数学の研究を始めよう (20) 2015/May
初めてあかされる擬素数の神秘

飯高 茂

平成 28 年 1 月 28 日

1　ユークリッド陪関数

$\sigma(a)$ とは自然数 a の約数の和でありこれを関数とみてユークリッド関数という. さらに $s(a)$ を a の相異なる素因子の個数とするとき $\widetilde{\sigma}(a) = \dfrac{\sigma(a)}{2^{s(a)}}$ とおきこれをユークリッド**陪関数**とよぶ. これは乗法性を持つ. すなわち a, b が互いに素な自然数なら

$$\widetilde{\sigma}(ab) = \widetilde{\sigma}(a)\widetilde{\sigma}(b)$$

が成り立つ. これは素因数分解の一意性によって成り立つ. 自然数での素因数分解の一意性はユークリッドらによる数学原論の最大の成果の 1 つだが, ユークリッド関数、陪関数のもつ乗法性はきわめて有用な結果である.

1.1　擬素数 の不思議

素数 p があれば $\sigma(p) = p + 1$ であり a を自然数とすると方程式 $\sigma(a) = a + 1$ の解である.

ポイントはこの逆が成り立つことである. $\sigma(a) = a + 1$ を満たすとき a は素数である.

これは定義からすぐ分かる: $a > 1$ のとき a の約数には $1, a$ があるがこの和が $1 + a$ なので $\sigma(a) = a + 1$ を満たすとき, 約数はもうない. だから a は素数.

同様に考えれば $\sigma(a) = a + 2$ を満たす自然数はないことが証明される. $\sigma(a) = a + 3$ を満たすとき $a = 4$.

1.2　素数 の 2 倍は何だ

素数は方程式 $\sigma(a) = a + 1$ の解として特徴づけられる. それなら素数 の 2 倍を特徴づける方程式は何だろう.

2013 年度から高校生の数学研究の助言活動を始めた私にとって高校生が興味を持ち, 研究して成果を出せるような問題を考えることが大切な課題となった.

そこで奇素数 p に対して,$a = 2p$ と書ける a の条件は何か, を問題とした.

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

まとめて $2\sigma(a) = 3a + 6$.

式はできたが手がかりを求めてエクセルに $\sigma(a)$ のデータを与えて $2\sigma(a) - 3a$ の順に並べ 6 になるときを調べてみた.

表 1: $2\sigma(a)=6$ の表

a	素因数分解	$2\sigma(a)-3a$
6	[2,3]	6
8	[2^3]	6
10	[2,5]	6
14	[2,7]	6
22	[2,11]	6
26	[2,13]	6
34	[2,17]	6
38	[2,19]	6
46	[2,23]	6
58	[2,29]	6
62	[2,31]	6

この表を観察すると $a=8=2^3$ を例外として $a=2p$ と書けることが推察できる.

1.3 $a=mp$ 問題の $\sigma(a)$ を用いた方程式

m の素因子でない素数 p について $a=mp$ とすると乗法性によって
$\sigma(a)=\sigma(mp)=\sigma(m)(p+1)=\sigma(m)(\frac{a}{m}+1)$ となるので

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

ができる. これが $a=mp$ 問題の $\sigma(a)$ を用いた方程式である.
とくに m が素数 q なら次の式をえる.

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

これの解は $a=qp(p\neq q,p$:素数) (通常解という) と $a=q^3$ (非通常解) だけである.
一般には, m が素数べき q^{ε} の場合非通常解は $a=q^{2\varepsilon+1}$ だけであることも容易に証明できる.
ユークリッド陪関数の方で素数の特徴付けを考えて見る.

