新規まき直し 第1期2017年11月10日
スーパー 完全数, スーパー オイラ完全数

飯高 茂

平成 29 年 11 月 6 日

0.1 スーパー完全数の定義

$a=2^e$ とおくと $\sigma(a)=2^{e+1}-1$ となる. これを素数と仮定し q とおく. $\alpha=aq$ はユークリッドの完全数.

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

が成り立つ. 記号 $\sigma^2(a)=\sigma(\sigma(a))$ を用いると $\sigma^2(a)=2a$ と書き直せる.

一般にこれを満たす a をスーパー完全数と呼ぶ.

0.2 スーパー完全数についてオイラーの定理の類似

定理 1.

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

を満たす a は偶数のとき 2^{p-1} とかける. ここで $q=2^p-1$ はメルセンヌ素数.

1 スーパー完全数の m だけ平行移動

m だけ平行移動 m した狭義の完全数 α は定義により $q=2^{e+1}-1+m$ が素数になる e によって $\alpha=2^eq$ と書ける.

$a=2^e$ および $N=2^{e+1}-1$ とおくと,$N=\sigma(a)$, $q=N+m=\sigma(a)+m, q+1=2a+m$ を満たす.

q :素数 により

$$\sigma(q)=q+1.$$

この式の左辺 $=\sigma(q)=\sigma(\sigma(a)+m)$. 右辺 $=q+1=2a+m$

かくて

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

これを平行移動 m のスーパー完全数の方程式といいこの解 a を平行移動 m のスーパー完全数という.

命題 1. $a=2^e$ が平行移動 m のスーパー完全数ならば $q=2^{e+1}-1+m$ は素数となる.

とくに $2^e q$ は平行移動 m の狭義の完全数になる.
Proof.
式 $\sigma(\sigma(a)+m)=2a+m$ に $a=2^e$ を代入すると

$$\sigma(2^{e+1}-1+m)=2^{e+1}+m.$$

$q=2^{e+1}-1+m$ とおくとき, $\sigma(q)=q+1$. よって, q は 素数.

注意 1. 実例にあたると, a が偶数の仮定だけでも $a=2^e$ が導ける可能性がある.

1.1 $m=0$ のとき.

$m=0$ のときパソコンで計算してみる.

表 1: $\sigma^2(a)=2a$ の解

a	素因数分解	$2a-1$ (メルセンヌ素数)
16	2^4	31
64	2^6	127
4096	2^{12}	8191
65536	2^{16}	131071
262144	2^{18}	524287

偶数スーパー完全数は 2 のべき, すなわち $a=2^e$ であることはすでに示された.
パソコンで計算してみても奇数の解は見つからない.

1.2 $m=2$ のとき.

$m=2$ のとき, パソコンで計算してみると驚天動地の世界が現れた.
表を眺めた結果

- a が偶数なら 2 のべきになり,$2a+1$ にはフェルマ素数が並ぶ.
- a が奇数の場合は, 11,41, 107 などの素数が出る一方, 65,959 などの合成数も並ぶ.

2 素数解 p

$\sigma(\sigma(a)+m)=2a+m$ に素数の解 p があるとする. すると定義より $\sigma(p+1+m)=2p+m$ を満たす.
与えられた m に対し上式の解となる素数 p を探した.
$\sigma(p+1+m)=2p+m$ を満たす素数の表

表 2: $\sigma(\sigma(a)+2)=2a+2$

a	素因数分解	$2a+1$(Fermat 素数あり)
1	2^0	$3=2+1$
2	2^1	$5=2^2+1$
8	2^3	$17=2^4+1$
11	11	
41	41	
65	$5*13$	
107	107	
128	2^7	$257=2^8+1$
149	149	
881	881	
959	$7*137$	
2141	2141	
14363	$53*271$	
21119	7^2*431	
32768	2^{15}	$65537=2^{32}+1$
238895	$5*47779$	
967679	$23*42073$	

表 3: petit Fermat primes

m	prime	prime	prime	prime	prime	prime
-6	17					
-4	23	107	467	653	130307	
-2	7	29				
2	11	41	107	149	881	2141
3	5					
4	47	587				

$m=4$,$\sigma(p+5)=2p+4$ を満たす.
$p=$47,587.

これらの素数は居場所を探して彷徨っている難民のようだ. どこかに定住地を探したい.

3 通常解

$-49 \leq m \leq 9$ の範囲で調べた結果 $m = -28, -18, -14$ に限って無数の素数に対応した無数解があることが分かった. これらは通常解であり B 型解といってよい.

元祖完全数の平行移動 m で B 型解 αp がある場合,α は完全数, $m = -2\alpha$ に限っていた. 同様のことが究極の完全数でもありこの場合は超完全数が出てきた.

これと同様なことをスーパー完全数に期待しよう. すなわち、$m = -58, -28, -18, -14$ のとき B 型解が出てきたことに新しい研究の芽を感じる.

$m = -28$

この場合, $7p(p \neq 7:$ 素数$)$ の形の解が多い. ただし $q = 2p - 5$ は素数と仮定する.

