数学の研究を始めよう (3)
オイラー関数の値

飯高 茂

平成 25 年 7 月 17 日

1　オイラー関数 φ の値

自然数 n のオイラー関数 $\varphi(n)$ は分母が n の真分数 $\frac{k}{n}$ のうち既約分数になるものの個数である. 言い換えれば $k < n$ で k と n が互いに素な数 k の総数が $\varphi(n)$ と言ってよい.

たとえば分母が 10 の既約分数は $\frac{1}{10}, \frac{3}{10}, \frac{7}{10}, \frac{9}{10}$ なので $\varphi(10) = 4$ である. 後に示すが $\varphi(100) = 40, \varphi(1000) = 400$ となる. 分母が 100 の既約分数をすべて書き出してその個数を数えることは難しい.

定義自身は中学生でもわかるが, オイラー関数は昔から今に至るまで数学においてきわめて重要な関数であり数多くの研究が積まれてきたが未だに分からぬことが多い.

最近は、コンピュータのセキュリティに関してオイラー関数の性質が使われることが多く、オイラー関数の重要性はむしろ増している.

そこで今回はオイラー関数 φ の値を研究してみよう. 最初に基本性質を挙げる.

基本性質

1. n が素数 p なら p より小さい分子はすべて p と互いに素なので $\varphi(p) = p - 1$.
2. n が素数 p^2 なら分子は p の倍数でないとき p^2 と互いに素なので $\varphi(p^2) = p^2 - p = p(p-1)$.
3. 一般には $\varphi(p^e) = p^{e-1}(p-1)$.
4. 分母が相異なる 2 つの素数 p, q の積 pq のとき. 分子が p の倍数なら $n/p = q$ 個, 分子が q の倍数なら $n/q = p$ 個. 分子が pq の倍数なら分子は pq のみ. pq は重複して数えているのでこれを引く.

$$\varphi(pq) = pq - (p + q - 1) = (p-1)(q-1).$$

このような考え方は高校数学でも使われていた。

実は n, m が互いに素なら

$$\varphi(nm) = \varphi(n)\varphi(m)$$

が成り立つ. これを**オイラー関数の乗法性**という. オイラー関数 $\varphi(n)$ を求めるには n を素因数分解して乗法性を用いれば素数の累乗 p^e のオイラー関数 $\varphi(p^e)$ の計算に持ち込めばよい. この値は $p^{e-1}(p-1)$ なので素因数分解さえできればオイラー関数の値は簡単にわかる.

そこでパソコン君に頼んで次の数表を作ってもらった. 単にオイラー関数の値 $e = \varphi(n)$ を求めるだけではなく, それらの素因数分解も表の中に入れた. 素因数分解はリスト表示で表した. たとえば [2,2] は 2×2 のことである.

表 1: オイラー関数

n	n の素因数分解	$e = \varphi(n)$	e の素因数分解
2	[2]	1	[1]
3	[3]	2	[2]
4	[2,2]	2	[2]
5	[5]	4	[2,2]
6	[2,3]	2	[2]
7	[7]	6	[2,3]
8	[2,2,2]	4	[2,2]
9	[3,3]	6	[2,3]
10	[2,5]	4	[2,2]
11	[11]	10	[2,5]
12	[2,2,3]	4	[2,2]
13	[13]	12	[2,2,3]
14	[2,7]	6	[2,3]
15	[3,5]	8	[2,2,2]
16	[2,2,2,2]	8	[2,2,2]
17	[17]	16	[2,2,2,2]
18	[2,3,3]	6	[2,3]
19	[19]	18	[2,3,3]
20	[2,2,5]	8	[2,2,2]
21	[3,7]	12	[2,2,3]
22	[2,11]	10	[2,5]
23	[23]	22	[2,11]
24	[2,2,2,3]	8	[2,2,2]
25	[5,5]	20	[2,2,5]
26	[2,13]	12	[2,2,3]
27	[3,3,3]	18	[2,3,3]
28	[2,2,7]	12	[2,2,3]
29	[29]	28	[2,2,7]
30	[2,3,5]	8	[2,2,2]

この表をみると, オイラー関数は単調ではないことがわかる. 値が微妙に上下しているが $\varphi(2) = 1$ 以外は必ず偶数であり, したがって $\varphi(3) = \varphi(4) = \varphi(6) = 2$ 以外なら合成数になっている.

