書泉講義2018/6/14
スーパー双子素数 , フェルマー素数のファミリ

飯高 茂

平成 30 年 6 月 14 日

1　出版記念会での問題

平成 30 年 3 月 8 日 (木) に行われた『完全数の新しい世界』の出版記念会で提出した問題は次の 2 つであった.

1.1　スーパー双子素数

与えられた 整数 $(a>0,b)$ に対して, $p=aq+b$ とおくとき p,q がともに素数なら (p,q) を a,b に関しての 超 (スーパー) 双子素数という.

1. 超双子素数が無限にある a,b はどんな条件を満たすか
2. 超双子素数が有限個の a,b は存在するか
3. 与えられた $(a>0,b)$ に対して超双子素数を無限に生成する方程式 ($\sigma(a)$,$\varphi(a)$ を用いてよい) を作れ

1.2　ウルトラ 3 つ子素数

与えられた 整数 $(a>0,b)$ に対して, 整数 $(a>0,b,c>0,d)$ に対して $p=aq+b, r=cq+d$ とおくとき p,q,r がともに素数なら (p,q,r) を a,b,c,d に関してのウルトラ 3 つ子素数という.

- ウルトラ 3 つ子素数が無限にある a,b,c,d はどんな条件を満たすか
- ウルトラ 3 つ子素数が有限個の a,b,c,d は存在するか
- 与えられた (a,b,c,d) に対して超双子素数を無限に生成する方程式 ($\sigma(a)$,$\varphi(a)$ を用いてよい) を作れ

高橋洋翔の解答.
1)
1.1 (i)$a+b\equiv 1 \mod 2$, (ii)a,b は互いに素
1.2 $a=1, b=Q-2$(Q:奇素数)
1.3 超双子素数を生成する方程式は
$\varphi(a\varphi(q)+a+b)=aq+b-1$
(このとき $q, p=aq+b$ はともに素数)

2)
2.1 (i) $a+b\equiv 1 \mod 2$, (ii) a,b は互いに素,(iii)$c+d\equiv 1 \mod 2$, (iv)c,d は互いに素.
ただし $b\not\equiv 0 \mod 3$: (水谷一による修正)
($a=c=1, b+d\equiv$ mod6 は除く)
2.2 $a=b=c=1, d=3$
2.3 $\varphi(a\varphi(q)+a+b)+\varphi(c\varphi(q)+c+d)=(a+c)q+b+d-2$
($q, p=aq+b, r=cq+d$ はともに素数)

2　ウルトラ三つ子素数の除外条件

水谷一さんはウルトラ三つ子素数の除外条件をより精密にすることを提案した

注意 1 (水谷一, 除外条件の精密化)**.**
$ac\equiv -bd\not\equiv 0 \mod 3$ を満たすときウルトラ三つ子素数は有限個 *(ただ 1 つ).*

Proof
I. $a\equiv c\equiv 1 \mod 3$ のとき $bd\equiv 2 \mod 3$.
i. $b\equiv 1, d\equiv 2 \mod 3$.
$p=aq+b\equiv q+1 \mod 3$. $r=cq+d\equiv q+2 \mod 3$.
$q\equiv 1 \mod 3$ なら $r\equiv 0 \mod 3$. $r=3$.
$q\equiv 2 \mod 3$ なら $p\equiv 0 \mod 3$. $p=3$.
例 $a=1, b=4, c=1, d=2$

解 :
```
q= 3 tab  p= 7 tab  r= 5
```

ii. $b\equiv 2, d\equiv 1 \mod 3$ 略
II. $a\equiv c\equiv 2 \mod 3$ のとき $bd\equiv 2 \mod 3$.
i. $b\equiv 2, d\equiv 1 \mod 3$.
$p=aq+b\equiv 2q+2 \mod 3$. $r=cq+d\equiv 2q+1 \mod 3$.
$q\equiv 1 \mod 3$ なら $r\equiv 0 \mod 3$. $r=3$.
$q\equiv 2 \mod 3$ なら $p\equiv 0 \mod 3$. $p=3$.
例 $a=2, b=1, c=2, d=5$

解 :

```
 q= 3 tab  p= 7 tab  r= 11
```

ii. $b \equiv 1, d \equiv 2 \bmod 3$.

