$Ba - C\varphi(a) = 0$ の解について

梶田 光

2019 年 12 月 12 日

1　オイラー関数

初めに, オイラーのトーシェント関数 (またはオイラー関数)$\varphi(a)$ を次のように定義する.

定義 1. $\varphi(a) = \sum_{1 \leq k \leq a, \gcd(a,k)=1} 1$

つまり, $\varphi(a)$ とは 1 から a までの自然数のうち, a と互いに素である自然数の個数である.
例えば, 1 から 6 までの自然数の中で 6 と互いに素なものは 2 個 (1 と 5) なので $\varphi(6) = 2$ となる.

命題 1. p が素数 $\iff \varphi(p) = p - 1$

Proof. p は素数なので, 1 から $p - 1$ までの自然数はすべて p と互いに素である.
よって $\varphi(p) = p - 1$.
次に逆を示す.
$p = 1$ とすると 1 と 1 は互いに素なので $\varphi(1) = 1$, つまり $\varphi(p) \neq p - 1$ であるから $p \neq 1$ である.
したがって p と p は互いに素でないので 1 から $p - 1$ までのすべての自然数が p と互いに素でなければならない.
素数の定義より p は素数である.

命題 2 (乗法性)**.** a と b が互いに素 $\implies \varphi(ab) = \varphi(a)\varphi(b)$

これは中国剰余定理から証明できる.

命題 3. $p \in \text{prime}, k > 0 \implies \varphi(p^k) = p^{k-1}(p - 1)$

Proof. p は素数なので p^k 以下で p^k と互いに素でない自然数は $p, 2p, 3p, ..., p^{k-1}p$ しかない.
よって p^k と互いに素でない自然数は p^{k-1} 個あり, 他のすべての自然数は p^k と互いに素であるから
$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$ となる.

命題 2 と命題 3 から次の公式が得られる:

命題 4. $a = p_1^{e_1} p_2^{e_2} ... p_n^{e_n} (\forall i \ \ p_i \in \text{prime}, e_i \in \text{prime})$ とおく.
このとき $\varphi(a) = \prod_{i=1}^{n} p_i^{e_i - 1}(p_i - 1) = p_1^{e_1 - 1} p_2^{e_2 - 1} ... p_n^{e_n - 1}(p_1 - 1)(p_2 - 1)...(p_n - 1)$ である.

Proof. $\varphi(a)$
$= \varphi(p_1^{e_1} p_2^{e_2} ... p_n^{e_n})$
$= \varphi(p_1^{e_1})\varphi(p_2^{e_2})...\varphi(p_n^{e_n}) = \prod_{i=1}^{n} p_i^{e_i - 1}(p_i - 1) = p_1^{e_1 - 1} p_2^{e_2 - 1} ... p_n^{e_n - 1}(p_1 - 1)(p_2 - 1)...(p_n - 1)$

命題 5. $a \neq 1, 2$ のとき, $\varphi(a)$ は偶数である.

Proof. a 以下で a と互いに素な自然数のうち 1 つを d とおく.
$\gcd(a, d) = 1$ なので $a \neq 1, 2$, つまり $a > 2$ より $\gcd(a, a - d)$ も 1 となる.
同様にすべての d に対して d でない a 以下で a と互いに素な自然数を対応させることができる.
ゆえに $\varphi(a)$ は偶数となる.

命題 6. $a = \varphi(a) \Longleftrightarrow a = 1$

Proof. 定義より, $\varphi(a)$ は a 以下の自然数の中で a と互いに素である自然数の個数である.
しかし $a = \varphi(a)$ より, a 以下のすべての自然数が a と互いに素でなければならない.
つまり a と a は互いに素であるがこれを満たす a は 1 のみである.
次に逆を示す.
$\varphi(1) = 1$ であるから $a = \varphi(a) \Longleftrightarrow a = 1$ が証明された.

2 オイラー関数の一次関係式

2.1 係数が 1 の場合

注意 1. a が偶数のとき $a = 2^e L(e > 0, L : \text{odd})$ と書ける.

例えば 60 は偶数なので 2 で割れて $60 = 2^1 \cdot 30$ と書ける.
また 30 も偶数なので 2 で割れて $60 = 2^1 \cdot 2 \cdot 15 = 2^2 \cdot 15$ となる.
このように繰り返し 2 で割ることで偶数を 2 べき部分と奇数に分けることができる.
a が 2 のべき, 例えば 8 の場合では $\to 2 \cdot 4 \to 2^2 \cdot 2 \to 2^3 \cdot 1$ と奇数部分 L が 1 となる.
また一般に a が d の倍数であるとき $a = d^e L(e > 0, d \not| L)$ と書ける.

定理 1. $a = 2\varphi(a)$ が成り立つことと $a = 2^e (e > 0)$ と書けることは同値である.

