東海大学紀要情報通信学部
Vol.14,No.1,2021,pp.10-16

トピックス

大学初年次における数学教材の提案（その 35）
～ 数論的関数 ～

貴田 研司[*1]

A Suggestion on Mathematical Materials for Freshman Education Vol.35
~ Number-Theoretic Function ~

by

Kenshi KIDA[*1]

(received on May. 28, 2021 & accepted on Aug. 3, 2021)

あらまし

（整）数論的関数，その中でも特にオイラーの関数とメービウスの関数を取り上げる．この 2 つの関数の基本的な性質と，それらの応用として導かれる整数論の定理について述べる．

Abstract

In this paper, we give explanation of number-theoretic functions. We present specially the Euler function and the Möbius function. Furthermore, we present several applications to number theory.

キーワード：数論的関数，オイラー関数，フェルマーの定理，メービウスの関数，ウイルソンの定理，メービウスの反転公式
Keywords: *Number-Theoretic Function, Euler Function, Fermat's Theorem, Möbius Function, Wilson's Theorem, Möbius Inversion Formula*

1. はじめに

整数全体からなる集合$\mathbb{Z}$の部分集合の上で定義された実数値，または複素数値の関数を（整）数論的関数という．本論文においては，オイラーの関数とメービウスの関数について述べる．さらに，フェルマーの定理，オイラーの定理，ウイルソンの定理についても言及する．オイラーの関数$\varphi(n)$の特徴を証明するにあたって

メービウス（Möbius）の反転公式

$$F(n)=\sum_{d|n} f(d)$$

であるならば

$$f(n)=\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)\,.$$

が重要な役割を演じることにも注目されたい．

本論文の執筆にあたって，高木貞二「初等整数論講義　第 2 版」[1]と増田真郎「応用のための代数系入門」[2]が大いに役に立った．その他にも多くの好著を参考にさせていただいた[3)4)5)6)7)]．

*1 スチューデントアチーブメントセンター
（高輪教養教育センター） 教授
Student Achievement Center
(Liberal Arts Education Center, Takanawa Campus), Professor

2. オイラーの関数

今、整数nで割ったときの余りがr であるような整数の全体をC_r で表せば

$$\mathbb{Z} = C_0 \cup C_1 \cup \cdots \cup C_{n-1}, \qquad C_i \cap C_j = \phi \ (i \neq j)$$

となる．各C_k をn を法とする剰余類と呼ぶ．

$\mathbb{Z}$において，m を法とする剰余類$C_0, C_1, \cdots, C_{m-1}$のうち$(k,m) = 1$となる$C_k$ を既約剰余類と呼び，その個数を$\varphi(m)$ で表して，これをオイラー（Euler）の関数という．

次のことが知られている．

定理 2.1

pを素数とする．

(1) eを正の整数とすると，$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

特に，$e = 1$のとき$\varphi(p) = p - 1$.

(2) $(m,n) = 1$のとき，$\varphi(mn) = \varphi(m)\varphi(n)$.

(3) 正の整数nの素因子分解が$n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$ならば

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right).$$

（(3)の証明）

${p_1}^{e_1}, {p_2}^{e_2}, \cdots, {p_s}^{e_s}$はどの 2 つをとっても互いに素だから，(2)により

$$\begin{aligned}\varphi(n) &= \varphi({p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}) \\ &= \varphi({p_1}^{e_1})\varphi({p_2}^{e_2}\cdots{p_s}^{e_s}) \\ &= \varphi({p_1}^{e_1})\varphi({p_2}^{e_2})\varphi({p_3}^{e_3}\cdots{p_s}^{e_s}) \\ &= \cdots\cdots\cdots \\ &= \varphi({p_1}^{e_1})\varphi({p_2}^{e_2})\cdots\varphi({p_s}^{e_s})\end{aligned}$$

さらに(1)を用いると

$$\begin{aligned}&= ({p_1}^{e_1} - {p_1}^{e_1-1})({p_2}^{e_2} - {p_2}^{e_2-1})\cdots({p_s}^{e_s} - {p_s}^{e_s-1}) \\ &= {p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)\end{aligned}$$

（証明終）

ところで，既約剰余類の集合は乗法を演算として群をなし，mを法とする既約剰余類群と呼ばれる．

例（既約剰余類群）

$m = 12$のとき，の中で12と互いに素な整数は1,5,7,11 の 4 つだから、12を法とする既約剰余類は

$$C_1, C_5, C_7, C_{11}$$

である．そこで，12を法とする既約剰余類群を$\{\bar{1},\bar{5},\bar{7},\overline{11}\}$と表すことにすれば，乗積表は次のようになる．