略

3 プログラム

wxmaxima でのプログラムを公開する.

最初は, 手堅く次のプログラムを作った. (素数判定 の組み込み関数 (primep) を使うので気に入らない.)

```
super_twin(k,l,aa,bb):= for a:aa thru bb
do(if primep(a) then (b:k*a+l,
(if primep(b) then print(a,"tab",b)  else 1=1)) else 1=1);
```

$a = 4, b = 3$ で実行した結果

```
2 tab 11
5 tab 23
7 tab 31
11 tab 47
17 tab 71
19 tab 79
31 tab 127
```

高橋君の解答にある $\varphi(a)$ を用いた式による解答

```
  twin_primes(a,b,aa,bb):= for q:aa thru bb
do(w:totient(a*totient(q)+a+b)-(a*q+b-1),
if w=0 then (p:a*q+b, print(q,"=",factor(q),"tab",p,"=",factor(p))) else 1=1);
```

$a = 2, b = 3$ で実行した結果

```
2 = 2 tab 7 = 7
5 = 5 tab 13 = 13
7 = 7 tab 17 = 17
13 = 13 tab 29 = 29
17 = 17 tab 37 = 37
19 = 19 tab 41 = 41
29 = 29 tab 61 = 61
```

```
  super_triplet(k,l,s,t,aa,bb):= for a:aa thru bb
do(if primep(a) then (b:k*a+l,(if primep(b) then
(c:s*b+t, (if primep(c) then print(a,"tab",b,"tab",c) else 1=1))
else 1=1)) else 1=1);
```

$\sigma(a)$ による解答

```
  twin_primes_sigma(a,b,aa,bb):= for q:aa thru bb
do(w:divsum(a*divsum(q)-a+b)-(a*q+b+1),
if w=0 then (p:a*q+b, print(q,"=",factor(q),"tab",p,"=",factor(p))) else 1=1);
```

p=3q-2

```
3 = 3 tab 7 = 7
5 = 5 tab 13 = 13
7 = 7 tab 19 = 19
11 = 11 tab 31 = 31
13 = 13 tab 37 = 37
23 = 23 tab 67 = 67
37 = 37 tab 109 = 109
43 = 43 tab 127 = 127
47 = 47 tab 139 = 139
53 = 53 tab 157 = 157
61 = 61 tab 181 = 181
67 = 67 tab 199 = 199
71 = 71 tab 211 = 211
```

$\sigma(a)$ によるウルトラ 3 つ子素数を生成するプログラム

```
  triplet_primes_sigma(a,b,c,d,aa,bb):= for q:aa thru bb
do(w:divsum(a*divsum(q)-a+b)+divsum(c*divsum(q)-c+d)-((a+c)*q+b+d+2),
if w=0 then (p:a*q+b,r:c*q+d, print("q=",q,"tab","p=",p,"tab","r=",r)) else 1=1);
```

```
p=q+2,r=2q+3
 q= 5 tab  p= 7 tab  r= 13
 q= 17 tab  p= 19 tab  r= 37
 q= 29 tab  p= 31 tab  r= 61
 q= 137 tab  p= 139 tab  r= 277
 q= 197 tab  p= 199 tab  r= 397
 q= 227 tab  p= 229 tab  r= 457
 q= 269 tab  p= 271 tab  r= 541
 q= 599 tab  p= 601 tab  r= 1201
 q= 617 tab  p= 619 tab  r= 1237
 q= 659 tab  p= 661 tab  r= 1321
 q= 809 tab  p= 811 tab  r= 1621
 q= 827 tab  p= 829 tab  r= 1657
 q= 1277 tab  p= 1279 tab  r= 2557
 q= 1427 tab  p= 1429 tab  r= 2857
 q= 1607 tab  p= 1609 tab  r= 3217
 q= 2027 tab  p= 2029 tab  r= 4057
 q= 2087 tab  p= 2089 tab  r= 4177
 q= 2129 tab  p= 2131 tab  r= 4261
 q= 2309 tab  p= 2311 tab  r= 4621
 q= 2549 tab  p= 2551 tab  r= 5101
 q= 2789 tab  p= 2791 tab  r= 5581
```

定理 1. $\varphi(a\varphi(q)+a+b)=aq+b-1$ を満たすとき $q, p=aq+b$ はともに素数.

