オイラー関数 $\phi(n)$

1　$\phi(n)$ の定義

自然数 n に対して，n と互いに素である (n との最大公約数が 1 である)1 以上 n 以下の自然数の個数を $\phi(n)$ と表し，これをオイラーのトーシェント関数 (Euler's totient function) と呼んでいる．これは慣例的にギリシャ文字のファイ ϕ（あるいは φ）で表記されるため，オイラーの ϕ 関数 (phi function)，略して**オイラー関数**とも呼ばれている．

例えば，$\phi(6)$ については，1, 2, 3, 4, 5, 6 のうち 6 と互いに素な自然数 x は 1, 5 の 2 個であるから

$$\phi(6) = 2 \quad (x = 1,\ 5)$$

である．その他の自然数 n の $\phi(n)$ の値をいつくか並べてみると

$$\begin{aligned}
&\phi(1) = 1 \quad (x = 1)\\
&\phi(2) = 1 \quad (x = 1)\\
&\phi(3) = 2 \quad (x = 1,\ 2)\\
&\phi(4) = 2 \quad (x = 1,\ 3)\\
&\phi(5) = 4 \quad (x = 1,\ 2,\ 3,\ 4)\\
&\phi(7) = 6 \quad (x = 1,\ 2,\ 3,\ 4,\ 5,\ 6)\\
&\qquad \cdots
\end{aligned}$$

である．

2　$\phi(n)$ の基本性質

定理 1

p を素数とする．

(1) $\phi(p) = p - 1$

(2) $\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \dfrac{1}{p}\right)$　(a は自然数)

【証明】(1) p は素数であるから，1 以上 p 以下の自然数のうち p と互いに素である自然数は

$$1,\ 2,\ 3,\ \cdots,\ p-1$$

の $p-1$ 個である．よって

$$\phi(p) = p - 1$$

……(証明終わり)

(2) p は素数であるから，p^a と互いに素でない自然数，すなわち p の倍数である自然数は kp とかくことができる．したがって，1 以上 p^a 以下の自然数のうち p^a と互いに素でない自然数は

$$1\cdot p,\ \ 2\cdot p,\ \ 3\cdot p,\ \ \cdots,\ \ p^{a-1}\cdot p$$

の p^{a-1} 個である．よって

$$\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$$

……(証明終わり)

補助定理

(1) $a,\ b,\ c$ を自然数とするとき

「c と ab が互いに素である」

$\Longleftrightarrow$

「c と a が互いに素であり，かつ c と b が互いに素である」

(2) $s,\ t,\ b$ を自然数とするとき

「$s+tb$ と b が互いに素である」

$\Longleftrightarrow$

「s と b が互いに素である」

【証明】(1) $\Longrightarrow$ の証明) 背理法を用いる．

「c と a が互いに素でない，または c と a が互いに素でない」と仮定する．

c と a が互いに素でないとすると

$$c = pc' \text{ かつ } a = pa' \quad (p \text{ は素数},\ c',\ a' \text{は整数})$$

と表すことができる．これは c と ab が互いに素であることに反する．

同じく，c と b が互いに素でないときも矛盾が生じる．

$\Longleftarrow$ の証明) 背理法を用いる．

「c と ab が互いに素でない」と仮定すると

$$c = pc' \text{ かつ } ab = pq \quad (p \text{ は素数},\ c',\ q \text{ は整数})$$

と表すことができる．p は素数なので $a,\ b$ の少なくとも一方は p を因数にもつ．これは「c と a が互いに素であり，かつ c と b が互いに素である」ことに反する．

(2) $\Longrightarrow$ の証明) 背理法を用いる．

「s と b が互いに素でない」と仮定すると

$$s = ps' \text{ かつ } b = pb' \quad (p \text{ は素数},\ s',\ b' \text{は整数})$$

と表すことができる．このとき

$$s + tb = p(s' + tb')$$

となり「$s+tb$ と b が互いに素である」ことに反する．

$\Longleftarrow$ の証明) 背理法を用いる．

「$s+tb$ と b が互いに素でない」と仮定すると

$$s + tb = pl \text{ かつ } b = pb' \quad (p \text{ は素数},\ l,\ b' \text{は整数})$$

と表すことができる．このとき

$$s = pl - t(pl') = p(l - tl')$$

となり，「s と b が互いに素である」ことに反する．

定理 2

$m,\ n$ が互いに素ならば

$$\phi(mn) = \phi(m)\phi(n)$$

が成り立つ．

【証明】補助定理 (1) より，1 以上 mn 以下の互いに素な自然数は，

m と互いに素 かつ n と互いに素な自然数

である．1 以上 mn 以下の自然数を下のように並べる．

$$\begin{array}{cccccc}
1 & 2 & \cdots & \boxed{s} & \cdots & n-1 & n \\
1+n & 2+n & \cdots & s+n & \cdots & (n-1)+n & 2n \\
1+2n & 2+2n & \cdots & s+2n & \cdots & (n-1)+2n & 3n \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
1+(m-1)n & 2+(m-1)n & \cdots & s+(m-1)n & \cdots & (n-1)+(m-1)n & mn
\end{array}$$

