数学の研究を始めよう (V)

オイラーをモデルに数論研究

# 第1章 完全数と $a = mp$ 問題

飯高 茂

平成 30 年 4 月 5 日

# 1　abc 予想

2017 年 12 月に 東京の広尾学園で開かれた高校生の数学研究集会 X'Math で高校生向けに「$abc$ 予想」について解説をした. ここにその予稿を少し直して載せる.

次の定理の結果は「$abc$ 予想」と呼ばれていた. 京都大学教授の望月新一が新しい理論「宇宙際タイヒミューラ理論」(Inter-universal Teichmueller theory) をつくり, その結果「$abc$ 予想」が証明され (2017 年 12 月) 今や定理になった.

自然数 $N$ についてその相異なる素因子すべての積を $\mathrm{rad}(N)$ (根基; radical) と書く.

**定理 1 ($abc$ 予想, 望月の定理)** 自然数 $a, b, c$ がどの 2 つも互いに素で $c = a + b$ の 2 条件をみたすとき,$N = abc$ とおく. 任意の正の数 $\varepsilon$ に対して $R(\varepsilon) = (rad(N))^{1+\varepsilon}$ とおくとき, 不等式

$$c > R(\varepsilon)$$

を満たし上の 2 条件を満足する $(a, b, c)$ は有限個.

例 1 $\mathrm{rad}(N)$ の計算例

- $a = 3^2, b = 4^2, c = 5^2$ とすると $N = abc = 60^2$.
  よって $\mathrm{rad}(N) = 2 * 3 * 5 = 30$; $25 = c < 30 = \mathrm{rad}\ (N)$. ここで $\mathrm{rad}\ (N) = R(0)$.
- $a = 1, b = 63, c = b + 1 = 2^6 = 64$ とすると $N = abc = 2^6 * 3^2 * 7$.
  よって $\mathrm{rad}(N) = 42$; $c = 64 > \mathrm{rad}\ (N) = 42$.

そこで $c > R(\varepsilon)$ を満たす $(a, b, c)$ は有限個, という結果の書き換えを行う.

不等式を $R(\varepsilon)$ で割ると $\dfrac{c}{R(\varepsilon)} > 1$ になる. これらは有限個なので, この上界を 1 つとり $K_\varepsilon$ とすると $K_\varepsilon > \dfrac{c}{R(\varepsilon)}$ がつねに成り立つ.
さらに書き換えると $c < K_\varepsilon R(\varepsilon)$ が常に成り立つ.
これが $abc$ 予想 でよく使われる表現である.

注釈
$\varepsilon > 0$ は大切な仮定で $\varepsilon = 0$ のときは成立しない.
その例 (英文の wikipedia にある $abc$ conjecture の説明を参考にし紹介する)

奇素数 $p$ を 1 つとりさらに自然数 $n$ をとる.
$a = 1, b = 2^{p(p-1)n} - 1, c = b + 1 = 2^{p(p-1)n}$ とおく.
フェルマーの小定理によると $2^{p-1} - 1 \equiv 0 \bmod p$ となるので ある自然数 $k$ によって
$2^{p-1} - 1 = pk$ とかける. $A = 2^{p(p-1)}$ とおくとき,, $b = A^n, A = (2^{p-1})^p = (1 + pk)^p$.
2 項定理により $A - 1 = (1 + pk)^p - 1 = 1 + p^2k + \cdots - 1 = p^2m$ とある自然数 $m$ で書ける.

$$A^n - 1 = (A - 1)(A^{n-1} + \cdots + 1) = p^2m(A^{n-1} + \cdots + 1)$$

を使うと $A^n - 1 = p^2 t$ と書けるような自然数 $t$ があることがわかる.

よって,$b = A^n - 1 = 2^{p(p-1)n} - 1 = p^2 t$ .

$t$ の素因数分解での $p$ べき部分を $p^e$ とおくと,$t = p^e t_0$,($t_0$ は $p$ で割れない) と書ける.

$b = p^2 t = p^{2+e} t_0$ により $\mathrm{rad}(b) = p \ \mathrm{rad}\ t_0 \leq p t_0 \leq pt$.

$t = \dfrac{b}{p^2} < \dfrac{c}{p^2}$ なので $p \geq 3$ に注意して

$$rad(N) = rad(abc) = 2rad(b) \leq 2pt = 2p\frac{b}{p^2} < 2p\frac{c}{p^2} = \frac{2c}{p} < c.$$

素数 $p$ は無限にあるので $c > rad(abc)$ を満たす $a, b, c$ は 無限にあることになる.

## 1.1 $abc$ 予想の応用例

素数 $p > 2$ に関して, フェルマの小定理によれば $2^{p-1} - 1$ は $p$ で割れる.

そこで $2^{p-1} - 1$ が $p^2$ で割れるとき, 素数 $p$ を Wieferich 素数 という.

これまで Wieferich 素数としては 1093 と 3511 しか知られていない. このように Wieferich 素数はまことにレアな存在であるが, Wieferich 素数でない素数は無限にある. このことは $abc$ 予想を使えば証明できる (Silverman).

Wieferich 素数でない素数は無限にあるという結果は自然なことであるが,$abc$ 予想を使わないと証明できないとは不思議なことだ.

本書第 7 章で 一般化された Wieferich 素数が出てくる. 一般化された Wieferich 素数 にならない素数は無限にあるに違いはないが $abc$ 予想をから証明ができるのだろうか.

## 2　完全数を知った頃

高校 1 年生になってはじめての夏休みの直前, 数学の H 先生が『数と図形』(ラーデマッヘルとテプリッツ著 , 山崎三郎訳) という本を紹介してくださいました. 放課後, 直ちに千葉市内の古本屋に寄るとこの本はすぐ見つかった (昭和 16 年初版, 昭和 27 年 4 版; 戦争中に出されたことに感銘を受けた).

難しい本と思ったが読んでみると意外によく分かる. 集合論, 無限濃度, 素数の話, 四色問題など興味深く読み私は数学の世界にはまっていった. 当時は自分の将来像などは何も考えていなかったがこの本を読んだ経験が後に数学者となるきっかけのひとつになった.

私は数の計算が苦手でよく計算ミスをした. 計算のいらない論理中心で展開された集合論の話などはとても面白かった. この本の後半第 17 章 a で完全数が扱われていた.

$\sigma(a)$ で自然数 $a$ の約数の和を示す. $\sigma(a)$ は $a$ の関数なのでユークリッド関数と呼ぶ. 約数関数 (divisor function), またはシグマ関数 (sigma function) とも呼ばれる.

$\sigma(a) = 2a$ となるとき $a$ を完全数 (perfect number) という. 6,28,496,8128 ,$\cdots$ などがその例である. 素因数分解するとこれらは $2^e p, (p = 2^{e+1} - 1$:素数) の形をしている. 実際, $6 = 2*(2^2-1), 28 = 2^2 * (2^3 - 1), 496 = 2^4 * (2^5 - 1), 8128$.

4 世紀の人ヤンブリコス は, 完全数は $2^e p, (p = 2^{e+1} - 1$:素数) の形をしているものしかないだろう, と述べた. このような形の完全数をユークリッドの完全数と呼ぶ.

当時の数学界では完全数をたくさん (できれば全部) 見つけることが目標の 1 つとであった. しかし 5 番目の完全数 33550336 は 15 世紀になってようやく発見された.

記号 $\sigma(a)$ を使ってみよう. たとえば

$$\sigma(2^e) = 1 + 2 + 4 + \cdots + 2^e = 2^{e+1} - 1$$

は高校生にもよく知られている等比数列の和の公式である.

偶数の完全数はユークリッドの完全数になる. このことは 18 世紀になってオイラーが証明し, その証明はオイラーの没後に発表された.『数と図形』にはその証明がでている. しかしその証明を読んだが高校生の私にはなかなか理解できなかった. 計算の上では証明できてるようだが何か腑に落ちないものがあった.

**定理 2 (L.Euler)** 偶数の完全数は $2^e p, (p = 2^{e+1} - 1$:素数$)$ の形をしている.

Proof

$a$ を偶数の完全数とする. すなわち, $\sigma(a) = 2a$ を満たし, 素因数分解すると,$a = 2^e L, (, e > 0, L$ は奇数) の形になる.

$2^e$ と $L$ は互いに素なので,$\sigma(a)$ の乗法性により $\sigma(a) = \sigma(2^e)\sigma(L)$. $N = 2^{e+1} - 1$ とおくと $\sigma(2^e) = N$ なので $\sigma(a) = N\sigma(L)$ となる.

一方 $2a = 2^{e+1}L = (N + 1)L$ なので $N\sigma(L) = \sigma(a) = 2a = (N + 1)L$.

これより $N(\sigma(L) - L) = L$ をえる. これがキモになる式であり $\sigma(L) - L$ は $L$ の約数になることがわかる.

### 2.1　ラーデマッヘルの説明

『数と図形』においてラーデマッヘルはここから次のように結論を導く.(少し変更した)

$u = L, U = \sigma(L)$ とすると

$$(2^{e+1} - 1)(U - u) = u.$$

$U$ は $u$ 自身をも約数と考えたときの $u$ の約数の総和であるから $U - u$ は $u$ 以外の $u$ の約数の総和である.

左辺は $U - u$ で割り切れるから右辺 $u$ も $U - u$ で割り切れねばならぬ. すなわち $U - u$ は $u$ 以外の $u$ の 約数である.

依って $U - u$ は $u$ の総ての $u$ 以外の約数の総和であり同時に $u$ の一つの約数であるということになる. これは $u$ が唯一個の約数のみを有し, しかもそれが $U - u$ であることに他ならない.