Proof

$A=a\varphi(q)+a+b$ とおくと, $\varphi(A)=aq+b-1$.

$A>1$ のとき, $\varphi(A)\leq A-1=a\varphi(q)+a+b-1\leq aq+b-1$. 条件式から $\varphi(A)=aq+b-1$. よって等号成立になって $\varphi(A)=A-1, \varphi(q)\leq q-1$.

ゆえに, A, q : 素数. $A=a\varphi(q)+a+b=aq+b$ は素数.

end

定理 2.

$$\varphi(a\varphi(q)+a+b)+\varphi(c\varphi(q)+c+d)=(a+c)q+b+d-2$$

を満たすとき $q, p=aq+b, r=cq+d$ はどれも素数.

Proof

$$A=a\varphi(q)+a+b, B=c\varphi(q)+c+d$$

とおくと $\varphi(A)+\varphi(B)=(a+c)q+b+d-2$.

$$\varphi(A)+\varphi(B)\leq A-1+B-1=(a+c)\varphi(q)+a+b+c+d-2.$$

$\varphi(A)+\varphi(B)=(a+c)q+b+d-2$ を左辺に代入すると

$$(a+c)q+b+d-2=\varphi(A)+\varphi(B)\leq(a+c)\varphi(q)+a+b+c+d-2.$$

ゆえに, 等号が成り立つので $\varphi(A)=A-1, \varphi(B)=B-1, \varphi(q)=q-1$.

A, B, q が素数であり, $A=a\varphi(q)+a+b=aq+b=p, B=cq+d=r$ になり $q, p=aq+b, r=cq+d$ はどれも素数.

end

問題 1. $\sigma(a\sigma(\alpha)-a+b)=a\alpha+b+1$ を満たすとき $\alpha, p=a\alpha+b$ はともに素数.

4 History

wiki にはスーパー双子素数やウルトラ三つ子素数に関連した素数の例が載っている.

1. Twin primes :$p, q = p + 2$ がともに素数.
2. Triplet primes :$p, q = p + 2$(または $p + 4$), $r = p + 6$ が素数
3. Cousin primes :$p, q = p + 4$ がともに素数
4. Sexy primes :$p, q = p + 6$ がともに素数 (最近 2011,2017 が sexy なことが注目された)
5. Sophie Germain primes :$p, q = 2p + 1$ がともに素数
6. Safe primes : $p, q = (p - 1)/2$ がともに素数
7. Balanced primes :$q = p - n, p, r = p + n$ (n は偶数)

双子素数が無限にあるだろうと最初に言ったのは Paul Staeckel (1862-1919).

wiki で取り上げたどの例も素数の対や三つ子の素数の例が無限にありそうなのだがもっとも簡単そうな双子素数の場合をこめて証明ができていない. 最良の結果は $(p, p+2, \cdots, p+246)$ の中に素数が複数あることは無限に起きる.

5 Dirichlet の定理

$p = aq + b$ において, $q = 2n + 1$ とおくと, $p = 2an + a + b$
高橋の条件をつける.
1.1 (i)$a + b \equiv 1 \mod 2$, (ii)a, b は互いに素
すると, $2a, a + b$ は互いに素となり次の定理が使える.
Proof
$\gcd(a, b)$ を a, b の最大公約数とする. $a - b = 1 + 2k$ とおく.

$$\begin{aligned} gcd(2a, a + b) &= gcd(a - b, a + b) \\ &= gcd(a - b, 2b) \\ &= gcd(a - b, 2a, 2b) \\ &= gcd(a - b, 2) \\ &= gcd(a - b, 2) \\ &= gcd(1 + 2k, 2) = 1. \end{aligned}$$

よって, $2a, a + b$ は互いに素.

定理 3 (Dirichlet の定理)**.** $p = an + b$ において,n をすべての自然数とするとき a, b が互いに素なら, 無限の素数 p が出る.

End

6　状況説明

超双子素数の概念はスーパーオイラー完全数の研究の過程でてきたものである (『 数学の研究をはじめよう (IV)』にあり, これは飯高と高橋の共同研究).

