

書泉グランデでの講義
高校生も十分わかる新しい数論研究
New Series, 第2期 予稿1改良
2016年2月26日

飯高 茂

平成28年2月23日

1 オイラー関数

自然数 $a > 1$ に対して $1 \leq b < a$ を満たし, a と互いに素な自然数 b の個数を $\varphi(a)$ と書き, これを自然数 a の関数とみてオイラー関数という. ただし $\varphi(1) = 1$ とする.

オイラー関数 $\varphi(a)$ の性質 ($a > 1$) を列挙してみよう.

1. $a - 1 \geq \varphi(a)$,
2. a が素数なら $\varphi(a) = a - 1$. さらに $\varphi(a) = a - 1$ なら a は素数,
3. a が素数でないなら $a \geq \varphi(a) + \sqrt{a}$,
4. a, b が互いに素なら $\varphi(ab) = \varphi(a)\varphi(b)$ (乗法性).

$a = p^2$ のとき $a = \varphi(a) + \sqrt{a}$. 逆も成り立つ.

オイラー関数 $\varphi(a)$ を小学生に説明するなら 分母が a の既約な真分数の個数を $\varphi(a)$ と書くのだ, と言えよ.

1.1 Gauss の公式

一般に自然数が分母, 分子の真分数 $\frac{b}{a}$ があるとき a, b の最大公約数を d をすれば $a = da', b = db'$ とかけて $\frac{b'}{a'}$ は既約な真分数になる. 分母が a' の既約な真分数の個数は $\varphi(a')$ と書ける. したがって分母が a の真分数の個数は a 個ありこれらは分母が a の約数 a' の既約な真分数の全体として表せるのでこれら a' の $\varphi(a')$ の和が a になる. すなわち

$$a = \sum_{a'|a} \varphi(a') \quad (1)$$

となる. ここに $a'|a$ は a' が a の約数を意味する. これを Gauss の公式という.

たとえば $a = 12$ とおくと, $a' = 12, 6, 4, 3, 2, 1$ であり,

$$\varphi(12) = 4, \varphi(6) = 2, \varphi(4) = 2, \varphi(3) = 2, \varphi(2) = 1, \varphi(1) = 1.$$

これらを加えると $4 + 2 + 2 + 2 + 1 + 1 = 12$ となって分母が出て来る.

この公式を使うと, オイラー関数 $\varphi(a)$ の値が楽に計算できる.

a が素数 $p > 1$ なら p の約数は $p, 1$ なので $p = \varphi(p) + \varphi(1) = \varphi(p) + 1$ により $\varphi(p) = p - 1$. (これは当たり前の結果ではあるが)

a が素数の平方 p^2 なら約数は $p^2, p, 1$ なので $p^2 = \varphi(p^2) + \varphi(p) + 1 = \varphi(p^2) + (p - 1) + 1$ により $\varphi(p^2) = p^2 - p = p(p - 1)$.

同様にして $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1)$ が示される.

p, q を相異なる素数とすると pq の約数は $pq, q, p, 1$ なので $pq = \varphi(pq) + \varphi(p) + \varphi(q) + 1 = \varphi(pq) + (p - 1) + (q - 1) + 1$ により $\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1)$.

1.2 乗法性

a, b を互いに素な自然数とすると, $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これがオイラー関数の乗法性である.

乗法性を Gauss の公式を用いて ab についての数学的帰納法で証明する.

$ab = 1$ なら $a = b = 1$ なので成立.

ab のとき証明するが, $nm < ab$ であれば $\varphi(nm) = \varphi(n)\varphi(m)$ が成り立つことが仮定される.

互いに素な a, b について, a, b の約数を代表的にそれぞれ d, δ で表す. Gauss の公式により,

$$a = \sum_{d|a} \varphi(d), b = \sum_{\delta|b} \varphi(\delta)$$

これらを掛けると

$$ab = \sum_{d|a, \delta|b} \varphi(d)\varphi(\delta)$$

$(d, \delta) \neq (a, b)$ のとき $d\delta < ab$ なので数学的帰納法の仮定により $\varphi(d)\varphi(\delta) = \varphi(d\delta)$. よって,

$$ab = \sum_{d|a, \delta|b} \varphi(d)\varphi(\delta) = \sum_{(d, \delta) \neq (a, b)} \varphi(d\delta) + \varphi(a)\varphi(b)$$

ab の約数は $d\delta$ と書けるので Gauss の公式によって,

$$ab = \sum_{d\delta|ab} \varphi(d\delta) = \sum_{(d, \delta) \neq (a, b)} \varphi(d\delta) + \varphi(ab).$$

よって,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

1.3 オイラーの公式

$a = p_1^{e_1} \cdots p_s^{e_s}$ と素因数分解するとき $\bar{p}_1 = p_1 - 1, \dots, \bar{e}_1 = e_1 - 1, \dots$ を用いると

$\varphi(p_1^{e_1}) = p_1^{\bar{e}_1} \bar{p}_1, \dots$ が成り立つので

$$\varphi(a) = p_1^{\bar{e}_1} \bar{p}_1 \cdots p_s^{\bar{e}_s} \bar{p}_s.$$

$\varphi(p_1^{e_1}) = p_1^{e_1} \left(1 - \frac{1}{p_1}\right), \dots$. これより

$$\frac{\varphi(a)}{a} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

をえる. これをオイラーの公式という. 右辺から指数 e_j が消えていることに注意.

1.4 オイラー関数のギャップ値

$N = \varphi(a)$ と a で書けない N をオイラー関数のギャップ値という.

素数 p を用いて $N = 2p(2p + 1)$; 非素数) と表せる N はギャップ値である. $N = 14, 26$ などいくらでもある.

1.5 カーマイケルの予想

$N = \varphi(a)$ と書けるとき a と異なる自然数 b があり $N = \varphi(b)$ となる.

この主張をカーマイケルの予想という.

カーマイケルは最初, 証明できたと思い証明を発表したが, 間違いがみつかった. その後, 誰も証明に成功していない. 反例があるなら $n > 10^{400}$ を満たすなどが示されている.

オイラーの逆関数は 1 価にならない, と言い換えてもよいがオイラー関数の問題は 一見やさしそうですが証明の困難な問題が多い例としてあげておく. なお, $k > 1$ ならオイラーの逆関数で k 価になるものが無限に存在する (Ford, 1999).

1.6 Sophie Germain の素数

p : 素数, $2p + 1 = q$: 素数, のとき p を Sophie Germain¹ の素数 という.

p が Sophie Germain の素数のとき $m = 2p$ について, オイラーの逆関数は 2 価になる.

実際, $\varphi(q) = \varphi(2q) = 2p$. $q, 2q$ 以外の a で, $\varphi(a) = 2p$ とする.

a : 奇数なら, a の素因子は 1 つになるので $a = P^j$. $\varphi(P^j) = P^{j-1}\bar{P} = 2p$ によって,

$j > 1$ なら $j = 2, P = p, P - 1 = 2, a = 6$. しかし $a = 2 * 3, a + 1 = 7$: 素数.

$j = 1$ なら $2p = P - 1$. したがって, $P = 2p + 1$: 素数.

a : 偶数なら, $a = 2P$ になり, $\varphi(a) = \bar{P} = 2p$ となるので $\bar{P} = 2p$. よって, $2p + 1 = P$: 素数.

Sophie Germain の素数は無限に存在すると予想されている. もしこれが正しいなら, オイラーの逆関数で 2 価になるものが無限に存在する例になる.