$u$ が唯一個の約数を持つにすぎないとすれば, その約数は 1 以外にない. ゆえに $U - u$ は 1 に等しく $u$ は素数である.

## 2.2 勉強会

その後, 年月が流れ私は成人し, 国立大学から私立大学に勤務先が変更になった. 推薦入試で入学許可のでた高校生を対象に大学入学前の準備教育として推薦入試合格者のための勉強会があった. その講師をするようになった.

勉強会の仕方は講師に任されている. そこで『数と図形』の中で面白そうな章をコピーして高校生に配布し, あらかじめ勉強してもらいその内容をみんなの前で発表してもらうことにした. 結果的にこれは大成功であった. 大学に入る前の高校生は良く勉強し, 発表を実によく準備してくれた. (高校生の頃はよくやったのに, 大学生になるとやらなくなる. 不思議なことがあるものだと大学の先生はよく言う)

あるときは『数と図形』の完全数の部分をテキストにした. 完全数の話は高校生にとってぜひ学びたい素材になると見えて, 熱心に深く読んでくる.

そして偶数完全数はユークリッドの完全数になることを証明する箇所になった. 発表にあたった高校生 Y 君は思考が追いつかなくなった. 説明がうまくできないので, 呼吸すら停止しかねないほど悩んでいた. そこで, 助け船を出すつもりで「ではこのように考えたらどうですか」 とヒントを出そうとしたら,Y 君は「いやです. 自分で考えます」と絶叫する. その真剣さに私は打たれ感心したものである.

それから 20 年もたったあるときその勉強会に参加していたことを明かしたある卒業生が当時を懐かしくを回想してこういった. 「Y 君の迫力がすごかった. 先生が挑発されたと思い激高したらどうなるか僕たちはとても心配した」

## 2.3 よく分かる証明

ところで,1930 年代には集合の概念を基礎に置く現代数学が確立された. そこでドイツの一般市民に現代数学を説明する意図で数学の公開講義が行われた. それが基になって名著『数と図形』ができたのである.

数式を嫌う一般市民に式を避けて詳しく説明して説得したいという彼の意図はわかる. しかしこれがよくない. 式で説明したほうが分かりやすいことが多い.

私が講師なら次のように説明するであろう.

$d = \sigma(L) - L$ とおけば $N = 2^{e+1} - 1$ なので $Nd = L$. これより, $d$ は $L$ の約数である.

次の 3 つの場合がある.

⟨1⟩ $d=1$ のとき. $d=\sigma(L)-L=1$. したがって, $\sigma(L)=1+L$. これから $L$ の約数は $1, L$ だけになり, したがって $L$ は素数. $N=Nd=L$ なので $N=2^{e+1}-1=L.a=2^eL$ の形で $L=2^{e+1}-1$ は素数になり. $a=2^eL$ . これはユークリッドの完全数. 予想通りである.

⟨2⟩ $d=L$ のとき. $Nd=L$ より $N=1$. $N=2^{e+1}-1=1$ によって, $2^{e+1}=2;e=0$. これは矛盾.

⟨3⟩ $1<d<L$ のとき. すると $1, d, L$ は $L$ の 異なる約数なので $\sigma(L)\geq 1+d+L$.
一方 $d=\sigma(L)-L$ により $\sigma(L)=d+L$. $d+L=\sigma(L)\geq 1+d+L$ . これは矛盾.

このように議論をすると, だいぶ分かりやすくなる. オイラーの証明では, 既約分数の性質を使っていると Dickson の数論の歴史の本に書いてある.

**補題 1 (既約分数の原理)** $a, b, c, d$ は自然数で $\dfrac{a}{b}=\dfrac{c}{d}$ を満たす.
もし $\dfrac{a}{b}$ が既約分数なら , $\dfrac{c}{d}$ の分子と分母は $\dfrac{a}{b}$ の自然数倍となる.
すなわち $k$ があり $c=ak, d=bk$ と書ける.

既約分数の原理を使っても偶数完全数の問題は解ける. 志ある読者は試みてほしい.

# 3 研究の発端

ここで私が大学を定年退職した頃のことを書く. 2013 年の 3 月に退職し 4 月に入ってすぐ, 都内のある私立高校に行った. 高校生のクラブ活動としての数学研究を支援することが目的である.

クラブ活動中の高校生と話してみると, このクラブでは「数学の研究をするのが目的」なので,「完全数を研究したい」あるいは「自分はオイラー関数の研究をしたい」などと高校生が口々に言う. これにはいささか驚かされた. そこで高校生の研究しやすい課題や目標を作る必要性を痛感するにいたった.

偶数完全数のオイラーの証明では $\sigma(L)=1+L$ ならば $L$ は素数, が基本的に使われていることに注目しこれをヒントに高校生の研究課題を作ることにした.

## 3.1 2 倍素数の特徴づけ

そこで素数 $p$ の 2 倍 $a=2p$ を $\sigma(a)$ を用いて特徴づけることを高校生に考えてもらうことにした. しかし, 備えがないままこの問題を高校生にぶつけるのはどうかと思い事前にいろいろ考えてみた.

$p$ を 2 より大きい素数とし,$a=2p$ とすると $\sigma(a)=\sigma(2)\sigma(p)=3(p+1)$ になりこれを 2 倍して

$$2\sigma(a)=3(2p+2)=3a+6$$

中抜き (中間の項を抜く) すると

$$2\sigma(a)=3a+6.$$

こうして $p$ が消えた. そこでこの式を自然数 $a$ を未知数とする方程式と見てこれを満たす解 $a$ を探すこととした. 一見して解けそうもないので, パソコンを用いた. すると

$$6 = 2 * 3, 8 = 2 * 4, 10 = 2 * 5, \cdots, 2p = 2 * p, , \cdots$$

となり, $2p$ の他 8 が現れた. これにはびっくりした.

$2p$ のみが解になるあてがはずれて伏兵 8 が現れた. 8=2*4 なので合成数である 4 が「おまけでもいいから素数の仲間にいれてね」, と独りごとを言っているように感じた. そこで擬素数 (pseudo prime) と呼ぶことにした.

同様に, $a = 3p$ を特徴づける方程式を作りそれを解くとと, $3p$ 以外に $27 = 3*9$ が登場し $a = 4p$ を特徴づける方程式からは $4p$ 以外の解 $32 = 4 * 8$ が登場した.

これらはパソコンでの数値実験の結果であるがこれらの結果を証明することは案外手間がかかることであった. しかし数値実験の結果を基に推論したのでうまくできた.

この問題を整理して 一般に自然数 $m$ が与えられたとき同様に議論することにし, これを $a = mp$ 問題と名前をつけた.

## 4 $a = mp$ 問題

与えられた $m$ に対して, $m$ を割らない素数 $p$ をとるとき $a = mp$ とおくと

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

を満たす.

分母を払って,

$$m\sigma(a) = \sigma(m)a + m\sigma(m)$$

これを $a$ を未知数とする ($a = mp$ 問題の) 方程式とみる.$m$ を割らない素数 $p$ をとると $mp$ は解になるのでこれらを通常解という. 通常解以外の解があればそれをすべて探したい. 最初に簡単な通常解以外の解が見つかった.

**命題 1** $m$ の素因数 $r$ をとり, $m = r^e m'$ とおく. $\alpha = r^{2e+1}m'$ は $a = mp$ 問題の解になる.

このような解を一般に擬素数解という. また $r^{e+1}$ を擬素数 (pseudo prime) という.

Proof

$a = r^{2e+1}m'$ について計算し $m\sigma(a) = \sigma(m)a + m\sigma(m)$ を確認すればよい.

$W = r^{2e+2} - 1, \overline{r} = r - 1, N = r^{e+1} - 1,$ とおく. 左辺の計算をする.

$\sigma(a) = \sigma(r^{2e+1})\sigma(m') = \frac{W}{\overline{r}}\sigma(m'). \ \sigma(m) = \frac{N}{\overline{r}}\sigma(m')$

によって, $m\sigma(a) = r^e m' \frac{W}{\overline{r}}\sigma(m') = r^e m' W\sigma(m')/\overline{r}.$

次に右辺は

$$\begin{aligned}\sigma(m)a + m\sigma(m) &= \sigma(m)(a+m)\\ &= \sigma(m)\frac{N}{\overline{r}}\sigma(m')(r^{2e+1}m' + r^e m')\\ &= (r^{e+1}+1)Nr^e m'\sigma(m')/\overline{r}\\ &= (r^{2e+2}-1)r^e m'\sigma(m')/\overline{r}\\ &= r^e m' W\sigma(m')/\overline{r}\\ &= m\sigma(a).\end{aligned}$$

したがって, 等式が確認された.
End

水谷一さんは次の見方を教えてくれた.

**注意 1** $m$ の素因数ではない素数 $p$ を $1 = p^0$ と見ると, $p^{0+1} = p$ なので $pm$ を解と見れないことはない. こう見ると, 擬素数解は通常解 $pm$ を含む.

## 4.1 $m$ が素数べきの場合

**定理 3** $m$ が素数べき $r^\varepsilon$ なら $a = r^\varepsilon p$ 問題の解は $r^\varepsilon p, (p : r$ 以外の素数$)$ と擬素数解 $r^{2\varepsilon+1}$.

