

# オイラー関数の多重合成に対応する自然な余関数について

梶田光

2025/08/05

## 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.

さて, これの知られている重要な性質を列挙すると:

- $\text{co}\varphi(n) = 0 \iff n = 1$
- $\text{co}\varphi(n) = 1 \iff n : \text{prime}$
- $n : \text{composite} \implies \text{co}\varphi(n) \geq \sqrt{n}$

つまり,  $\varphi(n)$  は,  $n$  が素数という条件ではほぼ  $n$  だが, 合成数のときはその差は  $\sqrt{n}$  以上になる.

定数  $A, B$  について,  $An - B\varphi(n) = C$  を求める問題は,  $A > B$  のとき簡単すぎ,  $A < B$  のとき解けないほど難しい.

余関数はこの丁度いい境目に位置していると考えることができる.

さて, オイラー関数の合成  $\varphi^2(n) := \varphi(\varphi(n))$  について上のような余関数を定義することを考える.

まずすぐにわかることは,  $n - \varphi(\varphi(n))$  はうまくいかないであろうということである.

というのも, 一般に大きい  $n$  について,  $\varphi(n)$  は偶数であるから,  $\varphi(\varphi(n))$  は最大でも  $\frac{n}{2}$  程度にしかない.

そこで, 係数を補って  $\text{co}\varphi^2(n) := n - 2\varphi^2(n)$  と定義すると, 以降議論するような面白い性質が得られる.

以下に示すのは, 小さい整数の定数  $C$  と,  $\text{co}\varphi^2(n) = C$  の解を列挙した表である.

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

以降,  $p$  はすべて素数を指すものとする.

**定理 1.1:**  $n > 2$  ならば,  $\text{co}\varphi^2(n) > 0$ .

*Proof:*  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$  の  $n$  に  $\varphi(n)$  を代入すると,  $\varphi^2(n) = \varphi(n) \prod_{p|\varphi(n)} \left(1 - \frac{1}{p}\right)$ .

さて,  $n > 2$  ならば  $\varphi(n)$  は偶数なので,  $p = 2$  は  $p | \varphi(n)$  を満たす.

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

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

そして, 一般に  $n > 1$  のとき  $\text{co}\varphi(n) > 0$  であるから,  $\text{co}\varphi^2(n) \geq \text{co}\varphi(n) > 0$ . ■

さて,  $\text{co}\varphi^2(1) = -1, \text{co}\varphi^2(2) = 0$  より以下が従う:

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

主定理の証明のための補題として, 以下のよく知られた結果を紹介する.

**補題 1.1:**  $n$  が合成数のとき,  $\varphi(n) \leq n - \sqrt{n}$ .

*Proof:*  $n$  の最小の素因数を  $p_0$  とすると,  $n$  は合成数なので  $p_0 \leq \sqrt{n}$  が成り立つ.

さて,  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \leq n \left(1 - \frac{1}{p_0}\right) \leq n \left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}$ . ■

**定理 1.2:**  $\text{co}\varphi^2(n) = C > 0$  が成り立っているとする.

$n > C^2$  がさらに成り立つとき,  $n, C$  は以下のいずれかに当てはまる:

- $C = 1$  で,  $n$  はフェルマ素数
- ある正整数  $e$  を用いて  $C = 2^e + 1$  と書け,  $n$  は素数で  $\frac{n-1}{2^e}$  も奇素数.

*Proof:*  $\text{co}\varphi^2(n) > 0$  より,  $n > 2$ .

このとき  $\varphi(n)$  は偶数なので,  $2\varphi^2(n) = 2\varphi(n) \prod_{p|\varphi(n)} \left(1 - \frac{1}{p}\right) = 2\varphi(n) \cdot \left(1 - \frac{1}{2}\right) \cdot \prod_{p|\varphi(n), p \neq 2} \left(1 - \frac{1}{p}\right) = \varphi(n) \prod_{p|\varphi(n), p \neq 2} \left(1 - \frac{1}{p}\right)$  が成り立つ.

$n$  が合成数とすると,  $\varphi(n) \leq n - \sqrt{n}$ .

先の式から  $2\varphi^2(n) \leq \varphi(n)$  より,  $\text{co}\varphi^2(n) = n - 2\varphi^2(n) \geq n - (n - \sqrt{n}) = \sqrt{n}$ .