2 オイラー余関数

$a > 1$ に対して $a - \varphi(a) \geq 1$. かつ $a - \varphi(a) = 1$ なら a : 素数.

そこで $\text{co}\varphi(a) = a - \varphi(a)$ とおき, オイラー余関数という.

¹フランスの数学者 1776 - 1831

表 1: オイラー余関数 $co\varphi(a)$ の順, a :非素数

a	$\varphi(a)$	$co\varphi(a)$	a	$\varphi(a)$	$co\varphi(a)$		
4	$[2^2]$	2	2	57	$[3, 19]$	18	21
9	$[3^2]$	6	3	85	$[5, 17]$	16	21
6	$[2, 3]$	2	4	30	$[2, 3, 5]$	4	22
8	$[2^3]$	4	4	95	$[5, 19]$	36	23
25	$[5^2]$	20	5	119	$[7, 17]$	48	23
10	$[2, 5]$	4	6	143	$[11, 13]$	60	23
15	$[3, 5]$	4	7	529	$[23^2]$	506	23
49	$[7^2]$	42	7	36	$[2^2, 3^2]$	6	24
12	$[2^2, 3]$	2	8	40	$[2^3, 5]$	4	24
14	$[2, 7]$	6	8	44	$[2^2, 11]$	10	24
16	$[2^4]$	8	8	46	$[2, 23]$	22	24
21	$[3, 7]$	6	9	69	$[3, 23]$	22	25
27	$[3^3]$	18	9	125	$[5^3]$	100	25
35	$[5, 7]$	12	11	133	$[7, 19]$	18	25
121	$[11^2]$	110	11	63	$[3^2, 7]$	6	27
18	$[2, 3^2]$	6	12	81	$[3^4]$	54	27
20	$[2^2, 5]$	4	12	115	$[5, 23]$	44	27
22	$[2, 11]$	10	12	187	$[11, 17]$	80	27
33	$[3, 11]$	10	13	52	$[2^2, 13]$	12	28
169	$[13^2]$	156	13	161	$[7, 23]$	66	29
26	$[2, 13]$	12	14	209	$[11, 19]$	90	29
39	$[3, 13]$	12	15	221	$[13, 17]$	48	29
55	$[5, 11]$	20	15	841	$[29^2]$	812	29

次ページに繋がる.

表 2: オイラー余関数 $co\varphi(a)$ の順, a :非素数

a	$\varphi(a)$	$co\varphi(a)$	a	$\varphi(a)$	$co\varphi(a)$		
24	$[2^3, 3]$	4	16	42	$[2, 3, 7]$	6	30
28	$[2^2, 7]$	6	16	50	$[2, 5^2]$	20	30
32	$[2^5]$	16	16	58	$[2, 29]$	28	30
65	$[5, 13]$	12	17	87	$[3, 29]$	28	31
77	$[7, 11]$	30	17	247	$[13, 19]$	36	31
289	$[17^2]$	272	17	961	$[31^2]$	930	31
34	$[2, 17]$	16	18	48	$[2^4, 3]$	8	32
51	$[3, 17]$	16	19	56	$[2^3, 7]$	12	32
91	$[7, 13]$	12	19	62	$[2, 31]$	30	32
361	$[19^2]$	342	19	64	$[2^6]$	32	32
38	$[2, 19]$	18	20	93	$[3, 31]$	30	33
45	$[3^2, 5]$	12	21	145	$[5, 29]$	28	33

表 3: オイラー余関数 $co\varphi(a)$ の順, a :非素数

a	$\varphi(a)$	$co\varphi(a)$	a	$\varphi(a)$	$co\varphi(a)$		
253	[11, 23]	110	33	407	[11, 37]	180	47
75	[3, 5 ²]	20	35	527	[17, 31]	240	47
155	[5, 31]	60	35	551	[19, 29]	252	47
203	[7, 29]	84	35	72	[2 ³ , 3 ²]	12	48
299	[13, 23]	132	35	80	[2 ⁴ , 5]	8	48
323	[17, 19]	144	35	88	[2 ³ , 11]	20	48
54	[2, 3 ³]	18	36	92	[2 ² , 23]	22	48
68	[2 ² , 17]	16	36	94	[2, 47]	46	48
217	[7, 31]	30	37	141	[3, 47]	46	49
74	[2, 37]	36	38	301	[7, 43]	42	49
99	[3 ² , 11]	30	39	343	[7 ³]	294	49
111	[3, 37]	36	39	481	[13, 37]	36	49
319	[11, 29]	140	39	589	[19, 31]	90	49
391	[17, 23]	176	39	235	[5, 47]	92	51
76	[2 ² , 19]	18	40	451	[11, 41]	40	51
185	[5, 37]	36	41	667	[23, 29]	308	51
341	[11, 31]	30	41	329	[7, 47]	138	53
377	[13, 29]	84	41	473	[11, 43]	210	53
437	[19, 23]	198	41	533	[13, 41]	120	53
82	[2, 41]	40	42	629	[17, 37]	144	53
123	[3, 41]	40	43	713	[23, 31]	330	53
259	[7, 37]	36	43	78	[2, 3, 13]	12	54
403	[13, 31]	60	43	106	[2, 53]	52	54
60	[2 ² , 3, 5]	4	44	159	[3, 53]	52	55
86	[2, 43]	42	44	175	[5 ² , 7]	60	55
117	[3 ² , 13]	12	45	559	[13, 43]	84	55
129	[3, 43]	42	45	703	[19, 37]	36	55
205	[5, 41]	40	45	98	[2, 7 ²]	42	56
493	[17, 29]	112	45	104	[2 ³ , 13]	12	56
66	[2, 3, 11]	10	46	105	[3, 5, 7]	12	57
70	[2, 5, 7]	12	46	153	[3 ² , 17]	48	57
215	[5, 43]	84	47	265	[5, 53]	52	57
287	[7, 41]	120	47	517	[11, 47]	230	57
				697	[17, 41]	80	57

2016年2月に高校生 小室慶太君は $\text{co}\varphi(a) \leq 50$ について a とその素因数分解をすべて求めた.

その結果, ギャップ値は 10,26,34,50 であることが分かった.

余関数について次の公式を示せ:

$$a - \varphi(a) = p_1^{\overline{e_1}} \cdots p_s^{\overline{e_s}} (p_1 \cdots p_s - \overline{p_1} \cdots \overline{p_s}).$$

上記の公式によれば, $s(a) \geq 3$ のとき, $a = 2*3*5 = 30, 2*3*7 = 42, 4*3*5 = 60$ のとき $\text{co}\varphi(a) = a - \varphi(a)$ は それぞれ 22,30,44 となりこれらが最小の値と次点, 次次点である.

たぶん, $s(a) \geq 3$ のとき, $a > 60$ なら $\text{co}\varphi(a) > 44$.

3 オイラー余関数の値が小さい場合

$\text{co}\varphi(a) \leq 12$ の場合の a を調べる.

1)

a が素数なら $\text{co}\varphi(a) = 1$ なので以下 a が非素数の場合について調べる.

$s(a)$ を a の相異なる素因子の個数とする.

2)

$s(a) = 1$; すなわち $a = P^j$ なら $\text{co}\varphi(a) = P^{j-1}$ なのでこの場合をはじめに計算しておく.

$\text{co}\varphi(a) = P^{j-1} \leq 12$ とすると, $P^j = 4, 8, 16, 9, 27, 25, 49, 121$ のときそれぞれ $\text{co}\varphi(a) = 2, 4, 8, 3, 9, 5, 7, 11$.

以後, $s(a) \geq 2$ の場合を考える.