Proof
$m$ が素数べき $r^\varepsilon$ の場合, まず $a = mp = r^\varepsilon p$ (ここで $p \neq r$, 素数) とおきあらかじめ 記号 $N = r^{\varepsilon+1} - 1, \overline{r} = r - 1$ を導入しておく.

$$\sigma(a) = \sigma(r^\varepsilon)\sigma(p) = \frac{N}{\overline{r}}(p+1) = \frac{N}{\overline{r}}(\frac{a}{r^\varepsilon}+1)$$

となる. 分母を払うと,

$$r^\varepsilon \overline{r}\sigma(a) = N(a + r^\varepsilon).$$

さてこれを $a$ を未知数とする方程式と考える. そしてこの式を分数に組み替える.

$$\frac{\overline{r}\sigma(a)}{a + r^\varepsilon} = \frac{N}{r^\varepsilon}$$

$\frac{N}{r^\varepsilon}(= \frac{r^{\varepsilon+1}-1}{r^\varepsilon})$ は既約分数なので, 既約分数の原理により, 自然数 $k$ があり,

$$\overline{r}\sigma(a) = kN, a + r^\varepsilon = kr^\varepsilon.$$

$k_1 = k - 1$ とおくと右の式から $a = kr^\varepsilon - r^\varepsilon = k_1 r^\varepsilon$.

1). $k_1$ と $r$ が互いに素のとき.

$a = k_1 r^{\varepsilon}$ より $\sigma(a) = \sigma(k_1)\sigma(r^{\varepsilon}) = \sigma(k_1)\dfrac{N}{\overline{r}}$. これより $\overline{r}\sigma(a) = N\sigma(k_1)$.

しかし, $\overline{r}\sigma(a) = kN$ も成り立つので, $N\sigma(k_1) = kN$. よって, $\sigma(k_1) = k = k_1 + 1$; $k_1$ は素数になり, $k_1 = q$ とすれば $a = k_1 r^{\varepsilon} = r^{\varepsilon} q$. これは通常解.

2). $k_1$ と $r$ が互いに素でないとき.

$k_1 = r^e L, (e > 0$ ,$L$ は $r$ で割れない) と書ける.

$$\overline{r}\sigma(a) = kN = (k_1 + 1)N = (r^e L + 1)(r^{\varepsilon+1} - 1).$$

一方, $a = k_1 r^{\varepsilon} = r^{\varepsilon} r^e L = r^{\varepsilon+e} L$ によって, $\overline{r}\sigma(a) = W\sigma(L)$, ( ただし $W = r^{\varepsilon+e+1} - 1$). よって,

$$(r^e L + 1)(r^{\varepsilon+1} - 1) = W\sigma(L).$$

i) $L = 1$ のとき. $a = r^{\varepsilon+e}$ になるが, $e = \varepsilon + 1$ を以下で証明する.

$(r^e L + 1)(r^{\varepsilon+1} - 1) = W\sigma(L)$ に $L = 1$ を代入すると,

$$(r^e + 1)(r^{\varepsilon+1} - 1) = r^{e+\varepsilon+1} - 1.$$

左辺を展開すると

$$(r^e + 1)(r^{\varepsilon+1} - 1) = r^{\varepsilon+e+1} - r^e + r^{\varepsilon+1} - 1$$

これが右辺と等しいとおけば

$$r^{\varepsilon+e+1} - r^e + r^{\varepsilon+1} - 1 = r^{e+\varepsilon+1} - 1.$$

$r^e = r^{\varepsilon+1}$ によって, $e = \varepsilon + 1$. したがって $a = r^{\varepsilon+e} = r^{2\varepsilon+1}$. これは擬素数解.

ii) $L > 1$ のとき. $\sigma(L) \geq L + 1$ を用いると矛盾がでる. これを以下で示す.

$$(r^e L + 1)N = W\sigma(L) \geq WL + W.$$

中の項を消すと,

$$(r^e L + 1)N \geq WL + W.$$

これより

$$N - W \geq L(W - r^e N).$$

.

両辺を計算して $N - W = r^{\varepsilon+1} - r^{\varepsilon+e+1} = r^{\varepsilon+1}(1 - r^e) < 0$,

一方 $W - r^e N = r^{\varepsilon+e+1} - 1 - r^{\varepsilon+e+1} + r^e = r^e - 1 > 0$. 矛盾

End

表 1: $a = mp(, m = 6)$ 問題の解

| $a$ | 素因数分解 | 解の名前 |
|---|---|---|
| 24 | $2^3 * 3$ | 擬素数解 |
| 30 | $2 * 3 * 5$ | 通常解 |
| 42 | $2 * 3 * 7$ | 通常解 |
| 54 | $2 * 3^3$ | 擬素数解 |
| 66 | $2 * 3 * 11$ | 通常解 |
| 78 | $2 * 3 * 13$ | 通常解 |
| 102 | $2 * 3 * 17$ | 通常解 |
| 114 | $2 * 3 * 19$ | 通常解 |
| 138 | $2 * 3 * 23$ | 通常解 |
| 174 | $2 * 3 * 29$ | 通常解 |
| 186 | $2 * 3 * 31$ | 通常解 |
| 222 | $2 * 3 * 37$ | 通常解 |
| 246 | $2 * 3 * 41$ | 通常解 |
| 258 | $2 * 3 * 43$ | 通常解 |
| 282 | $2 * 3 * 47$ | 通常解 |
| 304 | $2^4 * 19$ | エイリアン解 |

$a = 6p$ 型の解は当然であるが $a = 24 = 6 * 2^2, a = 54 = 6 * 3^2$ は擬素数解として理解できる.

$a = 304 = 2^4 * 19$ はまったく異質な解なのでこれが出たときは本当に驚いた. そこでこのような異質の解をエイリアン解と呼ぶことにした. この用語なら高校生に喜ばれるに違いないと思ったのである. 結果的には小学生にも喜ばれることとなった.

パソコンで探すとさらにエイリアン解がでてきた.

表 2: $a = mp, m = 6$ のときの エイリアン解の一部

| $m = 6$ | $2 * 3$ |
|---|---|
| $a$ | 素因数分解 $(2^e q)$ |
| 304 | $2^4 * 19$ |
| 127744 | $2^8 * 499$ |
| 33501184 | $2^{12} * 8179$ |

エイリアン解とはいうものの $a$ の末尾の数は 4. 素因数分解は $2^e q$ の形をしており完全数と類似した美しい性質を持っている.

## 4.2 決定問題の解決

$\sigma(a) = 2a + 12$ を一般に解くことは難しい. 完全数の決定問題よりさらに難しい. オイラーに範をとって, $a$ を偶数と仮定してもなお証明が困難である. 思い切って 6 の倍数と仮定すれば完全な解決にいたる.

**定理 4** *$\sigma(a) = 2a + 12$ の解が 6 の倍数なら $a = 6p(e, f > 0, p \neq 2, 3$ :素数$)$ . ただし素因数分解が $a = 2^e 3^f$ の場合を除外する.*

Proof.

$a$ を素因子分解して $a = 2^e 3^f k$ $(k > 1, k$ は 2,3 で割れない$)$ とおく. このとき, $k$ が素数になることを示す.

$X = 2^e, Y = 3^f, A = 2X - 1, B = 3Y - 1$ とおくとき $2\sigma(a) = AB\sigma(k)$. よって次の基本式ができる.

$$AB\sigma(k) = 4XYk + 24.$$

$AB\sigma(k) = 3Y\sigma(k)A - A\sigma(k) = 4XYk + 24$ を整理して

$$(3\sigma(k)(2X - 1) - 4kX)Y = 24 + (2X - 1)\sigma(k).$$

$Y \geq 3$ により,

$$24 + (2X - 1)\sigma(k) \geq 3(3\sigma(k)(2X - 1) - 4kX) = 9\sigma(k)(2X - 1) - 12kX.$$

$$24 + 8\sigma(k) \geq (16\sigma(k) - 12k)X.$$

よって 4 で割り

$$2(\sigma(k) + 3) \geq X(4\sigma(k) - 3k).$$

$X \geq 2$ によって,

$$2\sigma(k) + 6 \geq X(4\sigma(k) - 3k) \geq 8\sigma(k) - 6k.$$

ゆえに

$$6k+6 \geq 6\sigma(k) \geq 6k+6.$$

$\sigma(k) = k+1$ が成り立ち, $k$ が素数になる.
End

$\sigma(k) = k+1$ が成り立てば素数になるという結果を使う点でオイラーの証明を想起させるものがある. 読者は本書の題名 (オイラーをモデルに数論研究) に偽りなしと思ってほしい.

さらに次の形で 擬素数解が求まる.

**命題 2** $\sigma(a) = 2a+12$ の解 $a$ が $a = 2^e 3^f (e, f \geq 1)$ となるなら, $a = 24$ または $54$.

Proof. (記号は踏襲する) ただし $k = 1$.
$A = 2X-1, B = 3Y-1$ とおくと,

$$AB = 4XY + 24.$$

これより計算を行うと

$$(2X-3)(Y-1) = 26.$$

$2X-3$ は奇数なので $26 = \alpha\beta$ において i) $\alpha = 1, \beta = 26$; $2X-3 = 1$ より $X = 2, Y = 27 = 3^3$.$a = 54$.
ii) $\alpha = 13, \beta = 2$; $X = 8, Y = 3$.$a = 24$.
End

**注意 2** $\sigma(a) = 2a+12$ の解 $a$ が $a = 2^e k$(*k* は *6* と互いに素 *)* となるなら, $k$ は素数で $k = 2^{e+1}-13$ を満たすことになるか.

これを示すことは可能かもしれない.
次の結果はそのための小さい一歩である.

**定理 5** $\sigma(a) = 2a+12$ の解 $a$ が $a = 2^e q^f, (e \geq 1, f \geq 2, q$ は 奇素数 *)* となるなら, $q = 3, f = 3, e = 1$. すなわち擬素数.