2 $\widetilde{\sigma}(a)$ を用いた素数の定義方程式

素数 p があれば $\widetilde{\sigma}(p)=\frac{p+1}{2}$ なので方程式 $2\widetilde{\sigma}(a)=a+1$ ができる. この解は素数しかない, と言いたいところだが実は成り立たない.
実際 $a=20$ とおくと ,$s(a)=2$ なので $4\widetilde{\sigma}(a)=\sigma(a)$.
$\sigma(20)=\sigma(4)\sigma(5)=7\times 6=42=2(a+1)$. これより $4\widetilde{\sigma}(a)=\sigma(a)=2(a+1)$. よって $2\widetilde{\sigma}(a)=a+1$.
$20=2^2\times 5$ によって $e=2$ とおくと $e+1=3$ なので $2^{e+1}-3=5$ を満たす.
$r=2^{e+1}-3$ が素数のとき $2^e r$ を指数 e の擬素数 $\mathbf{p}_e$ という.
実は条件 : $2\widetilde{\sigma}(a)=a+1$ は a が素数または, e を指数とする擬素数となる必要十分条件なのである.

3　指数 e の擬素数

指数 e の擬素数を復習しておく.
$r = 2^{e+1} - 3$ が素数のとき $2^e r$ を指数 e の擬素数 $\mathbf{p}_e$ という. 例は次の通り.

- $2^2 \times 5 = 20 = \mathbf{p}_2$
- $2^3 \times 13 = 104 = \mathbf{p}_3$
- $2^4 \times 29 = 464 = \mathbf{p}_4$
- $2^5 \times 61 = 1952 = \mathbf{p}_5$
- $2^8 \times 509 = 130304 = \mathbf{p}_8$
- $2^9 \times 1021 = 522752 = \mathbf{p}_9$
- $2^{11} \times 4093 = 8382464 = \mathbf{p}_{11}$
- $2^{13} * 16381 = 134193152 = \mathbf{p}_{13}$
- $2^{19} \times 1048573 = 549754241024 = \mathbf{p}_{19}$

(続く)

指数 e の擬素数の指数 e は始めのうち順に 2,3,4,5 と並んでいる.
私はこれを見いだしたとき, ガリレオが望遠鏡で初めて木星を観察し 4 つの衛星を見いだした故事に思いをはせた.4 つの巨大衛星が衛星系をつくる様子が太陽系の雛形を連想させ宇宙観の革新へ導かれた.
最初の擬素数の指数が 4 つも小さいものがあった.5 番目の擬素数の指数は 8 であり, 次の指数は 9,11 となって擬素数自身もすぐに巨大化する. 巨大擬素数も発見が難しい.
しかし, メルセンヌ素数の発見に努めるより意味のある巨大擬素数ハンターになる方がかっこいいではないか.
$\widetilde{\vartheta}_2(a) = a - 2\widetilde{\sigma}(a)$ とおくとき a が素数なら $\widetilde{\vartheta}_2(a) = -1$ である. しかし指数 e の擬素数も $\widetilde{\vartheta}_2(a) = -1$ を満たし, 素数と擬素数が方程式 $\widetilde{\vartheta}_2(a) = -1$ の解の全てである. この事実が指数 e の擬素数の重要さを訴えている.

4　$a = mp$ 問題の $\widetilde{\sigma}(a)$ を用いた方程式

m の素因子でない素数 p について $a = mp$ とすると乗法性によって
$\widetilde{\sigma}(a) = \widetilde{\sigma}(mp) = \widetilde{\sigma}(m)\frac{p+1}{2}$, $p = \frac{a}{m}$ によって

$$\frac{2\widetilde{\sigma}(a)}{\widetilde{\sigma}(m)} = \frac{a}{m} + 1.$$

ができる. これが $a = mp$ 問題の $\widetilde{\sigma}(a)$ を用いた方程式である.
ここで $a = mp$ は自明な解であり通常解という.
$m = 2$ なら $\widetilde{\sigma}(2) = \frac{3}{2}$ により

$$8\widetilde{\sigma}(a) = 3a + 6.$$

$m = 3$ なら $\tilde{\sigma}(3) = 2$ により

$$3\tilde{\sigma}(a) = a + 3.$$

これらを方程式と見て解 a を決定したい. 見かけ上は簡単な問題のようだが, 現在のところこれらの完全解決にはほど遠い. そこで私が得た部分的な結果を紹介することに留める. 読者が $a = mp$ 問題の $\tilde{\sigma}(a)$ を用いた方程式を部分的にも解いて下されば問題提起者としてはとてもうれしい.