$m = -28$ に対し,$q = 2p - 5$ が素数のとき, $a = 7p$ が解になることを確認しよう.

$m = -28$ を式 $\sigma(\sigma(a) + m) = 2a + m$ に代入すると $\sigma(\sigma(a) - 28) = 2a - 28$.

$a = 7p, (p \neq 7)$ とおくと $\sigma(a) - 28 = 8(p + 1) - 28 = 8p - 20 = 4(2p - 5)$. ここで, $q = 2p - 7$ は素数と仮定すると, $\sigma(a) - 28 = 4q$. したがって, $\sigma(4q) = 7q + 7$.

一方, $2a + m = 14p - 28 = 7(2p - 4) = 7(q + 1)$. よって, $\sigma(\sigma(a) - 28) = 2a - 28$.

表 4: $m = -28$

m	a とその素因数分解
-28	$16 = 2^4$
	$26 = 2 * 13$
	$35 = 5 * 7$
	$77 = 7 * 11$
	$98 = 2 * 7^2$
	$107 = 107$
	$119 = 7 * 17$
	$128 = 2^7$
	$161 = 7 * 23$
	$203 = 7 * 29$
	$329 = 7 * 47$
	$371 = 7 * 53$

$m = -18$

この場合,2 べきの解以外に $a = 3p$ の解が多い. さらに $q = 2p - 7$ は素数.

$m = -18$ に対し,$a = 3p$ かつ $q = 2p - 7$ が素数なら $a = 3p$ の解ができることを確認しよう.

$m = -18$ を式 $\sigma(\sigma(a) + m) = 2a + m$ に代入すると $\sigma(\sigma(a) - 18) = 2a - 18$.

$a = 3p, (p \neq 5)$ とおくと $\sigma(a) - 18 = 4(p+1) - 28 = 4p - 14 = 2(2p-7)$. ここで, $q = 2p - 7$ は素数と仮定する. $\sigma((\sigma(a) - 18)) = \sigma(2q) = 3q + 3$.

一方, $2a+m = 6p-18 = 3(2p-6) = 3(q+7)-18 = 3q+3$. よって, $\sigma(\sigma(a)-18) = 2a-18$.

表 5: $m = -18$

a	factor	$q = a/3$	$p = 2q - 7$
21	$3 * 7$	7	7
27	3^3		
39	$3 * 13$	13	19
57	$3 * 19$	19	31
111	$3 * 37$	37	67
129	$3 * 43$	43	79
201	$3 * 67$	67	127
219	$3 * 73$	73	139
237	$3 * 79$	79	151
309	$3 * 103$	103	199
327	$3 * 109$	109	211
417	$3 * 139$	139	271
471	$3 * 157$	157	307
579	$3 * 193$	193	379
669	$3 * 223$	223	439
831	$3 * 277$	277	547
921	$3 * 307$	307	607

$m = -14$

この場合, 素数 $a = p$ の解が多い. ただし, $q = (p - 13)/6$ とおくとき q は素数とする.

$m = -14$ を式 $\sigma(\sigma(a) + m) = 2a + m$ に代入すると $\sigma(\sigma(a) - 14) = 2a - 14$.

$a = p, p \neq 2, 3$ とおくと $\sigma(a) - 14 = p - 13$. ここで, $6q = p - 13$. q は素数と仮定すると, $\sigma(a) - 14 = 6q$. さらに, $\sigma(6q) = 12q + 12$. よって,

$$\sigma(\sigma(a) - 14) = 12q + 12 = 2p - 26 + 12 = 2a - 14.$$

q は素数との仮定は本質的仮定である.

$a = 317$ については $b = a - 13 = 304$ は 6 の倍数ではない. $304 = 2^4 * 19$ であって, $620 = \varphi(304)$ となり $2a + m = 2 * 317 - 14 = 620$. これは正しいから 317 は解である.

317 は通常解ではない.

解 a に対して $q = (a - 13)/6$ を次に示した.

$b/6$ が整数にすらならない解は独自の解であり, 一匹狼 (lonely wolf) と呼ばれるにふさわしい.

表 6: $m = -14$

a	factor	$b = a - 13$	$b/6$
37	37	24	4
43	43	30	5
64	2^6	51	8.5
67	67	54	9
79	79	66	11
127	127	114	19
128	2^7	115	19.16666667
151	151	138	23
199	199	186	31
247	13*19	234	39
271	271	258	43
317	317	304	50.66666667
331	331	318	53
367	367	354	59
379	379	366	61
439	439	426	71
487	487	474	79
512	2^9	499	83.16666667
547	547	534	89
619	619	606	101
631	631	618	103
691	691	678	113
907	907	894	149
919	919	906	151
991	991	978	163
1051	1051	1038	173
1087	1087	1074	179
1171	1171	1158	193
1279	1279	1266	211

4 スーパーオイラー完全数 I 型

スーパーオイラー完全数 I 型の定義をする.

スーパーオイラー完全数の I 型定義方程式は

$$2\varphi(\varphi(a)+1+m) = a+2m.$$

定理 2. $2\varphi(\varphi(a)+1+m) = a+2m$ の解は $a = 2^e$ となる. ただし $q = 2^{e-1}+1+m$ は素数.