Proof
$a = 2^e k q^f, X = 2^e, Y = q^f$ とする. いつものように $A = 2^{e+1}-1, B = q^{f+1}-1$ とおくと,$\overline{q} = q-1$ とおくと $\overline{q}\sigma(a) = AB, A = 2X-1, B = qY-1$.
$\overline{q}\sigma(a) = 2\overline{q}a + 12\overline{q}$ を元に式を変形し

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

さらに式を変形して

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

ゆえに

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

$Y-1$ で割ると

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

$$2X-1=\overline{q}\frac{Y-1}{Y-1}+\frac{13\overline{q}}{Y-1}=\overline{q}+\frac{13\overline{q}}{Y-1}.$$

$f\geq 2$ なので順次調べる.

1) $Y=q^2$.
$\dfrac{13\overline{q}}{Y-1}=\dfrac{13}{q+1}$ は整数, $q+1$ は偶数. よって矛盾.

2) $Y=q^3$.
$\dfrac{13\overline{q}}{Y-1}=\dfrac{13}{q^2+q+1}$ は整数. $q^2+q+1=13$ になり, $q(q+1)=12$.
よって, $q=3$.
$2X-1=\overline{q}+\dfrac{13\overline{q}}{Y-1}=2+1$ によれば $X=2$. $a=2*3^3$, 擬素数.

3) $Y=q^f, f\geq 4$.
$q^{f-1}+\cdots+1>13$ が成り立つので矛盾.
End

次に $m\sigma(a)=\sigma(m)a+m\sigma(m)$ の解で $m$ の倍数ではないものを列挙する. したがって, 擬素数解と通常解以外の解を与えることになる. これらをエイリアン解という.

**注意 3** 擬素数解と通常解をあわせて *regular solutions,* それ以外を *singular solutions* というそうだ.

# 5 過剰数

$a$ が $\sigma(a) = 2a$ を満たすとき, $a$ を完全数という. そして, $a$ が $\sigma(a) > 2a$ を満たすとき, $a$ を過剰数という.

$k = \sigma(a) - 2a$ を過剰度 (abundance) という. たとえば $\sigma(a) = 2a + 12$ を満たす解を過剰度 12 の過剰数といい, これらは良く調べられてきた.

オンライン整数列大事典 (OEIS) というインターネットのサイトには膨大な情報が集められている.

私は OEIS で ($\sigma(a) = 2a + 12$ を満たす解) 24,30,42,54,66,78 を入力したら, 瞬時にこれは数列番号 A076496 という名前のついた数列であることを知らされた. そして次のように詳しい説明が続く.

```
A076496

Numbers n such that sigma(n) == 12 (mod n).

1, 24, 30, 42, 54, 66, 78, 102, 114, 121, 138, 174, 186, 222, 246, 258, 282, 304,
```

さらに $g(n) = 2n + 1 - \sigma(n)$ が定義され $g(n) = -11$ となる数 $n$ をタイプ $-11$ の cofacient numbers と呼ぶ, と書いてある.

同様に $\sigma(a) < 2a$ を満たすとき, $a$ を不足数という.

しかし, 過剰数, 不足数という用語があまり面白いものには思えなかった.

完全数の一般的研究を指向する私の立場に立ってみると $\sigma(a) = 2a + 12$ を満たす解 $a$ を平行移動 $-12$ の完全数というのが正しいのである.

なぜなら $p = 2^{e+1} - 1 + m$ が素数の時 $a = 2^e p$ は $\sigma(a) = 2a - m$ を満たすことが容易に示されるからである. これを平行移動 $m$ の完全数という.

## 6　エイリアン解の探索

$a = mp$ 問題を一般に考えて, エイリアン解のある場合を列挙してみよう. ここではエイリアン解を $m$ で割れない解と理解して探した.

実際には $3 \leq m \leq 500$ の範囲で $a$ が 100 万以下として探した.

やってみると意外なことに $m = 6, 28, 30, 44, 66$ などの場合はエイリアン解があるが, ある場合はむしろ少ない.

## 7　第 2 完全数 28 の場合

エイリアン解がある場合は 6 のつぎは,28. これら 6,28 は完全数という特殊な数である. 不思議だ. ここに何かあるのではないか.

表 3: $a = mp(m = 28)$ 問題の解

| $a$ | 素因数分解 | |
|---|---|---|
| 84 | $2^2 * 3 * 7$ | 通常解 |
| 140 | $2^2 * 5 * 7$ | 通常解 |
| 224 | $2^5 * 7$ | 擬素数解 |
| 308 | $2^2 * 7 * 11$ | 通常解 |
| 364 | $2^2 * 7 * 13$ | 通常解 |
| 476 | $2^2 * 7 * 17$ | 通常解 |
| 532 | $2^2 * 7 * 19$ | 通常解 |
| 644 | $2^2 * 7 * 23$ | 通常解 |
| 812 | $2^2 * 7 * 29$ | 通常解 |
| 868 | $2^2 * 7 * 31$ | 通常解 |
| 1036 | $2^2 * 7 * 37$ | 通常解 |
| 1148 | $2^2 * 7 * 41$ | 通常解 |
| 1204 | $2^2 * 7 * 43$ | 通常解 |
| 1316 | $2^2 * 7 * 47$ | 通常解 |
| 1372 | $2^2 * 7^3$ | 擬素数解 |

表 4: $a = mp, m = 28$

| $a$ | 素因数分解 |
|---|---|
| 4544 | $2^6 * 71$ |
| 9272 | $2^3 * 19 * 61$ |
| 14552 | $2^3 * 17 * 107$ |
| 25472 | $2^7 * 199$ |
| 74992 | $2^4 * 43 * 109$ |
| 495104 | $2^9 * 967$ |
| 6019264 | $2^6 * 163 * 577$ |
| 15317696 | $2^6 * 137 * 1747$ |
| 35019968 | $2^6 * 131 * 4177$ |
| 53032832 | $2^7 * 317 * 1307$ |

一般に, $m$ が完全数なら $\sigma(m) = 2m$ になり $a = mp$ 問題の方程式は

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

この解 $a$ は $-2m$ だけ平行移動した完全数である.

完全数においては, たとえば正規形の解 $2^e q$ ,(ここで $q = 2^{e+1} - 1 - 2m$:素数) があるので解が構成しやすい. また第 2 正規形の解 $2^e rq$ もアルゴリズムでかなり作れる.

$a = 28p$ 問題の方程式は $\sigma(a) = 2a + 56$ という簡単な形になる. それは $\sigma(28) = 56$ という特殊事情のせいである.

**定理 6** $\sigma(a) = 2a + 56$ の解が *28* の倍数であって $2^e 7^f$ でないなら $a = 28p(p \neq 2, 7$ :素数*)* と書ける.

Proof
$a = 2^e 7^f k(k > 1$ は 14 と互いに素, $e \geq 2, f > 0)$ と書けるので
$X = 2^e, Y = 7^f, A = 2X - 1, B = 7Y - 1$ とおくとき,
$a = XYk, 6\sigma(a) = AB\sigma(k)$ となるので
$6\sigma(a) = 12a + 6 * 56$ により, $\alpha = 6 * 56 = 336 = 2^4 * 3 * 7$ とおくと,
$6\sigma(a) = AB\sigma(k) = 12a + 6 * 56 = 12XYk + \alpha$ により

$$AB\sigma(k) = 12XYk + \alpha$$

を得る. これが基本式になる. これを $Y$ で整理すると

$$Y(7A\sigma(k) - 12Xk) = A\sigma(k) + \alpha.$$

$Y \geq 7$ によると

$$A\sigma(k) + \alpha = Y(7A\sigma(k) - 12Xk) \geq 7(7A\sigma(k) - 12Xk) = 49A\sigma(k) - 42(A + 1)k.$$

よって,

$$\alpha = 8 * 42 \geq 48A\sigma(k) - 42(A+1)k.$$

6 で割り,$A \geq 7 = 2 * 4 - 1$ によると

$$56 \geq A(8\sigma(k) - 7k) - 7k \geq 7(8\sigma(k) - 7k) - 7k = 56(\sigma(k) - k).$$

56 で除せば

$$1 \geq \sigma(k) - k.$$

これより $1 \geq \sigma(k) - k$ が導かれ, $k$ は素数. しかもここで等号が成り立つので, 遡ってみな等号になり, $Y = 7, A = 7, X = 4$.

End

次の結果は擬素数の解を与える.

**定理 7** $\sigma(a) = 2a + 56$ の解が $2^e 7^f$ と書けるなら $a = 2^5 * 7, 4 * 7^3$.

## 8 完全数の一定理

かくして $m = 28$ のとき $\sigma(a) = 2a + 2m$ の解 $\alpha$ が $m$ で割れると仮定すると,

$\alpha$ は $56p$ または擬素数解になる ($\alpha = 2^5 * 7, 4 * 7^3$).

という結果が証明できた. ほかの完全数でもできるかもしれない, と思った.

水谷さんは学習院大学でのゼミで同じ結果は一般の完全数でも成り立ち証明もできると伝えてくれた (2018 年 1 月).

$m = 28$ の場合ができたばかりだが, 水谷さんに背中を押されて一般の完全数での証明を試みた. できてみると, この定理は完全数の理論の中でも輝かしい成果と言ってもよいように思う.

**定理 8** $m$ が完全数のとき $\sigma(a) = 2a + 2m$ の解 $\alpha$ は $m$ で割れると仮定すると, $\alpha$ は通常解, または擬素数解になる.

Proof (by Iitaka)

$m$ は偶数完全数とする. $m = 2^\varepsilon q, (q = 2^{\varepsilon+1} - 1 :$ は素数) と書ける (オイラーの定理).

