数学の研究を始めよう (9)
オイラー関数による特徴付け

飯高 茂

平成 25 年 12 月 30 日

1　オイラー関数

自然数 $a>1$ に対して $1<b<a$ を満たし, a と互いに素な自然数 b の個数を $\varphi(a)$ と書き, これを自然数 a の関数とみて**オイラー関数**という. ただし $\varphi(1)=1$ とする.

オイラー関数 $\varphi(a)$ の性質 ($a>1$) をふたたび列挙してみよう.

⟨1⟩ $a-1\geq\varphi(a)$,

⟨2⟩ a が素数なら $\varphi(a)=a-1$. さらに $\varphi(a)=a-1$ なら a は素数 ,

⟨3⟩ a が素数でないなら $a\geq\varphi(a)+\sqrt{a}$,

⟨4⟩ a,b が互いに素なら $\varphi(ab)=\varphi(a)\varphi(b)$ (乗法性).

オイラー関数 $\varphi(a)$ を中学生に説明するなら 分母が a の既約な真分数の個数を $\varphi(a)$ と書く, と言えばよい.

1.1　オイラーの公式

一般に自然数が分母, 分子の真分数 $\frac{b}{a}$ があるとき a,b の最大公約数 d をとれば $a=da',b=db'$ とかけて $\frac{b'}{a'}$ は既約な真分数になる. 分母が a' の既約な真分数の個数は $\varphi(a')$ と書ける.

したがって分母が a の真分数の個数は a 個ありこれら真分数は分母が a の約数 a' の既約な真分数の全体として表せる. よってこれら a' の $\varphi(a')$ の和が a になる. すなわち

$$a=\sum_{a'|a}\varphi(a') \tag{1}$$

となる. ここに $a'|a$ は a' が a の約数を意味する. これを**オイラーの公式**という.

たとえば $a=12$ とおくと,$a'=12,6,4,3,2,1$ であり,

$$\varphi(12)=4,\varphi(6)=2,\varphi(4)=2,\varphi(3)=2,\varphi(2)=1,\varphi(1)=1.$$

これらを加えると $4+2+2+2+1+1=12$ となって分母が出て来る.

この公式を使うと, オイラー関数 $\varphi(a)$ の値が楽に計算できる.

a が素数 $p>1$ なら p の約数は $p,1$ なので $p=\varphi(p)+\varphi(1)=\varphi(p)+1$ により $\varphi(p)=p-1$. (これは当たり前の結果ではあるが)

a が素数の平方 p^2 なら約数は $p^2, p, 1$ なので $p^2 = \varphi(p^2) + \varphi(p) + 1 = \varphi(p) + (p-1) + 1$ により $\varphi(p^2) = p^2 - p = p(p-1)$.

同様にして $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ が示される.

p, q を相異なる素数とすると pq の約数は $pq, q, p, 1$ なので $pq = \varphi(pq) + \varphi(q) + \varphi(p) + 1 = \varphi(pq) + (q-1) + (p-1) + 1$ により $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

1.2 乗法性

a, b を互いに素な自然数とするとき, $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これがオイラー関数の乗法性である.

2 2のべきの場合

a が 2 のべきの場合, すなわちある自然数 ε によって $a = 2^\varepsilon$ と書けるとしよう.

$\varphi(a) = \varphi(2^\varepsilon) = 2^{\varepsilon-1} = a/2$ なので次のオイラー関数の関係式が得られた.

$$2\varphi(a) = a$$

この式を a について解く. a は偶数なので $a = 2^e L, e > 0, L$ は奇数, とおく.

$$2\varphi(a) = 2\varphi(2^e L) = 2\varphi(2^e)\varphi(L) = 2^e\varphi(L) = a = 2^e L.$$

ゆえに $\varphi(L) = L$ を得るので $L = 1$. したがって $a = 2^e$.

かくして次の結果をえた.

定理 1 $a = 2e$ $(e > 0)$ とかける必要十分条件は $2\varphi(a) = a$.