Proof.

解は偶数なので $a = 2^e L, (L:\text{奇数})$ と書ける. $\varphi(a)+1+m = 2^{e-1}\varphi(L)+1+m$ により

$$\varphi(\varphi(a)+1+m) \leq \varphi(a)+m = 2^{e-1}\varphi(L)+m.$$

$2\varphi(\varphi(a)+1+m) = a+2m$ を使うと $\varphi(L) \geq L$. よって $L=1$, $a = 2^e$.

$x = \varphi(a)+1+m = 2^{e-1}+1+m$ とおくとき $2\varphi(x) = 2\varphi(\varphi(a)+1+m) = a+2m$ により

$$a+2m = 2^e+2m = 2\varphi(x) \leq 2(x-1) = 2^e+2m = a+2m.$$

ゆえに $2\varphi(x) = 2(x-1)$. したがって x は素数.

解 $a = 2^e$ は $\alpha = 2^e x$ の 2 べき部分.

かくしてスーパーオイラー完全数 I 型の解は明快にわかった. 分かりすぎるので物足らない. そこでスーパーオイラー完全数 II 型を新たに導入した.

5 スーパーオイラー完全数 II 型

$\sigma(a)$ の代わりにオイラー関数 $\varphi(a)$ を用いて平行移動 m のスーパーオイラー完全数 II 型を定義してみよう.

$q_0 = 2^e+1+m$ は素数とする. $a = 2^e$ とおく.

$a = 2\varphi(a)$ により $q_0 = 2\varphi(a)+1+m$. 代入して $\varphi(q_0) = \varphi(2\varphi(a)+1+m)$.

q_0 は素数だから $\varphi(q_0) = q_0-1$.

一方, $q_0-1 = a+m$. これらを組み合わせると,

$$\varphi(2\varphi(a)+1+m) = a+m.$$

これを スーパーオイラー完全数 II 型の定義式といい, この解をスーパーオイラー II 型完全数という.

5.1 m:偶数の場合

$\varphi(2\varphi(a)+1+m) = a+m$ において, m を偶数と仮定する. オイラー関数は自然数について定義されるので, $x = 2\varphi(a)+1+m \geq 1$.

一般に $\varphi(x)$ は $x>2$ なら偶数なので,

$\varphi(x)=a+m$ は偶数. それゆえ a も偶数. よって奇数の L によって $a=2^eL$ と書ける.

I.$x=2\varphi(a)+1+m>2$ とする. $\varphi(x)\le x-1=2\varphi(a)+m$.

$$a+m=\varphi(2\varphi(a)+1+m)=\varphi(x)\le x-1=2\varphi(a)+m$$

$$2^eL+m=a+m\le x-1=2\varphi(a)+m=2^e\varphi(L)+m.$$

$L\le\varphi(L)$ により, $L=1, a=2^e$. $x=2\varphi(a)+1+m=2^e+1+m$,

$$\varphi(x)=\varphi(2\varphi(a)+1+m)=a+m=2^e+m=x-1.$$

ゆえに $x=2^e+1+m$ は素数.

2)$x=2\varphi(a)+1+m=1$ とする.

$2\varphi(a)+m=0$.

$\varphi(2\varphi(a)+1+m)=a+m$ により, $1=a+m$. $2\varphi(a)+m=0$ なので $2\varphi(a)=-m=a-1$.

ところで, $2\varphi(a)=a-1$ を満たす a は存在しない, という予想がある. そこでこれを仮説として使う.

したがって, $x=2\varphi(a)+1+m=1$ となる場合はないと理解する. この仮説を用いた結果次の定理ができた.

定理 3. *m を偶数と仮定する. $\varphi(2\varphi(a)+1+m)=a+m$ の解は $a=2^e$, ここで, $Q=2^e+1+m$ は素数. (これを擬メルセンヌ素数とよぶ)*

ここで, $m=0$ なら $Q=2^e+1$ はフェルマ素数.

$m=-2$ なら $Q=2^e-1$ はメルセンヌ素数.

表 8: スーパーオイラー II 型完全数

$m=0$			$m=4$		
a	factor	擬メルセンヌ素数	a	factor	擬メルセンヌ素数
2	2	3	2	2	7
4	2^2	5	8	2^3	13
16	2^4	17	32	2^5	37
256	2^8	257	2048	2^{11}	2053

II. $x=2\varphi(a)+1+m=2$ とする. 定義式から $\varphi(x)=1=a+m$ によって, $2\varphi(a)=a, 1=a+m$. これより, $a=2^e, m=1-2^e$. m:奇数の場合になるが, これは, $m=1-2^e$ のとき解 $a=2^e$ があることを意味する.

5.2 m:奇数の場合

$\varphi(2\varphi(a)+1+m)=a+m$ の解を求める.

m を奇数と仮定する. 一般に $x>2$ なら $\varphi(x)$ は 偶数なので a も奇数.

命題 2. m を奇数 $2N-1$ とする. $m \geq -1$ の場合は $\varphi(2\varphi(a)+1+m) = a+m$ の解があると仮定すると ,1)$N=0$ のとき $m=-1, a=2,$ またはフェルマ素数, *2)* $N=1$ のとき $x=1, a=1$.