仮定より $\alpha = 2^e q^f k, (e \geq \varepsilon, f > 0, k : 2, q$ で割れない数 $k)$ と書ける.

$X = 2^e, Y = q^f, A = 2X - 1, B = qY - 1, \overline{q} = q - 1$ とおくとき, $\alpha = XYk, \overline{q}\sigma(a) = AB\sigma(k)$ となるので $\sigma(\alpha) = 2\alpha + 2m$ に $\overline{q}$ を掛けて

$$\overline{q}\sigma(\alpha) = 2\overline{q}\alpha + 2m\overline{q}.$$

これを書き直すと,

$$AB\sigma(k) = 2\overline{q}XYk + 2m\overline{q}.$$

$B = qY - 1$ を用いて $Y$ について式を整理する.

$$A\sigma(k)(qY - 1) = Aq\sigma(k)Y - A\sigma(k) = 2\overline{q}XkY + 2m\overline{q},$$

となり

$$A\sigma(k) + 2m\overline{q} = (-2\overline{q}Xk + Aq\sigma(k))Y.$$

$Y \geq q$ を用いて

$$\begin{aligned} A\sigma(k) + 2m\overline{q} &= (-2\overline{q}Xk + Aq\sigma(k))Y \\ &\geq (-2\overline{q}Xk + Aq\sigma(k))q \\ &= -2q\overline{q}Xk + Aq^2\sigma(k) \\ &= -q\overline{q}k(A+1) + Aq^2\sigma(k) \\ &= A(q^2\sigma(k) - q\overline{q}k) - q\overline{q}k. \end{aligned}$$

よって,

$$2m\overline{q} \geq A(q^2\sigma(k) - q\overline{q}k - \sigma(k)) - q\overline{q}k.$$

$A = 2X - 1 \geq 2^{\varepsilon+1} - 1 = q, Q = q^2 - 1$ を使い式を整理する.

$$\begin{aligned} 2m\overline{q} &\geq A(Q\sigma(k) - q\overline{q}k) - q\overline{q}k \\ &\geq q(Q\sigma(k) - q\overline{q}k) - q\overline{q}k \\ &= qQ\sigma(k) - q\overline{q}k)(q+1) \\ &= qQ\sigma(k) - qk(q^2-1) \\ &= qQ(\sigma(k) - k) \end{aligned}$$

一方, $2m\overline{q} = 2^{\varepsilon+1}q\overline{q} = qQ$. ゆえに

$$2m\overline{q} = qQ \geq qQ(\sigma(k) - k).$$

よって,$qQ$ を払って,

$$1 \geq \sigma(k) - k.$$

$k > 1$ ならば $\sigma(k) - k \geq 1$ なので, $\sigma(k) - k = 1$ が成り立ち, $k$ は素数. 今までの不等号は等号になり, $e = \varepsilon, f = 1, \alpha = 2^{\varepsilon}qk = \alpha k$.

$k = 1$ ならば,

$$A\sigma(k)(qY - 1) = Aq\sigma(k)Y - A\sigma(k) = 2\overline{q}XkY + 2m\overline{q},$$

は

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

になり $2X = A + 1$ を代入して

$$A(qY - 1) = \overline{q}Y(A+1) + 2m\overline{q}$$

$A$ で揃えたら

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

$qY-\overline{q}Y-1=qY-(q-1)Y-1=Y-1$ によって,

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

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

$2m\overline{q}=qQ$ によって,

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

$$A=\overline{q}+\frac{q^3-1}{Y-1}.$$

$Y=q,q^2,q^3,q^f(f\geq 4)$ の場合ごとに計算する:

1) $Y=q$. $Y-1=\overline{q}$ になるので

$$A=\overline{q}+\frac{q^3-1}{q-1}=q-1+q^2+q+1=q^2+2q=(q+2)q=2^{2\varepsilon+2}-1.$$

$A=2X-1$ なので $2X-1=2^{2\varepsilon+2}-1$. よって, $X=2^{2\varepsilon+1}$

2) $Y=q^2$. 矛盾になる.
実際 $A=\overline{q}+\frac{q^3-1}{q^2-1}$, $\frac{q^3-1}{q^2-1}=\frac{q^2+q+1}{q+1}=q+1+\frac{-q}{q+1}$ は整数にならない.

3) $Y=q^3$.

$$A=\overline{q}+1=q=2^{\varepsilon+1}-1.$$

$A=2X-1$ により $X=2^{\varepsilon}$.
$\alpha=2^{\varepsilon}q^3$. 擬素数解.

4) $Y=q^f(f\geq 4)$.
$A=\overline{q}+\frac{q^3-1}{q^f-1}$ は $f\geq 4$ のとき整数にならない.
End

**定理 9 (広尾学園高校生 (外野亜美, 長洞花, 菅谷美羽))** $a = 21p$ 問題にはエイリアン解はない

$a = mp$ 問題でエイリアン解のある場合パソコンで調べると, $m = 6, 28, 44, \cdots$. これから $a = 21p$ 問題にはエイリアン解はない, ことが推定できる.

しかし, これは証明になっていない. 正しくは手計算できちんと証明する必要がある. 私がこの問題を高校生に提起したわけではない. 堀内先生の助言をえながら, 高校生が自分たちでやってこのような結果を得たのえある. 率直に言ってこれはスゴイと思う.

# 9　$m = 2r$,($r$:奇素数) の場合

ここからは少し一般論.

$a = mp$ 問題の研究において, $m = 2r$,($r$:奇素数) の場合,$r = 3$ のときエイリアンが出てきた. しかし, パソコンによる計算の結果によると $m = 10, 14, 22, 26$ などの場合はエイリアンが出てこないらしい.

次の著しい結果に到達した.

**定理 10**　$m = 2r$,($r$:奇素数) の場合,$r > 3$ とすると偶数のエイリアン解は無い.

Proof

$m = 2r$,($r$:奇素数) の場合, $\widetilde{r} = r + 1$ を使うと . $\sigma(m) = 3\widetilde{r}$ であり

$a = mp$, ($p \neq r$ の奇素数) については $a = mp = 2rp$ なので

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

$2r$ 倍して

$$2r\sigma(a) = 3\widetilde{r}a + 6r\widetilde{r}.$$

これを $a$ を未知数とする方程式とみなして解 $a$ を求める.

$r > 3$ としさらに (オイラーをモデルに) $a$ を偶数と仮定する.

方程式を $r$ を法としてみると,

$$3\widetilde{r}a \equiv 0 \mod r.$$

$3\widetilde{r}a \equiv 3a \equiv 0 \mod r$ によって, $r > 3$ と仮定しているので, $a \equiv 0 \mod r$. よって, $a$ は $r$ の倍数でさらに $a$ を偶数と仮定しているので, $a$ は $2r$ の倍数 でもある.

$a$ を素因数分解すれば ($k$ を 6 と互いに素の自然数とすると) $a = 2^e r^f k$ とおける.

$X = 2^e, Y = r^f$ と書くとき, $e \geq 1, f \geq 1$ なので, $X \geq 2, Y \geq r$.

$\overline{r} = r - 1$ を用いると,

$$\sigma(a) = \sigma(2^e r^f k) = (2^{e+1} - 1)\frac{r^{f+1} - 1}{\overline{r}}\sigma(k) = \frac{(2X - 1)(rY - 1)\sigma(k)}{\overline{r}}.$$

よって,

$$\overline{r}\sigma(a) = (2X - 1)(rY - 1)\sigma(k).$$

$A = 2X - 1, B = rY - 1$ を用いると, $\overline{r}\sigma(a) = AB\sigma(k)$ と簡潔に表せる.

$2r\sigma(a) = 3\widetilde{r}a + 6r\widetilde{r}$ に $\overline{r}$ を掛けると

$$2r\overline{r}\sigma(a) = 3\overline{r}\widetilde{r}a + 6r\overline{r}\widetilde{r}.$$

さらに $R = \overline{r}\widetilde{r} = r^2 - 1, B = rY - 1$ を用いて次のように式の変形を行う.

$$2r\overline{r}\sigma(a) = 3Ra + 6rR.$$

$$\begin{aligned}2r\bar{r}\sigma(a) &= 2rAB\sigma(k)\\ &= 2rA\sigma(k)(rY-1)\\ &= 2r^2A\sigma(k)Y - 2rA\sigma(k).\end{aligned}$$

$3Ra = 3RXYk$ により,$X = \dfrac{A+1}{2}$ を用いて

$$\begin{aligned}6rR &= 2r\bar{r}\sigma(a) - 3Ra\\ &= 2r^2A\sigma(k)Y - 2rA\sigma(k) - 3RXYk\\ &= 2r^2A\sigma(k)Y - 3RXYk - 2rA\sigma(k)\\ &= (2r^2A\sigma(k) - 3RXk)Y - 2rA\sigma(k)\\ &= (2r^2A\sigma(k) - 3R(\frac{A+1}{2})k)Y - 2rA\sigma(k).\end{aligned}$$

$Y \geq r$ によって

$$\begin{aligned}6rR &= (2r^2A\sigma(k) - 3R(\frac{A+1}{2})k)Y - 2rA\sigma(k)\\ &\geq (2r^2A\sigma(k) - 3R(\frac{A+1}{2})k)r - 2rA\sigma(k).\end{aligned}$$

$r$ で除して

$$6R \geq 2r^2A\sigma(k) - 3R(\frac{A+1}{2})k - 2A\sigma(k).$$

2 倍して,$A$ で括ると

$$12R \geq (4r^2A\sigma(k) - 3R(A+1)k - 4A\sigma(k) = (4r^2\sigma(k) - 3Rk - 4\sigma(k))A - 3Rk.$$

$A = 2X - 1 \geq 3$ によって

$$\begin{aligned}12R &\geq 3(4r^2\sigma(k) - 3Rk - 4\sigma(k)) - 3Rk\\ &= 3(4r^2-4)\sigma(k) - 12Rk\\ &= 12R\sigma(k) - 12Rk\\ &= 12R(\sigma(k) - k).\end{aligned}$$

$$12R \geq 12R(\sigma(k) - k).$$

それゆえ $1 \geq \sigma(k) - k$.