補助定理 (2) より，n と互いに素な数は，n と互いに素な s に対して，s を含む縦の列の数すべてに限る．このような列は $\phi(n)$ 個ある．

任意の自然数 s を固定するごとに

$$s,\ s+n,\ s+2n,\ \cdots,\ s+(m-1)n$$

の m 個の数を m で割った余りは，すべて異なり (順序を無視して) 0 から $m-1$ までの数がすべて現れる．すなわち，上の数の並びの各列の中には m と互いに素な数がちょうど $\phi(m)$ 個ある．

したがって，n と互いに素かつ m と互いに素な数は $\phi(m)\phi(n)$ 個ある．

よって

$$\phi(mn) = \phi(m)\phi(n) \qquad \cdots\cdots (\text{証明終わり})$$

【例題】 定理 2 の証明を 36 という具体例で振り返ってみておく．

証明のように 1 から 36 まですべてを書き並べると

①	2	3	4	⑤	6	⑦	8	9
10	⑪	12	⑬	14	15	16	⑰	18
⑲	20	21	22	㉓	24	㉕	26	27
28	㉙	30	㉛	32	33	34	㉟	36

$36 = 2^2 \cdot 3^2$ であり，$3^2 = 9$ と互いに素な数は 1, 2, 4, 5, 7, 8 を含む縦の列は $\phi(9) = 6$ 個ある．

各縦の列の 4 個の数を 4 で割った余りはすべて異なり 0, 1, 2, 3 であるから，各列の中に 4 と互いに素な数は $\phi(4) = 2$ 個ある．したがって

$$2 \times 6 = 12$$

- 定理 2，定理 1 を認めるならば

$$\phi(36) = \phi(2^2 \cdot 3^2) = \phi(2^2)\phi(3^2) = (2^2-2)(3^2-3) = 2 \cdot 6 = 12$$

- 入試の解答では，定理 2，定理 1 をそのまま使うわけにはいかない．使うならば証明してから使うべきである (穴埋め問題なら裏技として使う)．

  $\phi(36)$ ならば，1 から $36 = 2^2 \cdot 3^2$ までの自然数のうちで 2 の倍数の集合を A，3 の倍数の集合を B とし，集合 X の要素の個数を $n(X)$ とすると，36 と互いに素でない数の個数 $n(A \cup B)$ は

$$\begin{aligned} n(A \cup B) &= n(A) + n(B) - n(A \cap B) \\ &= \frac{36}{2} + \frac{36}{3} - \frac{36}{2 \cdot 3} = 18 + 12 - 6 = 24 \end{aligned}$$

  であるから

$$\phi(36) = 36 - 24 = 12$$

  である．

定理 3

$p,\ q, \cdots,\ r$ は異なる素数，$a,\ b, \cdots,\ c$ は自然数とする．

(1) $\phi(pq\cdots r) = (p-1)(q-1)\cdots(r-1)$

(2) $\phi(p^a q^b \cdots r^c) = p^a q^b \cdots r^c \left(1-\dfrac{1}{p}\right)\left(1-\dfrac{1}{q}\right)\cdots\left(1-\dfrac{1}{r}\right)$

【証明】定理 2，定理 1 を用いる．

(1) $p,\ q,\ \cdots,\ r$ は素数であり，どれも互いに素であるから

$$\begin{aligned}\phi(pq\cdots r) &= \phi(p)\phi(q)\cdots\phi(r) \quad (\because \text{ 定理 2})\\ &= (p-1)(q-1)\cdots(r-1) \quad (\because \text{ 定理 1(1)})\end{aligned}$$

……(証明終わり)

(2) $p^a,\ q^b,\ \cdots,\ r^c$ は素数であり，どれも互いに素であるから

$$\begin{aligned}\phi(p^a q^b \cdots r^c) &= \phi(p^a)\phi(q^b)\cdots\phi(r^c) \quad (\because \text{ 定理 2})\\ &= p^a\left(1-\frac{1}{p}\right)\cdot q^b\left(1-\frac{1}{q}\right)\cdot\cdots\cdot r^c\left(1-\frac{1}{r}\right) \quad (\because \text{ 定理 1(2)})\\ &= p^a q^b \cdots r^c\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\cdots\left(1-\frac{1}{r}\right)\end{aligned}$$

……(証明終わり)