 桁の数である.

$$33550336 = 2^{12} * (2^{13} - 1)$$

これは覚えやすい数の配列である. 末尾の数はまたしても 6 であった.

2 のべきから 1 引いた $Q = 2^{e+1} - 1$ が素数になるとき $a = 2^e Q$ は完全数 (perfect numbers) でありとくにこの形の数をユークリッドの完全数という.

$Q = 2^{e+1} - 1$ とかける素数 Q をメルセンヌの素数という.

一般に $2^{e+1} - 1$ が素数になるとき $e + 1$ は素数になることが証明できる.

4 ユークリッド

ユークリッド (エウクレイデス),『ユークリッド原論』(By Wikipedia) 第 9 巻, 命題 36 は次のようなものである.

もし単位から始まり順次に 1 対 2 の比をなす任意個の数が定められ，それらの総和が素数になるようにされ，そして全体が最後の数にかけられてある数をつくるならば，その数は完全数であろう.

[解説]

古代ギリシャの数学では 単位は 1 を指す.

1 から始まり, 順次 2 倍する. 任意個の数を n 個とする.

$$1, 2, 2^2, 2^3, \cdots, 2^{n-1}$$

それらの総和

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}$$

は等比数列の和の公式により

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1.$$

総和を p と書き素数と仮定する.

総和 p を 最後の数である 2^{n-1} とかけた数を a とおくとこれは完全数になる.

例

$n = 3$

$Q = 1 + 2 + 4 = 7$ は素数. $4 * 7 = 28$ は完全数

$n = 5$ の場合は各自やってみよう.

2 のべきから 1 引いた $Q = 2^{e+1} - 1$ が素数になるとき $a = 2^e Q$ は完全数でありとくにこの形の数をユークリッドの完全数という.

これを確認しよう. ユークリッド関数の乗法性によって,

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

2 のべきから 1 引いた $Q = 2^{e+1} - 1$ が素数になるとき $a = 2^e Q$ は $\sigma(a) = 2a$ を満たす. すなあちこれらは完全数 (perfect numbers) でありとくにこの形の数をユークリッドの完全数という.

$Q = 2^{e+1} - 1$ とかける素数 Q をメルセンヌの素数という.

一般に $2^{e+1} - 1$ が素数になるとき $e + 1$ は素数になることが証明できる.

$Q = 2^{e+1} - 1$ が素数になるという条件をはずして, $e + 1$ が素数になるという条件のみをつけるとき $a = 2^e Q$ を弱い完全数 (weakly perfect numbers) ということにする.

4.1 弱完全数

表 1: $P = 2$:弱完全数

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

* 非完全数 を指す.

弱完全数でも末尾の数は 6, 8 であり昔の数学者はなぜだろう, と神秘的な性質に打たれたらしい.

なおかつ $Q=2^p-1$ 末尾の数は (はじめの数 3 を除くと) 1,7 でありこれも不思議である.

最近 (2015 年 9 月 17 日)49 個目の完全数が発見された.
$e=74,207,281, q=2^e-1$: 素数で $a=2^e q$ がそれである.

4.2 Weil の見解

一方, プロの数学者は完全数を歓迎しない. たとえば A.Weil は『数論　歴史からのアプローチ』 足立恒雄・三宅克哉訳、日本評論社、1987 年。p6, 第 1 章 § III, で次のように完全数を軽んじる発言をしている.

ギリシャのみならずそれ以前においても, 完全性という観念が, そのすべての約数の和が自分自身と一致するような整数に結び付けられていた.
ユークリッドの数論に関する巻の最後の定理において $2^n(2^{n+1}-1)$ はその第二因子が素数であるときには完全数であることが主張されている;
著者自身も, これがその数論的な諸結果の中の白眉であると見ているように思える.　この題目とそれに伴って現れるいくつかのものは, 後世の著作にも散発的に顔を出す; 恐らくこれらの概念に付された呼称が特別な興味を惹くのだろう.
フェルマの同時代の人達、メルセンヌやフェルニクル、それにフェルマ自身も結構面白がっており、彼の初期の研究においてはそれなりの位置を占めていたことも事実である.(中略) しかし理論的にはほとんど意味のないものであり, このような歴史的事実がなければ, ここに取り上げる必要もなかったろう.

私は大学を退職後, 一般の市民を対象に「数学の研究をはじめよう」をスローガンにして公開の数学研究講座を開いている. そこでも完全数に関連した話しは歓迎される.
完全数についての一般的疑問:
1) 完全数は無限にあるか,
2) 奇数の完全数は無限にあるか
については現代数学は何も答えることができない.

2300 年後の数学者が解けない問題が完全数の問題である. これだけでも不朽の価値があるが, 完全数の一般化をするとそこから多くの興味ある問題が出てくる.

5　完全数の平行移動

m だけ平行移動した完全数とは何か.

$q = 2^{e+1} - 1 + m$: 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.

これは $\sigma(a) = 2a - m$ を満たす.

proof.

$a = 2^e q$ について

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

$$(2^{e+1} - 1)(q + 1) = 2^{e+1}q - q + 2^{e+1} - 1 = 2a - m$$

かくしてえられた

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

を m だけ平行移動した完全数の方程式という.

ここで話しを反転させて方程式 $\sigma(a) = 2a - m$ の解を考える. この解を m だけ平行移動した (広義の) 完全数という.

この方程式は $m = 0$ が古典的な完全数の定義に出る式である.

(広義の) 完全数のは (狭義の) 完全数となるかという問題は奇数完全数の存在予想と同等でこれは 2300 年経っても解けない難問である.

m だけ平行移動した (広義の) 完全数を研究することを完全数の水平展開 という. ここでは多くの興味ある例と課題があるが, 完全な解決にはほど遠い.

6　オイラーの証明

a が偶数のとき $\sigma(a) = 2a$ の解はユークリッドの完全数になることをオイラーが証明した.

やや一般にして 方程式 $\sigma(a) = 2a - m$ の解 a が偶数になると仮定してみよう.

a が偶数になるとしたのだから $a = 2^2 L, (L$:奇数$)$, の形に書く.

$\sigma(a) = (2^{e+1} - 1)\sigma(L)$, $2a - m = 2^{e+1}L - m$ なので, $N = 2^{e+1} - 1$ とおくとき $\sigma(a) = N\sigma(L), 2a - m = (N + 1)L - m$ によって

$$N\sigma(L) = (N + 1)L - m$$

これより

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

$d = \sigma(L) - L$ とおけば $Nd = L - m$.

ここから $m = 0$ に限定する.

$Nd = L$ なので d は L の約数になる

($m \neq 0$ のときはここから何もできない. そしてオイラーを参考にしても何も出てこないと悟る破目になる).

1. $1 < d < L$

$\sigma(L)$ は約数の和であり, 少なくとも $d, 1, L$ は約数なので,

$$\sigma(L) \geq 1 + L + d.$$

$d = \sigma(L) - L$ なので $d + L = \sigma(L)$ により

$$\sigma(L) \geq 1 + L + d = 1 + \sigma(L).$$

これは矛盾.

2. $d = 1$

$Nd = L$ なので $2^{e+1} - 1 = N = L$.

