オイラー余関数の逆関数について

梶田 光

2020 年 1 月 12 日

$\mathrm{co}\varphi(a) = 2^e (e > 0)$ の表を以下に示す.

a	pfac.
$e = 1$	
4	2^2
$e = 2$	
8	2^3
6	$2 \cdot 3$
$e = 3$	
16	2^4
12	$2^2 \cdot 3$
14	$2 \cdot 7$
$e = 4$	
32	2^5
24	$2^3 \cdot 3$
28	$2^2 \cdot 7$
$e = 5$	
64	2^6
48	$2^4 \cdot 3$
56	$2^3 \cdot 7$
62	$2 \cdot 31$

表 1

定理 1. $\mathrm{co}\varphi(a) = 2^e (e > 0)$ の解は $a = 2^{e+1}$ と $a = 2^\varepsilon p (p = 2^{e-\varepsilon+1} - 1, p \in \mathrm{prime})$ と書ける.

Proof. $a = 1$ とすると $\mathrm{co}\varphi(a) = 0$ より $2^e > 0$ に矛盾.
また $a = 2$ とすると $\mathrm{co}\varphi(a) = 1$ より $e > 0$ に矛盾.
したがって $a \neq 1, 2$ より $\varphi(a) : \mathrm{even}$ となる.
よって $a : \mathrm{even}$ であるから $a = 2^\varepsilon L (\varepsilon > 0, L : \mathrm{odd})$ と書ける.

これを $\mathrm{co}\varphi(a) = 2^e$ に代入すると

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

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

$2L - \varphi(L) = 2^{e-\varepsilon+1}$

$L = 1$ とすると $2 - 1 = 2^{e-\varepsilon+1}$ より $2^e = 2^{\varepsilon-1}$ である.

したがって $e = \varepsilon - 1$, つまり $\varepsilon = e + 1$ となるので $a = 2^{e+1}$ と書ける.

つぎに $L \neq 1$ の場合を考える.

$L > 1$ より L は少なくとも 1 つの素因数を持っているので

$L = p^f M(p : \mathrm{odd\,prime}, f > 0, M : \mathrm{odd}, p \not| M)$ と書ける.

これを $2L - \varphi(L) = 2^{e-\varepsilon+1}$ に代入すると

$2 \cdot p^f M - p^{f-1}(p-1)\varphi(M) = 2^{e-\varepsilon+1}$

$p^{f-1}\{2pM - (p-1)\varphi(M)\} = 2^{e-\varepsilon+1}$ $\gcd(p, 2) = 1$ より $p^{f-1} = 1$, つまり $f = 1$ となる.

よって $2pM - (p-1)\varphi(M) = 2^{e-\varepsilon+1}$

$pM - \dfrac{p-1}{2}\varphi(M) = 2^{e-\varepsilon}$ である.

(1) $\dfrac{p-1}{2}\varphi(M) : \mathrm{even}$ の場合

$pM : \mathrm{odd}$ より $2^{e-\varepsilon} = 1$ となるから $e = \varepsilon$ である.

したがって $pM - \dfrac{p-1}{2}\varphi(M) = 1$ となる.

(i) $M = 1$ の場合

$p - \dfrac{p-1}{2} = 1$ より $p + 1 = 2$, つまり $p = 1$ となるがこれは $p \in \mathrm{prime}$ に矛盾.

(ii) $M > 1$ の場合

このとき $M - \varphi(M) \geq 1$ である.

$M - \varphi(M) > 1$ とすると $\varphi(M) < M - 1$ となる.

これを $pM - \dfrac{p-1}{2}\varphi(M) = 1$ に代入すると

$pM - \dfrac{p-1}{2}(M-1) < 1$

$pM - \dfrac{p-1}{2}M + \dfrac{p-1}{2} < 1$

$M\dfrac{p+1}{2} + \dfrac{p-1}{2} < 1$

ここで $M\dfrac{p+1}{2} > 1, \dfrac{p-1}{2} \geq 1$ となるがこれは $M\dfrac{p+1}{2} + \dfrac{p-1}{2} < 1$ に矛盾.

よって $M - \varphi(M) = 1$, つまり $M \in \mathrm{prime}$ である.

同様に変形すると $M\dfrac{p+1}{2} + \dfrac{p-1}{2} = 1$ となるがこれは $M\dfrac{p+1}{2} > 1, \dfrac{p-1}{2} \geq 1$ に矛盾.

(2) $\dfrac{p-1}{2}\varphi(M) : \mathrm{odd}$ の場合

$\varphi(M) : \mathrm{odd}, M : \mathrm{odd}$ より $M = 1$ である.

よって $p - \dfrac{p-1}{2} = 2^{e-\varepsilon}$, つまり $p = 2^{e-\varepsilon+1} - 1$ となる.

以上より $\mathrm{co}\varphi(a) = 2^e (e > 0)$ の解は $a = 2^{e+1}$ と $a = 2^{\varepsilon}p(p = 2^{e-\varepsilon+1} - 1, p \in \mathrm{prime})$ と書けることが示された. □