2　オイラー関数の逆関数の多価性

今度はオイラー関数の値にしたがって並べ替えしてみよう. 実際には, オイラー関数の数値を表計算、たとえばエクセルに入れておいてエクセルのもつ並べ替えの機能を用いる. すると簡単に並べ替えができて次の数表ができる.

この数表をじっと眺めて、そこから観察できた結果を書いてみる. そして、証明を試みてみよう. うまく証明ができれば定理ができる. 自分でも定理が作れる. これはスゴイことです. 自分で作った定理は間違っているか, 価値がないか, すでに知られているかのどれかである可能性が大きい. それでも自分で見つけて証明できればその価値は大きい.

観察結果

1. $\varphi(2)=1$ 以外は偶数. (これはすでに示した)

2. 偶数でオイラー関数の値にならない数は 14 が最初で次に, 26,34.

それらの素因数分解は $14=2\times 7, 26=2\times 13, 34=2\times 17$ となっている.

さて,$m=2\times p(p$ は奇素数) がオイラー関数の値になるとしよう. すなわちある n により $\varphi(n)$ となるとしよう.

n の相異なる奇数の素因子が 2 つ以上あったとする. それを P,Q とおくと $P-1$ と $Q-1$ の約数としての 2 がともにでてくるのでその積は 4 以上. したがって $\varphi(n)=2\times p$ にはならない.

その上,2 の累乗 2^s が n の因子とすると $\varphi(n)=2\times p$ により $s=1$ となる. よって a) $n=P^e$ または b) $n=2P^e$ となる.

a). $n=P^e, P>2$ ならば $\varphi(n)=(P-1)P^{e-1}$ であり, $(P-1)P^{e-1}=2p$ となるには (1). $e=1, 2p=P-1$ または (2). $e=2, 2=P-1, P=p=3$ が必要である.

(1). のとき $P=2p+1$ なので $2p+1$ は素数. したがって次の定理ができる.

定理 1 奇素数 p に対して $2p+1$ が素数でないなら $2p$ はオイラー関数の値にならない.

$p=7,13,17$ のとき $2p+1$ は素数にならないので 14,26,34 はオイラー関数の値にならない

(2). のとき $n=9$ なので $\varphi(9)=6$. $p=3$ なら $2p=6$ はオイラー関数の値になる.

b). $n=2P^e, P>2$ ならば $\varphi(n)=\varphi(P^e)$ となるのですでに調べた.

2.1　オイラー関数の値は必ずダブっている

$N_\varphi(m)$ を $\varphi(n)=m$ を満たす n の個数として定義する. したがって上の予想は $N_\varphi(m)>1$ と書き換えられ, これはオイラー関数の逆関数の多価性を意味する.

3　カーマイケルの予想

このことは (1922 年) カーマイケルが証明したがその証明は正しくなかった. そこで現在はカーマイケルの予想と呼ばれているが, 未だ決着がついていない難問である。

Wikipedia(英語版) を見ると次の結果が出ている.

⟨1⟩ カーマイケルは $N<10^{37}$ となる N については カーマイケルの予想は成立することを示した。

⟨2⟩ Victor Klee は $N<10^{400}$ について成立することを 1947 年に示した。

⟨3⟩ Schlafly と Wagon は $N<10^{10^7}$ について成立することを示した。

⟨4⟩ Kelvin Ford は $N<10^{10^{10}}$ について成立することを 1998 年に示した。

4　2 価の場合

自分だけを頼りに数学の研究を始めると知らないままカーマイケルの予想のような大難問に意図しないで挑むことになる. このような難問は素人に手が出る問題ではない. 古今東西の数学者の実力をなめてはいけない。

そこで、やさしそうな問題を考える. たとえば 2 価の場合すなわち $N_\varphi(m)=2$ を満たす m を調べてみよう.