3)

$\text{co}\varphi(a)$ は 1 から a のうち, a と互いに素でないものの個数である.

a が非素数ならその最大素因子を P とすると $a = P\alpha$, ($P \geq \text{Maxp}(\alpha)$) とかけて P, a はともに a と互いに素でない. よって, $\text{co}\varphi(a) \geq 2$.

$\text{co}\varphi(a) = 2$ と仮定すると, a に P 以外の素因数はないので, $a = P^j$.

しかし $\text{co}\varphi(a) = P^{j-1}$ なので, $2 = P^{j-1}$. ゆえに $j - 1 = 1, P = 2; a = 2^2 = 4$.

以上によって $\text{co}\varphi(a) = 2$ と仮定すると $a = 4$.

4)

$\text{co}\varphi(a) = 3$ と仮定すると, a に P 以外の素因数がなければ, $a = P^j$, $\text{co}\varphi(a) = P^{j-1} = 3$. よって $a = 3^2 = 9$.

a に P 以外の素因数 q があれば $P, q, 2q, a$ が a とそれぞれ互いに素でない. $\text{co}\varphi(a) > 3$ となり矛盾.

$\text{co}\varphi(a) = 3$ と仮定すると $a = 9$.

5)

$j > 1$ とすると $\rho_0 = \text{co}\varphi(L) = L - \varphi(L)$ を用いて

$$\begin{aligned} \text{co}\varphi(P^j L) &= P^j L - P^{j-1} \overline{P} \varphi(L) \\ &= P^{j-1} (P L - \overline{P} \varphi(L)) \\ &= P^{j-1} (L + \overline{P} \rho_0). \end{aligned}$$

これより $\text{co}\varphi(P^j L) = P^{j-1} (L + \overline{P} \rho_0) \geq P (L + \overline{P} \rho_0) \geq P (P + L - 1) > P^2$.

$12 \geq \text{co}\varphi(P^j L)$ のとき, $P = 3$.

$a = 3^2 * 2^2 = 36$ のとき, $\varphi(36) = 12$. よって, $\text{co}\varphi(36) = 36 - 12 = 24$.

$a = 3^2 * 2 = 18$ のとき, $\varphi(18) = 6$. よって, $\text{co}\varphi(18) = 12$.

6)

$j = 1$ とすると $a = PL$, $\text{co}\varphi(PL) = L + \overline{P}\rho_0$.

L を素数とすると $P > L$ を満たす. $a = PL$ により $\text{co}\varphi(PL) = P + L - 1$.

ここで $\text{co}\varphi(PL) = P + L - 1 \leq 12$ のときは

$$PL = 3 * 2 = 6, P + L - 1 = 4.$$

$$PL = 5 * 2 = 10, P + L - 1 = 6.$$

$$PL = 7 * 2 = 14, P + L - 1 = 8.$$

$$PL = 5 * 3 = 15, P + L - 1 = 7.$$

$$PL = 7 * 3 = 21, P + L - 1 = 9.$$

$$PL = 7 * 5 = 35, P + L - 1 = 11.$$

7)

$j = 1, L$: 非素数の場合 $L \geq 4, \rho_0 = \text{co}\varphi(L) \geq 2$ なので

$$\text{co}\varphi(a) = L + \overline{P}\rho_0 \geq 4 + 2P - 2 = 2P + 2.$$

$11 \geq \text{co}\varphi(a)$ のときは $P \leq 3$.

$P = 3$ なら $a = 3 * 2^e$. $\text{co}\varphi(a) = 2^{e+1}$. $e = 2$ なら $a = 12, \text{co}\varphi(a) = 8$.

$e = 3$ なら $a = 24, \text{co}\varphi(a) = 16$.

さらに $\text{co}\varphi(12) = 8, \text{co}\varphi(24) = 16$,

$\text{co}\varphi(a) < 12$ を満たすのは上記で計算された場合のみ.

4 オイラー余関数の評価式

$s(a) \geq 2, a = P^j * L, j = 1$ とする. すなわち $a = PL$ のとき, $\rho_0 = L - \varphi(L)$ とおく.

$\text{co}\varphi(a) = L + \overline{P}\rho_0$ を用いて以下の計算をする.

$\rho_0 = 1$ のとき L : 素数, $a = PL$. $\text{co}\varphi(a) = P + L - 1$.

$\rho_0 = 2$ のとき $L = 4; a = 4 + 2P - 2 = 2P + 2$.

$\rho_0 = 3$ のとき $L = 9, a = 9P$. $\text{co}\varphi(a) = 9 + 3\overline{P} = 3P + 6$.

$\rho_0 = 4$ のとき $L = 6, a = 6P$. $\text{co}\varphi(a) = 6 + 4\overline{P} = 4P + 2$.

$L = 8, a = 8P$. $\text{co}\varphi(a) = 8 + 4\overline{P} = 4P + 4$.

$\rho_0 = 5$ のとき $L = 5^2, a = 25P$. $\text{co}\varphi(a) = 25 + 5\bar{P} = 5P + 20$.

$\rho_0 = 6$ のとき $L = 10, a = 10P$. $\text{co}\varphi(a) = 10 + 6\bar{P} = 6P + 4$.

$\rho_0 = 7$ のとき $L = 7^2, a = 49P$. $\text{co}\varphi(a) = 49 + 7\bar{P} = 7P + 42$.
 $L = 15, a = 15P$. $\text{co}\varphi(a) = 15 + 7\bar{P} = 7P + 8$.

$\rho_0 = 8$ のとき $L = 16, a = 16P$. $\text{co}\varphi(a) = 16 + 8\bar{P} = 8P + 8$.
 $L = 14, a = 14P$. $\text{co}\varphi(a) = 14 + 8\bar{P} = 8P + 6$.
 $L = 12, a = 12P$. $\text{co}\varphi(a) = 12 + 8\bar{P} = 8P + 4$

$\rho_0 = 9$ のとき $L = 27, a = 27P$. $\text{co}\varphi(a) = 27 + 9\bar{P} = 9P + 18$
 $L = 21, a = 21P$. $\text{co}\varphi(a) = 21 + 9\bar{P} = 9P + 12$.

$\rho_0 = 11$ のとき

$L = 35, a = 35P$. $\text{co}\varphi(a) = 35 + 11\bar{P} = 11P + 24$

$L = 121, a = 121P$. $\text{co}\varphi(a) = 121 + 11\bar{P} = 11P + 110$

以上を除外すると $\rho_0 \geq 12$ になるので次の評価式をえる.

$$\text{co}\varphi(a) \geq \frac{a}{P} + 12P^{j-1}\bar{P}.$$

4.1 オイラー余関数の値から評価

例題として $\text{co}\varphi(a) = 27 = 3^3$ となる a を決定してみよう.

1) $s(a) = 1$ のとき $a = P^j$, $\text{co}\varphi(a) = P^{j-1}$ なので $P = 3, j = 4$.

2) $s(a) \geq 2$ のとき $P = \text{Maxp}(a)$ とおくと $a = P^j L$ と書ける ($P > \text{Maxp}(L)$).

$\text{co}\varphi(P^j L) = P^{j-1}(L + \bar{P}\rho_0)$ なので $j > 1$ のとき $P = 3$.

$a = 3^j * 2^e$ とすると, $\text{co}\varphi(P^j L) = 3^{j-1} * 2^{e+1} \neq 27$.

3) $j = 1$, $a = PL$.

$L + \bar{P}\rho_0 = 3^3$ を解く.

$27 = L + \bar{P}\rho_0$ により, L は奇数になる.

