

# オイラー関数の反復に対応する自然な余関数について

梶田 光

2023年10月7日

## 1 $\text{co}\varphi^2$ の定義とその値

オイラー関数  $\varphi(n)$  には,  $\text{co}\varphi(n) = n - \varphi(n)$  で定義される余関数がある.

これを  $\varphi^2(n) := \varphi(\varphi(n))$  に対してまったく同じように  $\text{co}\varphi^2 = n - \varphi^2(n)$  と定義すると, いくつかのよい性質が満たされない.

例えば  $\text{co}\varphi^2$  の下限が 1 より大きい, 特定の条件を満たす  $n$  に対して  $\text{co}\varphi^2$  が一定にならない ( $\text{co}\varphi$  では  $n : \text{prime}$  のとき 1 であった) などである.

しかし,  $\text{co}\varphi^2(n) = n - 2\varphi^2(n)$  と定義することによりこの問題が解決される.

今回はこのようにしてできた  $\text{co}\varphi^2(n)$  が定数  $C$  に等しくなる場合, どのような  $n$  が生成されるかを調べる.

$C$	$n$
-1	1
0	2
1	3, 5, 17, 257, 65537
2	$2^2$
3	7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, ...
4	$2 \cdot 3, 2^3$
5	$3^2, 13, 29, 53, 149, 173, 269, 293, 317, 389, 509, 557, \dots$
6	$2 \cdot 5$
7	$3 \cdot 5, 19$
8	$2^2 \cdot 3, 2^4$
9	$5^2, 41, 89, 137, 233, 569, 809, 857, 1049, 1097, 1193, \dots$

表 1:  $\text{co}\varphi^2(n) = C$

**定理 1.**  $n > 2$  のとき  $\text{co}\varphi^2(n) \geq 1$ .

*Proof.*  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$  より,  $\varphi^2(n) = \varphi(\varphi(n)) = \varphi(n) \prod_{p|\varphi(n)} \left(1 - \frac{1}{p}\right)$ .

$n > 2$  のとき  $\varphi(n) : \text{even}$  であるから,  $p = 2$  は  $p|\varphi(n)$  を満たす.

したがって  $\varphi^2(n) \leq \frac{1}{2}\varphi(n)$ .

つまり  $\text{co}\varphi^2(n) = n - 2\varphi^2(n) \geq n - 2 \cdot \frac{1}{2}\varphi(n) = \text{co}\varphi(n)$ .

$n > 1$  のとき  $\text{co}\varphi(n) \geq 1$  であるから,  $\text{co}\varphi^2(n) \geq \text{co}\varphi(n) \geq 1$ . □

ここで  $\text{co}\varphi^2(1) = -1$  かつ  $\text{co}\varphi^2(2) = 0$  なので, まとめると一般に  $\text{co}\varphi^2(n) \geq -1$  が成り立つということになる.

また,  $\text{co}\varphi^2(n) = -1$  と  $n = 1$ ,  $\text{co}\varphi^2(n) = 0$  と  $n = 2$  はそれぞれ同値であることが従う.

**補題 1.**  $n$  が合成数ならば,  $\varphi(n) \leq n - \sqrt{n}$ .

*Proof.*  $n$  の最小素因数を  $q$  とすると,  $q \leq \sqrt{n}$ . したがって,

$$\varphi(n) \leq n \left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}. \quad \square$$

**定理 2.**  $\text{co}\varphi^2(n) = C$  に無限個の解があるならば,  $C = 1, 2^e + 1$ .

またそれぞれの  $C$  について, 方程式  $\text{co}\varphi^2(n) = C$  の

- $C = 1$  のとき,  $n$  はフェルマ素数
- $C = 2^e + 1$ ,  $n$  は  $\frac{n-1}{2^e}$  も素数となるような素数. ただし  $n$  がフェルマ素数の場合を除く.

という解以外は高々有限個のみ.

*Proof.* まず,  $n = 1, 2$  の場合は除外してよい.

このとき  $\varphi(n)$  : even であるから,

$$2\varphi^2(n) = 2\varphi(n) \prod_{p|\varphi(n)} \left(1 - \frac{1}{p}\right) = \varphi(n) \prod_{p|\varphi(n), p \neq 2} \left(1 - \frac{1}{p}\right) \text{ と表される.}$$

$n$  が合成数のとき,  $2\varphi^2(n) \leq n - \sqrt{n}$ .

よって  $\text{co}\varphi^2(n) = n - 2\varphi^2(n) \geq n - (n - \sqrt{n}) = \sqrt{n}$  が得られる.