上の表によると多分 $N_\varphi(10)=2$ である. エクセルの表を眺めれば $N_\varphi(m)=2$ を満たす他の例は

$10=2\cdot 5$,
$22=2\cdot 11$,
$28=2^2\cdot 7$,
$30=2\cdot 3\cdot 5$,
$46=2\cdot 23$,
$54=2\cdot 3^3$,
$56=2^3\cdot 7$

などである. これらが実際に 2 価であることは確かめられる.

さて $10=2\cdot 5$ の特徴を考えて見る. 5 も 11 も素数で $11=2\cdot 5+1$ を満たす.

4.1　ソフィー・ジェルマン素数

素数 p,q が $q=2p+1$ を満たすとしよう. たとえば $p=5,q=11$; $p=11,q=23$;$p=23,q=47$.

このような素数を **ソフィー・ジェルマン素数**という. [1]

[1] フランスの数学者 Sophie Germain

ソフィー・ジェルマン素数は沢山あるが無限にあるかどうかはわかっていない. 数学界で有名な難問の 1 つである. この場合 q は 2 価である。そこで, 2 価である数 m は無限にあるか, という問題を考えて見よう.

4.2 2 価である数

Ribenboim の本『素数の世界』(吾郷孝視訳、共立出版, 1995) に 2 価である数 m の例として $m = 2 \times 3^{6k+1}$ が挙げられている. ここで $k > 0$ である. このとき $M = m + 1$ は素数ではない.

しかし $k = 0$ なら $M = 7$ は素数であり $N_\varphi(7) = 4$. そのほかの場合は $N_\varphi(m) = 2$ になる. これは後に示すがそのために $k > 0$ のとき $M = 2 \times 3^{6k+1} + 1$ は素数ではないことを示したい. 最初, この問題が解けなかった. そこで, パソコン君に助けてもらい次の表を得た.

この結果を見ると, M が 7 の倍数なのであろう. そこで mod7 で考える.

$3^2 = 9 \equiv 2 \mod 7$ なので

$$3^3 \equiv 2 \times 3 \equiv -1 \mod 7.$$

$3^6 \equiv 1 \bmod 7$ によって

$$M = 2 \times 3^{6k+1} + 1 \equiv 2 \times 3^{6k} \times 3 + 1 \equiv 6 + 1 \equiv 0 \bmod 7.$$

よって M は 7 の倍数なので $k > 0$ なら合成数になる.

4.3 $N_\varphi(m) = 2$ の証明

$m = 2\times 3^{6k+1}$ のとき $\varphi(n) = m$ とすると n は素数ではない. 実際, n が素数なら $\varphi(n) = n-1 = m$ なので $n = m + 1$. しかし $M = m + 1$ は素数でないことが示されていたから矛盾.

さて $N = 3^{6k+2}$ とおくと $\varphi(N) = 3^{6k+2} - 3^{6k+1} = 2 \times 3^{6k+1} = m$.

また N と 2 は互いに素なので $\varphi(2 \times N) = \varphi(N) = 2 \times 3^{6k+1} = m$.

したがって, $\varphi(3^{6k+2}) = \varphi(2 \cdot 3^{6k+2}) = m$.

改めて, $\varphi(n) = m$ としこのような n を求めよう.

1). もし n が素数 p なら $\varphi(p) = p - 1$. よって,$p = 2 \times 3^{6k+1} + 1 = M$ となり, M が素数となって矛盾.

2).n が素数でないなら $\varphi(n) = 2 \times 3^{6k+1}$ になることより奇素数 P を用いて $n = P^e$, または $n = 2P^e$ と書ける.

i). $n = P^e$ のとき $\varphi(n) = (P-1)P^{e-1}, e > 1$. よって

$$(P-1)P^{e-1} = 2 \times 3^{6k+1}.$$

これより $P - 1 = 2, e - 1 = 6k + 1$. したがって $P = 3, e = 6k + 2$. よって $n = 3^{6k+2}$.

ii). $n = 2P^e$ のとき $\varphi(n) = (P-1)P^{e-1}$. よって $n = 2 \cdot 3^{6k+2}$.