Proof.

$m = 2N-1$ なので $2\varphi(a)+1+m = 2(\varphi(a)+N)$ によって

$$\varphi(2(\varphi(a)+N)) = a+2N-1.$$

$b = \varphi(a)+N$ とおくとき $\varphi(2b) = a+2N-1$.

$b = \varphi(a)+N = 2^{\varepsilon}L(L:$ 奇数$)$ の形に書く.

$\varphi(2b) = \varphi(22^{\varepsilon}L) = 2^{\varepsilon}\varphi(L)$ を用いて次のように式変形を行う.

$L > 2$ のとき, $L - \varphi(L) \geq 1$ により

$$\begin{aligned} a+2N-1 &= \varphi(2b) \\ &= 2^{\varepsilon}\varphi(L) \\ &\leq 2^{\varepsilon}(L-1) \\ &= \varphi(a)+N-2^{\varepsilon} \\ &\leq a-1+N-2^{\varepsilon}. \end{aligned}$$

これより

$$a+2N-1 \leq a-1+N-2^{\varepsilon}.$$

$N \leq -2^{\varepsilon} \leq -1$. よって $m \leq -3$.

$L=1$ のとき, $b = \varphi(a)+N = 2^{\varepsilon}$.

一方, $2^{\varepsilon} = \varphi(2b) = a+2N-1$, により

$$a+2N-1 = 2^{\varepsilon} = \varphi(a)+N$$

$a > 1$ ならば

$$a-\varphi(a)+2N-1 = N+1-2N = 1-N.$$

ゆえに $N=0, a-\varphi(a)=1$.

したがって, $b = 2^{\varepsilon} = \varphi(a)+N = a-1$.

ゆえに,$a = 1+b = 1+2^{\varepsilon}$ は素数なのでこれが奇数ならフェルマ素数. $\varepsilon = 0$ のとき, $a=2$. したがって, $a=2$, またはフェルマ素数

$a=1$ ならば $a+2N-1 = \varphi(a)+N$ に代入すれば, $2N = 1+N$. よって,$N=1$.

5.3　$m = 1 - 4k$ の場合

m が奇数のとき $m = 1 - 4k, m = -1 - 4k$ の 2 通りある.
高橋洋翔のプリントにしたがい,$m = 1 - 4k, (k > 0)$ とする.
$\varphi(2\varphi(a) + 2 - 4k) = a + 1 - 4k$ となる.
$b = \varphi(a) + 1 - 2k$ とおくと, これは奇数.
$k > 0, 2\varphi(a) \geq 4k - 2 + 2 \geq 4$ により $\varphi(a) \geq 2$. よって $a > 2$.
かくして

- $a + 1 - 4k = \varphi(b)$
- $b = \varphi(a) + 1 - 2k$

これを a, b についての連立方程式とみる.
ここにおいて, $b = 1$ と仮定すると, $\varphi(a) - 2k = 0, a = 4k$. よって, $2\varphi(a) = a$ が成り立つので, $a = 2^e, m = 1 - 2^e$.
したがって, $m = 1 - 2^e$ なら $a = 2^e$ は解のひとつ.

$b > 1$ の場合 $\varphi(b) \leq b - 1 = \varphi(a) - 2k$ によって,

$$a + 1 - 4k \leq \varphi(a) - 2k.$$

一般に $co\varphi(a) = a - \varphi(a)$ と定めこれをオイラー余関数と呼ぶ. すると,
$co\varphi(a) = a - \varphi(a) \leq 2k - 1$. $co\varphi(a) = 1, 2, \cdots, 2k - 1$ となる.
(a, b) についての連立方程式の両辺を加えると $a + b + 1 - 4k = \varphi(a) + 1 - 2k + \varphi(b)$
整理して

$$a + b - 2k = \varphi(a) + \varphi(b).$$

余関数を使うと,

$$co\varphi(a) + co\varphi(b) = 2k.$$

これは美しい関係式である.
$b > 1$ なので $co\varphi(b) \geq 1$. よって,$co\varphi(a) \leq 2k - 1$.

補題 1. $co\varphi(a) \leq 2k - 1$.

5.4　$k = 1$ のとき

$m = -3$.

$$co\varphi(a) + co\varphi(b) = 2k = 2.$$

これより
$co\varphi(a) = co\varphi(b) = 1$ になり, (a, b) は素数の対. 連立方程式より $b = a - 2$: 素数. よって (a, b) は双子素数.

5.5　$k = 2$ のとき

$m = -7$.

$$co\varphi(a) + co\varphi(b) = 2k = 4.$$

これより

i).$co\varphi(a) = 1, co\varphi(b) = 3$ のとき
$co\varphi(b) = 3$ によって, $b = 9$. $a + 1 - 4k = a + 1 - 8 = \varphi(b) = 6$. すなわち $a = 13$ は解.

ii). $co\varphi(a) = 3, co\varphi(b) = 1$ のとき
$a = 9 = 3^2$, $b = \varphi(a) + 1 - 2k = 6 + 1 - 4 = 3$. $a = 9 = 3^2$ は解.
$m = 1 - 2^3$ なので, $a = 2^3$ も解.