$1 = d = \sigma(L) - L$ によって, $\sigma(L) = L + 1$. これは L の約数は $1, L$ のみを意味するので. 定義によって, L は素数 $p.2^{e+1} - 1 = N = L = p, a = 2^e p$. これはユークリッドの完全数である.

3. $d = L$. $N = 1$ なので $e = 0$. a : 偶数の仮定に反する.

7　完全数の水平展開の俯瞰

$a \leq 2000$ について m が小さい場合の数表を最初に見てみよう.

表 2: $\sigma - 2a = -1$; 2 のべき

a	factor	σ	m
2	$[2]$	3	1
4	$[2^2]$	7	1
8	$[2^3]$	15	1
16	$[2^4]$	31	1
32	$[2^5]$	63	1
64	$[2^6]$	127	1
128	$[2^7]$	255	1
256	$[2^8]$	511	1
512	$[2^9]$	1023	1
1024	$[2^10]$	2047	1

表 3: $[P = 2, m = 0]$ 完全数

a	factor	σ	m
6	$[2, 3]$	12	0
28	$[2^2, 7]$	56	0
496	$[2^4, 31]$	992	0

8　$m \geq 0$ の場合

$m = 0$ なら完全数の式である.

$m = 2$ ならフェルマ素数が出てくる.

8.1　$[P = 2, m = 0]$ 完全数

次の結果はパソコンで $\sigma(a)$ の定義をそのまま用いて完全数の方程式 $\sigma(a) - 2a = 0$ となる a を 2 から 10,000,000 まで調べた結果である.

表 4: $[P = 2, m = 0]$ 完全数

a	素因数分解
6	$2 * 3$
28	$2^2 * 7$
496	$2^4 * 31$
8128	$2^6 * 127$

$a = 2^e q, (q = 2^{e+1} - 1 :$ メルセンヌ素数) の形.

一般に解 $a = 2^e q, (q :$ 素数) の形になす解を正規形とよぶ.

正規形 $2^e q$ が $\sigma(a) = 2a - m$ を満たすなら $q = 2^{e+1} - 1 + m :$ 素数となる.

$m = 0$ のとき広義の完全数は正規形になる, というのが古代の数学者の抱いた夢の 1 つで, 偶数の場合に解決したのがオイラーである.

これは言い方を変えれば広義の完全数は狭義の完全数になるという予想になる.

8.2　$[P = 2, m = 2]$ 完全数

表 5: $[P = 2, m = 2]$ 完全数

a	素因数分解
3	3
10	$2 * 5$
136	$2^3 * 17$
32896	$2^7 * 257$
2147516416	$2^{15} * 65537$

$a = 2^e q, (q = 2^{e+1} + 1 :$ フェルマ素数)

フェルマ素数 3,5,17,257,65537 が出てくる. これらはいわゆるフェルマ素数 5 兄弟である.

$m=2$ のとき広義の完全数は狭義の完全数になる, ということは正しそうである.

a が偶数に限ってでもこのことを証明したいができない.

以下広義の完全数に限って計算した結果を載せる.

8.3 $[P=2, m=4]$ 完全数

表 6: $[P=2, m=4]$ 完全数

a	素因数分解
5	5
14	$2*7$
44	2^2*11
110	$2*5*11$
152	2^3*19
884	$2^2*13*17$
2144	2^5*67
8384	2^6*131
18632	$2^3*17*137$
116624	$2^4*37*197$

正規形 $2^e q$ 以外に非正規形の解が次のように登場する.

$a=884=2^2*13*17$

$a=18632=2^3*17*137$

$a=116624=2^4*37*197$

これらは $2^e rq (r<q: primes)$ 形

$\sigma(a)=2a-$ を満たす.

かくして, $m=4$ の場合は広義の完全数で狭義の完全数にならないものが出てきた.

$m=0,2$ の場合のように, 広義の完全数は狭義の完全数になるという予想の反例がいくつもでたきた.

これを安易に予想をたてるものではない，という理解につなげてはいけない.

広義の完全数の解はコンピュータの計算によると千万以下の a については $2^e q, 2^e rq$ と書けている. これはいつも正しいか ?. これは大難問であると思う.

8.4 解 $a = 2^e qr$ を求めるアルゴリズム

$\sigma(a) = 2a - m$ の解として $a = 2^e qr (2 < q < r$:素数) があるとする.

$$\sigma(a) = (2^{e+1} - 1)\widetilde{qr}, 2a - m = 2^{e+1} qr - m$$

により $N = 2^{e+1} - 1, \Delta = q + r$ を使うことにより

$$N\widetilde{qr} = 2^{e+1} qr - m.$$

$\widetilde{qr} = qr + \Delta + 1$ なので

$$N(qr + \Delta + 1) = (N + 1)qr - m.$$

ゆえに

$$-qr + N(\Delta + 1) = m$$

$q_0 = q - N, r_0 = r - N$ を用いると $q_0 r_0 = qr - N\Delta + N^2$ なので,

$$q_0 r_0 = N(N + 1) + m.$$

$D = N(N + 1) + m$, とおけば, $q_0 r_0 = D$.

そこで与えられた e, m に対し, $D = N(N + 1) + m$, とおき,$q_0 r_0 = D$ ついて,$q = q_0 + N, r = r_0 + N$ ともに素数になれば $a = 2^e qr$ が解.

$N + 1 = 2^{e+1}$ は 4 の倍数なので N(N+1) も 4 の倍数. q_0, r_0 はともの偶数なので

$q_0 r_0$ も 4 の倍数. したがって m 4 の倍数. だから, $m = 2$ には $a = 2^e qr (2 < q < r$:素数) 型の解はない.

はじめに手計算で求める.

i. $e = 1, N = 3, D = 16, r_0 = 2, q_0 = 8, r = 5, q = 13$.

ii. $e = 2, N = 7, D = 60, r_0 = 6, q_0 = 10, r = 13, q = 17$.

iii. $e = 3, N = 15, D = 244, r_0 = 2, q_0 = 122, r = 17, q = 137$.

アルゴリズムを基に swiprolog で作ったプログラムによる解は次のとおり.

$a = 2^2 * 13 * 17$ 884

$a = 2^3 * 17 * 137$ 18632

$a = 2^4 * 37 * 197$ 116624

$a = 2^6 * 137 * 1753$ 15370304

$a = 2^7 * 293 * 1973$ 73995392

$e < 15$ まで調べたが解はこれ以上見つからない.

フェルマ素数 5 兄弟のように,$2^e qr$ と書ける解はこれら 5 個しかないかもしれない.

しかしこれが一般に正しい根拠はなにもない.

8.5 $[P = 2, m = 6]$ 完全数

表 7: $[P = 2, m = 6]$ 完全数

a	素因数分解
7	7
15	$3 * 5$
52	$2^2 * 13$
315	$3^2 * 5 * 7$
592	$2^4 * 37$
1155	$3 * 5 * 7 * 11$

ここの解は非常に特色があり面白い.

正規形の解は $a = 52 = 2^2 * 13$, $a = 5922^4 * 37$

で意外に少ない.

無理して探すと正規形の解はまだまだある.

$a = 2102272 = 2^{10} * 2053$

$a = 9903520314283394042913882112 = 2^{46} * 140737488355333$

さらに非正規形の解がいくつか登場する.