つまり  $C \geq \sqrt{n}$ , よって  $n \leq C^2$ .

したがって  $C$  が固定されている場合,  $\text{co}\varphi^2(n) = C$  に合成数の解は無限に存在できない.

$\text{co}\varphi^2(n) = C$  に無限個の解があるということは, したがって無限個の素数解があることと同値である.

$n$  : prime として再度  $\text{co}\varphi$  を計算すると

$$\text{co}\varphi^2(n) = n - 2\varphi^2(n) = n - \varphi(n) \prod_{p|\varphi(n), p \neq 2} \left(1 - \frac{1}{p}\right) = n - (n-1) \prod_{p|n-1, p \neq 2} \left(1 - \frac{1}{p}\right) = C.$$

ここで  $n-1 = 2^e L$  ( $e > 0, L$  : odd) とおき,  $L$  は合成数と仮定する.

$$\text{すると } C = n - (n-1) \prod_{p|n-1, p \neq 2} \left(1 - \frac{1}{p}\right) = n - 2^e \varphi(L).$$

$$\varphi(L) \leq L - \sqrt{L} \text{ より } C \geq n - 2^e(L - \sqrt{L}) = n - (n-1) + 2^e \sqrt{L} = 1 + 2^e \sqrt{L} \geq 1 + \sqrt{2^e L} = 1 + \sqrt{n-1}.$$

$\sqrt{n-1} \leq C-1$  より  $n \leq (C-1)^2 + 1$ , よって  $L$  が合成数の解は無限に存在できない.

したがって  $L = 1$  または  $L$  : prime.

(1)  $L = 1$  の場合

このとき  $n-1 = 2^e$  より  $n = 2^e + 1$  : prime となり  $n$  はフェルマ素数.

また,  $C = n - 2^e \varphi(L) = n - 2^e = 2^e + 1 - 2^e = 1$ .

(2)  $L$  : prime の場合

$L = q$  とおける.

すると  $n-1 = 2^e q$  より  $q = \frac{n-1}{2^e}$  が奇素数となる.

( $L = q : \text{odd}$  の条件が  $n$  がフェルマ素数の場合を除外している.)

このとき  $C = n - 2^e(q - 1) = 2^e q + 1 - 2^e(q - 1) = 2^e + 1$  が成り立つ. □

以下, 一般化された安全素数を  $\frac{n-1}{2^e}$  が素数となるような素数  $n$  と定義する. すると上の証明からいくつかの系が得られる.

- 合成数  $n$  が  $\text{co}\varphi^2(n) = C$  を満たすとき,  $n \leq C^2$
- 一般化された安全素数ではない素数  $n$  が  $\text{co}\varphi^2(n) = C$  を満たすとき,  $n \leq C^2 - 2C + 2$

したがって, 上の定理に示された  $C, n$  の組み合わせ以外で  $\text{co}\varphi^2(n) = C$  の解を求めるときは, 高々  $n \leq C^2$  までを計算すれば十分である.

## 2 $\text{co}\varphi^2(n) = 2^e$ の解

『オイラー余関数の逆関数について』では,  $\text{co}\varphi(n) = 2^e$  の解が  $a = 2^{e+1}, a = 2^e p (p = 2^{e-\epsilon+1} - 1 \in \text{prime})$  と書けることを示した.

$\text{co}\varphi^2(n) = 2^e$  の解はこれより厳しくなることが証明できる.

$2^e$	$n$
$2^1$	$2^2$
$2^2$	$2^3 \quad 2 \cdot 3$
$2^3$	$2^4 \quad 2^2 \cdot 3$
$2^4$	$2^5 \quad 2^3 \cdot 3$
$2^5$	$2^6 \quad 2^4 \cdot 3$
$2^6$	$2^7 \quad 2^5 \cdot 3$
$2^7$	$2^8 \quad 2^6 \cdot 3$
$2^8$	$2^9 \quad 2^7 \cdot 3$
$2^9$	$2^{10} \quad 2^8 \cdot 3$
$2^{10}$	$2^{11} \quad 2^9 \cdot 3$

表 2:  $\text{co}\varphi^2(n) = 2^e$

**定理 3.**  $\text{co}\varphi^2(n) = 2^e (e > 0)$  の解は

- $e = 1$  のとき  $n = 4$
- $e > 1$  のとき  $n = 2^{e+1}, 3 \cdot 2^{e-1}$

に限る.