5.6　$k = 3$ のとき

$m = -11$.

$$co\varphi(a) + co\varphi(b) = 2k = 6.$$

これより
i). $co\varphi(a) = 1, co\varphi(b) = 5$ のとき
$co\varphi(b) = 5$ によって, $b = 25$. $a + 1 - 4k = a + 1 - 12 = \varphi(b) = 20$. すなわち $a = 31$.

ii). $co\varphi(a) = 2, co\varphi(b) = 4$ のとき $a = 4$ なので矛盾.
iii). $co\varphi(a) = 3, co\varphi(b) = 3$ のとき
$a = 9, b = 9$ なので矛盾.
iv). $co\varphi(a) = 4, co\varphi(b) = 2$ のとき
$b = 4$, $a + 1 - 4k = a + 1 - 12 = \varphi(b) = 2$. すなわち $a = 13$.
v). $co\varphi(a) = 5, co\varphi(b) = 1$ のとき
$a = 25$,
$b = \varphi(a) + 1 - 2k = 20 + 1 - 6 = 15$. 素数にならないので矛盾

5.7　$k = 4$ のとき

$m = -15$. $a = 4k - 1 + \varphi(b) = 15 + \varphi(b) \geq 16$.

$$co\varphi(a) + co\varphi(b) = 2k = 8.$$

i). $co\varphi(a) = 1, co\varphi(b) = 7$ のとき
$co\varphi(b) = 7$ によって, $b = 49, 15$.
$b = 49$ のとき, $a = 1 - 4k = a + 1 - 16 = \varphi(b) = 42$. すなわち $a = 57$. 素数ではない.
$b = 15$ のとき, $a = 1 - 4k = a + 1 - 16 = \varphi(b) = 8$. すなわち $a = 23$. 素数.
ii) $co\varphi(a) = 2, 3, 4$ なら $a \geq 16$ に反する.

iii) $co\varphi(a) = 5$ なら $co\varphi(b) = 3, a = 25$. $b = \varphi(a) + 1 - 2k = 21 - 8 = 13$. $co\varphi(b) = 3$ に矛盾.

iv) $co\varphi(a) = 6$ なら $co\varphi(b) = 2, b = 4$. $a = 4k - 1 + \varphi(b) = 17$

v) $co\varphi(a) = 7$ なら $a = 49, 15; co\varphi(b) = 1$.

$a = 49$ なら $b = \varphi(a) + 1 - 2k = 42 + 1 - 8 = 35$; 素数ではない.

$a = 15$ なら $b = \varphi(a) + 1 - 2k =$; 素数ではない.

$m = -15 = 1 - 2^4$ により $a = 2^4 = 16$ も解.

以上によって, $a = 16, 23$.

5.8　$k = 5$ のとき

$m = -19$. $a = 4k - 1 + \varphi(b) = 19 + \varphi(b) \geq 21$.

$co\varphi(a) + co\varphi(b) = 2k = 10$ により分類.

i). $co\varphi(a) = 1, co\varphi(b) = 9$ のとき

$co\varphi(b) = 9$ によって, $b = 27, 21$.

$b = 27$ のとき, $a + 1 - 4k = a + 1 - 20 = \varphi(b) = 18$. すなわち $a = 37$.

$b = 21$ のとき, $a + 1 - 4k = a + 1 - 20 = \varphi(b) = 12$. すなわち $a = 31$.

ii).

$co\varphi(a) = 2, 3, 4, 5$ のとき $a = 4, 9, 6, 25$

$a = 25$ ならば,$b = \varphi(a) + 1 - 2k = 20 - 9 = 11$; 素数なので矛盾.

iii).

$co\varphi(a) = 6$ のとき $a = 10$.

iv). $co\varphi(a) = 7, co\varphi(b) = 3$. このとき $a = 49, 15$. $b = 9$.

$a = 49$ なら $\varphi(a) = 42$. $b = \varphi(a) + 1 - 2k = 42 - 9 = 31 \neq 9$; 矛盾

$a = 21$ なら $\varphi(a) = 12$. $b = \varphi(a) + 1 - 2k = 12 - 9 = 3$; 矛盾

v). $co\varphi(a) = 8, co\varphi(b) = 2$. $b = 4$.

$a + 1 - 4k = \varphi(b) = 2$ により $a = 11$. 矛盾

vi). $co\varphi(a) = 9, co\varphi(b) = 1$. $a = 27, 21$.

$a = 27$ なら, $b = \varphi(a) + 1 - 2k = 10 - 10 = 0$; 矛盾.

$a = 21$ なら, $b = \varphi(a) + 1 - 2k = 13 - 10 = 3$. 素数なので矛盾しない.

結局, $a = 37, 31, 21$.