$C \geq \sqrt{n}$  より,  $n \leq C^2$ .

よって以降  $n$  が素数の場合のみを考える.

$n > 2$  より,  $n$  は奇素数で,  $n - 1$  は偶数なのである正整数  $e$  と奇数  $L$  を用いて  $n - 1 = 2^e L$  と書ける.

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

ここで  $2^e L$  の奇数の素因数は  $L$  の素因数と同じなので,  $\text{co}\varphi^2(n) = n - 2^e L \prod_{p|L} \left(1 - \frac{1}{p}\right) = n - 2^e \varphi(L)$ .

ここで  $L$  が合成数であると仮定する.

すると  $\text{co}\varphi^2(n) = n - 2^e \varphi(L) \geq n - 2^e (L - \sqrt{L}) = n - 2^e L - 2^e \sqrt{L} = 1 + 2^e \sqrt{L} \geq 1 + \sqrt{2^e L} \geq 1 + \sqrt{n-1} > \sqrt{n}$ .

したがってこの場合も  $C > \sqrt{n}$  より  $n \leq C^2$  が成り立つ.

つまり,  $n > C^2$  ならば  $L$  は 1 もしくは素数でなければならない.

$L = 1$  の場合,  $n - 1 = 2^e$  より  $n$  はフェルマ素数である.

$L$  が素数の場合,  $\frac{n-1}{2^e} = L$  は奇素数で,  $C = n - 2^e \varphi(L) = n - 2^e (L - 1) = n - (n - 1) + 2^e = 1 + 2^e$ . ■

## 2. 一般の $k$ に対応する $\text{co}\varphi^k$

一般の  $n$  について  $\varphi^2(n)$  は最大でも  $\frac{n}{2}$  ほどにしかならないことから  $\text{co}\varphi^2(n) := n - 2\varphi^2(n)$  と定義した.

次に,  $\varphi^3(n) = \varphi(\varphi^2(n))$  は一般の  $n$  について  $\varphi^2(n)$  が偶数であることから  $\varphi^2(n)$  のさらに半分ほどが限界であろう.

したがって  $\text{co}\varphi^3(n) := n - 4\varphi^3(n)$  が自然な余関数の定義である.

これらの議論から, 一般の正整数  $k$  について,  $\text{co}\varphi^k(n) := n - 2^{k-1}\varphi^k(n)$  と定義する.

以下,  $k > 2$  について考え, また便宜上  $\varphi^0(n) = n$  とする.

また,  $k$  は  $n$  に依らない定数とする.

**定理 2.1:**  $\text{co}\varphi^k(n) \leq 0$  ならば,  $\varphi^k(n) = 1$ .

*Proof:* 対偶法で証明する. つまり, まず  $\varphi^k(n) \geq 2$  と仮定する.

すると,  $\varphi(n), \varphi^2(n), \varphi^3(n), \dots, \varphi^k(n)$  はすべて 2 以上の整数である.

さて,  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$  より  $\varphi^2(n) = \varphi(n) \prod_{p|\varphi(n)} \left(1 - \frac{1}{p}\right)$  と書けた.

ここから  $\varphi^3(n) = \varphi^2(n) \prod_{p|\varphi^2(n)} \left(1 - \frac{1}{p}\right) = \varphi(n) \left\{ \prod_{p|\varphi(n)} \left(1 - \frac{1}{p}\right) \right\} \left\{ \prod_{p|\varphi^2(n)} \left(1 - \frac{1}{p}\right) \right\}$  と書ける.

この議論を繰り返すと, 一般に  $\varphi^k(n) = \varphi(n) \prod_{1 \leq j < k} \prod_{p|\varphi^j(n)} \left(1 - \frac{1}{p}\right)$  のように書ける. (これは単純な帰納法によって証明できる.)

ここで  $\varphi(n), \varphi^2(n), \dots, \varphi^k(n)$  がすべて偶数なので,  $\varphi^k(n) \leq \varphi(n) \prod_{1 \leq j < k} \left(1 - \frac{1}{2}\right) = \frac{\varphi(n)}{2^{k-1}}$ .

いま  $\varphi(n)$  は偶数なので,  $n > 2$  から  $\varphi(n) < n$  がわかる.

したがって  $\varphi^k(n) < \frac{n}{2^{k-1}}$  より,  $2^{k-1}\varphi^k(n) < n$ .