$8\widetilde{\sigma}(a)-3a=6$ の解を調べるために $8\widetilde{\sigma}(a)-3a$ の数表を作ってみた.

表 2: $8\widetilde{\sigma}(a)-3a$ の数表; 6 になる場合を中心に

a	素因数分解	$s(a)$	$\sigma(a)$	$\widetilde{\sigma}(a)$	$8\widetilde{\sigma}(a)-3a$
21	[3,7]	2	32	8	1
15	[3,5]	2	24	6	3
		中略			
94	[2,47]	2	144	36	6
106	[2,53]	2	162	40.5	6
118	[2,59]	2	180	45	6
122	[2,61]	2	186	46.5	6
134	[2,67]	2	204	51	6
142	[2,71]	2	216	54	6
146	[2,73]	2	222	55.5	6
158	[2,79]	2	240	60	6
166	[2,83]	2	252	63	6
178	[2,89]	2	270	67.5	6
180	$[2^2,3^2,5]$	3	546	68.25	6
3	[3]	1	4	2	7
171	$[3^2,19]$	2	260	65	7

$a<200000$ の範囲まで調べても $2p$(通常解) 以外の解は 180 だけである.$180=3^2\mathbf{p}_2$ と書ける.

5 $a=qp$ 問題

q を素数とし $\widetilde{q}=q+1,\overline{q}=q-1$ とおく.
$2\widetilde{\sigma}(a)=2\widetilde{\sigma}(qp)=\widetilde{q}\widetilde{\sigma}(p)=\frac{\widetilde{q}(p+1)}{2}=\frac{(a+q)\widetilde{q}}{2q}$ と変形すると

$$4q\widetilde{\sigma}(a)=\widetilde{q}(a+q). \tag{1}$$

これが $a=qp$ 問題のユークリッド陪関数での方程式である. これを解 a について解くのが課題である. 最初に $q=3$ のときパソコンでやってみよう.

$\mathbf{p}_2$ は指数 2 の擬素数である. 非通常解 60= $[2^2,3,5]$ も $3\times\mathbf{p}_2$ と書ける.

表 3: $a = 3p$ 問題の解

a	素因数分解
3	[3]
6	[2,3]
15	[3,5]
21	[3,7]
33	[3,11]
39	[3,13]
51	[3,17]
57	[3,19]
60	$[2^2, 3, 5] = 3 \times \mathbf{p}_2$
69	[3,23]
87	[3,29]
93	[3,31]
111	[3,37]

6 $a = qp$ 問題 の 例

6.1 $a = 2p$ 問題の非通常解

表 4: $a = 2p$ 問題; 非通常解のみ

a	素因数分解	$\widetilde{\sigma}(a)$	素因子の個数
2	[2]	1.5	1
180	$[2^2, 3^2, 5] = 3^2 \times \mathbf{p}_2$	68.25	5

$a = 2p$ 問題の非通常解は

$$a = 2, a = 3^2 \times \mathbf{p}_2 \tag{2}$$

しかないという結果である.

6.2 $a = 3p$ 問題の非通常解

しかるに $a = 3p$ 問題の非通常解は 3 から始まり 60,312,1392,5856,$\cdots$ と不思議な数が続く. これらを素因数分解すると,

$$[2^2, 3, 5], [2^3, 3, 13], [2^4, 3, 29], [2^5, 3, 61]$$

となりこれらは, 指数 2,3,4,5 の擬素数の 3 倍である. このことに気づいたとき私は深い感動に包まれた. 数学的感動を超えて神秘な世界の入り口にきたような気さえした.