$k > 1$ なら $\sigma(k) - k \geq 1$ なので, $\sigma(k) - k = 1$. よって $k$ は素数. $X = 2, A = 3, Y = r$.

End

次に $k = 1$ の場合を扱う. 擬素数の解になることの確認.

**命題 3** $X = 2^e 2, Y = 3^f, A = 2X - 1, e > 0, f > 0$ のとき $6rR = 2r^2AY - 2rA - 3RXY$ を満たすなら $X = 2, Y = r^3$ または $X = 8, Y = r$.

Proof

$X = 2$ のとき $Y = r^3$. $X = 8$ のとき $Y = r$. は計算で出る.

$X = 4$ のとき $Y = \dfrac{3r^3 + 4r}{r + 6}$. $Y = r^2$ は解にならない.

End

## 10 $m = 4r$,($r$:素数) の場合

$a = mp$ 問題の研究において, $m = 4r$,($r$:奇素数) の場合,$r = 7, 11$ のときエイリアンが出てきた. しかし, パソコンによる計算の結果によると次の著しい結果に到達した.

**定理 11** $m = 4r$,($r$:奇素数) の場合,$r > 7$ とする. 解 $a$ を $4$ の倍数に限ればエイリアン解は無い.

Proof

$m = 4r$,($r$:奇素数) の場合,$\sigma(m) = 7r + 7 = 7\widetilde{r}$.

$a = 4rp, (p > 11 : \text{素数})$ に対して, $\sigma(a) = 7\widetilde{r}(p + 1) = \dfrac{7\widetilde{r}a}{4r} + 7\widetilde{r}$. よって,

$$4r\sigma(a) = 7\widetilde{r}a + 28r\widetilde{r}.$$

法 $r$ のとき

$$0 = 7\widetilde{r}a \equiv 7a \mod r.$$

これより $r \neq 7$ によって $a$ は $r$ で割れる. 解 $a$ を 4 の倍数に限るという仮定の下で $a = 2^e r^f k, (e \geq 2, f \geq 1, k$ は $2r$ と互いに素な素数.)

$X = 2^e, Y = r^f$ とおき $A = 2X - 1, B = rY - 1, \overline{r} = r - 1$ を用いると

$$\overline{r}\sigma(a) = AB\sigma(k), \widetilde{r}a = \widetilde{r}XYk.$$

$4r\sigma(a) = 7\widetilde{r}a + 28r\widetilde{r}$ に代入するために, $\overline{r}$ を掛けて式を整理する.

$R = \widetilde{r}\overline{r} = r^2 - 1$ とおくと

$$4r\widetilde{r}\sigma(a) = 7Ra + 28rR.$$

$$4rAB\sigma(k) = 7RXYk + 28rR.$$

$AB\sigma(k) = Ar\sigma(k)Y - A\sigma(k)$ なので, $Y$ でまとめる.

$$\begin{aligned}28rR &= 4rAB\sigma(k) - 7RXYk \\ &= 4Ar^2\sigma(k)Y - 4rA\sigma(k) - 7RXYk \\ &= (4Ar^2\sigma(k) - 7RXk)Y - 4rA\sigma(k).\end{aligned}$$

$X = \dfrac{A+1}{2}$ を代入するため 2 倍する.

$$56rR = (8Ar^2\sigma(k) - 7R(A+1)k)Y - 8Ar\sigma(k).$$

$k > 1$ のとき $Y \geq r$ を代入する.

$$\begin{aligned}56rR &= (8Ar^2\sigma(k) - 7R(A+1)k)Y - 8Ar\sigma(k) \\ &\geq (8Ar^2\sigma(k) - 7R(A+1)k)r - 8Ar\sigma(k).\end{aligned}$$

これより $r$ が両辺から落ちて

$$56R \geq 8Ar^2\sigma(k) - 7R(A+1)k - 8A\sigma(k).$$

右辺を $A$ で括る.

$$56R \geq (8r^2\sigma(k) - 7Rk - 8\sigma(k))A - 7Rk$$

$A \geq 7$ を代入する.

$$\begin{aligned}56R &\geq (8r^2\sigma(k) - 7Rk - 8\sigma(k))A - 7Rk \\ &\geq 7(8r^2\sigma(k) - 7Rk - 8\sigma(k)) - 7Rk \\ &= 7((8r^2\sigma(k) - 8Rk) - 8\sigma(k).\end{aligned}$$

56 で割った結果は

$$r^2\sigma(k) - Rk - \sigma(k) = R\sigma(k) - Rk.$$

ゆえに

$$56R \geq 56(R\sigma(k) - k).$$

これよりまとめると

$$1 + k \geq \sigma(k).$$

$1 \geq co\sigma(k) = \sigma(k) - k$ が出るので, $k$ 素数でかつ等号のみ成立.
ゆえに $Y = r, X = 4$. $a = 4rk$. これは通常解.

$k = 1$ のとき

$$56rR = (8Ar^2 - 7R(A+1))Y - 8Ar.$$

よって,

$$56rR = (8(2X-1)r^2 - 2*7RX)Y - 8(2X-1)r.$$

$$28rR = (4(2X-1)r^2 - 7RX)Y - 4(2X-1)r.$$

$$28rR + 4r^2Y - 4r = X((8r^2 - 7R)Y - 8r = X((r^2+7)Y - 8r.$$

$Y_1 = Y/r$ とおき $r$ で割って整理すると,

$$28R + 4rY - 4 = X((r^2+7)Y_1 - 8).$$

$F_0 = (r^2+7)Y_1 - 8, G_0 = 28R + 4rY - 4$ とおくとき $F_0X = G_0$.
$Y = r, r^2, r^3, r^f (f \geq 4)$ にしたがって計算する.

1) $Y = r$.
$Y_1 = 1, F_0 = (r^2+7)Y_1 - 8 = r^2 - 1 = R, G_0 = 4(7R + r^2 - 1) = 32R$ になり $X = G_0/F_0 = 32$.
$X = 32, Y = r$ により $a = 2^5 r$. これは擬素数解.
2) $Y = r^3$.
$Y_1 = r^2, F_0 = (r^2+7)r^2 - 8 = r^4 + 7r^2 - 7, G_0 = 4(7r^2 + r^4 - 8)$ になり $X = G_0/F_0 = 4$.
$X = 4, Y = r^3$ により $a = 4r^3$. これは擬素数解.

3) $Y = r^2$.
$Y_1 = r, F_0 = r^3 + 7r - 8, G_0 = 4(r^3 + 7r^2 - 8)$ になり $X = G_0/F_0 = 4$.
$X \geq 8$ なので, $G_0 = F_0X \geq 8F_0$. よって,
$G_0 = 4(r^3 + 7r^2 - 8) \geq 8F_0 = 8(r^3 + 7r - 8)$ により
$r^3 + 7r^2 - 8 \geq 2(r^3 + 7r - 8)$ により

$$0 \geq 2r^3 + 14r - 16 - (r^3 + 7r^2 - 8) = r^3 + 14r - 7r^2 + 8 = r^2(r-7) + 2(7r-4).$$

これより $r > 7$ により, 矛盾

4) $Y = r^f, f > 3$. この場合も同様の議論から矛盾が出る.
End

$m = 4r(r$:奇素数) の場合 $r = 7$ と $r \neq 7$ はここで差が出るのである.

$a$ が偶数の仮定だけでエイリアン解を探せるだろうか.

たとえば $m = 44$ において $a = 2Yk, Y = 11^f, k \neq 11, k > 2$ を仮定してエイリアンを探すなどの課題があるが読者に委ねる.

—

# 11　高橋君との研究交流

ときは 2017 年.T は高橋洋翔,I は飯高茂 による mail での研究交流

## 11.1　11 月 11 日,T から I へ

ipad で送られた ノートのコピーの内容
$\sigma(a) = 2(a + 6)$; ($a = 6p$ 問題の方程式)
そのエイリアン解は $a = 24 = 2^2 * 6, 54 = 6 * 3^2$ (しかしこれらは 擬素数解 )

$36\sigma(a) = 91(a + 36)$; ($a = 36p$ 問題の方程式)　のエイリアン解は
$a = 36 * 2^3, 36 * 3^3$. (しかしこれらは 擬素数解であることが判明 )

## 11.2　11 月 16 日,I から T へ

I から T へ 出した mail

1. $a = 6p$ 問題, $a = 30p$ 問題, $a = 42p$ 問題 のそれぞれのエイリアン解を比べてみよう

2.$a = 28p$ 問題, $a = 140p$ 問題　のエイリアン解をそれぞれ比べてみよう

## 11.3　11 月 16 日,T から I へ

直ちに返事:

$a = (6q)p$ 問題, ここで $q = 1$ または 2,3 以外の素数.$p \neq 2, 3, q$: の素数.
このエイリアン解 $a = 2^4 * 19 * q$
$a = (28q)p$, 問題, ここで $q = 1$ または 2,7 以外の素数.$p \neq 2, 7, q$: の素数.
このエイリアン解 $a = 2^6 * 71 * q, a = 2^3 * 19 * 61 * q$.