つまり,  $\text{co}\varphi^k(n) = n - 2^{k-1}\varphi^k(n) < 0$ .

証明しなかった命題の対偶が示せたので, 命題は証明された. ■

この逆は成り立たないことに注意. (例:  $n = 4, k = 2$ )

**系 2.1:**  $C$  を整数の定数とする.

$C \leq 0$  について,  $\text{co}\varphi^k(n) = C$  の唯一の解は  $n = 2^{k-1} + C$ .

*Proof:*  $\text{co}\varphi^k(n) = C \leq 0$  とすると, 先の命題より  $\varphi^k(n) = 1$ .

したがって,  $\text{co}\varphi^k(n) = n - 2^{k-1}\varphi^k(n) = n - 2^{k-1}$  より,  $n = 2^{k-1} + C$  と書ける.

次に, これが実際に  $\text{co}\varphi^k(n) = C$  の解であることを示そう.

先の命題の証明の中で,  $\varphi^k(n) \geq 2$  ならば  $2^{k-1}\varphi^k(n) < n$  を示していた.

これはつまり  $\varphi^k(n) \geq 2$  ならば  $n > 2^k$  とも言い換えることができる.

したがって, いま  $n = 2^{k-1} + C \leq 2^{k-1} \leq 2^k$  より  $\varphi^k(n) = 1$ .

よって,  $\text{co}\varphi^k(n) = n - 2^{k-1} = (2^{k-1} + C) - 2^{k-1} = C$  になっていることが確かめられた. ■

さて, 主定理の証明の前に補助関数を用意し, それについてのいくつかの補題を証明する.

**定義 2.1:**  $\bar{\varphi}^k(n) := \varphi(n) \prod_{1 \leq j < k} \prod_{p \mid \varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right)$ .

**補題 2.1:**  $n$  が合成数ならば,  $\bar{\varphi}^k(n) \leq n - \sqrt{n}$ .

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

**補題 2.2:**  $n, k$  を正整数,  $e$  を非負整数とすると,  $\varphi^k(2^e n) = 2^f \varphi^k(n)$  を満たすような非負整数  $f$  が存在する.

*Proof:*  $e = 0$  の場合は  $f = 0$  とすれば良いことは明らかであろう.

それ以外の場合を  $k$  についての帰納法で証明する.

まず,  $k = 1$  の場合について考える.

$\varphi(2^e n)$  は  $n$  が奇数のとき  $2^{e-1}\varphi(n)$ ,  $n$  が偶数のとき  $2^e\varphi(n)$  に等しい.

よって命題は  $k = 1$  の場合に成り立つ.

次に,  $k = k'$  の場合に命題が成り立つと仮定する.

すると,  $\varphi^{k'}(2^e n) = 2^f \varphi^{k'}(n)$  を満たすような非負整数  $f$  が存在する.

このとき,  $\varphi^{k'+1}(2^e n) = \varphi(\varphi^{k'}(2^e n)) = \varphi(2^f \varphi^{k'}(n))$ .

$k = 1$  の場合の命題より,  $\varphi(2^f \varphi^{k'}(n)) = 2^g \varphi(\varphi^{k'}(n)) = 2^g \varphi^{k'+1}(n)$  を満たす非負整数  $g$  が存在する.

帰納法より, 命題は示された. ■

**補題 2.3:**  $n$  が  $\varphi^{k-1}(n) > 1$  を満たす奇素数とすると,  $n - 1 = 2^e L (e > 0, L : \text{odd})$  と書ける.  
 このとき,  $\overline{\varphi}^k(n) = 2^e \overline{\varphi}^{k-1}(L)$  が成り立つ.

*Proof:*  $\varphi(n) = n - 1 = 2^e L$  であることに注意して計算すると,

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

ここで先に示した 補題 2.2 より,  $\varphi^j(2^e L)$  と  $\varphi^j(L)$  の素因数を比較すると, 違いは 2 が含まれるかどうかしかない.

$$\text{よって } \prod_{0 \leq j < k-1} \prod_{p \mid \varphi^j(2^e L), p \neq 2} \left(1 - \frac{1}{p}\right) = \prod_{0 \leq j < k-1} \prod_{p \mid \varphi^j(L), p \neq 2} \left(1 - \frac{1}{p}\right).$$

