数学の研究を始めよう (4)
オイラー関数の値 (続き)

飯高 茂

平成 25 年 4 月 15 日

1　数学科の卒業研究

国立大学の理学部で数学研究と教育を 18 年間継続し, 私立大学の理学部数学科に移ったのは今から 28 年前である. 大学では数学の講義以外にゼミがある。そこでどんなゼミをするかで悩み抜いた。自分の専門を活かしてゼミをするとすれば、たとえば Fulton の代数曲線論 (英文) の本を読んで、理解したところをまとめて卒業発表することが考えられる.

しかし、これはなかなか困難である. 英語の専門書を読み数学的な理解にいたるまで相当な時間がかかる. また、数学の研究とは無縁な仕事につく大多数の学生にとってモーティベーションを維持することが難しい.

その上, 赴任前に「できたらコンピュータを使ったゼミをしてくれないか」などの話しがあった.

最初の頃は、ミニコンを使って Unix で vi を使って C のプログラムで数学のプログラムを書くようにしたがこれはこれで敷居が高く、必ずしも順調にいかない. ついでに Pascal, LISP などもしてみた. 中には変わった学生もいて、いつのまにか COMMON LISP の名人になった.

そのうち私が コンピュータ言語 Prolog にはまり、これを学生にも強制するようになった.

C ができる学生は Prolog に迷い不満一杯である. しかし少しコツがわかると、やはり Prolog にはまる. しかし、Prolog が分からぬまま卒業する学生もいた.

Windows で動く SWI-Prolog はフリーであるが故に非常に進化して使い勝手がよくなった. 今や、Prolog は完全に実用言語になったのである.

ゼミの最初は Prolog の実習である. 再帰の構文を覚えて、与えられた自然数の最小因子を求めるプログラムを理解する. そして、素因数分解のプログラムを作る.

素因数分解のプログラムができると、学生は大感激である.

そこで、オイラー関数の値を再帰プログラムで作る. ここまでくれば、2000 までの数 n に対して、その オイラー関数の値 $e = \varphi(n)$ とそれらの素因数分解のリストを出すことはすぐできる.

ここで Prolog を離れて、これらの出力結果をエクセルに移してエクセルで操作するのが便利である.

オイラー関数の値の順に並べ替えて観察しながら、定理を発見する話しは前回紹介した.

1.1　$n - \varphi(n)$ の順に並べ替え

次に $n - e(= n - \varphi(n))$ の順に並べ替えて観察する.

表 1: $n-\varphi(n)>1$ で並べ替え

n	素因子分解	$e=\varphi(n)$	e の素因子分解	$n-\varphi(n)$
4	[2,2]	2	[2]	2
9	[3,3]	6	[2,3]	3
6	[2,3]	2	[2]	4
8	[2,2,2]	4	[2,2]	4
25	[5,5]	20	[2,2,5]	5
10	[2,5]	4	[2,2]	6
15	[3,5]	8	[2,2,2]	7
49	[7,7]	42	[2,3,7]	7
12	[2,2,3]	4	[2,2]	8
14	[2,7]	6	[2,3]	8
16	[2,2,2,2]	8	[2,2,2]	8
21	[3,7]	12	[2,2,3]	9
27	[3,3,3]	18	[2,3,3]	9
35	[5,7]	24	[2,2,2,3]	11
121	[11,11]	110	[2,5,11]	11
18	[2,3,3]	6	[2,3]	12
20	[2,2,5]	8	[2,2,2]	12
22	[2,11]	10	[2,5]	12
33	[3,11]	20	[2,2,5]	13
169	[13,13]	156	[2,2,3,13]	13
26	[2,13]	12	[2,2,3]	14
39	[3,13]	24	[2,2,2,3]	15
55	[5,11]	40	[2,2,2,5]	15

2 観察結果

すぐ分かる結果.

⟨1⟩ 1 が多い.

⟨2⟩ $n-\varphi(n)$ が 1 になるとき, n は素数

このとき n が素数になるのはなぜかを考えよう.

$n-\varphi(n)=1$ ということは何を意味するかを定義にもどって考えよう.

$\varphi(n)=n-1$ なので, 分母が n の真分数はみな既約だから、n 未満の数はすべて n と互いに素になる. よって n 未満の数は n の約数になれない. すなわち n は素数だ.