そして a,b が与えられたとき $q,p=aq+b$ がともに素数となる場合 (超双子素数) が無限にあるか? という自然な問いかけができた. これほど一般化して (例外の場合はあるにせよ) 超双子素数が無限にあるという主張は数学界では荒唐無稽なものと言われかねない.

私としては詳しい検討は後回しにしていた. 2018 年 3 月 8 日に書泉グランデで『完全数の新しい世界』の出版記念会をすることになりと超双子素数を軸に 1 時間の講演を組み立てた. この講演の予稿ができたので前日に高橋君に予稿を添付ファイルとして送付しておいた. 翌朝になってメールを調べたが, 彼からの返事は無かった. 超双子素数の発表とともに高橋君の結果を報告できたら, 聴衆がみな感心するだろうと考えてはいたのだが. そうは問屋が卸さなかった.

翌日の夕方に超双子素数とウルトラ 3 つ子素数に関する問題への解答が ipad を通して彼から送られてきた. それは想像以上にすばらしい解答だった.

超双子素数とウルトラ 3 つ子素数が無限にでてくる条件を求めることが問題だが彼の解答では, 素数が有限個になる条件をいくつか与えられている.

高橋君は素数が有限個になるこれらの条件を満たさない場合は超双子素数やウルトラ 3 つ子素数での素数が無限にあると確信しているのだろうと思った.

若い人は大胆だなと私は思った. 後にゼミで高橋君の解答を詳しく検討した. そのとき水谷一さんはウルトラ 3 つ子素数が有限個になる条件をより精密にした.

$a = 1, b = Q - 2(Q$:奇素数$)$ のとき, $p = q + (Q - 2)$ は $q = 2$ なら $p = Q$: 素数 $q > 2$ が素数なら奇数なので $p = q + (Q - 2)$ は偶数になる. したがって素数ではない.

これは自明な反例である. この他に反例はないらしい.(素数として 2 を使わない反例があるか)

7 Firoozbakht と Hasler の共著論文

Variations on Euclid's formula for perfect rumbers 2010 , J. of Integer Sequences
ここには注目すべき結果が与えられていた.

- 与えられた m について, $\sigma(x) = 2(x+m)$ の解の研究は前例がないのでここで紹介する.
- $m|x$ の場合の解を admirable number という.(A111592)
- m が完全数の場合の解の研究を行う.
- 第二正規解の探求を行う.

以後, 通例の記号に戻す.
$\sigma(a) = 2a - m$ の解, $m = -2\mu, \mu$:完全数の場合に第二正規解の探求.
$a = 2^e pq$, p, q は相異なる奇素数. $N = 2^{e+1} - 1, B = pq, \Delta = p + q$ を使う.
$\sigma(a) = \sigma(2^e pq) = N(B+\Delta+1), 2a = (N+1)B$ なので, $-m = \sigma(a) - 2a = N\Delta + N - B$.
ゆえに $-m - N = N\Delta - B$.
$p_0 = p - N, q_0 = q - N, B_0 = p_0 q_0$ とおくとき, $B_0 = B - N\Delta + N^2$ により,

$$-m - N = N\Delta - B = N^2 - B_0.$$

$D = N(N+1) + m$ とおくとき $B_0 = D$.
$p_0 = 2L_1, q_0 = 2L_2$ と定めて, $B_0 = 4L_1L_2, D = 2 * 2^e * N + m$ により
完全数 μ によって $m = -2\mu$ とすると, $-\mu = 2L_1L_2 - 2^e N$ となる, $L_1, L_2; p, q$ を求めたい.
簡単な場合から, 考える.
$L_1 = -2^{e-1}, p_0 = 2L_1 = -2^e$ とすると, $p = N + 2L_1 = 2^{e+1} - 1 - 2^e = 2^e - 1$:素数とする.
メルセンヌ素数. $q = 2L_2 + N$ なので, $-\mu = 2L_1L_2 - 2^e N = -2^e L_2 - 2^e N = -2^e(L_2 + N)$.
$L_2 = \dfrac{Q - N}{2}$ によって, $L_2 + N = \dfrac{Q + N}{2}$.
ゆえに, $N = 2p + 1$ により

$$\mu = 2^{e-1}(N + Q) = 2^{e-1}(2p + 1 + Q) = 2^e(p + (1 + Q)/2).$$

例 $\mu = 496 = 2^4 * 31$
$2^4 * 31 = 2^e(p + (1 + Q)/2)$

D 型解の例

表 1: $\sigma(a) - 2a = 56$ の解,28:完全数

a	factor
14552	$2^3 * 17 * 107$
9272	$2^3 * 19 * 61$
74992	$2^4 * 43 * 109$
35019968	$2^6 * 131 * 4177$
15317696	$2^6 * 137 * 1747$
6019264	$2^6 * 163 * 577$
53032832	$2^7 * 317 * 1307$
3365232128	$2^9 * 1277 * 5147$