$a = 7$ (a が素数の場合は後でふれる)

$a = 15 = 3 * 5$ ($a = pq$ は $p < q$ 素数の場合は後でふれる)

これは易しい解である.

非正規形の解:

$a = 315 = 3^2 * 5 * 7$, $3 * 5 * 7 * 11$ が 2 つ出てきた.

これは今まで出てこない新種の解である. そこで, モンスターと呼んでみたい.

$a = 315 = 3^2 * 5 * 7$ なのでニックネームをつける.

モンスター 753 を シチゴサンと呼ぶ. これは奇数で $3^e rq$ に書ける.

一方 $a = 1155 = 3 * 5 * 7 * 11$ は小さいほうから奇素数 4 つの積であり, その姿形が美しい. これは和服の帯を連想させるものがあるのでオビと命名しよう.

8.6 オビ $1155 = 3 * 5 * 7 * 11$ の特徴づけ

i. $a = 3 * 5rq(5 < r < q)$: 素数を仮定すると, $r = 7, q = 11$.
Proof
$\sigma(a) = 24\widetilde{r}\widetilde{q}, 2a - 6 = 30rq - 6$ により

$$4\widetilde{r}\widetilde{q} = 5rq - 1.$$

a. $r = 7$ のとき
$32\widetilde{q} = 35q - 1$ により $32 = 3q - 1$. これより $q = 11$.
b. $r \geq 11$ のとき
$4r\widetilde{q} + 4\widetilde{q} = 5rq - 1$ によって

$$4\widetilde{q} + 1 = r(5q - 4\widetilde{q}) = r(q - 1) \geq 11q - 44.$$

$4q + 49 \geq 11q$ により $q < 5$. $q > r \geq 11$ に矛盾.

ii. $a = 3 * q * r * s, (3 < q < r < s)$:素数を仮定するとき, $q = 5, q = 7, r = 11$.
Proof
$q \geq 7$ を仮定して矛盾を導く.
$\sigma(a) = 4\widetilde{q}\widetilde{r}\widetilde{s}, 2a - 6 = 6qrs - 6$ により 2 で割って

$$2\widetilde{q}\widetilde{r}\widetilde{s} = 3qrs - 3.$$

$\Delta_0 = r + s, \Delta_1 = qr + qs + rs, \Delta_2 = q + r + s$ とおくとき
$\widetilde{q}\widetilde{r}\widetilde{s} = qrs + \Delta_1 + \Delta_2 + 1$ なので整理すると

$$2(q\Delta_0 + rs + \Delta_0 + 1) = qrs - 3.$$

$q \geq 7$ を思い出して

$$2(rs + \Delta_0 + 1) + 3 = q(rs - 2\Delta_0 - 2) \geq 7(rs - 2\Delta_0 - 2).$$

$$2\Delta_0 + 5 \geq 5rs - 14\Delta_0 - 14.$$

これより

$$16\Delta_0 + 19 \geq 5sr.$$

r で整理すると

$$r(16 - 5s) \geq -19 - 16s.$$

符号を変えると

$$r(5s - 16) \leq 19 + 16s.$$

$r \geq 11$ により

$$11(5s-16) = 55s - 176 \leq 19 + 16s.$$

ゆえに

$$39s \leq 19 + 176 = 195.$$

$s < 5$ がでて $s \geq r+2 \geq 13$ に矛盾.

iii. $a = pqrs, (2 < p < q < r < s)$:素数を仮定するとき, $p = 3, q = 5, q = 7, r = 11.$.

Proof

$p = 3$ のときは　ii で示したので $p \geq 5$ を仮定して矛盾を導く.

$\sigma(a) = \widetilde{pqrs}, 2a-6 = 2pqrs - 6$ により

$A = \widetilde{qrs}, B = qrs$ とおくと $\sigma(a) = (p+1)A, pqrs = pB.$

$$p(A-2B) = B - A - 6.$$

$C = \widetilde{rs}, D = rs$ とおくとき $A = (q+1)C, B = qD.$

よって,

$$A - 2B = (q+1)C - 2qD = q(C-2D) + C.$$

$$C - 2D = rs + \Delta_0 + 1 - 2rs = -(rs - \Delta_0 - 1) = 2 - \overline{rs} < 0$$

により $A - 2B < 0.$

$$B - A - 6 = p(A-2B) \geq 5(A-2B).$$

$11B - 6 = 11qD - 6 \geq 6(q+1)C$ なので $q(11D - 6C) < 6C + 6.$

$q \geq p + 2 \geq 7$ なので $11D - 6C = 11rs - 6\overline{rs} > 0$ によって

$$7(11D-6C) \leq q(11D-6C) < 6C + 6.$$

$$77D < 48C + 6.$$

$$77D = 77rs < 48(rs + \Delta_0 + 1) + 6.$$

整理して

$$29rs < 48(rs + \Delta_0) + 54.$$

$$r\,(29s - 48) < 48s + 54.$$

$11 \leq r < s$ によって,

$$11\,(29s - 48) = 11 * 29 - 11 * 48 < 48s + 54.$$

ゆえに

$$271s = (11 * 29 - 48)s < 11 * 48 + 54 = 582$$

$s < 5$ となり矛盾.

6 だけ平行移動した完全数で, 4 つの素数の積にかけるものはオビに限る, ことが証明できた.

8.7 シチゴサン $a = 315 = 3^2 * 5 * 7$ の特徴づけ

$a = 3^e qr$ $(3 < q < r:$ 素数$)$ とおくとき $e = 2, q = 5, r = 7$ を示す.

$\sigma(a) = \sigma(3^e qr) = \dfrac{3^{e+1} - 1}{2}\widetilde{qr}, 2a - 6 = 2 * 3^e qr - 6$ なので

$$(3^{e+1} - 1)\widetilde{qr} = 4 * 3^e qr - 12.$$

$N = 3^{e+1} - 1, \Delta = q + r$ とおけば, $\widetilde{qr} = qr + \Delta + 1$.

$$N\widetilde{qr} = 4 * 3^e qr - 12 = \frac{4(N+1)qr}{3} - 12.$$

3 倍して

$$3N\widetilde{qr} = 4(N+1)qr - 36.$$

整理して

$$3N(\Delta + 1) = (N + 4)qr - 36.$$

N で括ると

$$N(3(\Delta + 1) - qr) = 4(qr - 9).$$

$q_0 = q - 3, r_0 = r - 3$ とおくとき
$q_0 r_0 = qr - 3\Delta + 9$. これを用いて $qr - 3(\Delta + 1) = q_0 r_o - 12$. それゆえ

$$N(12 - q_0 r_0) = 4(qr - 9).$$

$r \geq q + 2 \geq 5 + 2, q \geq 5$ なので $4(qr - 9) > 0$.
これより $12 > q_0 r_0$. ここから $q_0 = 2, 3, 4$ に応じて各個撃破する.

i. $q_0 = 2$. $q = 5$ かつ $12 > q_0 r_0 = 2r_0$ により $6 > r_0 = r - 3$. $9 > r \geq q + 2 = 7$.