ここまで考えが進めば鋭い喜びに全身が包まれるであろう. 問題はこの次である.$n-\varphi(n)$ の値の表を眺めて自分で課題を出してみよう.

⟨1⟩ $n-\varphi(n)=2$ となる n は 4 であることを示せ

$\langle 2 \rangle$ $n - \varphi(n) = 3$ となる n は 9 であることを示せ

$\langle 3 \rangle$ $n - \varphi(n) = 4$ となる n は 6 と 8 であることを示せ

$\langle 4 \rangle$ $n - \varphi(n) = 10$ となる n は ないことを示せ

略解

1. $n - \varphi(n) > 1$ なので n は素数では無い. そこで素数のべき $n = p^e$ とすると $n - \varphi(n) = p^{e-1}$ なので仮定 $n - \varphi(n) = 2$ によれば $p^{e-1} = 2$. 故に $p = 2, e = 2$. したがって $n = 4$.

n が異なる素因数 p, q を持つとしよう. 真分数 $\frac{a}{n}$ において分子が p, q, pq のとき n と互いに素でないから $n - \varphi(n) \geq 3$. $n - \varphi(n) = 2$ と仮定したからこれは起きない.

2. 素数のべき $n = p^e$ としてみよう. $n - \varphi(n) = p^{e-1} = 3$ によれば故に $p = 3, e = 2$. したがって $n = 9$.

n が異なる素因数 p, q を持つとしよう. ここで $p < q$ とすれば 真分数 $\frac{a}{n}$ において分子が p, q, p^2, pq のとき n と互いに素でないから $3 = n - \varphi(n) \geq 4$. これは矛盾.

3. $n = p^e$ としてみよう. $n - \varphi(n) = p^{e-1} = 4$ のとき $p = 2, e = 3$. したがって $n = 8$.

n が異なる素因数 p, q を持つとしよう. $p < q$ とすれば 真分数 $\frac{a}{n}$ において分子が p, q, p^2, pq のとき n と互いに素でないから $4 = n - \varphi(n) \geq 4$.

$p = 2, q = 3$ なら $n = 6$. これは起きる.

$p = 2, q \geq 5$ なら $2, 4, 8, q, 2q$ のとき n と互いに素でないから $4 = n - \varphi(n) \geq 5$ となり矛盾.

$p \geq 3, q \geq 5$ なら $p, 2p, 3p, q, pq$ のとき n と互いに素でないら $4 = n - \varphi(n) \geq 5$ となり矛盾.

$n - \varphi(n) = 10$ となる n は ないことを示すのはすごく大変そうである.

2.1 n が素数の 2 乗 p^2 なら

オイラー関数は n が素数の 2 乗 p^2 なら $\varphi(p^2) = p^2 - p$ なので

$$n - \varphi(n) = p^2 - \varphi(p^2) = p = \sqrt{n}$$

になる. そこで関数 $F(n) = n - \varphi(n) - \sqrt{n}$ を導入する. $n = p^2$ のとき $F(n) = 0$.

素数でない数 n の場合 $F(n)$ に関して順に並べ替えてみよう.

3　素数でない場合

表 2: $F(n)$ について

n	素因子分解	$e=\varphi(n)$	e の素因子分解	$F(n)=n-\varphi(n)-\sqrt{n}$
4	[2,2]	2	[2]	0
9	[3,3]	6	[2,3]	0
25	[5,5]	20	[2,2,5]	0
49	[7,7]	42	[2,3,7]	0
121	[11,11]	110	[2,5,11]	0
169	[13,13]	156	[2,2,3,13]	0
289	[17,17]	272	[2,2,2,2,17]	0
361	[19,19]	342	[2,3,3,19]	0
529	[23,23]	506	[2,11,23]	0
841	[29,29]	812	[2,2,7,29]	0
961	[31,31]	930	[2,3,5,31]	0
8	[2,2,2]	4	[2,2]	1.171572875
6	[2,3]	2	[2]	1.550510257
10	[2,5]	4	[2,2]	2.83772234
15	[3,5]	8	[2,2,2]	3.127016654
27	[3,3,3]	18	[2,3,3]	3.803847577
16	[2,2,2,2]	8	[2,2,2]	4
14	[2,7]	6	[2,3]	4.258342613
21	[3,7]	12	[2,2,3]	4.417424305
12	[2,2,3]	4	[2,2]	4.535898385
35	[5,7]	24	[2,2,2,3]	5.083920217
33	[3,11]	20	[2,2,5]	7.255437353
22	[2,11]	10	[2,5]	7.30958424
20	[2,2,5]	8	[2,2,2]	7.527864045
55	[5,11]	40	[2,2,2,5]	7.583801513
18	[2,3,3]	6	[2,3]	7.757359313