約数の和関数では $a = 2^e$ とおくと

$$\sigma(a) = \sigma(2^e) = 2^{e+1} - 1 = 2a - 1.$$

そこで $\sigma(a) = 2a - 1$ を満たす a は 2 のべきになると思われるが, うまく証明できない.

しかしながらオイラー関数の場合はかくも簡単にできたのである.

諸君, オイラー先生のイラスト[1]の前に頭をたれよう.

[1](イラストは飯高順による)

図 1: オイラー: Leonhard Euler, 1707– 1783, 早期に片眼の視力を失い晩年には失明しても研究は継続

3　$a = 2p$ の場合

自然数 a が $\varphi(a) = a - 1$ を満たす必要十分条件は a が素数 p になることである.

このことの意味は意外にも重い. すなわち自然数 a が素数となることを定義から確かめることは大変だが, オイラー関数の関係式 $\varphi(a) - a + 1 = 0$ がわかれば直ちに a は素数と言える. これは素数の優れた判定法と言ってよい.

次に a が素数 p の 2 倍になる場合を考えよう. すなわち $a = 2p$ とし p は奇数とする. 2 と p は互いに素なので, 乗法性によって $a = 2p$ のとき

$$\varphi(a) = \varphi(2p) = \varphi(2)\varphi(p) = p - 1.$$

すると $2\varphi(a) = 2p - 2 = a - 2$. これより次の条件式をえる.

$$2\varphi(a) = a - 2. \tag{2}$$

そこで, 自然数 a が式 (2) を満たすとする.

$a = 2 + 2\varphi(a)$ となるので, a は偶数. よって $a = 2k$ と書ける.

1. k は奇数の場合.

$$2\varphi(a) = 2\varphi(2k) = 2\varphi(2)\varphi(k) = 2\varphi(k)$$

および, 式 (2) より $a-2=2\varphi(k)$.

$a=2k$ を思い出すと, $2\varphi(k)=2k-2$. これより $\varphi(k)=k-1$. したがって k は素数 p. よって $a=2k=2p$.

2. k は偶数の場合.

$k=2^eL(e>0, L:$ 奇数$)$ と表すと $a=2^{e+1}L$ であり式 (2) の左辺は

$$2\varphi(a)=2\varphi(2k)=2\varphi(2^{e+1}L)=2^{e+1}\varphi(L).$$

式 (2) の右辺は $a-2=2^{e+1}L-2$. ゆえに $2^{e+1}\varphi(L)=2^{e+1}L-2$.

これより

$$2^e\varphi(L)=2^eL-1.$$

よって, $1=2^e(L-\varphi(L))$ と書けるから $e=0$ となり $e>0$ に矛盾した.

この結果を定理として述べておこう.

定理 2 *$a=2p$ (p は奇素数) とかける必要十分条件は $2\varphi(a)=a-2$.*

読者は 8 月号で, $a=2p$ と書けるとき約数の和関数 $\sigma(a)$ を用いると $2\sigma(a)=3a+6$ となることを識った. 逆にこの式を満たす a は $a=2p$ と表されるが, この場合 p は 4 または奇素数である. この例外的な場合に $8=2\times4$ と書けるので 4 を擬素数と呼んだ.

擬素数やエイリアンが出てくような現象は美しいとも, 面白いともみることができる. しかし $a=2p$ を約数の和関数ではなくオイラー関数を用いて判定するとき擬素数やエイリアンなどの例外的な場合がでて来ない. これはオイラー関数がきわめて強力なことを示唆している.

3.1 $3p$ の場合

$a=3p$ の場合, (ただし $p\neq3$ は素数.)

$\varphi(a)=\varphi(3p)=2(p-1)=2\times\frac{a}{3}-2$ によれば

$$3\varphi(a)=2a-6. \tag{3}$$

次に自然数 a が式 (3) を満たすとき, $a=3p(p\neq3$ 素数$)$ と書けることを示したい. それは読者への宿題としよう.

3.2 $4p$ の場合

$a=4p$ の場合, (ただし $p\neq2$ は素数.)