スーパーオイラー II 型完全数,$m = 1 - 4k$ の解

m	a
-39	$51 = 3 * 17$, $71 = 71$, $91 = 7 * 13$
-35	$65 = 5 * 13$, $77 = 7 * 11$, $83 = 83$
-31	$32 = 2^5$, $49 = 7^2$, $71 = 71$
-27	$33 = 3 * 11$, $47 = 47$
-23	$35 = 5 * 7$, $47 = 47$
-19	$21 = 3 * 7$, $31 = 31$, 37=37
-15	$16 = 2^4$, $23 = 23$
-11	$31 = 31$
-7	$8 = 2^3$, $9 = 3^2$, $13 = 13$
-3	$4 = 2^2$, 5 , 7,13,19,31,43,61

$m = -3$ のとき $a = 4$ 以外は双子素数の兄. たぶん無限にある.

5.9 オイラー余関数の評価

一般に．$a > 1$ なら $co\varphi(a) \geq 1$. 次の結果はやさしいが有用.

1. $co\varphi(a) = 1$ なら a は素数. 逆も正しい
2. $co\varphi(a) = 2$ なら $a = 4$.
3. $co\varphi(a) = 3$ なら $a = 9$.
4. $co\varphi(a) = 4$ なら $a = 6, 8$.
5. $co\varphi(a) = 5$ なら $a = 25$.
6. $co\varphi(a) = 6$ なら $a = 10$.
7. $co\varphi(a) = 7$ なら $a = 49, 15$.
8. $co\varphi(a) = 8$ なら $a = 12, 14, 16$.
9. $co\varphi(a) = 9$ なら $a = 27, 21$.

6 解の無限性

高橋氏は $m = -1 - 2^\varepsilon$ のとき解は無限にあるのではないかとの推察を私への私信で述べた.

これができれば双子素数は無限にある, という予想まで解ける.

これは難しくできそうもないが解が無限にあるとき $m = -1 - 2^\varepsilon$ となることを示すことに成功した.

6.1 $m = 1 - 4k$ のとき

$co\varphi(a) + co\varphi(b) = 2k$. これより $k > 1$ なら, $co\varphi(a) > 1$ または $co\varphi(b) > 1$.
$co\varphi(a) > 1$ なら, $2k \geq co\varphi(a) \geq \sqrt{a}$. $a < 4k^2$ なので, a は有限個.
$co\varphi(a) = 1$ でも $co\varphi(b) > 1$ なら, $2k \geq co\varphi(b) \geq \sqrt{b}$ よって, b は有限個.
$k = 1$ のとき, $co\varphi(a) = co\varphi(b) = 1$ であり, ここに双子素数が出てくる.
双子素数の無限性は証明はされていないがほぼ確かである.

6.2 $m = -1 - 4k$ のとき

$m = -1 - 4k$ のときを考える. 条件式は $\varphi(2\varphi(a) - 4k) = a - 1 - 4k$ となる.

$b = \varphi(a) - 2k$ とおくとこれは偶数 ($a > 2$), $\varphi(2b) = a - 1 - 4k$ となる. b を素因数分解して, $b = 2^\varepsilon Q, Q$: 奇数とする. これより,

$$b = 2^\varepsilon Q = \varphi(a) - 2k,$$

$$\varphi(2b) = \varphi(2^{\varepsilon+1}Q) = 2^{\varepsilon}\varphi(Q) = a - 1 - 4k.$$

以上により, a, Q についての連立方程式がえられた.

- $a = 2^{\varepsilon}\varphi(Q) + 1 + 4k,$
- $2^{\varepsilon}Q = \varphi(a) - 2k.$

両辺を加えると,

$$2^{\varepsilon}\varphi(Q) + a = 2^{\varepsilon}\varphi(Q) + 1 + 4k + \varphi(a) - 2k.$$

移項して整理すると

$$2^{\varepsilon}co\varphi(Q) + co\varphi(a) = 1 + 2k.$$

以下において,
$2^{\varepsilon}co\varphi(Q) + co\varphi(a) = 1 + 2k$ をベースにして, 連立方程式を解く, というアルゴリズムを実行する.
a, Q がともに素数なら
$2^{\varepsilon}co\varphi(Q) + co\varphi(a) = 2^{\varepsilon} + 1 = 1 + 2k$ なので $2^{\varepsilon} = 2k$.
a :素数が成り立たないなら 評価式 $2k \geq co\varphi(a) \geq \sqrt{a}$ が成り立ち, a は有限個.
Q :素数が成り立たないなら Q は有限個.
結局 双子素数, 超双子素数　になる以外は a は有限個になる.

6.3 超双子素数

a が素数なら $co\varphi(a) = 1$. よって, $2^{\varepsilon}co\varphi(Q) = 2k$.
さらに Q が素数なら $co\varphi(Q) = 1$ ならば $2^{\varepsilon} = 2k$.

命題 3. p と $a = 2^{e}p + 2^{e} + 1$ がともに素数なら a は $m = -1 - 2^{e+1}$ のとき
$\varphi(2\varphi(a) + 1 + m) = a + m$ の解

$\alpha = 2^{e}, \beta = 1 + 2^{e}$ とおくとき, $p = \dfrac{a - \beta}{\alpha}$ とおくとき a, p はともに素数である. これは超双子素数.