$a = 3p$ 問題の解は $3P$ と書ける. P は 1, または 素数または擬素数になる, という美しい形でまとめられる.

表 5: $a = 3p$ 問題; 非通常解のみ

a	素因数分解	$\widetilde{\sigma}(a)$	素因子の個数
3	$[3]$	2	1
60	$[2^2, 3, 5] = 3 \times \mathbf{p}_2$	21	4
312	$[2^3, 3, 13] = 3 \times \mathbf{p}_3$	105	5
1392	$[2^4, 3, 29] = 3 \times \mathbf{p}_4$	465	6
5856	$[2^5, 3, 61] = 3 \times \mathbf{p}_5$	1953	7

6.3 $a = 5p$ 問題の非通常解

勇気をだして $a = 5p$ 問題の非通常解を探索する.

表 6: $a = 5p$ 問題; 非通常解のみ

a	素因数分解	$\widetilde{\sigma}(a)$	素因子の個数
5	$[5]$	3	1
150	$[2, 3, 5^2] = 3 \times \mathbf{p}_2$	46.5	4
520	$[2^3, 5, 13] = 3 \times \mathbf{p}_3$	157.5	5
2320	$[2^4, 5, 29] = 3 \times \mathbf{p}_4$	697.5	6
9760	$[2^5, 5, 61] = 3 \times \mathbf{p}_5$	2929.5	7

推測通り $a = 5p$ 問題の解は $5P$ と書ける. P は 1 または素数, または擬素数になる.

6.4 $a = 7p$ 問題の非通常解

表 7: $a = 7p$ 問題; 非通常解のみ

a	素因数分解	$\widetilde{\sigma}(a)$	素因子の個数
7	$[7]$	4	1
140	$[2^2, 5, 7] = 7 \times \mathbf{p}_2$	42	4
728	$[2^3, 7, 13] = 7 \times \mathbf{p}_3$	210	5
3248	$[2^4, 7, 29] = 7 \times \mathbf{p}_4$	930	6
13664	$[2^5, 7, 61] = 7 \times \mathbf{p}_5$	3906	7

私は推測結果の正しいことを信じつつ, パソコンに働いてもらい q =11,13,17,19,23,29 まで確認した. 結果は著しいものであった. しかし例外的な結果もあった.

6.5 $a = 13p$ 問題の非通常解

$\mathbf{p}_3 = 2^3 \times 13$ は出てこない. $a = 13p$ 問題の 13 が $\mathbf{p}_3$ の素因子と重なるからである.

表 8: $a = 13p$ 問題の非通常解

a	素因数分解
260	$[2^2, 5, 13] = 13 \times \mathbf{p}_2$
6032	$[2^4, 13, 29] = 13 \times \mathbf{p}_4$
25376	$[2^5, 13, 61] = 13 \times \mathbf{p}_5$

6.6 $a = 29p$ 問題の非通常解

表 9: $a = 29p$ 問題の非通常解

a	素因数分解
580	$[2^2, 5, 29] = 29 \times \mathbf{p}_2$
3016	$[2^3, 13, 29] = 29 \times \mathbf{p}_3$
56608	$[2^5, 29, 61] = 29 \times \mathbf{p}_5$

$\mathbf{p}_4 = 2^4 \times 29$ は出てこない. $a = 29p$ 問題の 29 が $\mathbf{p}_4$ の素因子と重なるからである.

私は結果をみながら次の推測をした.

6.7 $a = qp$ 問題の解

式 (1) の解は $q > 2$ かつ q が指数 e の擬素数 $\mathbf{p}_e$ の素数 Q (すなわち $\mathbf{p}_e = 2^e Q$ とかける) でなければ $a = q, qp, q\mathbf{p}_e$ と表せる.

7 $a = qp$ 問題の $\widetilde{\sigma}(a)$ を用いた擬素数解

$\widetilde{\sigma}(a)$ を用いた場合の方程式を再録すると $4q\widetilde{\sigma}(a) = \widetilde{q}(a+q)$.