$q=5$ なので $r_0 \geq q_0+2=2+2=4$. ゆえに $r \geq 7$. したがって ,$q=5, r=7$. $N(12-q_0r_0)=4(qr-9)$ により, $12-q_0r_0=12-4*2=4, qr-9=35-9=26$. $N=26=27-1=3^3-1, N=3^{e+1}-1$ によれば $e=2$. したがって $a=3^2*5*7$.

ii. $q_0=3$. $q=3+3=6$. 素数ではない.

iii.$q_0=4$. $12-q_0r_0=12-4*r_0$ によって, $r_0<3$. $r_0>q_0=4$ に矛盾する.

8.8 $[P=2, m=8]$ 完全数

表 8: $[P=2, m=8]$ 完全数

a	素因数分解
22	$2*11$
130	$2*5*13$
184	2^3*23
1012	$2^2*11*23$
2272	2^5*71
18904	$2^3*17*139$
33664	2^7*263
70564	$2^2*13*23*59$
85936	$2^4*41*131$
100804	$2^2*11*29*79$

$a=130=2*5*13$

$a=1012=2^2*11*23$
は 2^erq 形
$a=18904=2^3*17*139$
は 2^erq 形
$a=70564=2^2*13*23*59$
は $2^er_1r_2q$ 形
$a=85936=2^4*41*131$
は 2^erq 形
$a=100804=2^2*11*29*79$
は $2^er_1r_2q$ 形
$s(a)=3, s(a)=4$ の非正規形の解があるが形はわかりやすい.

アルゴリズム解
$a = 2 * 5 * 13 = 130$
$a = 2^2 * 11 * 23 = 1012$
$a = 2^3 * 17 * 139 = 18904$
$a = 2^4 * 41 * 131 = 85936$
$a = 2^5 * 73 * 467 = 1090912$

8.9 $[P = 2, m = 10]$ 完全数

表 9: $[P = 2, m = 10]$ 完全数

a	素因数分解
11	11
21	$3 * 7$
26	$2 * 13$
68	$2^2 * 17$
656	$2^4 * 41$
2336	$2^5 * 73$
8768	$2^6 * 137$
133376	$2^8 * 521$

$a = 11,$
$a = 21 = 3 * 7$

これら以外はみな正規形になっているのが不思議である．このことが正しいと証明できたらスゴイ．

8.10 $[P = 2, m = 12]$ 完全数

$a = 13$, $a = 45 = 3^2 * 5$

以外はみな正規形

8.11 $[P = 2, m = 16]$ 完全数

$a = 17,$

表 10: $[P=2, m=12]$ 完全数

a	素因数分解
13	13
45	$3^2 * 5$
76	$2^2 * 19$
688	$2^4 * 43$
8896	$2^6 * 139$
133888	$2^8 * 523$

表 11: $[P=2, m=16]$ 完全数

a	素因数分解
17	17
38	$2 * 19$
92	$2^2 * 23$
170	$2 * 5 * 17$
248	$2^3 * 31$
752	$2^4 * 47$
988	$2^2 * 13 * 19$
2528	$2^5 * 79$
8648	$2^3 * 23 * 47$
12008	$2^3 * 19 * 79$
34688	$2^7 * 271$
63248	$2^4 * 59 * 67$
117808	$2^4 * 37 * 199$

$a = 988 = 2^2 * 13 * 19$

$a = 8648 = 2^3 * 23 * 47$
$a = 12008 = 2^3 * 19 * 79$
$a = 63248 = 2^4 * 59 * 67$
$a = 117808 = 2^4 * 37 * 199$

これらは $2^e rq$ 形

アルゴリズム解

$a = 2 * 5 * 17 = 170$
$a = 2^2 * 13 * 19 = 988$
$a = 2^3 * 19 * 79 = 12008$
$a = 2^3 * 23 * 47 = 8648$
$a = 2^3 * 31 * 31 = 7688$
$a = 2^4 * 37 * 199 = 117808$
$a = 2^4 * 59 * 67 = 63248$
$a = 2^5 * 71 * 569 = 1292768$
$a = 2^5 * 109 * 151 = 526688$
$a = 2^6 * 139 * 1483 = 13192768$
$a = 2^6 * 199 * 353 = 4495808$
$a = 2^7 * 269 * 4919 = 169371008$
$a = 2^7 * 467 * 563 = 33653888$
$a = 2^8 * 557 * 6199 = 883927808$
$a = 2^8 * 787 * 1459 = 293947648$
$a = 2^9 * 1031 * 131969 = 69662739968$
$a = 2^9 * 1489 * 3271 = 2493705728$
$a = 2^{10} * 2053 * 700759 = 1473186024448$
$a = 2^{10} * 2089 * 101863 = 217898810368$
$a = 2^{11} * 4211 * 148691 = 1282330216448$
$a = 2^{11} * 4243 * 117427 = 1020401174528$
$a = 2^{11} * 4391 * 60761 = 546409576448$
$a = 2^{13} * 16411 * 9602779 = 1290987160936448$
$a = 2^{14} * 32839 * 14945393 = 8041132207751168$
$a = 2^{15} * 65557 * 195288343 = 419512906614407168$
$a = 2^{15} * 71563 * 778027 = 1824454941114368$
$a = 2^{15} * 65539 * 1073790979 = 2306054126720811008$
$a = 2^{16} * 182899 * 462547 = 5544305213636608$

8.12 $[P=2,m=28]$ 2 完全数

表 12: $[P=2,m=28]$ 2 完全数

a	素因数分解
29	29
62	$2*31$
182	$2*7*13$
230	$2*5*23$
344	2^3*43
944	2^4*59
6710	$2*5*11*61$
20264	$2^3*17*149$
36224	2^7*283
538112	2^9*1051

アルゴリズム解

$a=2*5*23=230$

$a=2*7*13=182$

$a=2^3*17*149=20264$

$a=2^7*257*32909=1082574464$

$a=2^7*313*1381=55328384$

$a=2^{12}*8221*2244881=75592362807296$

$a=2^{12}*8293*666041=22624165941248$

$a=2^{12}*9041*87133=3226703679488$

$a=2^{12}*15773*17041=1100954390528$

8.13 $[P=2, m=32]$ 完全数

表 13: $[P=2, m=32]$ 完全数

a	素因数分解
250	$2*5^3$
376	2^3*47
1276	$2^2*11*29$
12616	$2^3*19*83$
20536	$2^3*17*151$
396916	$2^2*13*17*449$
801376	$2^5*79*317$

$a=396916=2^2*13*17*449$ は $2^e r_1 r_2 q$ 形

アルゴリズム解
$a=2^2*11*29=1276$
$a=2^3*17*151=20536$
$a=2^3*19*83=12616$
$a=2^5*71*571=1297312$
$a=2^5*79*317=801376$
$a=2^7*257*32911=1082640256$
$a=2^7*263*8419=283417216$
$a=2^7*271*4337=150441856$
$a=2^7*281*2767=99523456$
$a=2^7*307*1511=59376256$
$a=2^7*359*883=$40575616
$a=2^7*463*569=$33721216
$a=2^8*953*1103=269096704$
$a=2^9*1061*28591=15531546112$
$a=2^{11}*4111*1052417=8860643915776$
$a=2^{11}*4129*497423=4206304393216$
$a=2^{11}*4271*99397=869426354176$
$a=2^{11}*5591*15307=175270782976$
$a=2^{12}*8609*168719=5949447663616$
$a=2^{12}*10223*41213=1725728763904$