$4=2^2$ なのでもう少し一般にして $\varepsilon>0$ に対して $m=2^\varepsilon$ とおき, $a=mp$ (ただし $p\neq2$) とする. $\varphi(m)=\varphi(2^\varepsilon)=2^{\varepsilon-1}=m/2$ に注意すると

$$2\varphi(a)=2\varphi(mp)=2\varphi(m)\varphi(p)=m(p-1)=a-m.$$

したがって

$$2\varphi(a)=a-2^\varepsilon. \tag{4}$$

$\varepsilon=4$ のときをパソコン君に計算してもらった.

表 1: $2\varphi(a) = a - 2^4$ の解

a	素因数分解	$\varphi(a)$
48	$[2^4, 3]$	16
80	$[2^4, 5]$	32
112	$[2^4, 7]$	48
176	$[2^4, 11]$	80
208	$[2^4, 13]$	96
272	$[2^4, 17]$	128
304	$[2^4, 19]$	144
368	$[2^4, 23]$	176
464	$[2^4, 29]$	224

自然数 a が 式 (4) を満たすとき a は偶数なので $a = 2^e L (e > 0, L$ 奇数$)$ と書ける.
そこで, 式 (4) の左辺を計算し

$$2\varphi(a) = 2\varphi(2^e L) = 2\varphi(2^e)\varphi(L) = 2^e\varphi(L).$$

式 (4) の右辺は

$$a - 2^\varepsilon = 2^e L - 2^\varepsilon.$$

よって

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

になり

$$2^e(\varphi(L) - L) = -2^\varepsilon.$$

故に 2^e は 2^ε の約数なので $e \leq \varepsilon$. かくしてこの場合も

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

1. $\varepsilon - e = 0$ の場合.
$\varphi(L) - L = -2^{\varepsilon - e} = -1$ により $\varphi(L) = L - 1$. したがって L は素数 p になり, $a = 2^e p = 2^\varepsilon p$.

2. $\varepsilon - e > 0$ の場合.
$\varepsilon - e > 0$ なので $2^{\varepsilon - e}$ は偶数. 一方, $L > 2$ ならオイラー関数の値 $\varphi(L)$ は偶数.
よって $L = \varphi(L) + 2^{\varepsilon - e}$ も偶数. しかし L は奇数だったので矛盾.

定理 3 $\varepsilon = 1, 2, 3, \cdots$ について $2\varphi(a) = a - 2^\varepsilon$ を満たすとき $a = 2^\varepsilon p (p:$ 奇素数$)$ となることが必要十分条件である.

かくして擬素数のないことが証明できた.

4　3のべき の場合

やや一般に整数 $\varepsilon > 0$ に対して $m = 3^\varepsilon$ とおき, $a = mp$ (ただし $p \neq 3$) とする. $\varphi(m) = \varphi(3^\varepsilon) = 2 \times 3^{\varepsilon-1}$ に注意すると $3\varphi(m) = 2m$ になり

$$3\varphi(a) = 3\varphi(mp) = 3\varphi(m)\varphi(p) = 2m(p-1) = 2a - 2m.$$

したがって

$$3\varphi(a) = 2a - 2 \times 3^\varepsilon. \tag{5}$$

4.1　計算例

$3\varphi(a) = 2a - 2 \times 3$ の解 a は $3p$ と書けることは容易に確認できる. 3^2 の場合も同様. $3\varphi(a) = 2a - 2 \times 3^3$ の解はパソコン君に任せたら次の通りでやはり $a = 3^3 \times p$ と書ける.

表 2: $3\varphi(a) = 2a - 2 \times 3^3$ の解

a	素因数分解	$\varphi(a)$
54	$[2, 3^3]$	18
135	$[3^3, 5]$	72
189	$[3^3, 7]$	108
297	$[3^3, 11]$	180
351	$[3^3, 13]$	216
459	$[3^3, 17]$	288
513	$[3^3, 19]$	324
621	$[3^3, 23]$	396
783	$[3^3, 29]$	504
837	$[3^3, 31]$	540

4.2 $3\varphi(a) = 2a - 2 \times 3^4$ の解

しかし 3^4 の場合は違ってくる.