指数 e の擬素数 $\mathbf{p}_e$ について q と $\mathbf{p}_e$ が互いに素と仮定する. すると $b = q\mathbf{p}_e$ が解となることを以下で確認しよう.

擬素数は

$$a - 2\widetilde{\sigma}(a) = -1$$

を満たす.

よって $\alpha = \mathbf{p}_e$ とおくとき $2\widetilde{\sigma}(\alpha) = \alpha + 1$ を満たすので

$$\begin{aligned} 4q\widetilde{\sigma}(b) &= 4q\widetilde{\sigma}(q\alpha) \\ &= 2q\widetilde{q}\widetilde{\sigma}(\alpha) \\ &= q\widetilde{q}(\alpha+1) \\ &= \widetilde{q}b + q\widetilde{q} \\ &= \widetilde{q}(b+q). \end{aligned}$$

q と $\mathbf{p}_e$ が互いに素であることは $\mathbf{p}_e = 2^e r$ とするとき $q \neq 2$ かつ $q \neq r$ がその条件である.

$q = 2$ では成り立たず, $q = r$ でもうまく行かない.

$\mathbf{p}_e = 2^e r$ と書ける素数 r は覚える価値がある.

$$r = 5, 13, 29, 61, 509, 1021, \cdots$$

この結果は重要なので定理としておく.

定理 1 q が素数のとき $a = qp$ 問題の $\widetilde{\sigma}(a)$ を用いた場合の方程式の解として指数 e の擬素数 $\mathbf{p}_e$ と q の積 $b = q\mathbf{p}_e$ がある. ただし q と $\mathbf{p}_e$ が互いに素とする.

ユークリッド関数 $\sigma(a)$ の場合は $a = qp$ 問題の擬素数解は q^3 だけであったが陪関数 $\widetilde{\sigma}(a)$ の場合は, 指数 e の擬素数 $\mathbf{p}_e$ を用いた解 $q \times \mathbf{p}_e$ が出てきた. しかも彼らは隊伍を組み威風堂々と出てきたのである. これらの擬素数解はたぶん無限にある. しかしその証明はきわめて困難であろう.

8 解の決定

以上の考察を踏まえて素数 q に対して 陪関数 $\widetilde{\sigma}(a)$ の場合の方程式

$$4q\widetilde{\sigma}(a) = \widetilde{q}(a+q)$$

の解を求めよう. しかしながら, 一般に解くことは困難なので $s(a) = 1, 2, 3$ に限定して考える.

9　$s(a)=1$ のときの解

$s(a)=1$ のとき $2\widetilde{\sigma}(a)$ は整数なので mod q で考えると

$$4q\widetilde{\sigma}(a)\equiv 0, \widetilde{q}(a+q)\equiv -a \bmod\ q$$

よって a は q の倍数.

しかし $s(a)=1$ によると $a=p^e$ と素数 p で書けるから $p=q$. よって $a=q^e$.

$e=1$ なら $a=q$ でこれは解になる.

$e>1$ なら $a=q^e$ により $Q=q^e$ とおくと $4q\widetilde{\sigma}(q^e)=2q\frac{qQ-1}{\overline{q}}=\widetilde{q}(q^e+q)$ によって $\overline{q}\widetilde{q}=q^2-1$ に注意すると

$$2q(qQ-1)=(q^2-1)(q^e+q).$$

q で除して

$$2(qQ-1)=(q^2-1)(q^{e-1}+1).$$

mod q で考えると $e>1$ によって

$$-2\equiv 2(qQ-1)=(q^2-1)(q^{e-1}+1)\equiv -1 \bmod\ q.$$

これより $-1\equiv 0 \bmod\ q$ なので矛盾.

したがって, このとき $a=q$ という最も簡単な解しかないことが分かった. ユークリッド関数 $\sigma(a)$ のときには q^3 のような非通常解があった. このことは 陪関数の方が強い性質を持つことを意味するのだろう.