	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\overline{11}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\overline{11}$	$\bar{1}$	$\bar{5}$
$\overline{11}$	$\overline{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

そして，mを法とする既約剰余類群に次の定理を適用する．

定理 2.2（一般のフェルマー（Fermat）の定理）

有限群Gの元σの位数はG の位数$|G|$の約数であり

$$\sigma^g = 1 \qquad (g = |G|)$$

が成り立つ．

位数は$\varphi(m)$であるから

定理 2.3（オイラーの定理）

a, mを正の整数，$(a, m) = 1$とすれば

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

が成り立つ．

が得られる．特に，mが素数pの場合を考えると$\varphi(p) = p - 1$ だから

定理 2.4（フェルマーの定理）

正の整数aと素数pについて，$(a, p) = 1$すなわち $p \nmid a$であれば

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．

となる．

定理 2.4 の系（ウイルソンの定理）

素数pについて

$$(p-1)! \equiv -1 \pmod{p}$$

が成り立つ．

（証明）

pが奇素数のとき，フェルマーの定理により，$\mathbb{Z}_p$の$\bar{0}$以外の元はすべて$x^{p-1} - \bar{1}$の根になる．したがって

$$x^{p-1}-\overline{1}=(x-\overline{1})(x-\overline{2})\cdots(x-\overline{p-1})$$

と素因子分解される．ここで，$x=\overline{0}$を代入すれば

$$-\overline{1}=(-\overline{1})(-\overline{2})\cdots(-\overline{p-1})$$

$$-\overline{1}=(-1)^{p-1}\cdot\overline{1}\cdot\overline{2}\cdot\cdots\cdot\overline{p-1}$$

$$-\overline{1}=\overline{1}\cdot\overline{2}\cdot\cdots\cdot\overline{p-1}$$

$$\overline{-1}=\overline{(p-1)\,!}$$

すなわち

$$(p-1)\,!\equiv-1\pmod{p}$$

が得られる．

$p=2$のとき，$1\equiv-1\pmod{2}$ は明らかに成り立つ．

（証明終）

一方，nの任意の約数をdとするとき，n個の数$1,2,3,\cdots,n$の中に$(x,n)=d$ であるxはいくつあるかを考える．

例えば，$n=15$のすべての約数dは$1,3,5,15$であり，15個の数$1,2,3,4,5,6,7,8,9,10,11,12,13,14,15$の中に$(x,15)=d$ であるxはいくつあるかを考えると，次のようになる．

d	x	個数	$\varphi\left(\frac{n}{d}\right)$
1	1,2,4,7,8,11,13,14	8	$\varphi\left(\frac{15}{1}\right)=\varphi(15)=\varphi(3\cdot5)=\varphi(3)\varphi(5)=(3-1)(5-1)=8$
3	3,6,9,12	4	$\varphi\left(\frac{15}{3}\right)=\varphi(5)=5-1=4$
5	5,10	2	$\varphi\left(\frac{15}{5}\right)=\varphi(3)=3-1=2$
15	15	1	$\varphi\left(\frac{15}{15}\right)=\varphi(1)=1$

これについて

$$\varphi\left(\frac{15}{1}\right)+\varphi\left(\frac{15}{3}\right)+\varphi\left(\frac{15}{5}\right)+\varphi\left(\frac{15}{15}\right)=\varphi(15)+\varphi(5)+\varphi(3)+\varphi(1)=8+4+2+1=15$$

が成り立つことがわかる．

nのすべての正の約数を$1,d_1,d_2,\cdots,d_t,n$とするとき

$$\frac{n}{1},\frac{n}{d_1},\frac{n}{d_2},\cdots,\frac{n}{d_t},\frac{n}{n}$$

も，nのすべての正の約数であることに留意して，上記のことを一般化すると，次の結果が得られる．

定理 2.5

正の整数 nに対して

$$\sum_{d|n}\varphi(d)=n$$

が成り立つ．ただし，和はn のすべての正の約数dにわたることを意味する．

3. メービウスの関数

正の整数 mに対して

$$\mu(m)=\begin{cases}1 & \cdots \quad m=1\\ (-1)^r & \cdots \quad m=p_1p_2\cdots p_r\ (p_i\ \text{は}m\text{の相異なる素因子})\\ 0 & \cdots \quad p^2|m\ (p\ \text{は}m\text{の素因子})\end{cases}$$