*Proof.*  $n - 2\varphi^2(n) = 2^e$  より,  $n : \text{even} = 2^f L (f > 0, L : \text{odd})$  と書ける.

これを代入すると,  $2^f L - 2\varphi(2^{f-1}\varphi(L)) = 2^e$ .

$L = 1$  を仮定すると  $2^f - 2\varphi(2^{f-1}) = 2^e$ .

$f = 1$  とすると  $n = 2$  となるが, これは  $\text{co}\varphi^2(n) = 2^e$  を満たさないため  $f > 1$  としてよい.

このとき  $2^f - 2^{f-1} = 2^e$ , つまり  $2^{f-1} = 2^e$ .

したがって  $f = e + 1$  より  $n = 2^{e+1}$  が得られる.

次に  $L > 1$  とする.

$L$ : odd より  $L > 2$ , したがって  $\varphi(L)$ : even.

よって  $2\varphi(2^{f-1}\varphi(L)) = 2^f\varphi(\varphi(L))$  が成り立つ.

これを代入すると  $2^f L - 2^f \varphi^2(L) = 2^e$ , したがって  $L - \varphi(\varphi(L)) = 2^{e-f}$  となる.

(1)  $\varphi(\varphi(L))$ : odd の場合

このとき  $\varphi(L) = 1, 2$  より  $L = 3$ .

$L - \varphi(\varphi(L)) = 3 - 1 = 2 = 2^{e-f}$  より  $f = e - 1$ .

ここから  $n = 3 \cdot 2^{e-1}$  が得られる.

ただし  $f = e - 1 > 0$  より  $e = 1$  の場合はこの解が存在しないことに注意.

(2)  $\varphi(\varphi(L))$ : even の場合

$L$ : odd より  $L - \varphi(\varphi(L)) = 2^{e-f}$ : odd, したがって  $e = f, L - \varphi(\varphi(L)) = 1$  が成り立つ.

ここで  $L - \varphi(\varphi(L)) = \text{co}\varphi^2(L) + \varphi(\varphi(L)) = 1$ .

つまり  $\text{co}\varphi^2(L) = 1 - \varphi(\varphi(L)) \leq 0$ .

この不等式を満たす  $L$  は  $1, 2$  しか存在しないが, どちらも  $L$ : odd,  $L > 1$  の仮定に反する. □

### 3 $\text{co}\varphi^k$ の定義とその値

これまでの議論を一般化し,  $\text{co}\varphi^k(n) = n - 2^{k-1}\varphi^k(n)$  と定義する.

以降  $k > 2$  は定数とする.

また,  $\varphi^0(n) = n$  とする.

**命題 1.**  $\text{co}\varphi^k(n) \leq 0$  を満たすならば,  $\varphi^k(n) = 1$ .

*Proof.*  $\varphi^k(n) \geq 2$  を仮定する.

このとき  $\varphi^j(n)$  はすべての  $1 \leq j \leq k$  に関して  $2$  以上である.

つまり  $\varphi^j(n)$ : even.

ここで  $\varphi^0(n) = n$  とすると,  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$  より  $\varphi^k(n) = n \prod_{0 \leq j < k} \prod_{p|\varphi^j(n)} \left(1 - \frac{1}{p}\right)$  が成り立つ.

$j > 0$  に対して  $2|\varphi^j(n)$  なので,  $2 \leq \varphi^k(n) \leq n \prod_{1 \leq j < k} \left(1 - \frac{1}{2}\right) = \frac{n}{2^{k-1}}$

したがって  $2 \cdot 2^{k-1} \leq n$ , つまり  $n \geq 2^k$ .

しかし,  $n$  が偶数のとき上の不等式の等号が成り立たないため,  $n > 2^k$ .

$\text{co}\varphi^k(n) = n - 2^{k-1}\varphi^k(n) > 2^k - 2 \cdot 2^{k-1} = 0$ .

命題の対偶が証明されたため, 命題も真である. □

**系 1.**  $\text{co}\varphi^k(n) = C$  ( $C \leq 0$ )  $\iff n = 2^{k-1} + C$ .

*Proof.*  $\text{co}\varphi^k(n) \leq 0$  より,  $\varphi^k(n) = 1$ .

したがって  $\text{co}\varphi^k(n) = n - 2^{k-1}\varphi^k(n) = n - 2^{k-1} = C$ .

つまり  $n = 2^{k-1} + C$ .

上の命題の証明から,  $\varphi^k(n) \geq 2$  ならば  $n > 2^k$  なので  $\varphi^k(n) = 1$ .