代入して続きを計算すると:

$$\overline{\varphi}^k(n) = 2^e L \prod_{0 \leq j < k-1} \prod_{p \mid \varphi^j(2^e L), p \neq 2} \left(1 - \frac{1}{p}\right) = 2^e L \left\{ \prod_{p \mid L, p \neq 2} \left(1 - \frac{1}{p}\right) \right\} \prod_{1 \leq j < k-1} \prod_{p \mid \varphi^j(2^e L), p \neq 2} \left(1 - \frac{1}{p}\right).$$

$L$  は奇数なので,  $\prod_{p \mid L, p \neq 2} \left(1 - \frac{1}{p}\right) = \prod_{p \mid L} \left(1 - \frac{1}{p}\right)$  となり, これを代入して整理すれば  $\overline{\varphi}^k(n) = 2^e \overline{\varphi}^{k-1}(L)$  が得られる. ■

**定義 2.2:** 正整数  $n$  と非負整数  $i$  について,  $R_i(n)$  を以下のように定義する.

$$R_i(n) := \begin{cases} n & \text{if } i = 0, \\ \frac{R_{i-1}(n) - 1}{2^{\nu_2(R_{i-1}(n) - 1)}} & \text{if } i > 0 \text{ and } R_{i-1}(n) > 1, \\ 0 & \text{otherwise.} \end{cases}$$

$R_i(n)$  が 1 になるまでは  $i$  について  $R_i(n)$  が狭義単調減少であることは明らかであろう.

**定義 2.3:** 正整数  $n$  と  $i$  について,  $E_i(n) := \begin{cases} \nu_2(R_{i-1}(n) - 1) & \text{if } R_{i-1}(n) > 1, \\ 0 & \text{otherwise.} \end{cases}$  と定義する.

**定義 2.4:** 正整数  $n$  について,  $R_i(n) = 1$  が成り立つ整数  $i$  を  $I(n)$  と定義する.

**補題 2.4:**  $n$  と  $i$  を正整数とし,  $i \leq I(n)$  とする.

$$\text{このとき, } n = \left\{ \sum_{1 \leq j \leq i} 2^{\sum_{1 \leq k < j} E_k(n)} \right\} + R_i(n) \cdot 2^{\sum_{1 \leq k \leq i} E_k(n)}.$$

*Proof:*  $i$  についての帰納法で示す.

$i = 1$  のとき,  $n = R_0(n)$  で,  $\frac{R_0(n)-1}{2^{E_1(n)}} = R_1(n)$  より  $n = 1 + R_1(n) \cdot 2^{E_1(n)}$ .

$i < I(n)$  のとき命題が成り立つと仮定すると,

$$\begin{aligned} n &= \left\{ \sum_{1 \leq j \leq i} 2^{\sum_{1 \leq k < j} E_k(n)} \right\} + R_i(n) \cdot 2^{\sum_{1 \leq k \leq i} E_k(n)} \\ &= \left\{ \sum_{1 \leq j \leq i} 2^{\sum_{1 \leq k < j} E_k(n)} \right\} + (1 + R_{i+1}(n) \cdot 2^{E_{i+1}(n)}) \cdot 2^{\sum_{1 \leq k \leq i} E_k(n)} \\ &= \left\{ \sum_{1 \leq j \leq i} 2^{\sum_{1 \leq k < j} E_k(n)} \right\} + 2^{\sum_{1 \leq k \leq i} E_k(n)} + R_{i+1}(n) \cdot 2^{\sum_{1 \leq k \leq i+1} E_k(n)} \\ &= \left\{ \sum_{1 \leq j \leq i+1} 2^{\sum_{1 \leq k < j} E_k(n)} \right\} + R_{i+1}(n) \cdot 2^{\sum_{1 \leq k \leq i+1} E_k(n)} \end{aligned}$$

つまり  $i+1$  のときも命題が成り立つ.

よって, 数学的帰納法より命題は示された. ■

**定理 2.2:**  $\text{co}\varphi^k(n) = C, \varphi^k(n) > 1$  が成り立っているとし,  $L = \min(I(n), k)$  とおく.

$n > C^2$  がさらに成り立つならば,  $0 \leq j < L$  の範囲のすべての整数  $j$  について  $R_j(n)$  が奇素数でなければならない.

このとき,  $C = \sum_{1 \leq j \leq L} 2^{\sum_{1 \leq k < j} E_k(n)}$  が成り立つ.