によって定義される数論的関数 $\mu(m)$を，メービウス（Möbius）の関数という．

例

(1) $\mu(12870)=\mu(2\cdot3^2\cdot5\cdot11\cdot13)=0$

(2) $\mu(4641)=\mu(3\cdot7\cdot13\cdot17)=(-1)^4=1$

(3) $\mu(33915)=\mu(3\cdot5\cdot7\cdot17\cdot19)=(-1)^5=-1$

また，次のことが知られている．

定理 3.1

(1) $(m,n)=1$のとき，$\mu(mn)=\mu(m)\mu(n).$

(2) $\mu(1)=1.$

(3) 正の整数 nに対して

$$\sum_{d|n}\mu(d)=0.$$

定理 3.2（メービウス（Möbius）の反転公式）

$f(n)$，$F(n)$ が，正の整数に関する関数で，これらの間に関係式

$$F(n)=\sum_{d|n}f(d)$$

が成り立つならば

$$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$$

が成り立つ．

4. オイラーの関数$\varphi(n)$の特徴

第 2 章で述べた定理 2.5 は，オイラーの関数$\varphi(n)$の特徴である．$\varphi(n)$の他には定理 2.5 の性質をもつ数論的関数は存在しない．言い換えると，数論的関数$\psi(n)$について，すべての正の整数にn対して

$$\sum_{d|n}\psi(d)=n$$

であるならば，$\psi(n)=\varphi(n)$である．これを証明するためには

$$\sum_{d|n}\psi(d)=n$$

から

$$\psi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)=\varphi(n)$$　　ただし，nの素因子分解が$n={p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$

となることを導けばよい．

第 3 章で述べた，定理 3.2（メービウス（Möbius）の反転公式）において

$$F(n)=\sum_{d|n}\varphi(d)$$

とおけば，$F(n)=n$であるから

$$\varphi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)d$$

が成り立つ．ここで

$$\frac{n}{d}=k\ \Leftrightarrow\ d=\frac{n}{k}$$

とおけば，nのすべての正の約数を$1,d_1,d_2,\cdots,d_t,n$とするとき

$$\frac{n}{1},\frac{n}{d_1},\frac{n}{d_2},\cdots,\frac{n}{d_t},\frac{n}{n}$$

も，nのすべての正の約数である．よって，変数の置き換えを行うと

$$\varphi(n)=\sum_{k|n}\mu(k)\frac{n}{k}$$

となる．$n={p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$とすれば，$\mu(k)=0$となるものを除いて表記すれば

$$\begin{aligned}\varphi(n)=&\mu(1)\cdot\frac{n}{1}+\mu(p_1)\cdot\frac{n}{p_1}+\mu(p_2)\cdot\frac{n}{p_2}+\cdots+\mu(p_s)\cdot\frac{n}{p_s}\\&+\mu(p_1p_2)\cdot\frac{n}{p_1p_2}+\mu(p_1p_3)\cdot\frac{n}{p_1p_3}+\cdots+\mu(p_{s-1}p_s)\cdot\frac{n}{p_{s-1}p_s}\\&\cdots\cdots\\&+\mu(p_1p_2\cdots p_s)\cdot\frac{n}{p_1p_2\cdots p_s}\end{aligned}$$

$$= n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_s}\right) + n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots + \frac{1}{p_{s-1} p_s}\right)$$

$$\cdots\cdots\cdots$$

$$+(-1)^s \cdot n \cdot \frac{1}{p_1 p_2 \cdots p_s}$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)$$

が得られる．

これにより次の結果が得られる．

定理 4. 1

すべての正の整数nの上で定義された数論的関数$\psi(n)$について

$$\psi(n) = \varphi(n), \qquad n \in \mathbb{N}$$

であることと，任意の正の整数 nに対して，dが nのすべての正の約数を動くとき

$$\sum_{d|n} \psi(d) = n$$

が成り立つこととは同値である．

参考文献

1）高木貞二「初等整数論講義　第2版」共立出版，1971
2）増田真郎「応用のための代数系入門」サイエンス社，1981
3）服部昭「現代代数学」朝倉書店，1968
4）横井英夫，硲野敏博共著「代数演習[新訂版]」サイエンス社，2003
5）永尾汎「代数学」朝倉書店，1983
6）服部昭「現代代数学演習」朝倉書店，1969
7）浅野重初「代数学I　基礎概念・環・加群」森北出版，1973