$\sigma(a) - 2a = 992$ の解,496:完全数

a	factor
1764512	$2^5 * 67 * 823$
1006496	$2^5 * 71 * 443$
857312	$2^5 * 73 * 367$
458144	$2^5 * 103 * 139$
33058112	$2^6 * 131 * 3943$
12445504	$2^6 * 139 * 1399$
4041152	$2^6 * 233 * 271$
279108224	$2^7 * 263 * 8291$
148221824	$2^7 * 271 * 4273$
92407424	$2^7 * 283 * 2551$
44818304	$2^7 * 337 * 1039$
41162624	$2^7 * 353 * 911$
38943104	$2^7 * 367 * 829$
34699904	$2^7 * 419 * 647$
1274024704	$2^8 * 541 * 9199$
524187392	$2^8 * 601 * 3407$
433401088	$2^8 * 631 * 2683$
307032832	$2^8 * 751 * 1597$

表 2: $\sigma(a)-2a=2*8128$ の解,8128:完全数

a	factor
814735232	$2^7*257*24767$
115129472	$2^7*271*3319$

8 $m=-(2\mu+2)$ の スーパー完全数の解

$A=\sigma(a)+m, \sigma(A)-m=2a$ について $m=1+2\mu$,(μ: 完全数のとき).

$a=p$: 素数の解があるとする.

$A=\sigma(a)+m=p-2\mu-1$ なので, $p=A+2\mu+1$.

$$\sigma(A)=m+2a=-2\mu-2+2p.$$

一方, $p=A+2\mu+1$ により $-2\mu-2+2p=-2\mu-2+2(A+2\mu+1)=2A+2\mu$. ゆえに

$$\sigma(A)=2A+2\mu.$$

μ : 完全数なのでこの解には

i. 通常解 (B 型)　　$A=\mu Q$, ここで Q は μ と互いに素な任意の素数.

$A=p-2\mu-1$ により, $\mu Q=p-2\mu-1$. よって, $p=2\mu+1+\mu Q$. (p,Q) はスーパー双子素数.

ii. 擬素数 $\mu=2^{\varepsilon}q$ とおくとき,　　$A=\mu q^2$ または $\mu 2^{\varepsilon+1}$. $A/\mu=q^2, 2^{\varepsilon+1}$.

iii. エイリアン　A 型解 $A=2^e\pi$. $A=\quad 2^e\pi, a=2^{e+1}$ $p=A+2\mu+1$ が素数なら, A はスーパー完全数の解 $A=\sigma(a)+m, \sigma(A)-m=2a$ $p=a$ からでる. $A=p-(2\mu+1)$

iv. エイリアン　D 型解 $A=2^f\pi_1\pi_2$. ??? 何がどうなるか不明.

これについては数表を参照

表 3: μ, コンピュータによる調査, $b = A + 2\mu + 1$ おおく.

$\mu = 6$				
e	a	factor	b	factor
4	304	$2^4 * 19$	317	317(素数)
8	127744	$2^8 * 499$	127757	$7 * 18251$
12	33501184	$2^{12} * 8179$	33501197	$577 * 58061$
$\mu = 28$				
e	a	factor	b	factor
5	224	$2^5 * 7$	281	281
6	4544	$2^6 * 71$	4601	$43 * 107$
7	25472	$2^7 * 199$	25529	$7^2 * 521$
9	495104	$2^9 * 967$	495161	495161 (素数)
15	2145615872	$2^{15} * 65479$	2145615929	$3463 * 619583$
$\mu = 496$				
e	a	factor	b	factor
9	15872	$2^9 * 31$	16865	$5 * 3373$
13	126083072	$2^{13} * 15391$	126084065	$5 * 311 * 81083$
16	8524857344	$2^{16} * 130079$	8524858337	8524858337(素数)

表 4: μ, コンピュータによる調査, $b = A + 2\mu + 1$ おおく.