$\rho_0 = 1$ のとき L は素数で $P + L - 1 = 27$. よって直ちに $L = 5, P = 23; L = 11, P = 17$.

$\rho_0 = 2$ のとき L は偶数なので L は奇数の仮定に反する.

$\rho_0 = 3$ のとき $L = 9, a = 9P = 45, 63, \dots$. $\text{co}\varphi(a) = L + \overline{P}\rho_0 = 9 + 3*\overline{P} = 27$.
 $18 = 3\overline{P}$. ゆえに $P = 7, L = 3^2, a = 3^2 * 7$.

$\rho_0 = 4$ のとき $L = 6$; 偶数. L は奇数の仮定に反する.

$\rho_0 = 5$ のとき $L = 5^2; a = 25P = 25 * 7, 25 * 11, \dots$. $\text{co}\varphi(a) = L + \overline{P}\rho_0 = 25 + \overline{P}\rho_0 \neq 27$.

$\rho_0 = 6$ のとき $L = 10$: 偶数. L は奇数の仮定に反する.

$\rho_0 = 7$ のとき $L = 7^2; a = 49P, L = 15; a = 15P, a = 49 * 11, \dots, a = 15P = 15 * 7 = 105 \dots$. $\text{co}\varphi(a) = L + \overline{P}\rho_0 > 49$: 矛盾

$\rho_0 = 8$ のとき $L = 16; a = 16P; L = 12; L = 14$: 偶数. L は奇数の仮定に反する.

$\rho_0 = 9$ のとき $L = 27; a = 27P, L = 21; a = 21P, a = 27 * 5, \dots, a = 3 * 7 * 11, \dots$, $\text{co}\varphi(a) = 21 + \overline{P} * 9 > 27$: 矛盾

以上を除外すると次の評価式をえる.

$$27 = \text{co}\varphi(a) \geq \frac{a}{P} + 11P^{j-1}\overline{P} > \frac{a}{P} + 11\overline{P}.$$

よって, $P = 3$. $P = 3 * 2^e$ は $\text{co}\varphi(a) = 3^{j-1} * 2^{e+1} \neq 27$.

以上により解は, $a = 3^4, 5 * 23, 11 * 17, 7 * 3^2$.

これは高校生:三谷樹さんの結果.

4.2 オイラー余関数のギャップ値

数表によると, $N = 10, 26, 34, \dots$ が余関数のギャップ値らしい.

そこで予想:

$N = 2p, p$: 素数, $N + 1$: 非素数 なら N は ギャップ値になるか?

これは $s(a) = 2$ なら正しいが, $s(a) = 3$ となる最小値 $a = 2 * 3 * 5 = 30$ のとき $\text{co}\varphi(a) = 30 - 8 = 22 = 2 * 11, 22 - 1 = 21 = 3 * 7$: 非素数. したがってこれは反例.

10, 26 はともにギャップ値であり, 以下で確認する.

$\text{co}\varphi(a) = 2p, 2p = 10, 26$ として矛盾を導く. 証明は手間がかかる.

1) $a = P^j$ なら $\text{co}\varphi(a) = P^{j-1}$ なのでこの場合は起きない.

2) $P = \text{Maxp}(a)$ とおくと, $a = P^j L$ と書けて

$$\text{co}\varphi(a) = P^{j-1}(PL - \overline{P}\varphi(L)) = 2p.$$

3) $j > 1$ なら $P = p, j = 2$.

$$PL - \overline{P}\varphi(L) = L + \overline{P}\text{co}\varphi(L) = 2.$$

$L \geq 2, \bar{P} \geq 2$ により矛盾.

4) $j = 1$ のとき $a = PL$. L が素数なら $\text{co}\varphi(a) = P + L - 1 = 2p$. $P + L = 2p + 1$ なので $L = 2, P = 2p - 1$.

$p = 5, 13$ のとき $2p - 1$ は素数ではない. 矛盾.

5) L が素数でないなら $\rho_0 = \text{co}\varphi(L) \geq 2$.

$\text{co}\varphi(a) = L + \bar{P}\rho_0$. $\text{co}\varphi(a) = 2p$ として矛盾を導く.

\bar{P} は偶数なので, $L \therefore$ よって,

$\rho_0 = 2$ のとき $L = 4; a = 4 + 2P - 2 = 2P + 2 = 2(P + 1) \neq 2p$.

$\rho_0 = 4$ のとき $L = 6, a = 6P$. $\text{co}\varphi(a) = 6 + 4\bar{P} = 4P + 2 = 2p$.

$p = 2P + 1$.

$L = 8, a = 8P$. $\text{co}\varphi(a) = 8 + 4\bar{P} = 4P + 4 \neq 2p$.

$\rho_0 = 6$ のとき $L = 10, a = 10P$. $\text{co}\varphi(a) = 10 + 6\bar{P} = 6P + 4 = 2p$. $p = 3P + 2$.
このとき $p \neq 5, 13$

$\rho_0 = 8$ のとき $L = 16, a = 16P$. $\text{co}\varphi(a) = 16 + 8\bar{P} = 8P + 8 \neq 2p$.

$L = 14, a = 14P$. $\text{co}\varphi(a) = 14 + 8\bar{P} = 8P + 6 = 2(4P + 3)$. $4P + 3 \neq 5, 13$.

$L = 12, a = 12P$. $\text{co}\varphi(a) = 12 + 8\bar{P} = 8P + 4 \neq 2p$

5 Goldbach の予想

P, L がともに奇数なら $P + L = N + 1$ は偶数. N は与えられた余関数の値なので, $N + 1 = P + L$ を満たす異なる奇素数があるためには $N + 1 \geq 8$.

$L = 2$ のとき, $N - 1 = P$. N が偶数で $N - 1$ が素数でない場合, オイラー余関数のギャップ値になることがあるかもしれない.

8以上の偶数は2個の奇素数の和にかけるという命題は Goldbach の予想と呼ばれ, 正しいと思われるが証明ができていない. 未解決の難問として有名である.

6 オイラー余関数の平方根評価

a が素数でないなら $a \geq \varphi(a) + \sqrt{a}$. かつ $a = \varphi(a) + \sqrt{a}$ である条件は $a = p^2$.
次にこの結果を精密化する.

1) $s(a) = 1$ のとき $a = P^j, j > 1$ なら $\text{co}\varphi(a) = P^{j-1} = a^{1-1/j} \geq a^{1/2}$.

2) $s(a) \geq 2$ のとき $P = \text{Maxp}(a)$ とおくと, $a = P^j L$ と書けて $\text{co}\varphi(a) = P^{j-1}(L + \bar{P}\rho_0)$, ここで $\rho_0 = \text{co}\varphi(L)$ とおいた.

$$P^{j-1}L = \frac{a}{P} \text{ となるので } \text{co}\varphi(a) = \frac{a}{P} + P^{j-1}\bar{P}\rho_0.$$

3) $j > 1$ なら $P^{j-1}\bar{P}\rho_0 \geq P\bar{P}\rho_0$ によって, 相加相乗平均式により

$$\text{co}\varphi(a) = \frac{a}{P} + P^{j-1}\bar{P}\rho_0 \geq \frac{a}{P} + P\bar{P}\rho_0 \geq 2\sqrt{\bar{P}\rho_0}\sqrt{a}$$