代入すると  $\text{co}\varphi^k(n) = n - 2^{k-1} = C$  となるから、これは実際に解である。  $\square$

このような  $n$  全体の集合を  $S$  とおく。

無限個の解が存在するときの条件の前に、補助関数とそれについての命題を証明する。

**定義 1.**  $\bar{\varphi}^k(n) := n \prod_{0 \leq j < k} \prod_{p|\varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right)$ .

**命題 2.**  $n$  が奇数かつ合成数のとき、 $\bar{\varphi}^k(n) \leq n - \sqrt{n}$ .

*Proof.*  $j = 0$  のときの  $p$  に  $n$  の最小素因数  $2 < q \leq \sqrt{n}$  が含まれるため、

$$\bar{\varphi}^k(n) = n \prod_{0 \leq j < k} \prod_{p|\varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right) \leq n \left(1 - \frac{1}{q}\right) \leq n \left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}. \quad \square$$

**命題 3.**  $n$  が  $\varphi^{k-1}(n) > 1$  を満たす奇素数で、 $n-1 = 2^e L (e > 0, L : \text{odd})$  と書けるとき、 $\bar{\varphi}^k(n) = 2^e \bar{\varphi}^{k-1}(L)$ .

*Proof.*

$$\begin{aligned} \bar{\varphi}^k(n) &= n \prod_{0 \leq j < k} \prod_{p|\varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right) = n \prod_{p|n, p \neq 2} \left(1 - \frac{1}{p}\right) \prod_{1 \leq j < k} \prod_{p|\varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right) \\ &= \varphi(n) \prod_{0 \leq j < k-1} \prod_{p|\varphi^j(n-1), p \neq 2} \left(1 - \frac{1}{p}\right) = (n-1) \prod_{0 \leq j < k-1} \prod_{p|\varphi^j(2^e L), p \neq 2} \left(1 - \frac{1}{p}\right) \\ &= 2^e L \prod_{0 \leq j < k-1} \prod_{p|\varphi^j(L), p \neq 2} \left(1 - \frac{1}{p}\right) \\ &= 2^e \bar{\varphi}^{k-1}(L). \end{aligned} \quad \square$$

これは  $k = 1$  のときも、空積を  $1$  (つまり  $\bar{\varphi}^0(n) = 1$ ) と定義すれば成り立つことに注意。

**命題 4.**  $n$  番目のフェルマ数を  $F_n$  と書いて、自然数  $E > 1$  について  $E+1 = 2^t L (t \geq 0, L : \text{odd})$  と書けるとする。このときすべての  $e > t$  について  $F_t | 2^E F_e + 1$ .

*Proof.* 以下の合同式ではすべて  $\text{mod } F_t$  で考える。

$$\begin{aligned} 2^E F_e + 1 &= 2^E (2^{2^e} + 1) + 1 = 2^E (2^{2^t \cdot 2^{e-t}} + 1) + 1 = 2^E ((F_t - 1)^{2^{e-t}} + 1) + 1 \\ &\equiv 2^E ((-1)^{2^{e-t}} + 1) + 1 \end{aligned}$$

ここで  $e > t$  より、 $2^{e-t}$  は偶数であるから、

$$\begin{aligned} 2^E F_e + 1 &\equiv 2^E (1 + 1) + 1 \equiv 2^{E+1} + 1 \equiv 2^{2^t L} + 1 \equiv (2^{2^t})^L + 1 \\ &\equiv (-1)^L + 1 \end{aligned}$$

$L$  は奇数なので、 $2^E F_e + 1 \equiv 0 \pmod{F_t}$ .  $\square$

$F_e > F_t > 1$  であるから、これは  $2^E F_e + 1$  と書ける素数は有限個であることを示している。

**定理 4.**  $\text{co}\varphi^k(n) = C$  が無限個の解を生成するならば、

$$C = 1, 1 + \sum_{1 \leq j < k} \prod_{1 \leq l \leq j} 2^{e_l} = 1 + 2^{e_1} + 2^{e_1} 2^{e_2} + \dots + 2^{e_1} 2^{e_2} \dots 2^{e_{k-1}}$$

のいずれかである。

このとき、

- $C = 1$  のときフェルマ素数全体の集合.
- $C = 1 + \sum_{1 \leq j < k} \prod_{1 \leq l \leq j} 2^{e_l} = 1 + 2^{e_1} + 2^{e_1} 2^{e_2} + \dots + 2^{e_1} 2^{e_2} \dots 2^{e_{k-1}}$  のとき  
 $n_0 = n, n_{i+1} = \frac{n_i - 1}{2^{e_{i+1}}}$  で定義される数列において, すべての  $0 \leq i < k$  に対して  $n_i$  が素数となるような  $n$  全体の集合.