## 11.4 $a = mp, m = 30$ の場合

$a = 30p$ 問題の解の表

表 5: $a = mp, m = 30$

| $m = 30$ | $2 * 3 * 5$ |
|---|---|
| $a$ | 素因数分解 |
| 1520 | $2^4 * 5 * 19$ |
| 638720 | $2^8 * 5 * 499$ |

$a = 30p$ 問題のエイリアン解は $a = 6p$ 問題のエイリアン解 $2^4 * 19$ の 5 倍としてえられた.

## 11.5 11 月 18 日,T から I へ

これらのことから高橋洋翔は次の結果を予想し, 証明した.

**定理 12** $a = mp$ 問題の解 $\alpha$ について, $m, \alpha$ と互いに素な自然数 $q$ について $m' = mq$ とおくと $a' = \alpha q$ は $a = m'p$ 問題の解となる.

**定理 13** $a = mp$ 問題 について, $m$ と互いに素な自然数 $q$ について $m' = mq$ とおく. $\alpha$ は $a = m'p$ 問題の解で *1* 回だけ $q$ で割れるとする.

$a = \dfrac{\alpha}{q}$ は $a = mp$ 問題 の解になる.

## 11.6　12 月 14 日,I から T へ

I から T へ mail の内容.

> $a = 36p$ 問題に はエイリアン解がないことは証明できました
> $a = 44p$ 問題は $10 * 11^2$ というエイリアン解が出ます
> $a = 44 * 7p$ 問題は 侵入者が 1 つ、Home Grown が 3 個で著しい性質です
> $m < 500$ で $a = mp$ 問題のエイリアン解は調べました

## 11.7　$m = 36$ の場合

**定理 14** $a = 36p$ は通常解と擬素数解しかない.

言い換えればエイリアン解はない.

Proof.

$m = 36$ のとき $\sigma(m) = 7 * 13 = 91$ により問題の方程式は $36a = 91a + \alpha, \alpha = 3276 = 36 * 91 = 2^2 3^2 * 7 * 13$.

この式により $a$ は 4 の倍数であり 6 の倍数でもある.

$a$ を素因子分解して $a = 2^e * 3^f k(k$ は 2,3 で割れない,) とおく.$e \geq 2, f \geq 2$ を元に $e = f = 2$, $k$ が素数になることを示せばよい.

$X = 2^e, Y = 3^f$ とおき式を整理する,

$A = 2X - 1, B = 3Y - 1$ とおくとき $2\sigma(a) = AB\sigma(k)$.

よって次の基本方程式ができる.

$$18 * 2\sigma(a) = 18AB\sigma(k) = 91a + \alpha = 91XYk + \alpha.$$

$18AB\sigma(k) = 91XYk + \alpha$ を変形して (途中式を略す.)

$$18\sigma(k) - \alpha = Y(91Xk - 54(2X - 1)\sigma(k)) + 36X\sigma(k).$$

$$2\sigma(k) - 3 * 91 \geq (91k - 108\sigma(k))X + 54\sigma(k).$$

$1 + k \geq \sigma(k)$ が出る. したがって $1 + k = \sigma(k)$ になるのですべて等号が成り立ち $e = f = 2$.

パソコンでの検算結果を書く.

`uu(X,Y,k,s):=(18*(2*X-1)*(3*Y-1)*s-91*X*Y*k-3276);` `wxmaxima` での関数の定義

`126*s*(3*Y-1)-364*k*Y-3276` (`X=4` を代入)

`3276*s-3276*k-3276` (`Y=9` を代入)

$m = 6 * 7$ なので, $a = 6p$ 問題のエイリアン解 $\alpha$ があれば $7\alpha$ は皆, $a = 42p$ 問題のエイリアン解になる.

表 6: $a = mp, m = 42$

| $m = 42$ | 6*7 |
|---|---|
| $a$ | 素因数分解 |
| 2128 | $2^4 * 7 * 19$ |

表 7: $a = mp, m = 44$

| $m = 44$ | $2^2 * 11$ |
|---|---|
| $a$ | 素因数分解 |
| 1210 | $2 * 5 * 11^2$ |

## 11.8 $m = 44$ の場合

この場合は手強い.

$\sigma(a) = \dfrac{a\sigma(m)}{m} + \sigma(m)$ において $m = 44$ のときは

$\sigma(m) = \sigma(4)\sigma(11) = 7 * 12$ なので, $\dfrac{\sigma(m)}{m} = \dfrac{21}{11}$. よって, $\sigma(a) = \dfrac{21}{11} + 7 * 12$ になり

$$11\sigma(a) = 21a + 7 * 12 * 11.$$

これより $a$ は 11 の倍数なので, $a = 11Q$ と自然数 $Q$ で表される.

1) $Q$ は 11 で割れないとする.

$\sigma(a) = 12\sigma(Q)$ により

$$11 * 12\sigma(Q) = 11 * 21 * Q + 7 * 12 * 11.$$

よって,11 で除して

$$4\sigma(Q) = 7Q + 7 * 4.$$

したがって, $Q$ は偶数になり $Q = 2^{\varepsilon}Q_1$ ($Q_1$ は奇数) とおく. ここで $\varepsilon \geq 2$.

$W = 2^{\varepsilon+1} - 1$ とおくとき, $\sigma(Q) = W\varepsilon(Q_1)$.

よって

$$4W\sigma(Q_1) = 7 * 2^{\varepsilon}Q_1 + 7 * 4.$$

4 で割ると

$$W\sigma(Q_1) = 7 * 2^{\varepsilon-2}Q_1 + 7.$$

$$7 * 2^{\varepsilon-2}Q_1 + 7 = W\sigma(Q_1) \geq W(Q_1 + 1) = WQ_1 + W.$$

$$(7 * 2^{\varepsilon-2} - W)Q_1 + 7 \geq W - 7 = 2^{\varepsilon+1} - 8 \geq 0.$$

$$7 * 2^{\varepsilon-2} - W = 7 * 2^{\varepsilon-2} - 2^{\varepsilon+1} + 1 = -2^{\varepsilon-2} + 1 \geq 0.$$

これより $\varepsilon - 2 = 0$. $W = 7$ なので, $4\sigma(Q_1) = 4Q_1 + 4$. 4 で割って $\sigma(Q_1) = Q_1 + 1$. したがって $Q_1 = p$ は素数で, $a = 44p$.

パソコンの結果によると, $Q$ は 11 で一度だけ割れる場合がある.
$a = 11^2 Q_2$ と自然数 $Q_2$ で表せて, $Q_2$ は 11 と互いに素.
$\sigma(11^2) = 12 + 121 = 133 = 7 * 19$ になり,

$$19\sigma(Q_2) = 33Q_2 + 12.$$

これを $Q_2$ の方程式と見るのだがこれを解くのが難しい.
パソコンによればこの解 $Q_2$ は 10 になるらしい.
実際, $19\sigma(10) = 19 * 3 * 6 = 342$, $33Q_2 + 12 = 342$.
しかし到底証明できそうもない. たぶん $a = 10 * 11^2$ が唯一のエイリアン解 がなのであろう.
この場合の研究はきわめて不十分.

### 11.9　12 月 14 日,I から T へ

## 12　$m = 44 * 7$ のエイリアン解

**事実 1** $m = 44 * 7$ に対する $a = mp$ 問題のエイリアン解
パソコンの結果をまず書く.

表 8: $a = mp, m = 44 * 7$ の解

| $m = 44 * 7$ | |
|---|---|
| $a$ | 素因数分解 |
| 8470 | $2 * 5 * 7 * 11^2$ |
| 49984 | $2^6 * 11 * 71$ |
| 101992 | $2^3 * 11 * 19 * 61$ |
| 160072 | $2^3 * 11 * 17 * 107$ |

解 $a = 8470 = 2 * 5 * 7 * 11^2$ は $m = 44$ でのエイリアン解 $a = 2 * 5 * 11^2$ が元になった侵入者であるが $a = 49984 = 2^6 * 11 * 71$,$101992 = 2^3 * 11 * 19 * 61$,$160072 = 2^3 * 11 * 17 * 107$ はすべて独立に生まれたエイリアンである.

これらを Home Grown と呼んでもいいかもしれない.

### 12.1　12 月 14 日,T から I へ

$a = 49984 = 2^6 * 11 * 71$,$101992 = 2^3 * 11 * 19 * 61$,$160072 = 2^3 * 11 * 17 * 107$ は $a = 28p$ 問題のエイリアンを 11 倍して得られた エイリアン, すなわち invador(侵入者) ではないでしょうか.
$a = mp, m = 44 * 7$ で見つけられたエイリアンは, $a = mp, m = 44$　からの　invador $a = 8470 = 2 * 5 * 7 * 11^2$ と $a = mp, m = 28$ とからの　invadors $a = 49984 = 2^6 * 11 * 71$,$101992 = 2^3 * 11 * 19 * 61$,$160072 = 2^3 * 11 * 17 * 107$ だったのです.
さらに探せば $a = mp, m = 44 * 7$ には本物の Home Grown エイリアンがいるかもしれない.

### 12.2　$a = mp, m = 66 = 6 * 11$

## 13　$m = 6q$ $(q \neq 2, 3$ **:素数)**

**注意 4** $m = 6q(q \neq 2, 3$*:素数)* の場合のエイリアン解 $\alpha$ は $a'q$ となる,*(*ここで $a'$ は $a = 6p$ 問題のエイリアン解.*)*

これらをとくに invador と呼ぶ.

これは正しそうであるが証明はできない. そこで証明の途中まで書いてみる.