Proof.
$a = 2^{e}p + 2^{e} + 1$ は素数なので $\varphi(a) = 2^{e}p + 2^{e} = 2^{e}(p + 1)$.
$2\varphi(a) + 1 + m = 2^{e+1}(p + 1) - 2^{e+1} = 2^{e+1}p$ なので $\varphi((2\varphi(a) + 1 + m)) = 2^{e}(p - 1)$
一方, $a + m = 2^{e}p + 2^{e} + 1 - 1 - 2^{e+1} = 2^{e}(p - 1)$.
よって $\varphi(2\varphi(a) + 1 + m) = a + m$ が確認された.

7　個別計算

7.1　$Q=1$ のとき.

$Q=1$ のときは簡単なので最初にこの場合を行う．ただし $k \leq 5$ とする.
$\varphi(a)-2k=b=2^{\varepsilon}$,$2^{\varepsilon}=a-1-4k$.
$a=1+4k+2^{\varepsilon}$, かつ $\varphi(a)=2^{\varepsilon}+2k$
これによって $\mathrm{co}\varphi(a)=a-\varphi(a)=2k+1$.

i) $k=1$; $m=-5$.
$\mathrm{co}\varphi(a)=2k+1=3$ なので $a=9$
$2^{\varepsilon}=\varphi(a)-2k=6-2=4$. よって, $b=2^{\varepsilon}=4$.
さらに $a=2^{\varepsilon}+1+4k=4+5=9$. したがって, $a=9=3^2$ は解.

ii) $k=2$; $m=-9$.
$\mathrm{co}\varphi(a)=2k+1=5$ なので $a=25$.
$2^{\varepsilon}=\varphi(a)-2k=20-4=16$. よって, $b=2^{\varepsilon}=16$.
さらに $a=2^{\varepsilon}+1+4k=16+9=25$. したがって, $a=25=5^2$ は解.

iii) $k=3$; $m=-13$.
$\mathrm{co}\varphi(a)=2k+1=7$ なので $a=49,15$.
a) $a=49$.
$2^{\varepsilon}=\varphi(a)-2k=42-6=36$. ; 矛盾.
b) $a=15$.
$2^{\varepsilon}=\varphi(a)-2k=8-6=2$. ;
さらに $a=2^{\varepsilon}+1+4k=2+13=15$. したがって, $a=15$ は解.

iii) $k=3$; $m=-13$.
$\mathrm{co}\varphi(a)=2k+1=7$ なので $a=49,15$.
a) $a=49$.
$2^{\varepsilon}=\varphi(a)-2k=42-6=36$. ; 矛盾.
b) $a=15$.
$2^{\varepsilon}=\varphi(a)-2k=8-6=2$. ;
さらに $a=2^{\varepsilon}+1+4k=2+13=15$. したがって, $a=15$ は解.

iv) $k=4$; $m=-17$.
$\mathrm{co}\varphi(a)=2k+1=9$ なので $a=27,21$.
a) $a=27$.
$2^{\varepsilon}=\varphi(a)-2k=18-8=10$. ; 矛盾.
b) $a=21$.
$2^{\varepsilon}=\varphi(a)-2k=12-8=4$. ;
さらに $a=2^{\varepsilon}+1+4k=21$. したがって, $a=21$ は解.

v) $k = 5$; $m = -21$.
co$\varphi(a) = 2k + 1 = 11$ なので $a = 121$,.
a) $a = 121$.
$2^\varepsilon = \varphi(a) - 2k = 110 - 10 = 100$. ; 矛盾.
b) $a =$.

7.2 $Q > 2$ のとき.

以下において,
$2^\varepsilon co\varphi(Q) + co\varphi(a) = 1 + 2k$ をベースにして, 連立方程式

- $a = 2^\varepsilon\varphi(Q) + 1 + 4k$,
- $2^\varepsilon Q = \varphi(a) - 2k$.

をとく.
i) $k = 1$. $m = -5$ 超双子素数.

ii) $k = 2$. $m = -9$.
$co\varphi(a) + 2^\varepsilon co(Q) = 1 + 2k = 5$.
$\varepsilon > 0, co\varphi(Q) \geq 2$ なので $co\varphi(a) = 1, 2^\varepsilon co\varphi(Q) = 4$.
$\varepsilon = 1, co\varphi(Q) = 2$ になるので $Q = 4$. Q は奇数なので矛盾.
$co\varphi(Q) = 1$ は超双子素数の場合.

iii) $k = 3$. $m = -13$.
$co\varphi(a) + 2^\varepsilon co\varphi(Q) = 1 + 2k = 7$.
$\varepsilon > 0, co\varphi(Q) \geq 2$ なので
a) $co\varphi(a) = 1, 2^\varepsilon co\varphi(Q) = 6$.
$\varepsilon = 1, co\varphi(Q) = 3$ になるので $Q = 9$.
$a = 2^\varepsilon\varphi(Q) + 1 + 4k = 12 + 1 + 12 = 25$. 素数ではない.
b) $co\varphi(a) = 5, 2^\varepsilon co\varphi(Q) = 2$.
$a = 25, \varepsilon = 1, co\varphi(Q) = 1$.
$2^\varepsilon Q = \varphi(a) - 2k = 20 - 6 = 14$. よって, $\varepsilon = 1, Q = 7$. $a = 25$ は解.