この表を観察すれば

⟨1⟩ n が素数でないとき $F(n)$ は非負.

⟨2⟩ 0 になるなら，n は素数の平方になるだろう,

と推察できる．これを証明しよう.

簡単な場合から始める.

n が異なる素数 $p_1, p_2, \cdots, p_r$ の積の場合はオイラー関数が計算しやすい. だからこの場合に特化して考えてみよう.

$n=p_1p_2\cdots p_r$ なら $\varphi(n)=(p_1-1)(p_2-1)\cdots(p_r-1)$,

$\sqrt{n}=\sqrt{p_1p_2\cdots p_r}$ であるが, 平方根が鬱陶しい.
そこで $a_1=\sqrt{p_1}, a_2=\sqrt{p_2}, \cdots, a_r=\sqrt{p_r}$ とおけば
$n-\varphi(n)-\sqrt{n}\geq 0$ を書き換えると

$$a_1{}^2a_2{}^2\cdots a_r{}^2-(a_1{}^2-1)(a_2{}^2-1)\cdots(a_r{}^2-1)-a_1a_2\cdots a_r$$

となり平方根が無くなってすっきりした. そこでこれを証明しよう.
$r\geq 2$ なので $1<a_1<a_2<\cdots<a_r$ は仮定して良い.
$r=2$ なら $a=a_1, b=a_2$ とおけば $1<a<b$ なので

$$a^2b^2-(a^2-1)(b^2-1)-ab=b^2+a^2-ab-1=b(b-a)+a^2-1>1.$$

$a=\sqrt{2}, b=\sqrt{3}$ とすると

$$b^2+a^2-ab-1=5-\sqrt{6}-1=4-2.4494\cdots=1.55\cdots>1$$

これが最小値である.
これを一般化して $a_1, a_2, \cdots, a_r$ を単調増大の自然数列として, これが $2\leq a_1{}^2<a_2{}^2<\cdots<a_r{}^2$ を満たし $r\geq 2$ のとき次の不等式を示そう.

$$a_1{}^2a_2{}^2\cdots a_r{}^2>(a_1{}^2-1)(a_2{}^2-1)\cdots(a_r{}^2-1)+a_1a_2\cdots a_r+r-1$$

$r\geq 3$ のとき $X=a_2{}^2\cdots a_r{}^2, Y=(a_2{}^2-1)\cdots(a_r{}^2-1), Z=a_2\cdots a_r$ とおけば $r-1\geq 2$ なので帰納法の仮定から $X>Y+Z+r-2$ が成り立つ. そこで

- $a_1{}^2a_2{}^2\cdots a_r{}^2=a_1{}^2X$,
- $(a_1{}^2-1)(a_2{}^2-1)\cdots(a_r{}^2-1)=(a_1{}^2-1)Y=a_1{}^2Y-Y$,
- $a_1a_2\cdots a_r=a_1Z$

と変形して X, Y, Z を使い $X>Y+Z+r-2$ に注意すると

$$a_1{}^2X-(a_1{}^2-1)Y-a_1Z-r+1>a_1{}^2(Y+Z+r-2)-(a_1{}^2-1)Y-a_1Z-r+1.$$

右辺は $a_1{}^2\geq 2$ なので

$$a_1{}^2(Z+r-2)+Y-a_1Z-r+1=(a_1{}^2-a_1)Z+a_1{}^2(r-2)-r+1>a_1(a_1-1)Z+2(r-2)-r+1>0.$$