$m = 6q$ のとき $\sigma(m) = \sigma(6)\sigma(q) = 12\widetilde{q}, (\widetilde{q} = q + 1)$ なので
$a = mp = 6qp(p \neq 2, 3, q$ : 素数$)$, とすると

$\sigma(a) = \sigma(mp) = \sigma(6qp) = 12(p+1)\widetilde{q}$ なので
$6q\sigma(a) = m\sigma(a) = 12(mp+m)\widetilde{q} = 12(a+6q)\widetilde{q}$ になり

$$q\sigma(a) = 2(a+6q)\widetilde{q}) = 2a\widetilde{q} + 12q\widetilde{q}.$$

ゆえに

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

mod$q$ で見ると分かるように $a$ は $q$ の倍数. よって $a = q\alpha$ と整数 $\alpha$ を用いて書ける.

1). $q$ と $\alpha$ が互いに素のとき.
$\sigma(a) = \widetilde{q}\sigma(\alpha)$ なので

$$q\widetilde{q}\sigma(\alpha) = 2q\alpha\widetilde{q} + 12q\widetilde{q}.$$

$q\widetilde{q}$ を払うと $\sigma(\alpha) = 2\alpha + 12$.
$\alpha$ は $a = 6p$ 問題の解になり, それを $q$ 倍して解 $a = q\alpha$ ができる.

2) 一般の場合
$a = q^{\varepsilon}\alpha_0$ と $q$ で割れない整数 $\alpha_0$ を用いて書ける. ここから先が難しい.

## 14 $m = 66p$ の場合

表 9: $a = mp, m = 66 = 6 * 11$

| $m = 66$ | $2 * 3 * 11$ |
|---|---|
| $a$ | 素因数分解 |
| 3344 | $2^4 * 11 * 19$ |
| 1405184 | $2^8 * 11 * 499$ |

## 15 $m = 6q$ の場合

さらに $m = 6q$ ($q \neq 2, 3$ :素数) となる $m$ を列挙する.
$m = 78 = 2 * 3 * 13 = 6 * 13$
$m = 102 = 2 * 3 * 17 = 6 * 17$

$m = 138$ $2 * 3 * 23$
$m = 222 = 2 * 3 * 37$
$m = 246 = 6 * 41$

$m = 258 = 2 * 3 * 43$ ,

$m = 282 = 6 * 47$
$m = 294 = 6 * 7^2$

$m = 318 = 6 * 53$

$m = 330 = 6 * 5 * 11$

$m = 354 = 6 * 59$

$m = 366 = 6 * 61$

$m = 402 = 6 * 67$

$m = 462 = 6 * 7 * 11$
$m = 474 = 6 * 79$
$m = 498 = 6 * 83$

**注意 5** $q$ を *2,3* と異なる素数とする. $m' = 6q$ とおく. $a = m'p$ 問題のエイリアンは $a = 6p$ 問題のエイリアンから来た　*invador.*

これは正しそうだ. しかし証明はまだできない.
$m = 150 = 2 * 3 * 5^2$ は $m = 6q^2$ $(q \neq 2, 3$ :素数$)$ の場合エイリアンは $a = 6p$ 問題のエイリアンから
$m = 210 = 2 * 3 * 5 * 7$ も同様. 実際解を調べてみよう.

表 10: $a = mp, m = 210$

| $m = 210$ | $2 * 3 * 5 * 7$ |
|---|---|
| $a$ | 素因数分解 |
| 10640 | $2^4 * 5 * 7 * 19$ |

## 15.1 $m = 28q$

$m = 28q(q \neq 2, 7$:素数) の場合もエイリアンは $a = 28p$ 問題のエイリアンから invador として来ることが推察できる.

$m = 476 = 28 * 7$ の場合は 第二完全数 28 からできた $a = 28p$ 問題のエリアンに 17 倍でできている.

表 11: $a = mp, m = 476$

| $a$ | 素因数分解 |
|---|---|
| 77248 | $2^6 * 17 * 71$ |
| 157624 | $2^3 * 17 * 19 * 61$ |
| 433024 | $2^7 * 17 * 199$ |

$m = 140 = 2^2 * 5 * 7$

$m = 252 = 2^2 * 3^2 * 7 = 9 * 28$
$m = 308 = 28 * 11$

$m = 364 = 28 * 13$
$m = 420 = 28 * 3 * 5$

$m = 476 = 28 * 17$
$m = 84 = 2^2 * 3 * 7 = 28 * 3$
$m = 476 = 2^2 * 7 * 17 = 28 * 17$

このように エイリアンは 完全数 $m$ についての $a = mp$ 問題のエイリアンからやってくる場合が多いらしい.

## 15.2 新しい顔

表 12: $a = mp, m = 132$

| $m = 132$ | $2^2 * 3 * 11$ |
|---|---|
| $a$ | 素因数分解 |
| 3630 | $2 * 3 * 5 * 11^2$ |

エイリアン解は $a = 3630 = 2 * 3 * 5 * 11^2$ だけだろうか.
これは新しい顔 (New face)

表 13: $a = mp, m = 270$

| $m = 270 = 2 * 3^3 * 5$ | |
|---|---|
| $a$ | 素因数分解 |
| 50508 | $2^2 * 3^2 * 23 * 61$ |
| 254208 | $2^8 * 3 * 331$ |

表 14: $a = mp, m = 224$

| $m = 224$ | $2^5 * 7$ |
|---|---|
| $a$ | 素因数分解 |
| 4240 | $2^4 * 5 * 53$ |
| 5096 | $2^3 * 7^2 * 13$ |
| 11968 | $2^6 * 11 * 17$ |
| 497536 | $2^7 * 13^2 * 23$ |

この場合のエイリアンは新しい顔 (New face) で規則性が見あたらない.
以上のニューフェースについては個々に調べる必要がある. しかしどれも難しいだろう.

## 15.3 第 3 完全数のとき

表 15: $a = mp, m = 496$ 第 3 完全数

| $m = 496$ | $2^4 * 31$ |
|---|---|
| $a$ | 素因数分解 |
| 2892 | $2^2 * 3 * 241$ |
| 6104 | $2^3 * 7 * 109$ |
| 170612 | $2^2 * 13 * 17 * 193$ |
| 458144 | $2^5 * 103 * 139$ |
| 10418176 | $2^{11} * 5087$ |
| 9223374165011070976 | $2^{31} * 4294968287$ |

これは第 3 完全数 から出てきたエイリアン解は今までのと違っている.

## 15.4 3 倍完全数のとき

表 16: $a = mp, m = 672$, 3 倍完全数 (By Hiroto Takahashi)

| $m = 672 = 2^5 * 3 * 7$ | | | |
|---|---|---|---|
| $a$ | 素因数分解 | エイリアン | $a = 224$ 問題から |
| 12720 | $2^4 * 3 * 5 * 53$ | invador | $4240 = 2^4 * 5 * 53$ |
| 15288 | $2^3 * 3 * 7^2 * 13$ | invador | $5096 = 2^3 * 7^2 * 13$ |
| 35904 | $2^6 * 3 * 11 * 17$ | invador | $11968 = 2^6 * 11 * 17$ |
| 96048 | $2^4 * 3^2 * 23 * 29$ | HomeGrown | |
| 1492608 | $2^7 * 3 * 13^2 * 23$ | invador | $497536 = 2^7 * 13^2 * 23$ |
| 16763328 | $2^6 * 3^3 * 89 * 109$ | HomeGrown | |

エイリアンのうち $a = mp = 224p$ 問題のエイリアンから 3 倍してできた invador はいくつもある.

## 15.5 高橋君の研究

$a = mp$ 問題では $m$ が完全数の場合が興味深い.

$m$ が完全数の定義は $\sigma(m) = 2m$. このとき, $a = mp$ 問題の方程式は $\sigma(a) = 2a + 2m$ となる. この場合は通常解, エイリアン解など多数の解が出てくる.

これに注目し高橋君は 3 倍完全数の場合に研究した.

3 倍完全数の定義は $\sigma(m) = 3m$ となる $m$ で例として 360,672 がある.

彼は私への ipad を用いたメールで, $a = 672p$ 問題でエイリアン解を複数発見したと知らせてくれた.

そのころ, 私はスマホを睡眠導入剤として使っていた.

あるとき, 夜も 11 時を過ぎたので寝ようとしてスマホを見ると,$a = 672p$ 問題でエイリアン解を複数発見したという知らせが高橋君から届いていた.

なぜ $a = 672p$ 問題に注目したのか, 彼の考えが分からず悩みを抱えたまま寝て, 翌朝パソコンで調べると彼の発見したエイリアンはすべて正しかった.

その後, 彼から 672 は 3 倍完全数なのでエイリアンが多いだろうと思って試みたという彼の説明を受けた.

同じく 3 倍完全数の 360 を用いた $a = 360p$ 問題ではエイリアン解は無いらしい, しかし $a = 672p$ 問題ではエイリアン解が続々と出てきたのである. 3 倍完全数に注目をした高橋君の目の付け所がシャープですね.

そこで私は 2 番煎じを試み,4 倍完全数を考えた. その定義は $\sigma(m) = 4m$ となる $m$.

例は $30240 = 2^5 * 3^3 * 5 * 7, 32760 = 2^3 * 3^2 * 5 * 7$. これらを発見したのはなんとデカルトだという.

$a = 30240p$ 問題ではエイリアン

$a = 687960 = 2^3 * 3^3 * 5 * 7^2 * 13, a = 1615680 = 2^6 * 3^3 * 5 * 11 * 17,$

$a = 10125360 = 2^4 * 3^2 * 5 * 7^3 * 41$　　が出てきた.
それに対して $a = 32760p$ 問題ではエイリアン解はないらしい.