表 3: $3\varphi(a) = 2a - 2 \times 3^4$ の解

a	素因数分解	$\varphi(a)$
162	$[2, 3^4]$	54
345 $*$	$[3, 5, 23]$	176
405	$[3^4, 5]$	216
561 $*$	$[3, 11, 17]$	320
567	$[3^4, 7]$	324
891	$[3^4, 11]$	540
1053	$[3^4, 13]$	648

$*$ 印はエイリアン解を意味する.

約数の和関数よりオイラー関数は強力であるが, これをこれを打ち破ってエイリアンが出てきた. 歓迎しよう.

4.3 $3\varphi(a) = 2a - 2 \times 3^5$ の場合の解

$\varepsilon = 5$ の場合の解は次の通り.

表 4: $3\varphi(a) = 2a - 2 \times 3^5$ の解

a	素因数分解	$\varphi(a)$
486	$[2,3^5]$	162
1035*	$[3^2,5,23]$	528
1215	$[3^5,5]$	648
1683*	$[3^2,11,17]$	960
1701	$[3^5,7]$	972
2343*	[3,11,71]	1400
2673	$[3^5,11]$	1620
3159	$[3^5,13]$	1944
4071*	[3,23,59]	2552
4131	$[3^5,17]$	2592
4611*	[3,29,53]	2912
4617	$[3^5,19]$	2916

$\varepsilon = 4$ のときの 2 つのエイリアンが $\varepsilon = 5$ のときにも引き続いて出ている. 一方素因数分解が [3,11,71],[3,23,59],[3,29,53] と書ける新しいエイリアンが 3 個でてきた. そしてこれらの 5 個だけがエイリアンである. このように見ると, これらは素性のわかるエイリアンなのである.

4.4 証明

自然数 a が 式 (5) を満たすとき a は 3 の倍数なので $a = 3^e L (e > 0, L$ は 3 で割れない) と書ける. そこで, 式 (5) の左辺を計算し

$$3\varphi(a) = 3\varphi(3^e L) = 3\varphi(3^e)\varphi(L) = 2 \times 3^e \varphi(L).$$

式 (5) の右辺は

$$2a - 2 \times 3^\varepsilon = 2 \times 3^e L - 2 \times 3^\varepsilon.$$

ゆえに

$$2 \times 3^e \varphi(L) = 2 \times 3^e L - 2 \times 3^\varepsilon.$$

これより

$$3^e \varphi(L) - 3^e L = -3^\varepsilon.$$

1. $\varepsilon - e = 0$ の場合.
$\varphi(L) - L = -3^{\varepsilon - e} = -1$ により $\varphi(L) = L - 1$. したがって L は素数 p になり, $a = 3^\varepsilon p$.

2. $\varepsilon - e > 0$ の場合.
$L - \varphi(L) = 3^{\varepsilon - e}$ になる. $e > 0$ なので $\varepsilon - e \leq 4$ の場合はパソコン君に作ってもらった次の表を使用する. (7 月号で $a - \varphi(a)$ の評価をした).

表 5: $L - \varphi(L) = 3^\eta; 3 \nmid L$ の解

L	素因数分解	$\varphi(L)$	$[q^\eta]$
115	[5,23]	88	$[3^3]$
187	[11,17]	160	$[3^3]$
781	[11,71]	700	$[3^4]$
1195	[5,239]	952	$[3^5]$
1357	[23,59]	1276	$[3^4]$
1537	[29,53]	1456	$[3^4]$
2563	[11,233]	2320	$[3^5]$
3859	[17,227]	3616	$[3^5]$

$L-\varphi(L)=3^{\eta}$ の解があれば $a=2^{\varepsilon-\eta}L$ により $3\varphi(a)=2a-2\times 3^{\varepsilon}$ のエイリアン解が得られる.
$L=115,\eta=3$ に対して $a=3\times L=345$ がエイリアン解である.
よって $\varepsilon\leq 3$ のときは, 解 a は $3^{\varepsilon}p$ ($p\neq 3$: 素数) だけである. すなわちエイリアンは出てこない.

5　5 のべきの場合

パソコン君によると $5\varphi(a)=4(a-5^3)$ の解に次のものがある.