10　$s(a)=2$ のときの解の決定

$s(a)=2$ を仮定するとき $4\widetilde{\sigma}(a)$ は整数なので mod q で考えると

$$\widetilde{q}a\equiv 0 \bmod\ q$$

になるので $\widetilde{q}a\equiv -a$ によって a は q で割れる.

$s(a)=2$ により $a=q^er^f$ の形にかける. ここで r は q と異なる素数である.

$X=q^e, Y=r^f, A=qX-1, B=rY-1$ とおくと

$$4q\widetilde{\sigma}(a)=\frac{qAB}{\overline{qr}}.$$

および

$$\widetilde{q}(a+q)=\widetilde{q}XY+\widetilde{q}q$$

に方程式を使うと

$$\frac{qAB}{\overline{qr}}=\widetilde{q}XY+\widetilde{q}q$$

$\rho=q^2-1$ とおくと $\overline{q}\widetilde{q}=\rho$ によって

$$qAB=\overline{r}\rho XY+\overline{r}q\rho. \tag{3}$$

これが基本方程式になる.

$-C = AB - qrXY$ とおけば $C = qX + rY - 1$. そこで基本方程式を変形して

$$\begin{aligned}\overline{r}q\rho &= qAB - \overline{r}\rho XY \\ &= q(qrXY - C) - \overline{r}\rho XY \\ &= RXY - q(qX + rY) + q \\ &= (RX - qr)Y - q^2X + q.\end{aligned}$$

ここで $R = q^2r - \rho\overline{r}$ とおいた. これを計算し

$$\begin{aligned}R &= q^2r - \rho\overline{r} \\ &= (\rho + 1)r - \rho(r - 1) \\ &= r + \rho.\end{aligned}$$

したがって $R = r + \rho = r^2 + r - 1$.

$RX - qr > 0, Y \geq r$ によって

$$\overline{r}q\rho \geq (RX - qr)r - q^2X + q = (Rr - q^2)X - qr^2 + q.$$

一方,

$$\begin{aligned}Rr - q^2 &= r^2 + \rho r - q^2 \\ &= r^2 + \rho r - \rho - 1 \\ &= r^2 - 1 + \rho(r - 1) \\ &= \overline{r}(r + 1 + \rho).\end{aligned}$$

$X \geq q$ なので

$$\overline{r}q\rho \geq (Rr - q^2)X - qr^2 + q \geq \overline{r}(r + 1 + \rho)q - q(r^2 - 1).$$

ゆえに

$$\overline{r}q\rho \geq \overline{r}(r + 1 + \rho)q - q\overline{r}(r + 1).$$

両辺を $\overline{r}q$ で割って整理すると

$$\rho \geq r + 1 + \rho - (r + 1) = \rho.$$

等号が成り立つことより $X = q, Y = r$. すなわち $a = qr$. これは通常解である.

11　$q=2$ のとき

$s(a)=3$ の場合の考察はなかなか難しいので最初は $q=2$ に限定して考える. すると方程式は次のようになる.

$$8\widetilde{\sigma}(a)=3a+6$$

この解を $s(a)=3$ の仮定のもとで求める.

11.1　a は偶数

$s(a)=3$ により相異なる素数 P,p,r を用いて a は $P^ep^fr^g$ の形にかける. ここで r は $P,p>2$ と異なる素数である. 以下, 議論の簡易化のため $g=1$ を仮定する.

このような仮定の下で a は 2 で割れることを示す. 背理法で証明するので P は奇数と仮定する.