iv) $k = 4$. $m = -17$.
$co\varphi(a) + 2^\varepsilon co\varphi(Q) = 1 + 2k = 9$.
$\varepsilon > 0, co\varphi(Q) \geq 2$ なので
a) $co\varphi(a) = 1, 2^\varepsilon co\varphi(Q) = 8$.
$co\varphi(Q) = 1$ のときは超双子素数である.
$co\varphi(Q) = 2$ なら $Q = 4, \varepsilon = 2$. $a = 2^\varepsilon\varphi(Q) + 1 + 4k = 8 + 1 + 16 = 25$. 矛盾.
$co\varphi(Q) = 4$ なら $Q = 8, 6, \varepsilon = 1$.
$Q = 8$ のとき,

$a = 2^{\varepsilon}\varphi(Q) + 1 + 4k = 8 + 1 + 16 = 25$. 素数でないから矛盾.
$Q = 6$ のとき,
$a = 2^{\varepsilon}\varphi(Q) + 1 + 4k = 4 + 1 + 16 = 21$. 素数でないから矛盾.
b) $co\varphi(a) = 3, 2^{\varepsilon}co\varphi(Q) = 6$.
このとき $a = 9, co\varphi(Q) = 3, \varepsilon = 1$.
$a = 2^{\varepsilon}\varphi(Q) + 1 + 4k = 12 + 17 = 29$; 矛盾
c) $co\varphi(a) = 5, 2^{\varepsilon}co\varphi(Q) = 4$. ゆえに $a = 25, \varepsilon = 1, Q = 4$.
$a = 2^{\varepsilon}\varphi(Q) + 1 + 4k = 4 + 1 + 16 = 21$. 矛盾
d) $co\varphi(a) = 7, 2^{\varepsilon}co\varphi(Q) = 2$. すると $\varepsilon = 1, co\varphi(Q) = 1.a = 49, 21$
$a = 49$ のとき, $2^{\varepsilon}Q = \varphi(a) - 2k = 42 - 8 = 34$. $\varepsilon = 1, Q = 17$; 素数.
$a = 2^{\varepsilon}\varphi(Q) + 1 + 4k = 32 + 1 + 16 = 49$. これより $a = 7^2 = 49$.

$$2^{\varepsilon}\varphi(Q) + a = 2^{\varepsilon}\varphi(Q) + 1 + 4k + \varphi(a) - 2k.$$

$*$	m	a
	-41	45=$3^2 * 5$,57=$3 * 19$,65=$5 * 13$,169=13^2
	-37	61=61,73=73,289=17^2,
$*$	-33	65=$5 * 13$,97=97,193=193,289=17^2,673=673,769=769,1153=1153
	-29	33=$3 * 11$,113=113,169=13^2,
	-25	33=$3 * 11$,61=61,
	-17	21=$3 * 7$,25=5^2,49=7^2,97=97,113=113,
	-13	15=$3 * 5$,25=5^2,
$*$	-9	17=17,25=5^2,73=73,97=97,193=193,241=241,
$*$	-5	9=3^2,13=13,17=17,29,37,41,61,89

$*$ は超双子素数の箇所を示す.

表 9: $\varphi(2\varphi(a)+1+m)=a+m$

$m=-3$		$m=-5$			$m=-9$		
a	$a-2$	a	$a-3$	b/2	a	$a-5$	$b/4$
5	3	13	10	5	17	12	3
7	5	17	14	7	73	68	17
13	11	29	26	13	97	92	23
19	17	37	34	17	193	188	47
31	29	41	38	19	241	236	59
43	41	61	58	29	337	332	83
61	59	89	86	43	409	404	101
73	71	97	94	47	433	428	107
103	101	109	106	53	457	452	113
109	107	137	134	67	601	596	149
139	137	149	146	73	673	668	167
151	149	181	178	89	769	764	191
181	179	197	194	97	937	932	233
193	191	229	226	113	1009	1004	251
199	197	257	254	127	1033	1028	257
$4=2^2$		$9=3^2$			$25=5^2$		

表 10: $\varphi(2\varphi(a)+1+m)=a+m$ 続き

$m=-17$			$m=-33$			$m=-65$		
a	$a-9$	b/8	a	$a-17$	b/16	a	$a-33$	$b/32$
97	88	11	97	80	5	193	160	5
113	104	13	193	176	11	257	224	7
193	184	23	673	656	41	449	416	13
241	232	29	769	752	47	577	544	17
257	248	31	1153	1136	71	641	608	19
337	328	41	2113	2096	131	769	736	23
353	344	43	2689	2672	167	1217	1184	37
433	424	53	3169	3152	197	1409	1376	43
577	568	71	4129	4112	257	2689	2656	83
593	584	73	4513	4496	281	3137	3104	97
641	632	79	4993	4976	311	3329	3296	103
21=3*7			65=5*13			$209=11*19$		
25=5*5			$289=17^2$			$961=31^2$		
49=7*7								