

新規まき直し 第2期2018年3月9日 スーパーオイラー完全数 update

飯高 茂

平成 29 年 12 月 10 日

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

End

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りない. そこでスーパーオイラー完全数 II 型を新たに導入した.

2 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.

2.1 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,

$2\varphi(a) + 1 + m$ とおく. $x > 2$ のとき, $\varphi(x) = a + m$ は偶数. それゆえ a も偶数. よって奇数の L によって $a = 2^e L$ と書ける.

$x = 1$ は仮説によりおきない.

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

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

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

よって, $L \leq \varphi(L)$. したがって, $L = 1, a = 2^e$. $x = 2\varphi(a) + 1 + m = 2^e + 1 + m$,

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

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 2. 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.

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.

表 1: 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

2.2 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. $x = 2\varphi(a) + 1 + m$.
 一般に $x > 2$ なら $\varphi(x)$ は偶数なので a も奇数.
 $x = 1, 2$ の場合はすでに示した.

命題 1. m を奇数 $2N - 1 \geq -1$ とする. $m \geq -1$ の場合.

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

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

$\varphi(2b) = \varphi(2^{\epsilon+1}L) = 2^\epsilon \varphi(L)$ 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

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

これより

$$a + 2N - 1 \leq a - 1 + N - 2^\epsilon.$$

$N \leq -2^\epsilon \leq -1$. 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 $1 + 2N - 1 \geq a - \varphi(a) + 2N - 1 = N$. $2N \geq N$. 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 a はフェルマ素数. $\varepsilon = 0$ のとき, $a = 2$. したがって, 解は 2 またはフェルマ素数.

End

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

2.3 $m = 1 - 4k$ 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

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

これを a, b についての連立方程式とみる.

1) $b = 1$ 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.

2) $b > 1$ 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 $\text{co}\varphi(a) = a - \varphi(a)$ と定めこれをオイラー余関数と呼ぶ. すると,

$\text{co}\varphi(a) = a - \varphi(a) \leq 2k - 1$. したがって, $\text{co}\varphi(a) = 1, 2, \dots, 2k - 1$ 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,

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

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

2.4 $k = 1$ 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.

2.5 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.

2.6 $k = 2$ のとき

$m = -7$. になり次の連立方程式が³できる.

- $a = \varphi(b) - 1 + 4k = \varphi(b) + 7 \geq 8$,
- $b = \varphi(a) + 1 - 2k = \varphi(a) - 3$.

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

これより

i). $co\varphi(a) = 1, co\varphi(b) = 3$ のとき

$co\varphi(b) = 3$ によって, $b = 9$. $a = \varphi(b) + 7 = 13$. $b = \varphi(a) - 3 = 12 - 3 = 9$. 連立方程式が³解けて解 = 13.

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.

表 2: $co\varphi(a) - \sqrt{a}$; a が平方数でないとき,

a	factor	$\varphi(a)$	$co\varphi(a)$	$co\varphi(a) - \sqrt{a}$
6 (8)	[2, 3]	2	4	1.550510257
10	[2, 5]	4	6	2.83772234
15 (49)	[3, 5]	8	7	3.127016654
14 (16)	[2, 7]	6	8	4.258342613
12	[2 ² , 3]	4	8	4.535898385
21 (27)	[3, 7]	12	9	4.417424305
35 (121)	[5, 7]	24	11	5.083920217
22	[2, 11]	10	12	7.30958424
20	[2 ² , 5]	8	12	7.527864045
18	[2, 3 ²]	6	12	7.757359313
33	[3, 11]	20	13	7.255437353
26	[2, 13]	12	14	8.900980486
55	[5, 11]	40	15	7.583801513
39	[3, 13]	24	15	8.755002002
28 (32)	[2 ² , 7]	12	16	10.70849738
24	[2 ³ , 3]	8	16	11.10102051
77	[7, 11]	60	17	8.225035613
65	[5, 13]	48	17	8.937742252
34	[2, 17]	16	18	12.16904811
91	[7, 13]	72	19	9.460607986
51	[3, 17]	32	19	11.85857157
38	[2, 19]	18	20	13.835586
85	[5, 17]	64	21	11.78045554
57	[3, 19]	36	21	13.45016556
45	[3 ² , 5]	24	21	14.29179607
30	[2, 3, 5]	8	22	16.52277442

2.7 $k = 3$ のとき

$$m = -11.$$

- $a = \varphi(b) - 1 + 4k = \varphi(b) + 11 \geq 12$,
- $b = \varphi(a) + 1 - 2k = \varphi(a) - 5$.