$X=P^e,Y=p^f,A=PX-1,B=pY-1$ とおけば

$$8\widetilde{\sigma}(a)=\frac{AB\widetilde{r}}{\overline{P}\overline{p}}=3XYr+6.$$

$$AB\widetilde{r}=3\overline{P}\overline{p}(XYr+2).$$

これより

$$\begin{aligned}6\overline{P}\overline{p}=&AB\widetilde{r}-3\overline{P}\overline{p}XYr\\=&RXY-\widetilde{r}(PX+pY-1).\end{aligned}$$

ここで $R=Pp\widetilde{r}-3\overline{P}\overline{p}r$ とした.

$$RXY=6\overline{P}\overline{p}+\widetilde{r}(PX+pY-1)>0$$

により $R>0$.

$$\begin{aligned}R&=Pp\widetilde{r}-3\overline{P}\overline{p}r\\&=Pp\widetilde{r}-3P\overline{p}r+3\overline{p}r\\&=P(p\widetilde{r}-3\overline{p}r)+3\overline{p}r.\end{aligned}$$

そこで $p\geq 3$ によって

$$p\widetilde{r}-3\overline{p}r=p(\widetilde{r}-3r)+3r\leq 3(1-2r)+3r=3-3r<0.$$

ゆえに $P\geq 3$ によって

$$P(p\widetilde{r}-3\overline{p}r)\leq 3(p\widetilde{r}-3\overline{p}r)=3p\widetilde{r}-9\overline{p}r=3p(r+1)-9(p-1)r=3pr+3p-9pr+9r=3p+9r-6pr.$$

$$\begin{aligned} R &= P(p\widetilde{r} - 3\overline{p}r) + 3\overline{p}r \\ &\leq 3p + 9r - 6pr + 3\overline{p}r \\ &= 3p + 6r - 3rp = 3(p + 2r - pr) < 0. \end{aligned}$$

これで $R > 0$ に矛盾した.

11.2 R の計算

$P = 2$ がしめされたことより

$$RXY = 6\overline{p} + \widetilde{r}(2X + pY - 1).$$

$R = 2p\widetilde{r} - 3\overline{p}r = r(3 - p) + 2p$ になり

$\langle 1 \rangle$ $p = 3$ のとき $R = 6, r \geq 5$.

$\langle 2 \rangle$ $p = 5$ のとき $R = 10 - 2r > 0$. よって $R = 4, r = 3$.

$\langle 3 \rangle$ $p = 7$ のとき $R = 14 - 4r > 0$. よって $R = 2, r = 3$.

$p \geq 11$ ならば $R = 3r - p(r - 2) \leq 22 - 8r < 0$. よってこれは起きない.

以上により次の 3 つの場合に整理された.
a) $(p = 3, r \geq 5)$,$R = 6$, b) $(p = 5, r = 3)$,$R = 4$, c) $(p = 7, r = 3)$, $R = 2$.
これを順次調べる.

11.3 a) $(p = 3, r \geq 5)$

a) $(p = 3, r \geq 5)$ のとき $R = 6$. すると

$$12 - \widetilde{r} = 6XY - \widetilde{r}(2X + 3Y).$$

書き直して

$$\widetilde{r}(2X + 3Y - 1) = 6(XY - 2).$$

$r \geq 5$ より $\widetilde{r} \geq 6$.
ここで $\widetilde{r} = 6$ とすると

$$2X + 3Y - 1 = XY - 2.$$

$XY - (2X + 3Y) = 1$ なので

$$XY - 2X - 3Y = X(Y - 2) - 3(Y - 2) - 6 = 1.$$

$(X-3)(Y-2) = 7$. これより $X-3 = 1, Y-2 = 7$. よって $X = 2^2, Y = 3^2, r = 5; a = 2^2 \times 3^2 \times 5 = 180$. これは擬素数解.

$r \geq 7$ なら解がないことを一般に示したかったができなかった. $r \leq 104$ なら解がないことはエクセルの計算で確認済み.

11.4 b) $(p=5, r=3)$

b)$(p=5, r=3)$ のとき $R=4, \widetilde{r}=4, \overline{p}=4$ なので
$-4+24=4XY-4(2X+5Y)$ になりその結果

$$5=XY-2X-5Y=X(Y-2)-5(Y-2)-10.$$

ゆえに $15=(X-5)(Y-2)$.