表 6: $5\varphi(a)=4(a-5^3)$ の解

a	素因数分解	$\varphi(a)$
250	[2,5^3]	100
345 $*$	[3,5,23]	176
375	[3,5^3]	200
665 $*$	[5,7,19]	432
875	[5^3,7]	600
1375	[5^3,11]	1000
1625	[5^3,13]	1200
2125	[5^3,17]	1600
2375	[5^3,19]	1800

5.1　$5\varphi(a)=4(a-5^4)$ の解

パソコン君によると $5\varphi(a)=4(a-5^4)$ の解に次のものがある. $5^4\times p$ の形が通常解なのでエイリアン解 $*$ はだいぶ多い.

表 7: $5\varphi(a) = 4(a - 5^4)$ の解

a	素因数分解	$\varphi(a)$
1250	[2,5^4]	500
1725 $*$	[3,5^2,23]	880
1875	[3,5^4]	1000
3325 $*$	[5^2,7,19]	2160
4375	[5^4,7]	3000
6875	[5^4,11]	5000
7345 $*$	[5,13,113]	5376
8125	[5^4,13]	6000
9265 $*$	[5,17,109]	6912
10165 $*$	[5,19,107]	7632
10625	[5^4,17]	8000
11845 $*$	[5,23,103]	8976
11875	[5^4,19]	9000
14065 $*$	[5,29,97]	10752
14375	[5^4,23]	11000
16465 $*$	[5,37,89]	12672
17845 $*$	[5,43,83]	13776
18125	[5^4,29]	14000
18565 $*$	[5,47,79]	14352
19345 $*$	[5,53,73]	14976
19375	[5^4,31]	15000
19765 $*$	[5,59,67]	15312

5.2 $L-\varphi(L)=5^{\eta}$ の解

これらのエイリアン解は 12 個あって統制がとれていないようであるが $L-\varphi(L)=5^{\eta};5 \nmid L$ の解が元になってこれからエイリアン解がでていることがよくわかる. 読者は実際に確かめてみるとよい.

表 8: $L-\varphi(L)=5^{\eta};5 \nmid L$ の解

L	素因数分解	$\varphi(L)$	$[q^{\eta}]$
69	$[3,23]$	44	$[5^2]$
133	$[7,19]$	108	$[5^2]$
1469	$[13,113]$	1344	$[5^3]$
1853	$[17,109]$	1728	$[5^3]$
2033	$[19,107]$	1908	$[5^3]$
2369	$[23,103]$	2244	$[5^3]$
2737	$[7,17,23]$	2112	$[5^4]$
2813	$[29,97]$	2688	$[5^3]$
3293	$[37,89]$	3168	$[5^3]$
3569	$[43,83]$	3444	$[5^3]$
3713	$[47,79]$	3588	$[5^3]$
3869	$[53,73]$	3744	$[5^3]$
3953	$[59,67]$	3828	$[5^3]$
4333	$[7,619]$	3708	$[5^4]$
7969	$[13,613]$	7344	$[5^4]$

$[q^{\eta}],\eta \geq 3$ となる場合の数は 12 個.

m に異なる素因数が複数個ある場合を考えよう.
$m=15$ のとき $a=mp=15p$ (p は $p\neq 3,5$ を満たす素数) とすると

$$\varphi(a)=15\varphi(mp)=\varphi(m)\varphi(p)=8(p-1)$$

なので $15\varphi(a)=\varphi(mp)=15\times 8(p-1)=8a-120$.
かくて次の方程式ができる.

$$15\varphi(a)=8a-120. \tag{6}$$

さて自然数 a が式 (6) を満たすとき $a=15p$ と書けることを示す. ここで p は $p\neq 3,5$ を満たす素数である.
条件式から $8a=15(\varphi(a)+8)$ になり, 整数 k によって $a=15k, \varphi(a)+8=8k$ と書ける.

1. k が 15 と互いに素の場合.
$\varphi(a)=\varphi(15k)=8\varphi(k), \varphi(a)=8(k-1)$ によって $\varphi(k)=k-1$.
このとき k は素数になるのでこれを p とおけば $a=15p$.