$\lambda_0 = \sqrt{(P-1)\rho_0}$ とおけば

$$\text{co}\varphi(a) \geq 2\lambda_0\sqrt{a}$$

$P \geq 3, \rho_0 \geq 1$ により, $\lambda_0 = \sqrt{(P-1)\rho_0} \geq \sqrt{2}$ なので

$$\text{co}\varphi(a) \geq 2\sqrt{2}\sqrt{a} \geq 2.8\sqrt{a}.$$

実際に $a = 18 = 3^2 * 2$ とおけば $\text{co}\varphi(a) = 12, \sqrt{a} = 3\sqrt{2}$ によって,

$$\frac{\text{co}\varphi(a)}{\sqrt{a}} = 2\sqrt{2}.$$

これ以外なら $\rho_0 \geq 2$ または $P \geq 5$. したがってこれを唯一の例外として, 次の評価が得られる.

$$\text{co}\varphi(a) \geq 4\sqrt{a}.$$

4) $j = 1$ のとき $a = PL$ になり

$$\text{co}\varphi(a) \geq 2\lambda\sqrt{a}, (\lambda = \sqrt{(1-1/P)\rho_0})$$

$\rho_0 = 2$ なら $L = 4, a = 4P$. $\text{co}\varphi(a) = 2P + 2, \sqrt{a} = 2\sqrt{P}$ により

$$\text{co}\varphi(a) \geq \frac{4}{\sqrt{3}}\sqrt{a}.$$

$\rho_0 = 3$ なら $L = 9, a = 9P, P \geq 5$. $\text{co}\varphi(a) = 3P + 6, \sqrt{a} = 3\sqrt{P}$ により $\lambda = \sqrt{(1-1/P)\rho_0} \geq \sqrt{4/5 * 3} = 1.54 \dots$

$$\text{co}\varphi(a) \geq 2 * \sqrt{4/5 * 3}\sqrt{a} > 3.08\sqrt{a}.$$

$\rho_0 \geq 4$ なら $P \geq 3$ として

$$\lambda = \sqrt{(1-1/P)\rho_0} \geq \sqrt{(1-1/P) * 4} > \sqrt{(8/3)} = 1.63 \dots$$

5) $j = 1$, $\rho_0 = 1$ なら L : 素数 になり

$$\text{co}\varphi(a) = P + L - 1 \geq 2\sqrt{a} - 1.$$

これより良い評価 $\text{co}\varphi(a) = P + L - 1 \geq 2\sqrt{a}$ は双子素数のときは成り立たない.

6.1 双子素数

$P, P + 2 = L$ がともに素数のとき双子素数という.

双子素数は無数にあるという予想がある. 2016 年現在, まだ解けていない. しかし, 事実としてこれは正しいと思われている.

$P, P + 4 = L$ がともに素数のとき, いとこ素数という.

$\text{co}\varphi(a) = P + L - 1 = 2L + 1, \sqrt{a} = \sqrt{L(L + 2)}$ なので, 次の数表ができる.

表 4: 双子素数の場合

P	L	a	$co\varphi(a)$	\sqrt{a}	$co\varphi(a) - 2\sqrt{a} + 1$	$co\varphi(a) - 2\sqrt{a}$
3	5	15	7	3.872983346	0.254033308	-0.745966692
5	7	35	11	5.916079783	0.167840434	-0.832159566
11	13	143	23	11.95826074	0.083478514	-0.916521486
17	19	323	35	17.97220076	0.055598489	-0.944401511
29	31	899	59	29.9833287	0.033342598	-0.966657402
41	43	1763	83	41.98809355	0.023812899	-0.976187101
59	61	3599	119	59.99166609	0.016667824	-0.983332176
71	73	5183	143	71.99305522	0.013889559	-0.986110441
101	103	10403	203	101.9950979	0.009804157	-0.990195843
107	109	11663	215	107.9953703	0.009259458	-0.990740542
137	139	19043	275	137.9963768	0.007246472	-0.992753528
149	151	22499	299	149.9966666	0.006666741	-0.993333259
179	181	32399	359	179.9972222	0.005555598	-0.994444402

表 5: $P = L - 4$:cousin primes

P	L	a	$co\varphi(a)$	\sqrt{a}	$co\varphi(a) - 2\sqrt{a} + 1$	$co\varphi(a) - 2\sqrt{a}$
3	7	21	9	4.582575695	0.83484861	-0.16515139
7	11	77	17	8.774964387	0.450071225	-0.549928775
13	17	221	29	14.86606875	0.267862505	-0.732137495
19	23	437	41	20.90454496	0.190910079	-0.809089921
37	41	1517	77	38.94868419	0.102631623	-0.897368377
43	47	2021	89	44.95553359	0.088932828	-0.911067172
67	71	4757	137	68.9710084	0.057983196	-0.942016804
79	83	6557	161	80.97530488	0.049390245	-0.950609755
97	101	9797	197	98.97979592	0.040408164	-0.959591836
103	107	11021	209	104.9809507	0.038098694	-0.961901306
109	113	12317	221	110.9819805	0.036038961	-0.963961039
163	167	27221	329	164.9878783	0.024243315	-0.975756685
193	197	38021	389	194.9897433	0.02051336	-0.97948664

7 copm

$s(a) \geq 2$ のとき余関数の値 $\text{co}\varphi(a)$ を下から評価するとき, 平方根ではなくより直接的な評価をした方がよい. たとえば, a の最大素因子 $\text{Maxp}(a)$ 用いて下から評価してみよう.

$P = \text{Maxp}(a)$ とおくと, $a = P^j L$, $P > \text{Maxp}(L)$, と書いてみる.
 $\text{copm}(a) = \text{co}\varphi(a) - \text{Maxp}(a)$ と新しい不変量を導入すると

$$\text{copm}(a) = P^{j-1}(L + \bar{P}\rho_0) - P$$

1) $j \geq 2$.

下限の評価なので, $j = 2$ のとき計算する.

$$\text{copm}(a) = P(L + \bar{P}\rho_0 - 1).$$

a). $\rho_0 = 1$. すなわち L は素数のとき

$$\text{copm}(a) = P(L + \bar{P}\rho_0 - 1) = P(L + P - 2).$$

$P = 3$ のときは $L = 2$ になり $\text{copm}(a) = 9$.

$P = 5$ のときは $L = 3, 2$ になる. それに応じて $\text{copm}(a) = 5(L + 3) = 30, 25$.

$P = 7$ のときは $L = 5, 3, 2$ になる. それに応じて $\text{copm}(a) = 7(L + 5) = 70, 56, 49$.

b). $\rho_0 = 2$. すなわち $L = 4$.

$\text{copm}(a) = P(2P+1)$. $L = 7, 5, 3$ とすると, それに応じて $\text{copm}(a) = 105, 55, 21$.

$j = 3, P = 3, \rho_0 = 1$. すなわち $a = 3^3 * 2$. すると, $\text{co}\varphi(a) = 3^2 * 2^2 = 36$, $\text{copm}(a) = 33$

2) $j = 1$.

a). $\rho_0 = 1$. すなわち L は素数 p のとき

$$L = p, P > p: \text{となる素数 } P \text{ について } \text{copm}(a) = P + p - 1 - P = p - 1.$$

このとき解 $a = Pp$ は無数にある.

$L = 23, 19, 17, 13, 11, 7, 5, 3, 2$ とすると, それに応じて $\text{copm}(a) = 22, 18, 16, 12, 10, 6, 4, 2, 1$.

b). $\rho_0 = 2$. このとき $L = 4$.

$$\text{copm}(a) = 2P + 2 - P = P + 2.$$

$P = 11, 7, 5, 3$ とすると, それに応じて $\text{copm}(a) = 13, 9, 7, 5$.

c). $\rho_0 = 3$. このとき $L = 9$.

$$\text{copm}(a) = 3P + 6 - P = 2P + 6.$$

$P = 11, 7, 5$ とすると, それに応じて $\text{copm}(a) = 28, 20, 16$.

d). $\rho_0 = 4$. このとき $L = 8, 6$.