$X-5=1,3,5$ になりその結果 $X=6,8,10$. そのうち $X=2^e$ は $X=8=2^3$. しかし $Y-2=5$ から $Y=7\neq 5^f$. 矛盾

11.5 c) $(p=7, r=3)$

c)$(p=7, r=3)$ のとき $R=2, \widetilde{r}=4, \overline{p}=6$ なので式 (**??**) によって

$$6\overline{p}-\widetilde{r}=36-4=32; 6\overline{p}-\widetilde{r}=RXY-\widetilde{r}(2X+pY)=2XY-4(2X+7Y)$$

したがって

$$16=XY-2(2X+7Y)=XY-4X-14Y=Y(X-14)-4X.$$

これより $X-14>0$. $Y\geq 7$ により
$16=Y(X-14)-4X\geq 7(X-14)-4X=3X-98$, なので $X\leq 34$. 結局 $X=16,32$.

$X=16$ ならば , $16=Y(X-14)-4X=2Y-64$. $Y=32+8=40\neq 7^f$. 矛盾
$X=32$ ならば , $16=Y(32-14)-4\times 32$.
$8+64=9Y.Y=8\neq 7^f$. 矛盾

12 $q\geq 3$ のとき

q が 3 以上の素数のとき問題の方程式は次のようになる.

$$4q\widetilde{\sigma}(a)=\widetilde{q}(a+q).$$

$\widetilde{\sigma}(a)$ は整数でないかもしれない. しかし分母は 2 のべきなので適当な $I=2^h(h:\text{整数})$ を乗じれば $I\widetilde{\sigma}(a)$ は整数である. そこで mod q で考える.

$$4Iq\widetilde{\sigma}(a)=\widetilde{q}(a+q)I \mod q.$$

これより

$$0\equiv\widetilde{q}(a+q)\equiv -aI \mod q.$$

よって, $Ia\equiv 0$. I, a は互いに素なので $a\equiv 0$.

以下では議論を簡単にするため $s(a)=3$ を仮定する.

12.1　解を $a = 2^e qr$ に限定

さらに, a は偶数で $a = 2^e qr(2 < q, r)$ と素因数分解できるとする. [1]
$8\widetilde{\sigma}(a) = \sigma(a) = (2^{e+1} - 1)\widetilde{qr}$ によって $\Gamma = 2^{e+1} - 1, \Delta = q + r$, および
$8\widetilde{\sigma}(a) = \Gamma(qr + \Delta + 1), a = (\Gamma + 1)qr$ を使うと基本方程式は

$$q\Gamma(qr + \Delta + 1) = \widetilde{q}(\Gamma + 1)qr + 2q\widetilde{q}.$$

q を払うと

$$\Gamma(qr + \Delta + 1) = \widetilde{q}(\Gamma + 1)r + 2\widetilde{q}.$$

さらに変形して

$$\Gamma(qr + \Delta + 1) = qr\Gamma + \Gamma r + \widetilde{q}r + 2\widetilde{q}$$

と変形して Γqr を両辺から引くと

$$\Gamma(\Delta + 1) = \Gamma r + \widetilde{q}r + 2\widetilde{q}.$$

Γr を左辺に移項して

$$\Gamma\widetilde{q} = \widetilde{q}r + 2\widetilde{q}.$$

よって $\widetilde{q}$ で除すと

$$r + 2 = \Gamma = 2^{e+1} - 1.$$

$r = 2^{e+1} - 3$ が素数なので $2^e r$ は指数 e の擬素数 $\mathbf{p}_e$ である.
したがって,$a = 2^e qr = q\mathbf{p}_e$ となり，指数 e の擬素数の素数倍となった.

これは, いくつかの条件付きとはいえ十分美しい結果である. 2015 年になって得られた最初の大成果となった.

[1] このような仮定は不自然で過大あるが現状ではやむを得ない. 読者の研究でこのような困難が克服できればよいのだが.