オイラー関数の値の評価

奥山 有人 学習院大学理学部数学科

Contents

1. 目的

本研究では,オイラー関数の値について考察していく。オイラー関数の基本事項を確認し、規則や性質について研究・証明していく。

2. オイラー関数とは？

オイラー関数とは

自然数nを与えたとき、1からnの間の数の中で、nと互いに素となる数の個数のこと .$\varphi(n)$と表す .

一般に

(1)$n = p$（pは素数)のとき
オイラー関数 $\varphi(n) = p - 1$

(2)素数でない自然数nを与えたとき
nをある素数pで割ったものをmとする。$m = n/p$
pがmを割った商が
☒自然数なら
オイラー関数$\varphi(n) = p \cdot \varphi(m)$

☒自然数でないなら
$\varphi(n) = (p - 1) \cdot \varphi(m)$

が成立 .

これを使うと、$\varphi(100)$ を求めるとき、100 は素数ではないから、一般の (2) を利用 .

素数 $p = 5$ とすると、$m = 20$
$m/p = 4$ より、自然数なので、
$\varphi(100) = 5 \cdot \varphi(20)$

$$\begin{aligned} \varphi(20) &= 4 \cdot 2 \\ &= 8 \end{aligned}$$

より

$$\begin{aligned} \varphi(100) &= 5 \cdot \varphi(20) \\ &= 5 \cdot 8 \\ &= 40 \end{aligned}$$

と求めることが出来る .

性質としては

$(1)n = p \cdot q$ のとき（ただし、p, q は互いに素な数）

$\varphi(n) = \varphi(p) \cdot \varphi(q)$
$(2)n = p^r$ のとき $(r$ は自然数$)$

$\varphi(n) = p^r - p^{r-1}$

$(3)n = p^{s_1} \cdot q^{s_2} \cdot ... \cdot r^{s_r}$ のとき（$p, q, .., r$ は、相異なる素数、$s_1, s_2, .., s_r$ は、自然数）
$\varphi(n) = (p^{s_1} - p^{s_1-1}) \cdot (q^{s_2} - q^{s_2-1}) \cdot ... \cdot (r^{s_r} - r^{s_r-1})$

が成立する．

3. 証明

3.1. その1. オイラー関数の値は、偶数であることの証明$(n \geq 3)$

$(1) n = p$のとき$(p \geq 3$の素数$)$
$\varphi(n) = p - 1$で、pは素数なので、$\varphi(n)$は偶数。
$(2) n = p^{s_1} \cdot q^{s_2} \cdot \ldots \cdot r^{s_r}$のとき（$p, q, .., r$は、相異なる素数、$s_1, s_2, .., s_r$は、自然数）
$\varphi(n) = (p^{s_1} - p^{s_1 - 1}) \cdot (q^{s_2} - q^{s_2 - 1}) \cdot \ldots \cdot (r^{s_r} - r^{s_r - 1})$で、$p, q, .., r$は、すべて素数であることから、
$p^m (m$は自然数$)$は、すべて奇数となるので、$p^m - p^{m-1}$は、偶数になる。
よって、$n = p^{s_1} \cdot q^{s_2} \cdot \ldots \cdot r^{s_r}$のとき$\varphi(n)$は偶数になる。

結果

すべての$n(n \geq 3)$において、$\varphi(n)$は偶数。（ちなみに$n = 2$のとき、$\varphi(n) = 1$）

3.2. **その2.** オイラー関数の値として表れない値がある。なぜ表れないかを証明をしていく
出てこないオイラー関数$\cdots 14, 26, 34, 38, 50, .., 1402, ..,$

(a)オイラー関数$\varphi(N) = 14$が存在しないことを示す .

(1)$N = p$（pは素数）とすると、

$$\begin{aligned}\varphi(N) &= \varphi(p)\\ &= p - 1\\ &= 14.\end{aligned}$$

よって　$p = 15$　となり、pが素数であることに矛盾

(2)$N = p^2$のとき

$$\begin{aligned}\varphi(N) &= \varphi(p^2) \\ &= p^2 - p \\ &= p(p-1) \\ &= 14\end{aligned}$$

pは素数より、$(p, p-1) = (7, 2)$が考えられるが、明らかに不適

(3)$N = p \cdot q$のとき(qはpとは異なる素数)

$$\begin{aligned}\varphi(N) &= \varphi(p \cdot q) \\ &= \varphi(p) \cdot \varphi(q) \\ &= (p-1) \cdot (q-1) \\ &= 14.\end{aligned}$$

p, qは素数で、$p-1, q-1$は偶数であることから、明らかに不適。

以上から$\varphi(N) = 14$を満たすNは存在しない。

3.3. その3. $N-\varphi(N)-\sqrt{N}\geq 0$を示す。ただし、$N$は素数ではない

$N=p_1\cdot p_2\cdots p_r(2\leq p_1<p_2<\cdots<p_r)(r\geq 2)$とする。

$\varphi(N)=(p_1-1)\cdot(p_2-1)\cdots(p_r-1)$
$\sqrt{p_1}=a_1,\cdots,\sqrt{p_r}=a_r$とすると
$N=a_1^2\cdot a_2^2\cdots a_r^2$より

$\varphi(N)=(a_1^2-1)\cdot(a_2^2-1)\cdots(a_r^2-1)$となり、
$\sqrt{N}=a_1\cdots a_r(a_1>1,r\geq 2)$　とすると、
与式は

$$a_1^2\cdots a_r^2-(a_1^2-1)\cdots(a_r^2-1)-a_1\cdot a_2\cdots a_r\geq 0$$

を証明することと同値である。

ここから以下の証明をする。

(1)$r = 2$のときが成立すること

(2)$r \geq 3$のとき、$r-1$で、与式が成立すると仮定して数学的帰納法より、
$N = p_1 \cdot p_2 \cdots p_r (2 \leq p_1 < p_2 < \cdots < p_r)$で成立すること。

(3)$N = p_1^{e_1} \cdot p_2^{e_2} \cdots \cdot p_r^{e_r}$のとき成立すること。

(4)素数では、与式が成立しないこと。
以上のことを証明する。

結果

素数を除く数Nにおいて、$N - \varphi(N) - \sqrt{N} \geq 0$が成立する。

3.4. その4. $g(N) = N - \varphi(N) - \sqrt{N} - 4 > 0$となる$N$について示す

以下のことを考える。
(ただしpは素数、mは自然数)

(0)$N = p$のとき
(1)$N = p^2$のとき
(2)$N = 2^m$のとき$(m \geq 5)$
(3)$N = 3^m$のとき$(m \geq 4)$
(4)$N = 2 \cdot p$のとき$(p \geq 7\ )$
(5)$N = 3 \cdot p$のとき$(p \geq 7\ )$
(6)$N = 5 \cdot p$のとき$(p \geq 7\ )$
以上(0)〜(6)より

結果

$g(N) = N - \varphi(N) - \sqrt{N} - 4 > 0$が成立する。
(ただし$N = p, p^2, 6, 8, 10, 15, 16, 27$は除く。$p$は素数)