を  $S_C$  とおくと,  $\varphi^k(n) > 1$  を満たす  $n \in S_C$  は  $\text{co}\varphi^k(n) = C$  の解になっており, また  $S_C$  に含まれない解は有限個である.

*Proof.* 証明の方法はほぼ同じである.

さらに, Pillai (1929)[1] より,  $\varphi^k(n) = 1$  を満たすとき,  $k \geq \left\lfloor \log_3 \frac{n}{2} \right\rfloor + 1$  が成り立つ.

整理すれば  $n \leq 2 \cdot 3^{k-1}$  となって, これは有限個である.

したがってこの場合も除外してよい.

この場合  $\varphi^k(n) \geq 2$ , つまりすべての  $1 < j \leq k$  について  $\varphi^j(n) : \text{even}$  である.

すると  $\varphi^k(n) = \varphi^{k-1}(\varphi(n))$  であるから,

$$2^{k-1} \varphi^k(n) = 2^{k-1} \varphi(n) \prod_{1 \leq j < k} \prod_{p | \varphi^j(n)} \left(1 - \frac{1}{p}\right) = \varphi(n) \prod_{1 \leq j < k} \prod_{p | \varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right) \text{ と表される.}$$

$n$  が合成数のとき,  $2^{k-1} \varphi^k(n) \leq n - \sqrt{n}$ .

$$\text{よって } \text{co}\varphi^k(n) = n - 2^{k-1} \varphi^k(n) \geq n - (n - \sqrt{n}) = \sqrt{n}.$$

したがって  $C$  が固定されている場合,  $\text{co}\varphi^2(n) = C$  に合成数の解は無限に存在できない.

$$\text{つまり } n \text{ は奇素数なので, } 2^{k-1} \varphi^k(n) = n \left\{ \prod_{p|n} \left(1 - \frac{1}{p}\right) \right\} \left\{ \prod_{1 \leq j < k} \prod_{p | \varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right) \right\} = \bar{\varphi}^k(n).$$

$$\text{よって } \text{co}\varphi^k(n) = n - \bar{\varphi}^k(n).$$

$$n - 1 = 2^{e_1} n_1 (e_1 > 0, n_1 : \text{odd}) \text{ と表すと } \text{co}\varphi^k(n) = n - 2^{e_1} \bar{\varphi}^{k-1}(n_1).$$

$n_1$  が合成数とすると,

$$C = \text{co}\varphi^k(n) = n - 2^{e_1} \bar{\varphi}^{k-1}(n_1) \geq n - 2^{e_1} (n_1 - \sqrt{n_1}) = 1 + 2^{e_1} \sqrt{n_1} \geq 1 + \sqrt{2^{e_1} n_1} = 1 + \sqrt{n - 1}.$$

したがってこの場合も無限に存在する解の列として不適切である.

$n_1 = 1$  の場合,  $n = 2^{e_1} + 1$  はフェルマ素数. また,  $C = n - 2^{e_1} = 1$ .

次に  $n_1$  は素数のとき,  $n_1 - 1 = 2^{e_2} n_2$  と表すと  $\text{co}\varphi^k(n) = n - 2^{e_1 + e_2} \bar{\varphi}^{k-2}(n_2)$ .

この操作を繰り返していく.

厳密にすると,  $1 \leq i < k$  において,  $\text{co}\varphi^k(n) = n - \bar{\varphi}^{k-i}(n_i) \prod_{1 \leq j \leq i} 2^{e_j}$  とする.

ただし,  $n_0 = n$  として, すべての  $1 \leq j \leq i$  について  $n_{j-1} - 1 = 2^{e_j} n_j, n_{j-1} : \text{odd prime}$  を仮定する.

$n_i$  が合成数とすると,  $\bar{\varphi}^{k-i}(n_i) \leq n_i - \sqrt{n_i}$ .