Proof. $\varphi(a)$ は自然数なので a は偶数, よって $a = 2^e L(e > 0, L : \text{odd})$ と書ける.
これを $a = 2\varphi(a)$, つまり $a - 2\varphi(a) = 0$ に代入すると
$2^e L - 2 \cdot \varphi(2^e L) = 0$
ここで L は奇数であるから 2^e と L は互いに素である.

よって $\varphi(2^eL)=\varphi(2^e)\varphi(L)$ となる.
また命題 3 から $\varphi(2^e)=2^{e-1}(2-1)=2^{e-1}$ であるから $\varphi(2^eL)=2^{e-1}\varphi(L)$ となる.
したがって $2^eL-2\cdot 2^{e-1}\varphi(L)=0$ である.
ここで $2\cdot 2^{e-1}=2^e$ なので $2^eL-2^e\varphi(L)=0$ となる.
これを 2^e でくくると $2^e\{L-\varphi(L)\}=0$
$2^e>0$ より $L-\varphi(L)=0$ である.
命題 6 から $L=1$ となる.
したがって $a=2^e(e>0)$ と書ける.
次に逆を示す.
$a=2^e$ のとき $\varphi(a)=2^{e-1}(2-1)=2^{e-1}$.
よって $2\varphi(a)=2^e$, したがって $a=2\varphi(a)$ が成り立つ.

定理 2. $a=3\varphi(a)$ が成り立つことと $a=2^f3^e(e>0,f>0)$ と書けることは同値である.

Proof. $\varphi(a)$ は自然数なので a は 3 の倍数となるから $a=3^eL(e>0,3\not|L)$ と書ける.
これを $a=3\varphi(a)$, つまり $a-3\varphi(a)=0$ に代入すると
$3^eL-3\cdot\varphi(3^eL)=0$
ここで L は 3 の倍数でないから 3^e と L は互いに素である.
よって $\varphi(3^eL)=\varphi(3^e)\varphi(L)$ となる.
また命題 3 から $\varphi(3^e)=3^{e-1}(3-1)=2\cdot 3^{e-1}$ であるから $\varphi(3^eL)=2\cdot 3^{e-1}\varphi(L)$ となる.
したがって $3^eL-3\cdot 2\cdot 3^{e-1}\varphi(L)=0$ である
ここで $3\cdot 3^{e-1}=3^e$ なので $3^eL-2\cdot 3^e\varphi(L)=0$ となる.
これを 3^e でくくると $3^e\{L-2\varphi(L)\}=0$
$3^e>0$ より $L-2\varphi(L)=0$ である.
命題 1 から $L=2^f(f>0)$ と書ける.
したがって $a=2^f3^e(e>0,f>0)$ と書ける.
次に逆を示す.
$a=2^f3^e$ のとき $\varphi(a)=2^{f-1}\cdot 2\cdot 3^{e-1}=2^f3^{e-1}$.
よって $3\varphi(a)=2^f3^e$, したがって $a=3\varphi(a)$ が成り立つ.

$a-2\varphi(a)=0$, $a-3\varphi(a)=0$ の解はとても多いのだが, $a-4\varphi(a)=0$ の解などは出てこない.
$a-4\varphi(a)=0$ や $a-5\varphi(a)=0$, 一般に $a-C\varphi(a)=0(C\in\mathbb{N},C>3)$ の解は存在しないことが証明できる.

定理 3. $a-C\varphi(a)=0(C\in\mathbb{N},C>3)$ の解は存在しない.

Proof. (1) C : even の場合
a は偶数なので $a=2^eL(e>0,L:\text{odd})$ と書ける.
これを $a-C\varphi(a)=0$ に代入すると,
$2^eL-C\cdot\varphi(2^eL)=0$
ここで L は奇数であるから, 2^e と L は互いに素である.
したがって $\varphi(2^eL)=\varphi(2^e)\varphi(L)$
また $\varphi(2^e)=2^{e-1}$ であるから $\varphi(2^eL)=2^{e-1}\varphi(L)$ となる.

よって

$2^eL - C \cdot 2^{e-1}\varphi(L) = 0$

$2^{e-1}\{2L - C\varphi(L)\} = 0$

$2^{e-1} > 0$ より,$2L - C\varphi(L) = 0$, つまり $L = \dfrac{C}{2}\varphi(L)$ となる.

また C : even なので $\dfrac{C}{2}$ は自然数である.

ここで $L \neq 1$ とすると,$\varphi(L)$ は偶数であるから $\dfrac{C}{2}\varphi(L)$ は偶数となる.

しかしこれは L : odd に矛盾.

よって $L = 1$ となる.

これを $2L - C\varphi(L) = 0$ に代入すると $2 - C = 0$, つまり $C = 2$ となるがこれは $C > 3$ に矛盾.