8.14 $[P=2, m=64]$ 完全数

表 14: $[P=2, m=64]$ 完全数

a	素因数分解
134	$2*67$
284	2^2*71
410	$2*5*41$
632	2^3*79
1292	$2^2*17*19$
1628	$2^2*11*37$
4064	2^5*127
9752	$2^3*23*53$
12224	2^6*191
22712	$2^3*17*167$
66992	$2^4*53*79$
72944	$2^4*47*97$
403988	$2^2*13*17*457$
556544	2^9*1087

$a=403988=2^2*13*17*457$ は $2^e r_1 r_2 q$ 形

8.15 $[P = 2, m = 128]$ 完全数

表 15: $[P = 2, m = 128]$ 完全数

a	素因数分解
262	$2 * 131$
442	$2 * 13 * 17$
730	$2 * 5 * 73$
2332	$2^2 * 11 * 53$
6112	$2^5 * 191$
11224	$2^3 * 23 * 61$
16264	$2^3 * 19 * 107$
27064	$2^3 * 17 * 199$
49024	$2^7 * 383$
67024	$2^4 * 59 * 71$
75952	$2^4 * 47 * 101$
117370	$2 * 5 * 11^2 * 97$
550432	$2^5 * 103 * 167$
589312	$2^9 * 1151$
635104	$2^5 * 89 * 223$
719776	$2^5 * 83 * 27$

$a = 117370 = 2 * 5 * 11^2 * 97$ 異形の形

アルゴリズム解

$a = 2 * 5 * 73 = 730$

$a = 2 * 13 * 17 = 442$

$a = 2^2 * 11 * 53 = 2332$

$a = 2^3 * 17 * 199 = 27064$

$a = 2^3 * 19 * 107 = 16264$

$a = 2^3 * 23 * 61 = 11224$

$a = 2^4 * 47 * 101 = 75952$

$a = 2^4 * 59 * 71 = 67024$

$a = 2^5 * 67 * 1103 =$2364832

$a = 2^5 * 73 * 479 = 1118944$

$a = 2^5 * 83 * 271 = 719776$

$a = 2^5 * 89 * 223 = 635104$

$a = 2^5 * 103 * 167 =$550432

$a = 2^6 * 191 * 383 =$4681792

$a = 2^7 * 263 * 8431 = 283821184$
$a = 2^7 * 283 * 2591 = 93856384$
$a = 2^7 * 311 * 1423 = 56646784$
$a = 2^7 * 367 * 839 =$39412864
$a = 2^7 * 479 * 547 =$33537664

8.16 $[P = 2, m = 496]$ 3完全数

表 16: $[P = 2, m = 496]$ 3完全数

a	素因数分解
998	$2 * 499$
2012	$2^2 * 503$
2570	$2 * 5 * 257$
4028	$2^2 * 19 * 53$
15128	$2^3 * 31 * 61$
19688	$2^3 * 23 * 107$
30248	$2^3 * 19 * 199$
52088	$2^3 * 17 * 383$
96128	$2^7 * 751$

アルゴリズム解
$a = 2 * 5 * 257 = 2570$
$a = 2^2 * 19 * 53 = 4028$
$a = 2^3 * 17 * 383 = 52088$
$a = 2^3 * 19 * 199 = 30248$
$a = 2^3 * 23 * 107 = 19688$
$a = 2^3 * 31 * 61 = 15128$
$a = 2^6 * 139 * 1523 = 13548608$

9　$m < 0$ の場合

9.1　$[P = 2, m = -2]$ 完全数

表 17: $[P = 2, m = -2]$ 完全数

a	素因数分解
20	$2^2 * 5$
104	$2^3 * 13$
464	$2^4 * 29$
650	$2 * 5^2 * 13$
1952	$2^5 * 61$
130304	$2^8 * 509$

解 $a = 650 = 2 * 5^2 * 13$ は異形だが他は正規形.

$2 * 5^2 * 13$ はヒトコブラクダを連想させる形なのでヒトコブと呼ぶ.

命題 1 $pr^2q, (p < r < q :$ 素数$)$ が $\sigma(a) = 2a + 2$ の解なら $a = 2 * 5^2 * 13$. すなわちヒトコブ になる.

pr^2q のとき $R = 1 + r + r^2$ とすると

$$\sigma(a) = \widetilde{p}R\widetilde{q} = 2a + 2 = pr^2q + 2$$

によって,q でまとめると

$$q(2pr^2 - \widetilde{p}R) = \widetilde{p}R - 2.$$

$q \geq r + 2$ によって,

$$2pr^2 - \widetilde{p}R \geq (r + 2)(\widetilde{p}R - 2) = \widetilde{p}Rr - 2r - 2((\widetilde{p}R - 2)).$$

9.2 $[P=2, m=-4]$ 完全数

表 18: $[P=2, m=-4]$ 完全数

a	素因数分解
12	$2^2 * 3$
70	$2 * 5 * 7$
88	$2^3 * 11$
1888	$2^5 * 59$
4030	$2 * 5 * 13 * 31$
5830	$2 * 5 * 11 * 53$

$a = 4030 = 2 * 5 * 13 * 31$
$a = 5830 = 2 * 5 * 11 * 53$

$2^e rq$ 型

9.3 $[P=2, m=-6]$ 完全数

表 19: $[P=2, m=-6]$ 完全数

a	素因数分解
8925	$3*5^2*7*17$
32445	$3^2*5*7*103$
442365	$3*5*7*11*383$
151115727449904501489664	$2^{38}*549755813881$

3 つとも異形.
4 番目は正規形

9.4 $[P=2, m=-8]$ 完全数

表 20: $[P=2, m=-8]$ 完全数

a	素因数分解
56	2^3*7
368	2^4*23
836	$2^2*11*19$
11096	$2^3*19*73$
17816	$2^3*17*131$
45356	$2^2*17*23*29$
77744	$2^4*43*113$
91388	$2^2*11*31*67$
128768	2^8*503

正規形と,$2^erq, 2^er_1r_2q$ 形

9.5 $[P=2, m=-10]$ 完全数

表 21: $[P=2, m=-10]$ 完全数

a	素因数分解
40	$2^3 * 5$
1696	$2^5 * 53$
518656	$2^9 * 1013$

9.6 $[P=2, m=-12]$ 完全数

表 22: $[P=2, m=-12]$ 完全数

a	素因数分解
24	$2^3 * 3$
30	$2 * 3 * 5$
42	$2 * 3 * 7$
54	$2 * 3^3$
66	$2 * 3 * 11$
78	$2 * 3 * 13$
102	$2 * 3 * 17$
114	$2 * 3 * 19$
138	$2 * 3 * 23$
174	$2 * 3 * 29$
186	$2 * 3 * 31$
222	$2 * 3 * 37$

$a = 24 = 2^3 * 3$

$a = 54 = 2 * 3^3$

はいわゆる擬素数解である.
$a = 6p$ が続くので途中略す.
ここで異常な解
$a = 304 = 2^4 * 19$
が出てきた. これをエイリアンという.