$L = 8$,

$$\text{copm}(a) = 4P + 4 - P = 3P + 4.$$

$P = 7, 5, 3$ とすると, それに応じて $\text{copm}(a) = 25, 19, 13$.

$L = 6$,

$$\text{copm}(a) = 4P + 2 - P = 3P + 2.$$

$P = 7, 5$ とすると, それに応じて $\text{copm}(a) = 23, 17$.

e). $\rho_0 = 5$. このとき $L = 25$.

$$\text{copm}(a) = 5P + 20 - P = 4P + 20.$$

$P = 11, 7$ とすると, それに応じて $\text{copm}(a) = 64, 48$.

f). $\rho_0 = 6$. このとき $L = 10$.

$$\text{copm}(a) = 6P + 4 - P = 5P + 4.$$

$P = 11, 7$ とすると, それに応じて $\text{copm}(a) = 59, 39$.

g). $\rho_0 = 7$. このとき $L = 49$.

$$\text{copm}(a) = 7P + 8 - P = 6P + 8.$$

$P = 11$ とすると, それに応じて $\text{copm}(a) = 108$.

h). $\rho_0 = 8$. このとき $L = 12, 14, 16$.

$$\text{copm}(a) = L + 8P - 8 - P = L + 7P - 8.$$

$L = 12$ とすると, $\text{copm}(a) = 4 + 7P$.

$P = 5$ とすると, $\text{copm}(a) = 39$

$L = 14$ とすると, $\text{copm}(a) = 6 + 7P$.

$P = 11$ とすると, $\text{copm}(a) = 83$

$L = 16$ とすると, $\text{copm}(a) = 8 + 7P$.

$P = 3, 5$ とすると, それに応じて $\text{copm}(a) = 29, 43$.

i). $\rho_0 = 9$. このとき $L = 21, 27$.

$$\text{copm}(a) = 8P - 9 + L.$$

$L = 21$ とすると, $\text{copm}(a) = 12 + 8P$. $P = 11$ なら $\text{copm}(a) = 100$.

$L = 27$ とすると, $\text{copm}(a) = 27 + 8P$. $P = 5$ なら $\text{copm}(a) = 67$.

$$\text{copm}(a) = L + 8P - 8 - P = L + 7P - 8.$$

i). $\rho_0 \geq 12$ のとき copm が最小になるのは, $P = 3, j = 1, L = 2^e e \geq 5$ になるに違いない.

$$\text{copm}(a) = 2^{2+1} - 3 \geq 2^6 - 3 = 64 - 3 = 61.$$

以上によると次のパソコンの結果が肯定できる.

表 6: copm その 1

a	factor	$s(a)$	$\varphi(a)$		Maxp(a)	copm
6	[2, 3]	2	2	12	3	1
$2p$	[2, p]	—	—	—	—	1
15	[3, 5]	2	8	24	5	2
$3p$	[3, p]	—	—	—	—	2
35	[5, 7]	2	24	48	7	4
$5p$	[5, p]	—	—	—	—	4
12	[2 ² , 3]	2	4	28	3	5
77	[7, 11]	2	60	96	11	6
$7p$	[7, p]	—	—	—	—	6
20	[2 ² , 5]	2	8	42	5	7
18	[2, 3 ²]	2	6	39	3	9
28	[2 ² , 7]	2	12	56	7	9
143	[11, 13]	2	120	168	13	10
$11p$	[11, p]	—	—	—	—	10
221	[13, 17]	2	192	252	17	12
$13p$	[13, p]	—	—	—	—	12

表 7: copm その 2

a	factor	$s(a)$	$\varphi(a)$		Maxp(a)	copm
24	$[2^3, 3]$	2	8	60	3	13
44	$[2^2, 11]$	2	20	84	11	13
52	$[2^2, 13]$	2	24	98	13	15
45	$[3^2, 5]$	2	24	78	5	16
323	$[17, 19]$	2	288	360	19	16
$17p$	$[17, p]$	—	—	—	—	16
30	$[2, 3, 5]$	3	8	72	5	17
437	$[19, 23]$	2	396	480	23	18
551	$[19, 29]$	2	504	600	29	18
$19p$	$[19, p]$	—	—	—	—	18
40	$[2^3, 5]$	2	16	90	5	19
68	$[2^2, 17]$	2	32	126	17	19
63	$[3^2, 7]$	2	36	104	7	20
36	$[2^2, 3^2]$	2	12	91	3	21
76	$[2^2, 19]$	2	36	140	19	21
667	$[23, 29]$	2	616	720	29	22
$23p$	$[23, p]$	—	—	—	—	22
99	$[3^2, 11]$	2	60	156	11	28
899	$[29, 31]$	2	840	960	31	28
$29p$	$[29, p]$	—	—	—	—	28
48	$[2^4, 3]$	2	16	124	3	29

表 8: copm その 3

a	factor	$s(a)$	$\varphi(a)$		Maxp(a)	copm
$31p$	$[31, p]$	—	—	—	—	30
116	$[2^2, 29]$	2	56	210	29	31
117	$[3^2, 13]$	2	72	182	13	32
54	$[2, 3^3]$	2	18	120	3	33
124	$[2^2, 31]$	2	60	224	31	33
66	$[2, 3, 11]$	3	20	144	11	35
1517	$[37, 41]$	2	1440	1596	41	36
$37p$	$[37, p]$	—	—	—	—	36
88	$[2^3, 11]$	2	40	180	11	37
60	$[2^2, 3, 5]$	3	16	168	5	39
70	$[2, 5, 7]$	3	24	144	7	39
148	$[2^2, 37]$	2	72	266	37	39
153	$[3^2, 17]$	2	96	234	17	40
1763	$[41, 43]$	2	1680	1848	43	40
$41p$	$[41, p]$	—	—	—	—	40

8 $a = 2p$ の方程式

$p > 2$ を素数とし, $a = 2p$ に関してそのオイラー関数を調べる.

$$\varphi(a) = \varphi(2p) = \varphi(p) = p - 1 = a/2 - 1.$$

これより,

$$2\varphi(a) = a - 2$$

をえる. これを $a = 2p$ の方程式という.

逆にこの方程式の解 a を求めよう. $a = 2\varphi(a) + 2$ により a は偶数.

$a = 2^e L$, ($e > 0$, L : 奇数) と書けるので

$$2\varphi(a) = 2\varphi(2^e L) = 2\varphi(2^e)\varphi(L) = 2^e\varphi(L), 2\varphi(a) = a - 2 = 2^e L - 2$$

になるので,

$$2^e\varphi(L) = 2^e L - 2.$$

これより,

$$2^{e-1}(L - \varphi(L)) = 1.$$

$e > 1$ なら左辺は偶数. よって, $e = 1, L - \varphi(L) = 1$. $\text{co}\varphi(L) = 1$ により, L は素数 p . したがって $a = 2p$.

$2\varphi(a) = a - 2$ は $a = 2p$ を決定する方程式であり, 美しい結果といえることができる.

9 $a = P^\varepsilon p$ の方程式

P を素数ととし, その累乗 P^ε を考え $a = P^\varepsilon p$ に関してそのオイラー関数を調べる.