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

これより

i). $\text{co}\varphi(a) = 1, \text{co}\varphi(b) = 5$ のとき
 $\text{co}\varphi(b) = 5$ によって, $b = 25$. $a + 1 - 4k = a + 1 - 12 = \varphi(b) = 20$. すなわち $a = 31$.
 $b = \varphi(a) - 5 = 30 - 5 = 25$. $a = 31$ は解.

ii). $\text{co}\varphi(a) = 2, \text{co}\varphi(b) = 4$ のとき $a = 4$ なので矛盾.

iii). $\text{co}\varphi(a) = 3, \text{co}\varphi(b) = 3$ のとき

$a = 9, b = 9$ なので矛盾.

iv). $\text{co}\varphi(a) = 4, \text{co}\varphi(b) = 2$ のとき

$b = 4, a + 1 - 4k = a + 1 - 12 = \varphi(b) = 2$. すなわち $a = 13$. $b = \varphi(a) - 5 = 7$, 矛盾.

v). $\text{co}\varphi(a) = 5, \text{co}\varphi(b) = 1$ 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

2.8 $k = 4$ のとき

$m = -15$.

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

- $b = \varphi(a) + 1 - 2k = \varphi(a) - 7$.

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

i). $\text{co}\varphi(a) = 1, \text{co}\varphi(b) = 7$ のとき $\text{co}\varphi(a) = 1$: 素数. $\text{co}\varphi(b) = 7$ によって, $b = 49, 15$.

$b = 49$ のとき, $a = \varphi(b) + 15 = 42 + 15$. 素数ではない.

$b = 15$ のとき, $a = \varphi(b) + 15 = 8$. すなわち $a = 23$: 素数. $b = \varphi(a) - 7 = 15$. $a = 23$ は解.

ii) $\text{co}\varphi(a) = 2, 3, 4$ なら $a \geq 16$ に反する.

iii) $\text{co}\varphi(a) = 5$ なら $\text{co}\varphi(b) = 3, a = 25$. $b = \varphi(a) - 7 = 20 - 7 = 13$. $\text{co}\varphi(b) = 3$ に矛盾.

iv) $\text{co}\varphi(a) = 6$ なら $\text{co}\varphi(b) = 2, b = 4$. $a = \varphi(b) + 15 = 17$ $b = \varphi(a) - 7 = 16 - 7 = 9$.

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

$a = 49$ なら $b = \varphi(a) - 7 = 42 - 7 = 35$; 素数ではない.

$a = 15$ なら $b = \varphi(a) - 7 = 1$; 素数ではない.

一方, $m = -15 = 1 - 2^4$ により $a = 2^4 = 16$ も解.

以上によって, $a = 16, 23$.

2.9 $k = 5$ のとき

$m = -19$.

- $a = \varphi(b) - 1 + 4k = \varphi(b) + 19 \geq 20$,

• $b = \varphi(a) + 1 - 2k = \varphi(a) - 9$.

$co\varphi(a) + co\varphi(b) = 2k = 10$ 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, $a = \varphi(b) + 19 = 18 + 19$. すなわち $a = 37$. $b = \varphi(a) - 9 = 36 - 9 = 27$.
 $a = 37$ は解.

$b = 21$ のとき, $a = \varphi(b) + 19 = 12 + 19$. すなわち $a = 31$. $b = \varphi(a) - 9 = 21$. $a = 31$
 は解.

ii).