表 23: $[P=2, m=-12]$ 完全数 続き

a	素因数分解
282	$2*3*47$
304	2^4*19
318	$2*3*53$
354	$2*3*59$
366	$2*3*61$
402	$2*3*67$

以上見たように, $a=6p, (2<3<p:$ 素数$)$, $a=24=2^3*3$, $a=54=2*3^3$ 擬素数解 の他に全く異質のエイリアン解の 3 種の解がある.

もっともこの他の形もあるかもしれない.

9.7 $6r$ の特徴づけ

3 素数の積 $a = pqr, (p < q < r)$: 素数 , が $\sigma(a) = 2a + 12$ の解となるとき $a = 6r$ を示す.

$a = pqr$ のとき

$$\sigma(a) = \widetilde{pqr}, 2a + 12 = 2pqr + 12.$$

$A = \widetilde{qr}, B = qr$ とおくと

$$(p + 1)A = 2pB + 12.$$

すると

$$p(A - 2B) = 12 - A.$$

$\Delta = q + r$ とおくとき

$$A - 2B = \widetilde{qr} - 2qr = \Delta + 1 - qr.$$

$12 - A = 12 - (qr + \Delta + 1)$ によって,

$$p(\Delta + 1 - qr) = 12 - (qr + \Delta + 1)$$

これより式を整理して

$$12 = (1 - p)qr + \Delta(p + 1) + p + 1.$$

ここで $p = 2$ と仮定する.

$$12 = -qr + 3\Delta + 3.$$

よって,

$$qr = 3\Delta - 9.$$

$q_0 = q - 3, r_0 = r - 3$ とおくと

$q_0 r_0 = 0$. $0 \le q_0 < r_0$ により $q_0 = 0; q = 3, p = 2$. r は単なる素数で条件がつかない. $a = 6r$ が解.

次に $p > 2$ と仮定して矛盾を導く.

$12 = (1 - p)qr + \Delta(p + 1) + p + 1$ を p で整理すると,

$$12 = -p(qr - \Delta - 1) + qr + \Delta + 1.$$

$$p(qr - \Delta - 1)) = qr + \Delta - 11.$$

$p \geq 3$ により

$$p(qr - \Delta - 1)) = qr + \Delta - 11 \leq 3(qr - \Delta - 1).$$

$$0 \leq 2qr - 4\Delta + 8.$$

$q_2 = q - 2, r_2 = r - 2$ とおくとき $q_2 r_2 = qr - 2\Delta + 4$ によって

$$0 \geq qr - 2\Delta + 4 = q_2 r_2$$

なので $q_2 \leq 0$. ゆえに $q \leq 2$ となり矛盾.

9.8 解 $a = 2^e q^f$

$\sigma(a) = 2a + 12$ の解で $a = 2^e q^f$ となるものを調べよう.
$X = 2^e, Y = q^f$ とおくとき
$\sigma(a) = (2X - 1)\dfrac{qY - 1}{\overline{q}}$ なので

$$2X + qY - 1 = 2XY - 12\overline{q}.$$

$12\overline{q} + 2X - 1 = Y(2X - q)$ より $2X - q > 0$.
$12\overline{q} + 2X - 1 = 12\overline{q} + 2X - q + \overline{q} = Y(2X - q)$ から

$$12\overline{q} + \overline{q} = (Y - 1)(2X - q).$$

そこで $Z = 1 + q + \cdots + q^{f-1}$ とおくとき $\dfrac{Y - 1}{\overline{q}} = Z$ なので

$$13 = Z(2X - q).$$

$Z = 1$ または $Z = 13$.

i $Z = 1$. $2X - q = 13$ より $q = 2^{e+1} - 13$.
$e = 3$ のとき $q = 2^{e+1} - 13 = 3$. ここで $a = 2^3 * 3$. 擬素数解.
$2^{e+1} - 13$ が素数になる例はいろいろある.
$e = 4$ のとき $q = 2^{e+1} - 13 = 32 - 13 = 19$ によって, $a = 2^4 * 19 = 403$ はエイリアン解.

ii $Z = 13$. $Z = 1 + q + \cdots + q^{f-1} = 13$ によって, $f = 3, q = 3$. $2X - q = 1$ より $q = 2^{e+1} - 1$. したがって $e = 1$. $a = 2 * 3^3$ は擬素数解

10　素数べきの解

$\sigma(a)=2a-m$ に素数べき p^e の解があるとしよう.
$a=p^e$, のとき
$\sigma(a)=\dfrac{p^{e+1}-1}{\overline{p}}$　$, 2a-m=2p^e-m$ によって

$$p^{e+1}-1=(2p^e-m)(p-1)$$

を変形して

$$m\overline{p}-1=p^e(\overline{p}-1)$$

これより

$$\overline{p}(m-p^e)=1-p^e.$$

$\overline{p}$ で除して

$$p^e-m=p^{e-1}+\cdots+1.$$

これより

$$m=p^e-(p^{e-1}+\cdots+1).$$

10.1　解 p

そこで $e=1$ とすれば $m=p-1$.

例
$m=4$ とすると $p=5$.
$\sigma(a)=2a-4$ の解に $a=5$

$m=6$ とすると $p=7$.
$\sigma(a)=2a-6$ の解に $a=7$

$m=10$ とすると $p=11$.
$\sigma(a)=2a-10$ の解に $a=11$

10.2　解 p^2

$e=2$ とすれば $m=p^2-p-1$.

例
$p=3$ とすれば $m=p^2-p-1=9-4=5$.
$\sigma(a)=2a-5$ の解に $a=3^2$.

$p=5$ とすれば $m=p^2-p-1=25-6=19$.
$\sigma(a)=2a-19$ の解に $a=5^2$.

$p=7$ とすれば $m=p^2-p-1=49-8=41$.
$\sigma(a)=2a-41$ の解に $a=7^2$.

10.3　解 p^3

$e=3$ とすれば $m=p^3-p^2-p-1$.

例
$p=3$ とすれば $m=27-9-3-1=14$.
$\sigma(a)=2a-14$ の解に $a=3^3$.

10.4　解 p^4

$e=4$ とすれば $m=p^4-p^3-p^2-p-1$.

例
$p=3$ とすれば $m=81-27-9-3-1=41$.
$\sigma(a)=2a-41$ の解に $a=3^4$.

$\sigma(a)=2a-41$ の解に $a=7^2, 3^4$.

11　2素数の積の解

$a=pq(p<q:$ 素数$)$ が $\sigma(a)=2a-m$ の解とする.
$\sigma(a)=\sigma(pq)=\widetilde{p}\cdot\widetilde{q}=pq+\Delta+1$ ここで $\Delta=p+q$.

$$\widetilde{p}\cdot\widetilde{q}=pq+\Delta+1=2pq-m$$

によって

$$m + 2 = p_0 q_0$$

ここで $p_o = p - 1 . q_0 = q - 1.$

1) $m = 2$. $4 = p_0 q_0$ により $p_0 = 1, q_0 = 4; p = 2, q = 5; a = 10.$

2) $m = 4$. $6 = p_0 q_0$ により $p_0 = 1, q_0 = 6; p = 2, q = 7; a = 14,$ 矛盾.