*Proof:* 定理 2.1 の対偶より,  $C \geq 1$ .

$\varphi^k(n) > 1$  より,  $\varphi(n), \varphi^2(n), \dots, \varphi^k(n)$  はすべて偶数である.

さて, 定理 2.1 での式変形より  $\varphi^k(n) = \varphi(n) \prod_{1 \leq j < k} \prod_{p \mid \varphi^j(n)} \left(1 - \frac{1}{p}\right)$ .

いま  $\varphi(n), \dots, \varphi^k(n)$  はすべて偶数なので  $2^{k-1} \varphi^k(n) = \varphi(n) \prod_{1 \leq j < k} \prod_{\varphi^j(n), p \neq 2} \left(1 - \frac{1}{p}\right) = \bar{\varphi}^k(n)$ .

$n = 1$  の場合,  $\varphi^k(n) = 1$  なのでそもそも除外する.

$n$  が合成数ならば, 補題 2.1 から  $\bar{\varphi}^k(n) \leq n - \sqrt{n}$  より,  $\text{co}\varphi^k(n) = n - \bar{\varphi}^k(n) \geq n - (n - \sqrt{n}) = \sqrt{n}$ .

したがって  $n \leq C^2$  なので, 以降  $n$  は素数とする.

特に  $\varphi(2) = 1$  なので  $n$  は奇素数である.

すると, 以下の命題 (\*) が証明できる:

$i$  を  $1 \leq i < k$  の範囲の整数とする.

$R_{i-1}(n)$  が奇素数で,  $\text{co}\varphi^k(n) = n - \bar{\varphi}^{k-i}(R_i(n)) 2^{\sum_{1 \leq j \leq i} E_j(n)}$  と表せ,  
 $n > C^2$  ならば, 以下のいずれかが成り立つ:

- $R_i(n) = 1, \text{co}\varphi^k(n) = \sum_{1 \leq j \leq i} 2^{\sum_{1 \leq k < j} E_k(n)}$
- $R_i(n) : \text{odd prime}, \text{co}\varphi^k(n) = n - \bar{\varphi}^{k-i-1}(R_{i+1}(n)) 2^{\sum_{1 \leq j \leq i+1} E_j(n)}$

命題 (\*) の証明:

$R_i(n)$  が合成数であると仮定する.

すると, 補題 2.1 より  $\bar{\varphi}^{k-i}(R_i(n)) \leq R_i(n) - \sqrt{R_i(n)}$  であるから,  $\text{co}\varphi^k(n) \geq n - 2^{\sum_{1 \leq j \leq i} E_j(n)} \{R_i(n) - \sqrt{R_i(n)}\}$ .

補題 2.4 から,  $X = \sum_{1 \leq j \leq i} 2^{\sum_{1 \leq k < j} E_k(n)}$  とおくと,  $n = X + R_i(n) \cdot 2^{\sum_{1 \leq j \leq i} E_j(n)}$ .

よって,  $\text{co}\varphi^k(n) \geq X + 2^{\sum_{1 \leq j \leq i} E_j(n)} \sqrt{R_i(n)}$ .

したがって,  $C = \text{co}\varphi^k(n) \geq X + \sqrt{2^{\sum_{1 \leq j \leq i} E_j(n)} R_i(n)} = X + \sqrt{n - X}$

$C - X \geq \sqrt{n - X}$  で, 両辺は正なので 2 乗して  $C^2 - 2CX + X^2 \geq n - X$  を得る.

$C \geq X$  から,  $C^2 - 2CX + X^2 \leq C^2 - 2X^2 + X^2 = C^2 - X^2$  より,  $C^2 - X^2 + X \geq n$ .

$X \geq 1$  なので  $C^2 \geq n$  を得る.

したがって,  $n > C^2$  ならば  $R_i(n)$  は 1 もしくは奇素数でなければならない.

$R_i(n) = 1$  の場合,  $\bar{\varphi}^{k-i}(R_i(n)) = 1$  より,  $\text{co}\varphi^k(n) = n - 2^{\sum_{1 \leq j \leq i} E_j(n)} = X$ .

$R_i(n)$  が奇素数の場合, 補題 2.3 より  $\bar{\varphi}^{k-i}(R_i(n)) = \bar{\varphi}^{k-i-1}(R_{i+1}(n)) \cdot 2^{E_{i+1}(n)}$ .