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

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

iii).

$co\varphi(a) = 6$ のとき $a = 10$. $a \geq 19$ に矛盾.

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

$a = 15$ 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, $a = 37, 31, 21$.

次の結果はパソコンによる.

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.

3 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.

3.1 $m = 1 - 4k$ 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.

3.2 $m = -1 - 4k$ 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.

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

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

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

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

a :素数が成り立たないなら 評価式 $2k \geq \text{co}\varphi(a) \geq \sqrt{a}$ 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.

解が無限にあれば a, Q はともに素数.

3.3 超双子素数

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

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

命題 2. 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, $p = \frac{\alpha - \beta}{\alpha}$ 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 $\varphi(2\varphi(a) + 1 + m) = a + m$.

End

4 個別計算

4.1 $Q = 1$ のとき.

$Q = 1$ のとき $\text{co}\varphi(Q) = 0$ になる. 簡単なので最初にこの場合を扱う. ただし $k \leq 5$ とする.

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

$$a = 1 + 4k + 2^\varepsilon, \text{ かつ } \varphi(a) = 2^\varepsilon + 2k$$

$$\text{これによって } \text{co}\varphi(a) = a - \varphi(a) = 2k + 1.$$

i) $k = 1; m = -5$.

$$\text{co}\varphi(a) = 2k + 1 = 3 \text{ なので } a = 9$$

$$2^\varepsilon = \varphi(a) - 2k = 6 - 2 = 4. \text{ よって, } b = 2^\varepsilon = 4.$$

さらに $a = 2^\varepsilon + 1 + 4k = 4 + 5 = 9$. したがって, $a = 9 = 3^2$ は解.

ii) $k = 2; m = -9$.

$$\text{co}\varphi(a) = 2k + 1 = 5 \text{ なので } a = 25.$$

$$2^\varepsilon = \varphi(a) - 2k = 20 - 4 = 16. \text{ よって, } b = 2^\varepsilon = 16.$$

さらに $a = 2^\varepsilon + 1 + 4k = 16 + 9 = 25$. したがって, $a = 25 = 5^2$ は解.

iii) $k = 3; m = -13$.

$\text{co}\varphi(a) = 2k + 1 = 7$ 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) $k = 3; m = -13$.

$\text{co}\varphi(a) = 2k + 1 = 7$ 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) $k = 4; m = -17$.

$\text{co}\varphi(a) = 2k + 1 = 9$ 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) $k = 5; m = -21$.

$\text{co}\varphi(a) = 2k + 1 = 11$ なので $a = 121$.

a) $a = 121$.

$2^\varepsilon = \varphi(a) - 2k = 110 - 10 = 100$. ; 矛盾.

4.2 $Q > 2$ のとき.

以下において,

$2^\varepsilon \text{co}\varphi(Q) + \text{co}\varphi(a) = 1 + 2k$ 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) $k = 1. m = -5$.

- $a = 2^\varepsilon \varphi(Q) + 5,$

- $2^\varepsilon Q = \varphi(a) - 2.$

$2^\varepsilon \text{co}\varphi(Q) + \text{co}\varphi(a) = 1 + 2k = 3$. $\text{co}\varphi(Q) > 0$ なので, $\varepsilon = 1, \text{co}\varphi(Q) = \text{co}\varphi(a) = 1$.
 $a = 2^\varepsilon \varphi(Q) + 1 + 4k = 2Q + 5, b = 2^\varepsilon Q = 2Q = a - 3$. $a, Q = \frac{b}{2}$ はともに素数.

ii) $k = 2. m = -9$.

- $a = 2^\varepsilon \varphi(Q) + 9,$
- $b = 2^\varepsilon Q = \varphi(a) - 4.$

をとく.

$$\text{co}\varphi(a) + 2^\varepsilon \text{co}\varphi(Q) = 1 + 2k = 5.$$

1) $\text{co}\varphi(Q) \geq 2$ のとき $\varepsilon > 0, \text{co}\varphi(Q) \geq 2$ なので $\text{co}\varphi(a) = 1, 2^\varepsilon \text{co}\varphi(Q) = 4$.