2. $k=3^eL(e>0$, L は 3 で割れない) の場合.

$$\varphi(a)=\varphi(15k)=\varphi(3^{e+1}5L)=2\times 3^e\varphi(5L).$$

一方, $\varphi(a)=8(k-1)=8(3^eL-1)$ なので $4(3^eL-1)=3^e\varphi(5L)$ になるので $-4=3^e(\varphi(5L)-4L)$. よって $e=0$. これは仮定に反する..

3. $k=5^fL, (f>0$, L は 15 で割れない) の場合.

$$\varphi(a)=\varphi(15k)=\varphi(5^{f+1}3L)=4\times 5^f\varphi(3L).$$

一方, $\varphi(a)=8(k-1)=8(5^fL-1)$. ゆえに

$$4\times 5^f\varphi(3L)=8(5^fL-1).$$

よって

$$5^f(\varphi(3L)-2L)=-2.$$

これより $f=0$. これは仮定に反する. したがってこの場合も起きない.
以上によって $a=15p$ が示されエイリアンは出てこないことが確認された.

5.3 解の例

念のためパソコン君に依頼して解を探してもらった.

表 9: $15\varphi(a) = 8a - 120$ の解

a	素因数分解	$\varphi(a)$
30	[2,3,5]	8
105	[3,5,7]	48
165	[3,5,11]	80
195	[3,5,13]	96
255	[3,5,17]	128
285	[3,5,19]	144
345	[3,5,23]	176
435	[3,5,29]	224
465	[3,5,31]	240

これから a の解は $30 = 2 \times 15, 105 = 7 \times 15, 165 = 11 \times 15, \cdots$ となっていて期待通りである.
研究課題 (1)$a = 14p$ (2)$a = 30p$ (3) $a = 105p$ の場合について同様のことを確かめよ.

6 $a = mp$ の場合

以上の結果から m が異なる素因数の積の場合は,エイリアンが出ないように思われる. そこで一般的であっても計算しやすい場合を扱うことにする. すなわち,

仮定: m と $\varphi(m)$ が互いに素とする.

このとき m は異なる素因数の積になっている.

さて $a = mp$ とおき p は m の素因子でない素数とする.

$\varphi(a) = \varphi(mp) = \varphi(m)\varphi(p) = \varphi(m)(p-1)$ なのでこれを m 倍し $m\varphi(a) = \varphi(m)(mp - m) = \varphi(m)(a - m)$ を得る.

$$m\varphi(a) = \varphi(m)a - \varphi(m)m \tag{7}$$

このような $\varphi(a)$ と a の間の関係式を **オイラー関数の 1 次関係式**という. これを,a についての方程式として解くことが基本的な問題である.

さて

$$m(\varphi(a) + \varphi(m)) = \varphi(m)a$$

と変形し, 仮定により m と $\varphi(m)$ が互いに素なので

$$\varphi(a) + \varphi(m) = \varphi(m)k, a = mk$$

となる整数 k がある. よって

$$\varphi(mk) = \varphi(m)(k-1) \tag{8}$$

をえる. m の素因子 q をとり k の q での指数を e とおけば $m = qm_1, k = q^e L(q : m_1 L$ の素因子ではない) と書くと

$$\varphi(mk) = \varphi(q^{e+1} m_1 L) = q^e (q-1)\varphi(m_1 L).$$

一方

$$q^e (q-1)\varphi(m_1 L) = \varphi(mk) = \varphi(m)(q^e L - 1). \tag{9}$$

変形して

$$q^e((q-1)\varphi(m_1 L) - \varphi(m)(L)) = -\varphi(m).$$

$m = qm_1$ と $\varphi(m)$ が互いに素なので $\varphi(m)$ は q で割れないから $e = 0$.

この操作を k のすべての素因子について行うと k と m は互いに素になることがわかる. 乗法性によって

$$\varphi(a) = \varphi(mk) = \varphi(m)\varphi(k).$$

式 (8) に注意すると $\varphi(mk) = \varphi(m)(k-1)$ なので $\varphi(k) = k-1$. これは k が素数 p となることを意味するので $a = mk = mp$ となる.