すると

$$\begin{aligned} \text{co}\varphi^k(n) &\geq n - (n_i - \sqrt{n_i}) \prod_{1 \leq j \leq i} 2^{e_j} = n + \sqrt{n_i} \prod_{1 \leq j \leq i} 2^{e_j} - n_i \prod_{1 \leq j \leq i} 2^{e_j} \\ &= n + \sqrt{n_i} \prod_{1 \leq j \leq i} 2^{e_j} - (n_{i-1} - 1) \prod_{1 \leq j \leq i-1} 2^{e_j} \geq n + \sqrt{n_i} \prod_{1 \leq j \leq i} 2^{e_j} - n_{i-1} \prod_{1 \leq j \leq i-1} 2^{e_j} \\ &= \dots \\ &\geq n + \sqrt{n_i} \prod_{1 \leq j \leq i} 2^{e_j} - n = \sqrt{n_i} \prod_{1 \leq j \leq i} 2^{e_j} \end{aligned}$$

これを二乗すると  $C^2 \geq n_i \prod_{1 \leq j \leq i} (2^{e_j})^2$ .

ここで  $n = 1 + \sum_{1 \leq j < i} \prod_{1 \leq l \leq j} 2^{e_l} + n_i \prod_{1 \leq j \leq i} 2^{e_j}$  を証明する.

(読みやすくすると  $n = 1 + 2^{e_1} + 2^{e_1}2^{e_2} + 2^{e_1}2^{e_2}2^{e_3} + \dots + 2^{e_1}2^{e_2} \dots 2^{e_i}n_i$  ということになる.)

まず  $i = 1$  のときは  $n = 1 + 2^{e_1}n_1$  より成り立つ.

$i - 1$  のとき成り立つとすると

$$\begin{aligned} n &= 1 + \sum_{1 \leq j < i-1} \prod_{1 \leq l \leq j} 2^{e_l} + n_{i-1} \prod_{1 \leq j \leq i-1} 2^{e_j} = 1 + \sum_{1 \leq j < i-1} \prod_{1 \leq l \leq j} 2^{e_l} + (1 + 2^{e_i}n_i) \prod_{1 \leq j \leq i-1} 2^{e_j} \\ &= 1 + \sum_{1 \leq j < i-1} \prod_{1 \leq l \leq j} 2^{e_l} + \prod_{1 \leq l \leq i-1} 2^{e_l} + n_i \prod_{1 \leq j \leq i} 2^{e_j} \\ &= 1 + \sum_{1 \leq j < i} \prod_{1 \leq l \leq j} 2^{e_l} + n_i \prod_{1 \leq j \leq i} 2^{e_j} \end{aligned}$$

より成り立つ.

$$\frac{n}{C^2} \leq \frac{1}{4^i} + \sum_{1 \leq j < i} \frac{1}{2^i} + \frac{1}{2^i} \leq \frac{i+1}{2^i} \leq 1$$

よって  $n \leq C^2$ , つまり  $n_i$  が合成数の解は無限に存在できない.

$n_i = 1$  とするとこれは解で, このとき  $I = i$ . 帰納法から導かれた  $n$  の展開式から,

$$C = n - \prod_{1 \leq j \leq i} 2^{e_j} = 1 + \sum_{1 \leq j < i} \prod_{1 \leq l \leq j} 2^{e_l}.$$

ここで  $C$  は固定されているから,  $e$  のあり得る組み合わせも有限個である.

$i > 1$  とすると,  $n_{i-1} = 1 + 2^{e_i}n_i = 1 + 2^{e_i}$  はフェルマ素数.

$$n_{i-2} = 2^{e_{i-1}}n_{i-1} + 1.$$

この形の素数は有限個しかありえないので,  $i = 1$ .

このとき  $n = n_0 = 2^{e_1}n_1 + 1 = 2^{e_1}$  がフェルマ素数で,

$$C = 1 + \sum_{1 \leq j < 1} \prod_{1 \leq l \leq j} 2^{e_l} \text{ が空和となって } C = 1.$$

$n_i$  : odd prime とすると  $n_i - 1 = 2^{e_{i+1}}n_{i+1}$  と書けて, これを繰り返すことができる.

$i = k - 1$  のときに  $n_i$  : odd prime となったとすると,  $I \geq k$ .

$$\text{co}\varphi^k(n) = n - \varphi^0(n_{k-1}) \prod_{1 \leq j \leq k} 2^{e_j} = n - \prod_{1 \leq j \leq k} 2^{e_j}.$$

$$\text{このとき, 上の計算と同様に, } C = 1 + \sum_{1 \leq j < k} \prod_{1 \leq l \leq j} 2^{e_l}.$$

□

## 参考文献

- [1] Pillai, S. S. (1929). On some functions connected with  $\varphi(n)$ . *Bulletin of the American Mathematical Society*, 35(6), 837-841.