3) $m = 6$. $8 = p_0 q_0$ により $p_0 = 2, q_0 = 4; p = 3, q = 5; a = 15.$

4) $m = 8$. $10 = p_0 q_0$ により $p_0 = 1, q_0 = 10; p = 2, q = 11; a = 22.$

5) $m = 10$. $12 = p_0 q_0$ により $p_0 = 1, q_0 = 12; p = 2, q = 13; a = 26; p_0 = 2, q_0 = 6; p = 3, q = 7; a = 21.$

6) $m = 14$. $16 = p_0 q_0$ により $p_0 = 1, q_0 = 16; p = 2, q = 17; a = 34.$

7) $m = 16$. $18 = p_0 q_0$ により $p_0 = 1, q_0 = 18; p = 2, q = 19; a = 38.$

8) $m = 18$. $20 = p_0 q_0$ により $p_0 = 2, q_0 = 10; p = 3, q = 11; a = 33.$

9) $m = 20$. $22 = p_0 q_0$ により $p_0 = 1, q_0 = 22; p = 2, q = 23; a = 46.$

10) $m = 22$. $24 = p_0 q_0$ により $p_0 = 2, q_0 = 12; p = 3, q = 13; a = 39.$

12 m : 奇数の場合

次の結果は $a \leq 1000000$ についてパソコンで調べた結果である.

表 24: $[P=2, m>0 :]$ 奇数, 完全数

m	a	素因数分解
$m=1$	2	2
	4	2^2
	8	2^3
	16	2^4
	32	2^5
	64	2^6
	128	2^7
	256	2^8
	512	2^9
	1024	2^{10}
	2048	2^{11}
	4096	2^{12}
	8192	2^{13}
	16384	2^{14}
	32768	2^{15}
	65536	2^{16}

$m=1$ のとき方程式は $\sigma(a)=2a-1$ になりこの解は $m=1$ のときの広義の完全数は $a=2^e$ に限りそうなコンピュータの計算結果である.

$\sigma(a)=2a-1$ の解は almost perfect number (準完全数) と呼ばれているがこれは $a=2^e$ に限るという古来からの予想があるが解決されていない.

1. $m=1$, すなわち $\sigma(a)=2a-1$ の場合. $a=2^e$ は明らかに解である. したがって解は無数にある. この他に解があるかどうかは不明.

($\sigma(a)=2a-1$ の解を 概完全数という. 概完全数は 2^e と書けるか? は奇数完全数の存在問題に匹敵する難問らしい.)

2. $m=3$, すなわち $\sigma(a)=2a-3$ の場合. 解はないらしい.

以上からわかることは m : 奇数のとき解は, ごく少ない. 解は有限個しかない. このことをいつの日かを証明したいものだ.

表 25: $[P=2, m>0:]$ 奇数, 完全数

m	a	素因数分解
$m=5$	9	3^2
$m=7$	50	$2*5^2$
$m=11$	244036	$2^2*13^2*19^2$
$m=19$	25	5^2
	2312	2^3*17^2
$m=25$	98	$2*7^2$
$m=37$	484	2^2*11^2
$m=41$	49	7^2
	81	3^4
$m=47$	225	3^2*5^2
$m=61$	2888	2^3*19^2
$m=71$	676	2^2*13^2
$m=85$	242	$2*11^2$

13 $m<0$:奇数の場合

次の結果は $a \leq 1000000$ についてパソコンで調べた結果である.

表 26: $[P=2, m<0:]$ 奇数, 完全数

$m=$	a	素因数分解
$m=-89$	13456	2^4*29^2
$m=-71$	392	2^3*7^2
$m=-65$	200	2^3*5^2
$m=-59$	968	2^3*11^2
$m=-51$	72	2^3*3^2
$m=-41$	1352	2^3*13^2
$m=-39$	162	$2*3^4$
$m=-31$	15376	2^4*31^2
$m=-19$	36	2^2*3^2
$m=-7$	196	2^2*7^2
$m=-3$	18	$2*3^2$

1. $m=-1$, すなわち $\sigma(a)-2a=1$ の場合. 解は無いと予想されている.

$\sigma(a)-2a=1$ を満たす a は pseudo perfect number と呼ばれているが実際には存在しないと思われている.

ある日, 新聞紙上で $\sigma(a)-2a=1$ を満たす a が見つかったと報道されるかもしれない. その数は疑似完全数と呼ばれている.

私は, 宇宙生物の発見より可能性が低いと思う.

2. $m=-3$ すなわち $\sigma(a)-2a=3$ の場合. $a=2*3^2$ は解. 他の解は無いと予想されている.

これらを証明することはきわめて難しい.

ここでは $s(a)=1,2$ を満たす場合に絞って証明する.

最初に簡単な場合を扱う.

a) $m=5$ のとき

1). $s(a)=1$ を仮定する.

$\sigma(a)=2a-5$ なので, $a=p^e$ とおくと

$\sigma(a)=1+p+\cdots+p^e$, $2a-5=2p^e-5$ により

$p(1+p+\cdots+p^{e-2}-p^{e-1})=-6$ によれば p は3で割れるから $p=3$.

$$3^{e+1}-1=2(2*3^e-5)$$

によって,

$$3^{e+1}-1=4*3^e-10.$$

ゆえに, $9=3^e$. よって $e=2, a=3^2$.

2). $s(a)=2$ を仮定し矛盾を導く.

$a=p^eq^f, p<q$:素数, として $X=p^e, Y=q^f$ とおく. さらに $\overline{p}=p-1, \overline{q}=q-1, \rho'=\overline{p}\,\overline{q}$ を使うと

$$\frac{(pX-1)(qY-1)}{\rho'}=2XY-5$$

$$(pX-1)(qY-1)-\rho'(2XY-5)=0$$

を得るがこの左辺の XY の係数を R とおくと, $R=pq-2\rho'=-(p-2)(q-2)+2$.

次の定理を使うことにより $R>0$.

よって, $p=2, R=2, \rho'=\overline{q}$.

$$2XY-(2X+qY-1)=-5\overline{q}.$$

$Y(2X-q)-2X+1=5\overline{q}$ を変形して

$$Y = \frac{2X - 1 - 5\overline{q}}{2X - q} = \frac{2X - q - 4\overline{q}}{2X - q}.$$

さらに変形して

$$Y - 1 = \frac{-4\overline{q}}{2X - q}.$$

ここで場合を分ける.

i. $f = 1$. $Y = q$ なので

$$Y - 1 = \overline{q} = \frac{-4\overline{q}}{2X - q}.$$

$4 = q - 2X$, から $q = 4 + 2X$ なので $q = 2$; 矛盾.

ii. $f > 1$. $Y = q^f$ なので

$$Y - 1 = \overline{q}(q^{f-1} + \cdots + q + 1) = \frac{-4\overline{q}}{2X - q}.$$

$4 = (q - 2X)(q^{f-1} + \cdots + q + 1)$ から $f = 2, q = 3$. $q = 1 + 2X$ なので $X = 1$; 矛盾.

14　m : 奇数の場合の証明

$\sigma(a) - 2a = -m$ の解で $s(a) = 2$ を満たすと仮定する.