(2) C : odd の場合

$C \neq 1$ なので $C = pD(p \in \text{prime}, p : \text{odd}, D : \text{odd})$ と書ける.

これを $a - C\varphi(a) = 0$ に代入すると $a - pD\varphi(a) = 0$ となる.

よって a は p の倍数であるから $a = p^eL(e > 0, p \not| L)$ と書ける.

これを $a - pD\varphi(a) = 0$ に代入すると

$p^eL - pD \cdot \varphi(p^eL) = 0$　　ここで $p \not| L$ であるから, p^e と L は互いに素である.

したがって $\varphi(p^eL) = \varphi(p^e)\varphi(L)$

また $\varphi(p^e) = p^{e-1}(p-1)$ であるから $\varphi(p^eL) = p^{e-1}\varphi(L)$ となる.

よって

$p^eL - pD \cdot p^{e-1}(p-1)\varphi(L) = 0$

$p^e\{L - D(p-1)\varphi(L)\} = 0$

$p^e > 0$ より $L - D(p-1)\varphi(L) = 0$ である.

p : odd なので $p-1$ は偶数, よって $D(p-1)$ も偶数となる.

ここで $D(p-1) > 3$ とすると前述のように解は存在しない.

よって $D(p-1) \leq 3$, つまり $D = 1, p = 3$ となる.

したがって $C = 3$ となるがこれは $C > 3$ に矛盾.

以上より $a - C\varphi(a) = 0(C > 3, C \in \mathbb{N})$ の解は存在しない.

また, 次のことが言える.

定理 4. $Ba - C\varphi(a) = 0(B : \text{odd}, \gcd(B, C) = 1, B > 1, C > 1)$ の解が存在するときある奇素数 p を用いて $B = \dfrac{p-1}{2}$, $C = p$ と書ける.

Proof. $\gcd(B, C) = 1$ より $B \neq C$ なので $a \neq 1$ となり $\varphi(a)$ は偶数である.

よって a は偶数であるから $a = 2^eL(e > 0, L : \text{odd})$ と書ける.

これを $Ba - C\varphi(a) = 0$ に代入すると

$B \cdot 2^eL - C \cdot 2^{e-1}\varphi(L) = 0$

$2^{e-1}\{2BL - C\varphi(L)\} = 0$

$2^{e-1} > 0$ より $2BL - C\varphi(L) = 0$ となる.

(1) C : even の場合

$2BL - C\varphi(L) = 0$ は $L = \dfrac{C}{2}\dfrac{\varphi(L)}{B}$ と書ける.

C は偶数なので $\dfrac{C}{2}$ は自然数である.

$\gcd(B,C)=1$ より解が存在するためには $\dfrac{\varphi(L)}{B}$ は自然数でなければならない.

しかし $L\neq 1$ なので $\varphi(L)$ は偶数,B は自然数なので $\dfrac{\varphi(L)}{B}$ は偶数となる.

したがって $\dfrac{C}{2}\dfrac{\varphi(L)}{B}$ は偶数, つまり L は偶数となるがこれは $L:\text{odd}$ に矛盾.

(2) $C:\text{odd}$ の場合

B,L,C はすべて奇数であるので $\varphi(L)$ の 2 べき部分は 2^1 となる.

$L=p_1^{e_1}p_2^{e_2}...p_n^{e_n}(\forall i\ p_i\in\text{prime},p_i:\text{odd},e_i>0)$ とおくと

$\varphi(L)=p_1^{e_1-1}p_2^{e_2-1}...p_n^{e_n-1}(p_1-1)(p_2-1)...(p_n-1)$ である.

ここで $p_1-1,p_2-1,...,p_n-1$ はすべて偶数であるが $\varphi(L)$ の 2 べき部分は 2^1 なので

L の素因子はただ 1 つとなる.

よって $L=p^{\varepsilon}(\varepsilon>0,p\in\text{prime},p:\text{odd})$ と書けてこれを $2BL-C\varphi(L)=0$ に代入すると

$2B\cdot p^{\varepsilon}-C\cdot p^{\varepsilon-1}(p-1)=0$

$p^{\varepsilon-1}\{2Bp-C(p-1)\}=0$

$p^{\varepsilon-1}>0$ より $2Bp-C(p-1)=0$, つまり $Bp=C\dfrac{p-1}{2}$ である.

C は p の倍数であるから $C=p\lambda(\lambda:\text{odd},\gcd(B,\lambda)=1)$ とおくと $B=\lambda\dfrac{p-1}{2}$ となる.

しかし $\gcd(B,\lambda)=1$ となるから $\lambda=1$ となって $C=p,B=\dfrac{p-1}{2}$ である.

このとき $L=p^{\varepsilon}$ なので $a=2^ep^{\varepsilon}(e>0,\varepsilon>0)$ と書ける.

B が素数のときは B はソフィー・ジェルマン素数となる.