$a = P^\varepsilon p$ のとき

$$P\varphi(a) = \overline{P}P^\varepsilon(p - 1) = \overline{P}a - \overline{P}P^\varepsilon.$$

よって

$$P\varphi(a) = \overline{P}a - \overline{P}P^\varepsilon$$

をえる. これを $a = P^\varepsilon p$ の方程式という.

10 計算例

$a = 3^4 p$ の場合, その方程式は

$$3\varphi(a) = 2a - 2 * 3^4$$

コンピュータで確認してみる.

10.1 $P = 3, a = 3^4 p$ の場合

$a = 3^4 p$ の場合, その方程式は

$$3\varphi(a) = 2a - 2 * 3^4$$

表 9: $a = 3^4 p$ の場合

a	$\varphi(a)$	a 素因数分解
162	54	$[2, 3^4]$
345	176	$[3, 5, 23]$
405	216	$[3^4, 5]$
561	320	$[3, 11, 17]$
567	324	$[3^4, 7]$
891	540	$[3^4, 11]$

$m = 3^4$ のとき通常解 $a = 3^4 p$, エイリアン解が $a = 3 * 5 * 23, a = 3 * 11 * 17$.

10.2 $P = 3, a = 3^5 p$ の場合

$a = 3^4 p$ の場合, その方程式は $3\varphi(a) = 2a - 2 * 3^5$

$m = 3^5$ のとき通常解 $a = 3^5 p$,

エイリアン解が $a = 1035 = 3^2 * 5 * 23, a = 1683 = 3^2 * 11 * 17$

$a = 2343 = 3 * 11 * 71, a = 4071 = 3 * 23 * 59, a = 4611 = 3 * 29 * 53$.

これらしかないことを証明することは今や容易であろう.

[研究課題] 最大のエイリアン解を評価せよ.

[研究課題] $2 * P^\varepsilon$ が最小の解.

表 10: $a = 3^5 p$ の場合

a	$\varphi(a)$	a 素因数分解
486	162	$[2, 3^5]$
1035	528	$[3^2, 5, 23]$
1215	648	$[3^5, 5]$
1683	960	$[3^2, 11, 17]$
1701	972	$[3^5, 7]$
2343	1400	$[3, 11, 71]$
2673	1620	$[3^5, 11]$
3159	1944	$[3^5, 13]$
4071	2552	$[3, 23, 59]$
4131	2592	$[3^5, 17]$
4611	2912	$[3, 29, 53]$
4617	2916	$[3^5, 19]$
5589	3564	$[3^5, 23]$
7047	4536	$[3^5, 29]$
7533	4860	$[3^5, 31]$
8991	5832	$[3^5, 37]$
9963	6480	$[3^5, 41]$
10449	6804	$[3^5, 43]$

10.3 $P = 5, a = 5^3 p$ の場合

$a = 3^4 p$ の場合, その方程式は

$$5\varphi(a) = 4a - 4 * 5^3$$

$m = 5^3$ のとき通常解 $a = 5^3 p$, エイリアン解が

$$a = 345 = 3 * 5 * 23$$

$$a = 375 = 3 * 5^3$$

$$a = 665 = 5 * 7 * 19$$

10.4 $P = 7, a = 7^2 p$ の場合

$a = 7^2 p$ の場合, その方程式は $7\varphi(a) = 6a - 6 * 7^2$.

$m = 7^2$ のとき通常解 $a = 7^2 p$, エイリアン解が $a = 105 = 3 * 5 * 7$

$a = 7 * 5 * 3$ の解なのでおめでたいかも.

表 11: $a = 5^3 p$ の場合

a	$\varphi(a)$	a 素因数分解
250	100	$[2, 5^3]$
345	176	$[3, 5, 23]$
375	200	$[3, 5^3]$
665	432	$[5, 7, 19]$
875	600	$[5^3, 7]$
1375	1000	$[5^3, 11]$
1625	1200	$[5^3, 13]$

表 12: $a = 7^2 p$ の場合

a	$\varphi(a)$	a 素因数分解
98	42	$[2, 7^2]$
105	48	$[3, 5, 7]$
147	84	$[3, 7^2]$
245	168	$[5, 7^2]$
539	420	$[7^2, 11]$
637	504	$[7^2, 13]$
833	672	$[7^2, 17]$
931	756	$[7^2, 19]$

10.5 $a = P^\varepsilon p$ の場合

$a = P^\varepsilon p$ のとき

$$P\varphi(a) = \overline{P}P^\varepsilon(p-1) = \overline{P}a - \overline{P}P^\varepsilon.$$

よって

$$P\varphi(a) = \overline{P}a - \overline{P}P^\varepsilon$$

をえる. これを $a = P^\varepsilon p$ の方程式という.

逆にこの方程式の解 a を求めよう.

P を法として考えるとすぐわかるように a は P の倍数.

$a = P^e L$, ($e > 0$, $L : P$ で割れない,) と書ける.

$P\varphi(a) = \overline{P}P^e\varphi(L)$ により

$$\overline{P}P^e\varphi(L) = \overline{P}P^eL - \overline{P}P^e.$$

これより

$$L - \varphi(L) = P^{\varepsilon-e}.$$

$\eta = \varepsilon - e$ とおくと

$$\text{co}\varphi(L) = P^\eta.$$

逆に、オイラーの余関数について $\text{co}\varphi(L) = P^\eta$ を満たす $L : P$ と互いに素、があれば、 $a = P^eL, \varepsilon = e + \eta$ について、 $a = P^\varepsilon p$ を満たす。

$\varepsilon = 1$ のとき、 $e > 0$ により $\eta = 1 - e = 0$. $\text{co}\varphi(L) = 1$. L は素数 p になり $a = Pp$.

$P = 2$ のとき、 $e > 0$ により $\eta = 1 - e = 0$. $\text{co}\varphi(L) = 1$. L は素数 p になり $a = Pp$. $\text{co}\varphi(L) = 2^\eta$ が成立するが、 L は奇数なので $\text{co}\varphi(L) = L - \varphi(L) = 2^\eta$ より $\eta = 0$. L は素数 p になり $a = 2^e p$.

$a = 2^e p$ と素数 p で書ける条件は $2\varphi(a) = a - 2^e$.

$2\varphi(a) = a - 2^e$ の解は $2^e * p$ なので解は無限にある。

[研究課題]

$2\varphi(a) = a - x$ の解が無限になる場合は $x = 2^e$ になるか?

$P = 3, \varepsilon = 2$ のとき、 $e = 1, \eta = 2 - e = 1$. $\text{co}\varphi(L) = 3, L = 3^2$. しかし L は 3 で割れないので矛盾。

$P = 3, \varepsilon = 3$ のとき、 $e = 1, \eta = 3 - e = 2$. $\text{co}\varphi(L) = 9, L = 3^3, L = 3 * 7$. しかし L は 3 で割れないので矛盾。

$P = 3, \varepsilon = 4$ のとき、 $e = 1, \eta = 4 - e = 3$. $\text{co}\varphi(L) = 27, L = 3^4, L = 3^2 * 7, 5 * 23, 11 * 17$. L は 3 で割れないので $L = 5 * 23, 11 * 17$ のみ残る。

$a = 3 * 5 * 23, a = 3 * 11 * 17$ が解になり、これらをエイリアン解という。

$P = 3, \varepsilon = 5$ のとき、 $e = 1, \eta = 5 - e = 4$. $\text{co}\varphi(L) = 81$,

$a = 1035 = 3^2 * 5 * 23, a = 1683 = 3^2 * 11 * 17, a = 2343 = 3 * 11 * 71, a = 4071 = 3 * 23 * 59, a = 4611 = 3 * 29 * 53$.