さて自然数 n の相異なる素因数 $p_1, p_2, \cdots, p_r$ は 2 個以上とする.
$n=p_1{}^{e_1}p_2{}^{e_2}\cdots p_r{}^{e_r}$ とし $a_1=p_1{}^{e_1/2}, a_2=p_2{}^{e_2/2}, \cdots, a_r=p_r{}^{e_r/r}$ とおくとき $n=a_1{}^2a_2{}^2\cdots a_r{}^2$ なので先の不等式を用いることができて

$$n=a_1{}^2a_2{}^2\cdots a_r{}^2>(a_1{}^2-1)(a_2{}^2-1)\cdots(a_r{}^2-1)+a_1a_2\cdots a_r+r-1.$$

ところで

$$\varphi(n)=(p_1{}^{e_1}-p_1{}^{e_1-1})(p_2{}^{e_2}-p_2{}^{e_2-1})\cdots(p_r{}^{e_r}-p_r{}^{e_r-1})$$

$p_1{}^{e_1}-1>p_1{}^{e_1}-p_1{}^{e_1-1}$, 等が成り立つので

$$n>\varphi(n)+\sqrt{n}+r-1>\varphi(n)+\sqrt{n}.$$

よって $F(n) > 0$.

次に $r = 1$ とすれば $n = p^e$, $\varphi(n) + \sqrt{n} = (p^e - p^{e-1}) + p^{e/2}$. $e \geq 2$ のとき

$$n - (\varphi(n) + \sqrt{n}) = p^{e-1} - p^{e/2} \geq 0.$$

かつ, $p^{e-1} - p^{e/2} = 0$ になるのは $e = 2$ に限る.

3.1 素数の平方で無いとき

n が素数でも素数の平方でもないとき $F(n) > 0$ になるが表によればその値は

$F(8) = 1.171572875$, $F(6) = 1.550510257\cdots$,$F(27) = 3.803847577$, $F(16) = 4$.

したがって $F(n) \leq 4$ なら $n = 8, 6, 10, 15, 27, 16$ は成立しそうである. これを証明しよう.

$e \geq 3$ なら $n = p^e$ のとき

$$F(n) = p^{e-1} - p^{e/2} \geq p^2 - p\sqrt{p} = p(p - \sqrt{p})$$

$F(8) = 1.171572875 < 4$, $F(16) = 4$, $F(27) = 3.803847577 < 4$ なので $r = 1, e > 2$ で $F(n) \leq 4$ になるのは $n = 2^3, 3^3, 2^4$.

$r \geq 3$ のとき $F(n)$ の最小値はどうなるだろう.

$r = 3$ のときが最小になり,$30 = 2 \times 3 \times 5$ のときの $F(30)$ が最小値であるが, さらに $F(30) > 16$ がわかる.

$r = 2$ のときの $F(n)$ の最小値は下から $n = 2 \times 3, 2 \times 5, 2 \times 7, 3 \times 5, 2 \times 7$.

$F(14) > 4$ なので $6, 10, 15$ のみが $F(n) \leq 4$ を満たす. つぎの形にまとめよう. 学生の定理としてはなかなかのものである.

定理 n が素数ではなく素数の平方でもないとき $n \neq 6, 8, 10, 15, 16, 27$ なら $F(n) > 4$.

以上は, 学習院大学理学部の学生であった奥山有人君の研究結果を参考にしてまとめたものです.

3.2 課題の解決

$n - \varphi(n) = 10$ となる n は無いことを上の不等式を使って示そう.

$n = 8, 6, 10, 15, 27, 16$ のとき $n - \varphi(n) = 10$ とはならない. よって $n - \varphi(n) = 10$ のとき $F(n) \geq 4$ なので

$$F(n) = 10 - \sqrt{n} \geq 4.$$

よって $n \leq 6^2 = 36$.

$n \leq 36$ のとき $n - \varphi(n)$ を求めると 10 にならないことは先月号の表でわかる.

研究課題

⟨1⟩ $n - \varphi(n) = 5$ となる n を求めよ.

⟨2⟩ $n - \varphi(n) = 6$ となる n を求めよ.

⟨3⟩ $n - \varphi(n) = 7$ となる n を求めよ.

⟨4⟩ $n - \varphi(n)$ と表せない 10 より大きい数を与えよ.