したがって $m = 2 \times 3^{6k+1}$ は 2 価の数.

5 研究課題

研究課題 1.

$N_\varphi(m) = 3$ を満たす m を見つけよ.

答え. $m = 2$.

次の課題: $N_\varphi(m) = 3$ を満たす 2 より大きい m を見つけよ.

研究課題 2.

$N_\varphi(m) = 3$ を満たす m を見つけよ.

答え. $m = 8$.

次の課題: $N_\varphi(m) = 5$ を満たす 8 より大きい m を見つけよ.

研究課題 3. オイラー関数の値にならない例を 16 個あげて, その理由を述べよ.

ヒント たとえば 14,26,34,50,62,68,74,76,86,90,94,98,114

研究課題 4. 奇素数 p に対して $4p$ がオイラー関数の値にならない例を探せ. またその理由を述べよ.

あとがき

26 がオイラー関数の値にならないことを示すことは大学 1 年生の期末試験問題に出した. 学生諸君はいろいろ説明をつけてくれたが, ぴりっとした解答が少なかった.

卒業研究の材料になりうるものは研究課題 3,4 などである. オイラー関数の値を評価することは 2012 年度の卒業研究で行った. その結果は十分興味のあるものだが, すでに今月号分のページ数を超えたので次号にまわすことになった.

表 2: オイラー関数の値順 1

n	n の因数分解	$e = \varphi(n)$	e の因数分解
2	[2]	1	[1]
3	[3]	2	[2]
4	[2,2]	2	[2]
6	[2,3]	2	[2]
5	[5]	4	[2,2]
8	[2,2,2]	4	[2,2]
10	[2,5]	4	[2,2]
12	[2,2,3]	4	[2,2]
7	[7]	6	[2,3]
9	[3,3]	6	[2,3]
14	[2,7]	6	[2,3]
18	[2,3,3]	6	[2,3]
15	[3,5]	8	[2,2,2]
16	[2,2,2,2]	8	[2,2,2]
20	[2,2,5]	8	[2,2,2]
24	[2,2,2,3]	8	[2,2,2]
30	[2,3,5]	8	[2,2,2]
11	[11]	10	[2,5]
22	[2,11]	10	[2,5]
13	[13]	12	[2,2,3]
21	[3,7]	12	[2,2,3]
26	[2,13]	12	[2,2,3]
28	[2,2,7]	12	[2,2,3]
36	[2,2,3,3]	12	[2,2,3]
42	[2,3,7]	12	[2,2,3]
17	[17]	16	[2,2,2,2]
32	[2,2,2,2,2]	16	[2,2,2,2]
34	[2,17]	16	[2,2,2,2]
40	[2,2,2,5]	16	[2,2,2,2]
48	[2,2,2,2,3]	16	[2,2,2,2]
60	[2,2,3,5]	16	[2,2,2,2]
19	[19]	18	[2,3,3]
27	[3,3,3]	18	[2,3,3]
38	[2,19]	18	[2,3,3]
54	[2,3,3,3]	18	[2,3,3]
25	[5,5]	20	[2,2,5]
33	[3,11]	20	[2,2,5]
44	[2,2,11]	20	[2,2,5]
50	[2,5,5]	20	[2,2,5]
66	[2,3,11]	20	[2,2,5]
23	[23]	22	[2,11]
46	[2,23]	22	[2,11]
35	[5,7]	24	[2,2,2,3]
39	[3,13]	24	[2,2,2,3]
45	[3,3,5]	24	[2,2,2,3]
52	[2,2,13]	24	[2,2,2,3]

表 3: $M = 2 \times 3^{6k+1} + 1$ の素因数分解

k	$m = 2 \times 3^{6k+1} + 1$	$M = m + 1,$	M の素因数分解
0	6	7	[7]
1	4374	4375	[5,5,5,5,7]
2	3188646	3188647	[7,11,41411]
3	2324522934	2324522935	[5,7,587,113143]