$\mu = 6, 28, 496, 8128$

μ	$1 + 2\mu$	c_1	c_2	$A1 = c_1 * \mu$	$A2 = c_2 * \mu$	b_1	b_2
6	13	4	9	24	54	37	67
28	57	8	49	224	1372	281	1429
496	993	16	961	7936	476656	8929	477649
8128	16257	128	16129	1040384	131096512	1056641	131112769

9　平行移動 m の スーパー完全数

$A=\sigma(a)$ とおくとき $\sigma(A)=2a+m$ を満たす.

解 a に素数解 p があるとする.

$A=\sigma(p)+m=p+1+m$ なので $\sigma(A)=\sigma(p+1+m)=2p+m$. $p=A-1-m$ を代入し,

$$\sigma(A)=2p+m=2A-2-m.$$

これは平行移動 $2+m$ の完全数の方程式とみる. さて一般に μ を完全数とするとき $\sigma(A)=2A+2\mu$ の解はよく分かっている.

i. 通常解 (B 型解)　ii. 擬素数解, iii. A 型解, iv. D 型解 v. 未知の解

そこで $-2-m=2\mu$ とおくとき, $m=-2\mu-2$ になり,5 つの型に応じて解がある.

i. 通常解 (B 型解). $A=\mu Q(Q:\mu$ と互いに素な素数). $A=p+1+m=\mu Q$ になり, $p=\mu Q+2\mu+1$:素数, Q :素数. すなわち, $Q,p=\mu Q+2\mu+1$ はスーパー双子素数.

ii. 擬素数解, $\mu=2^{\varepsilon}q,(q=2^{\varepsilon+1},q:$ 素数) のとき, $A_1=\mu q^2$, $A_2=\mu 2^{\varepsilon+1}$ が 2 つの擬素数解.

$b_1=1+2*\mu+A_1, b_2=1+2*\mu+A_1$ が素数ならよい.

不思議なことにこれらは $\mu=6,28,496,8128$ のとき解になる.

10　解 $3p$ の場合

$A=\sigma(a)+m$ とおくとき $\sigma(A)=2a+m$ を満たす解 a に素数解の 3 倍 $3p$ があるとする.

$A=\sigma(3p)+m=4p+4+m$ なので $\sigma(A)=\sigma(4p+4+m)=2a+m=6p+m$. $4p=A-4-m$ を代入するためにまず 2 倍する.

$$2\sigma(A)=12p+2m=3(A-4-m)+2m=3A-12-m.$$

ところで, 一般に $2\sigma(a)=3a+6$ の解は $a=8,2p(p>2:$ 素数) なので,

$-12-m=6$ とおくとき , $m=-18$. このとき通常解 i. $A=2Q$. ii. 擬素数解 $A=8$.

i. $A=2Q$ のとき, $A=4p-14=2Q$. これより, $Q=2p-7$. $p,Q=2p-7$ はスーパー双子素数.

ii. $A=8$ のとき, $A=4p-14=8$. これより, 解は無い.

wwwwwwwwwwwwwwwwwwwwwwwwwwww

qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq

参考文献

[1] 高木貞治, 初等整数論講義第 2 版, 共立出版社,1971.

[2] C.F.Gauss(カール・フリードリヒ ガウス), ガウス 整数論 (数学史叢書)(高瀬正仁訳), 共立出版社, 1995.

[3] 飯高茂 , (雑誌の連載) 数学の研究をはじめよう , 現代数学社 ,2013 ∼ .

[4] 飯高茂 , 『数学の研究をはじめよう (I),(II)』, 現代数学社 ,2016.

[5] 飯高茂 ,『 数学の研究をはじめよう (III),(IV)』, 現代数学社 ,2017.

[6] D.Suryanarayana, Super Perfect Numbers. Elem. Math. 24, 16-17, 1969.

[7] Antal Bege and Kinga Fogarasi,Generalized perfect numbers,Acta Univ. Sapientiae, Mathematica, 1, 1 (2009) 73–82.