$\varepsilon = 1, \text{co}\varphi(Q) = 2$ になるので $Q = 4$. Q は奇数なので矛盾.

2) $\text{co}\varphi(Q) = 1$ のとき. $\text{co}\varphi(a) = 1, b = 2^\varepsilon = 4, \text{co}\varphi(Q) = 1$.

$b = \varphi(a) - 2k = a - 5$ により, $b = 4Q$ なので $Q = \frac{a-5}{4}$ はともに素数. 超双子素数.

iii) $k = 3. m = -13$.

連立方程式

- $a = 2^\varepsilon \varphi(Q) + 13,$
- $2^\varepsilon Q = \varphi(a) - 6.$

をとく.

$$\text{co}\varphi(a) + 2^\varepsilon \text{co}\varphi(Q) = 1 + 2k = 7.$$

1) $\text{co}\varphi(Q) > 1$.

$\varepsilon > 0, \text{co}\varphi(Q) \geq 2$ なので

a) $\text{co}\varphi(a) = 1, 2^\varepsilon \text{co}\varphi(Q) = 6$.

$\varepsilon = 1, \text{co}\varphi(Q) = 3$ になるので $Q = 9$.

$a = 2^\varepsilon \varphi(Q) + 13$: 素数ではない.

b) $\text{co}\varphi(a) = 5, 2^\varepsilon \text{co}\varphi(Q) = 2$.

$a = 25, \varepsilon = 1, \text{co}\varphi(Q) = 1$.

$2^\varepsilon Q = \varphi(a) - 2k = 20 - 6 = 14$. よって, $\varepsilon = 1, Q = 7. a = 25$ は解.

iv) $k = 4. m = -17$.

$$\text{co}\varphi(a) + 2^\varepsilon \text{co}\varphi(Q) = 1 + 2k = 9.$$

$\varepsilon > 0, \text{co}\varphi(Q) \geq 2$ なので

a) $\text{co}\varphi(a) = 1, 2^\varepsilon \text{co}\varphi(Q) = 8$.

$\text{co}\varphi(Q) = 1$ のときは超双子素数である.

$\text{co}\varphi(Q) = 2$ なら $Q = 4, \varepsilon = 2. a = 2^\varepsilon \varphi(Q) + 1 + 4k = 8 + 1 + 16 = 25$. 矛盾.

$\text{co}\varphi(Q) = 4$ 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) $\text{co}\varphi(a) = 3, 2^\varepsilon \text{co}\varphi(Q) = 6$.

このとき $a = 9, \text{co}\varphi(Q) = 3, \varepsilon = 1$.

$a = 2^\varepsilon \varphi(Q) + 1 + 4k = 12 + 17 = 29$; 矛盾

c) $\text{co}\varphi(a) = 5, 2^\varepsilon \text{co}\varphi(Q) = 4$. ゆえに $a = 25, \varepsilon = 1, Q = 4$.

$a = 2^\varepsilon \varphi(Q) + 1 + 4k = 4 + 1 + 16 = 21$. 矛盾

d) $\text{co}\varphi(a) = 7, 2^\varepsilon \text{co}\varphi(Q) = 2$. すると $\varepsilon = 1, \text{co}\varphi(Q) = 1, a = 49, 21$

$a = 49$ 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 $a = 7^2 = 49$.

*	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 3: $\varphi(2\varphi(a) + 1 + m) = a + m$

$m = -3$		$m = -5$			$m = -9$		
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 4: $\varphi(2\varphi(a) + 1 + m) = a + m$ 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								

5 $a = p^2$ のとき

連立方程式

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

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

において, $a = p^2$ のときを考える.

$$\text{co}\varphi(a) = p, \text{co}\varphi(a) + \text{co}\varphi(b) = p + \text{co}\varphi(b) = 1 + 2k,$$

$$b = 2^\varepsilon Q = p(p-1) - 2k.$$