したがって,  $\text{co}\varphi^k(n) = n - \bar{\varphi}^{k-i-1}(R_{i+1}(n)) 2^{\sum_{1 \leq j \leq i+1} E_j(n)}$ .

さて, 命題 (\*) の前提条件が  $i = 1$  で成り立つことは明らかであるから,  $R_1(n)$  は 1 または奇素数.

$R_1(n)$  が奇素数の場合は命題 (\*) が  $i = 2$  でも適用できるので,  $R_2(n)$  は 1 または奇素数. (今はわかりやすさのため  $k \geq 3$  とする)

まとめると,  $k \geq 3$  の場合は

- $R_1(n) = 1$
- $R_1(n) : \text{odd prime}, R_2(n) = 1$
- $R_1(n) : \text{odd prime}, R_2(n) : \text{odd prime}$  の 3 通りに分けることができる.

このような議論を繰り返すと, 一般の  $k$  について,  $n > C^2$  が成り立つには, 次のいずれかが成り立っている必要がある:

- $I(n) < k$  で,  $0 \leq j < I(n)$  の範囲のすべての整数  $j$  について  $R_j(n)$  が奇素数.
- $I(n) \geq k$  で,  $0 \leq j < k$  の範囲のすべての整数  $j$  について  $R_j(n)$  が奇素数.

前者の場合,  $\text{co}\varphi^k(n) = \sum_{1 \leq j \leq I(n)} 2^{\sum_{1 \leq k < j} E_k(n)}$ .

後者の場合,  $\text{co}\varphi^k(n) = n - R_k(n) 2^{\sum_{1 \leq j \leq k} E_j(n)} = \sum_{1 \leq j \leq k} 2^{\sum_{1 \leq k < j} E_k(n)}$ .

これらをまとめると証明したかった命題の形になる. ■

この定理の条件「 $0 \leq j < \min(I(n), k)$  の範囲のすべての整数  $j$  について  $R_j(n)$  が奇素数」は  $n > C^2$  が成り立つための必要条件であるが, 十分条件ではないことに注意.

さて,  $n > C^2, \varphi^k(n) > 1$  が成り立つような  $n$  で,  $I(n) < k$  であるような  $n$  は少ない.

これについて考えよう.

いま, 補題 2.4 より,  $n = \sum_{1 \leq j \leq I(n)+1} 2^{\sum_{1 \leq k < j} E_k(n)}$  で,  $C = \sum_{1 \leq j \leq I(n)} 2^{\sum_{1 \leq k < j} E_k(n)}$  より,

$Y = 2^{\sum_{1 \leq k \leq I(n)} E_k(n)}$  とおくと,  $n = C + Y$  より  $n > C^2$  と  $C + Y > C^2, Y > C^2 - C$  は同値である.

そしてかなり大雑把な評価であるが、 $C^2 - C = C(C - 1) > 2^{2\sum_{1 \leq k < I(n)} E_k(n)}$  より、 $E_{I(n)}(n) > \sum_{1 \leq k < I(n)} E_k(n)$  が従う。

さて、 $n_{I(n)-1} = 2^{E_{I(n)}(n)} + 1$  はフェルマ素数であるから、ここから  $E_1(n), \dots, E_{I(n)-1}(n)$  の組み合わせ、ひいては  $n$  自体も限定される。

正確には、フェルマ素数が有限個しか存在しないと仮定したとき、 $n > C^2, \varphi^k(n) > 1, I(n) < k$  を満たす  $n$  は ( $k$  を動かしても)有限個しかないことがわかる。

特に、フェルマ素数が現在知られている  $2^{2^0} + 1, 2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, 2^{2^4} + 1$  に限られると大胆に仮定すると、条件を満たす  $n$  と  $k$  は以下のリストにあるもののみになる。

$n$	$I(n)$	$E_1(n), \dots, E_{I(n)}(n)$	range of $k$	$C$
5	1	2	[2, 2]	1
17	1	4	[2, 4]	1
257	1	8	[2, 8]	1
65537	1	16	[2, 16]	1
11	2	1, 2	[3, 3]	3
137	2	3, 4	[3, 7]	9

これら以外の  $n > C^2, \varphi^k(n)$  を満たす  $n$  については、(フェルマ素数が現在知られているのものに限ると仮定すれば)すべて  $I(n) \geq k$  である。