これらをエイリアン解という。

$P = 5, \varepsilon = 3$ のとき、 $e = 1, \eta = 3 - e = 2$. $\text{co}\varphi(L) = 25, L = 5^3, L = 3 * 23$. L は 5 で割れないので $L = 3 * 23$ のみ残る。

$a = 3 * 5 * 23$ が解になり, これをエイリアン解という.

$P = 7, \varepsilon = 2$ のとき, $e = 1, \eta = 2 - e = 1$. $\text{co}\varphi(L) = 7, L = 7^2, L = 3 * 5$. L は7で割れないので $L = 3 * 5$ のみ残る.

$a = 3 * 5 * 7$ が解になり, これをエイリアン解という.

11 $a - 2\varphi(a) = x$ の表

表 13: $a - 2\varphi(a)$ その 1

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
29	[29]	28	1	-27
81	[3 ⁴]	54	27	-27
93	[3, 31]	60	33	-27
117	[3 ² , 13]	72	45	-27
189	[3 ³ , 7]	108	81	-27
357	[3, 7, 17]	192	165	-27
405	[3 ⁴ , 5]	216	189	-27
645	[3, 5, 43]	336	309	-27
693	[3 ² , 7, 11]	360	333	-27
55	[5, 11]	40	15	-25
87	[3, 29]	56	31	-25
375	[3, 5 ³]	200	175	-25
615	[3, 5, 41]	320	295	-25
23	[23]	22	1	-21
99	[3 ² , 11]	60	39	-21
147	[3, 7 ²]	84	63	-21
555	[3, 5, 37]	288	267	-21
69	[3, 23]	44	25	-19
19	[19]	18	1	-17

表 14: $a - 2\varphi(a) = x$ ㄗの 2

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
17	[17]	16	1	-15
25	[5 ²]	20	5	-15
57	[3, 19]	36	21	-15
225	[3 ² , 5 ²]	120	105	-15
273	[3, 7, 13]	144	129	-15
465	[3, 5, 31]	240	225	-15
35	[5, 7]	24	11	-13
51	[3, 17]	32	19	-13
435	[3, 5, 29]	224	211	-13
13	[13]	12	1	-11
11	[11]	10	1	-9
27	[3 ³]	18	9	-9
39	[3, 13]	24	15	-9
63	[3 ² , 7]	36	27	-9
135	[3 ³ , 5]	72	63	-9
231	[3, 7, 11]	120	111	-9
855	[3 ² , 5, 19]	432	423	-9

表 15: $a - 2\varphi(a) = x$ その 3

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
33	[3, 11]	20	13	-7
345	[3, 5, 23]	176	169	-7
7	[7]	6	1	-5
75	[3, 5 ²]	40	35	-5
5	[5]	4	1	-3
9	[3 ²]	6	3	-3
21	[3, 7]	12	9	-3
45	[3 ² , 5]	24	21	-3
285	[3, 5, 19]	144	141	-3
765	[3 ² , 5, 17]	384	381	-3
3	[3]	2	1	-1
15	[3, 5]	8	7	-1
255	[3, 5, 17]	128	127	-1
2	[2]	1	1	0
-	-	-	-	0
512	[2 ⁹]	256	256	0

この表から $N = a - 2\varphi(a) < 0$ のとき N は奇数に限ることが見て取れる。
案外簡単に証明できた。

N は偶数 $2M$ とおくと a も偶数なので $a = 2^e L, L: \text{奇数}$, と表される。

$$0 > N = 2M = a - 2\varphi(a) = 2^e L - 2^e \varphi(L) = 2^e (L - \varphi(L))$$

によって余関数が負になり矛盾。

表 16: $a - 2\varphi(a) = x$ その 4

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
6	[2, 3]	2	4	2
—	—	—	—	2
998	[2, 499]	498	500	2
195	[3, 5, 13]	96	99	3
12	[2 ² , 3]	4	8	4
—	—	—	—	4
964	[2 ² , 241]	480	484	4
165	[3, 5, 11]	80	85	5
18	[2, 3 ²]	6	12	6
88	[2 ³ , 11]	40	48	8
—	—	—	—	8
904	[2 ³ , 113]	448	456	8
105	[3, 5, 7]	48	57	9
585	[3 ² , 5, 13]	288	297	9

$a - 2\varphi(a) = 1$ のとき解はないように思われる. 証明は困難であろう.

$a - 2\varphi(a) = 6$ のとき解は 1 つだけ. これは容易に証明できる.

a は偶数なので $a = 2^e L$ と奇数 L を用いて書ける.

$2^e L - 2^e \varphi(a) = 6$ により $e = 1, L - \varphi(L) = 3$.

$\text{co}\varphi(L) = 3$ のとき $L = 3^2$ は容易にわかる. よって $a = 18$.

$a - 2\varphi(a) = -27, -9, -3, -1$ の場合の解は個数が多いこと解が類似していることに注意しよう.

12 方程式 $2\varphi(a) - a = 1$ の解

負の場合は気分的に良くないので符号を変えて $2\varphi(a) - a = 1$ の場合を調べる.

表 17: $2\varphi(a) - a = 1$, コンピュータによる全数調査

a	素因数分解
3	3
15	$3 * 5$
255	$3 * 5 * 17$
65535	$3 * 5 * 17 * 257$

方程式 $2\varphi(a) - a = 1$ の解は著しい性格を持っている.

解 a に対して $a < p$ となる素数 p があり ap が次の解になっている.

12.1 方程式 $2\varphi(a) - a = 3$ の解

表 18: $2\varphi(a) - a = 3$, コンピュータによる全数調査

a	素因数分解	*
5	5	new
9	3^2	*
21	$3 * 7$	new
45	$3^2 * 5$	*
285	$3 * 5 * 19$	new
765	$3^2 * 5 * 17$	*
27645	$3 * 5 * 19 * 97$	new
196605	$3^2 * 5 * 17 * 257$	*

12.2 $2\varphi(a) - a = 9, 27$

表 19: $2\varphi(a) - a = 9$, コンピュータによる全数調査

a	素因数分解	
11	11	new
27	3^3	*
39	$3 * 13$	new
63	$3^2 * 7$	**
135	$3^3 * 5$	*
231	$3 * 7 * 11$	new
855	$3^2 * 5 * 19$	**
2295	$3^3 * 5 * 17$	*
82935	$3^2 * 5 * 19 * 97$	**

表 20: $2\varphi(a) - a = 27$, コンピュータによる全数調査

a	素因数分解	
29	29	new
81	3^4	*
93	$3 * 31$	new
117	$3^2 * 13$	*
189	$3^3 * 7$	**
357	$3 * 7 * 17$	new
405	$3^4 * 5$	*
645	$3 * 5 * 43$	new
693	$3^2 * 7 * 11$	***
2565	$3^3 * 5 * 19$	**
6885	$3^4 * 5 * 17$	*
72165	$3 * 5 * 17 * 283$	new

12.3 $2\varphi(a) - a = 81$

表 21: $2\varphi(a) - a = 81$, コンピュータによる全数調査

a	素因数分解	
83	83	new
243	3^5	*
279	$3^2 * 31$	****
351	$3^3 * 13$	***
567	$3^4 * 7$	**
1071	$3^2 * 7 * 17$	****
1215	$3^5 * 5$	*
1455	$3 * 5 * 97$	new
1935	$3^2 * 5 * 43$	****
2079	$3^3 * 7 * 11$	***
7695	$3^4 * 5 * 19$	**
20655	$3^5 * 5 * 17$	*
85935	$3 * 5 * 17 * 337$	new