$a = p^e q^f, p < q$:素数, として $X = p^e, Y = q^f$ とおく. さらに $\overline{p} = p - 1, \overline{q} = q - 1, \rho' = \overline{p}\,\overline{q}$ を使うと

$$\frac{(pX - 1)(qY - 1)}{\rho'} = 2XY - m$$

$$(pX - 1)(qY - 1) - \rho'(2XY - m) = 0$$

を得るがこの左辺の XY の係数を R とおくと,

$$(pX - 1)(qY - 1) - \rho'(2XY - m) = RXY - pX - qY + 1 + \rho' m = 0$$

定義により

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

$R>0$ となる適当な条件を次に探そう.
$q>p\geq 3$ と仮定する.
$R=-(p-2)(q-2)+2\leq 4-q\leq -1$.

$$1+\rho' m=-RXY+pX+qY-1\geq XY+pX+qY-1.$$

これより $m<0$ は成り立たない.
不等式にして

$$mpq>m\rho'\geq XY+pX+qY-2.$$

相加・相乗平均により

$$pX+qY\geq 2\sqrt{pqXY}.$$

一方, $e=1$ なら $\sigma(X)=\sigma p=1+p$:偶数. このとき $\sigma(a)-2a$ は偶数.
m : 奇数 を仮定しているので $e\geq 2$. 同様に $f\geq 2$.
それゆえ $X\geq p^2, Y\geq q^2$ により

$$2+mpq>XY+pX+qY\geq p^2q^2+2\sqrt{p^3q^3}=pq(pq+2\sqrt{pq}).$$

$$2>pq(pq+2\sqrt{pq}-m).$$

$q>p\geq 3$ で評価すると,

$$2>pq+2\sqrt{pq}-m\geq 15+2\sqrt{15}-m>22-m.$$

これによって, $m>20$ になる.
$m\leq 20$ のとき矛盾する. よって $m\leq 20$ のとき $p=2, R=2$.
m が最小になる場合は $a=3^2*5^2$.
このとき計算すると $m=47$. したがって,
以上をまとめて定理とする.

定理 2 *1.* $m<1$ なら $p=2, R=2$.

2. m : 奇数なら $m<20$ のとき $p=2, R=2$.

以上の評価はかなり甘い. いくらでも精密化できるだろう.
m が最小になる場合は $a=3^2*5^2$.
このとき計算すると $m=47$. したがって, $m<47$ で定理は成立する.

15　$p = 2, R = 2$

$p = 2$ とすると $\rho' = \overline{q}, R = 2$ となり 基本方程式は

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

これより

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

$$Y - 1 = \frac{\overline{qm}}{q-2X}.$$

したがって $\overline{q}$ で割れば

$$q^{f-1} + \cdots + q + 1 = \frac{m-1}{q-2X}.$$

$q - 2X$ は　$\overline{m}$ の約数になる.

16 m:奇数で正の場合

16.1 $m = 5$

このとき $a = p^e$ の形の解があり $a = 3^2$.

16.2 $m = 7$

このとき $a = p^e$ の形の解はない.
$s(a) = 2$ とする.
$m = 7 < 21$ によって,

$$q^{f-1} + \cdots + q + 1 = \frac{6}{q - 2X}.$$

i. $q - 2X = 1$ $q^{f-1} + \cdots + q + 1 = 6$. によれば $q = 5, f = 2$.
$q - 2X = 5 - 2X = 1$ より $X = 2$. よって $a = 2 * 5^2$.

16.3 $m = 19$

このとき $a = p^e$ の形の解があり $a = 5^2$.
$s(a) = 2$ とする.
$m = 19 < 21$ によって,

$$q^{f-1} + \cdots + q + 1 = \frac{18}{q - 2X}.$$

$f = 1$ ならば $q - 2X = 18$. q : 偶数となり矛盾.
$\frac{18}{q - 2X} \geq 1 + q \geq 4$ によって,
i. $q - 2X = 3$.
$q^{f-1} + \cdots + q + 1 = 6$ によって, $f = 2, q = 5$. $q - 2X = 3; X = 1$ となり矛盾.
ii. $q - 2X = 1$.
$q^{f-1} + \cdots + q + 1 = 18$ によって, $f = 2, q = 17$. $q - 2X = 1; X = 8$. $a = 2^3 * 17^2$.

16.4 $m = 37$

このとき $a = p^e$ の形の解があり $a = 5^2$.
$s(a) = 2, p = 2$ とする.

$$q^{f-1} + \cdots + q + 1 = \frac{36}{q - 2X}.$$

$f=1$ ならば $q-2X=36$. q : 偶数となり矛盾.

$\dfrac{36}{q-2X} \geq 1+q \geq 4$ によって,

i. $q-2X=3$.

$q^{f-1}+\cdots+q+1=12$ によって, $f=2, q=11$. $q-2X=3; X=4$ となり $a=2^2*11^2$.

ii. $q-2X=1$.

$q^{f-1}+\cdots+q+1=36$ によって, $f=2, q=35$ 矛盾.

17 m 奇数で負の場合

17.1 $m=-3$

$m<0$ のとき条件は自動的に満たされ, $p=2, R=2$.

$$q^{f-1}+\cdots+q+1=\frac{-3-1}{q-2X}=\frac{4}{2X-q}.$$

i. $2X-q=1$. $q+1=4, f=2$ により, $2X=q+1=4.X=2, a=2*3^2$.

ii. $2X-q>1$ は起きない.

17.2 $m=-7$

$p=2, R=2$.

$$q^{f-1}+\cdots+q+1=\frac{-7-1}{q-2X}=\frac{8}{2X-q}.$$

i. $2X-q=1$. $q+1=8, q=7, f=2$ により, $2X=q+1=8.X=4, a=2^2*7^2$.

ii. $2X-q>1$ は起きない.

17.3 $m=-17$

$p=2, R=2$.

$$q^{f-1}+\cdots+q+1=\frac{18}{2X-q}.$$

i. $2X-q=3$. $q+1=6, q=5, f=2$ により, $2X-q=3.X=4, a=2^2*5^2$.

ii. $2X-q=1,2$ は起きない.

17.4　$m = -31$

$p = 2, R = 2.$

$$q^{f-1} + \cdots + q + 1 = \frac{-31 - 1}{q - 2X} = \frac{32}{2X - q}.$$

i. $2X - q = 1$. $q + 1 = 32, q = 31, f = 2$ により, $2X = q + 1 = 32. X = 16 = 2^4, a = 2^4 * 31^2.$

ii. $2X - q = 2, 4, 8$ は起きない.

17.5　$m = -39$

$m < 0$ のとき条件は自動的に満たされ, $p = 2, R = 2.$

$$q^{f-1} + \cdots + q + 1 = \frac{40}{2X - q}.$$

i. $2X - q = 1$. $q^3 + q^2 + q + 1 = 40, q = 3, f = 4$ により, $2X = q + 1 = 4. X = 2, a = 2 * 3^4.$

17.6　$m = -41$

$m < 0$ のとき条件は自動的に満たされ, $p = 2, R = 2.$

$$q^{f-1} + \cdots + q + 1 = \frac{42}{2X - q}.$$

i. $2X - q = 3$. $q + 1 = 14, q = 13, f = 2$ により, $2X = q + 3 = 16; a = 2^3 * 13^2$

ii. $2X - q = 7$. $q^{f-1} + \cdots + q + 1 = 6$ なので $f = 2, q = 5$. $2X - q = 7$ によれば $X = 1$; 矛盾