原始根，標数の性質
(等差数列上のEulerの$\frac{\varphi(td)}{\varphi(d)}$の応用)
Some Properties
of
Primitive Roots and Indices
(Application of Euler's Totient Function $\frac{\varphi(td)}{\varphi(d)}$ on Arithmetical Progressions)

中嶋眞澄
Masumi NAKAJIMA
Department of Economics
International University of Kagoshima
Kagoshima 891-0197, JAPAN
e-mail: nakajima@eco.iuk.ac.jp

概 要

Abstract

We prove here some properties of primitive roots and indices in Elementary Number Theory by applying Euler's totient function $\frac{\varphi(td)}{\varphi(d)}$ on arithmetical progressions [3].

Key words ; primitive roots, indices.

Mathematics Subject Classification ; 11A07.

以下アルファベット文字は自然数か整数を表わす。

Fermat の (小) 定理：

p を素数として，$(a,p)=1$ の場合，$a^{p-1}\equiv 1 \pmod{p}$
が成り立つ．

から

p を素数として，$(a,p)=1$ の場合，
$a^x \equiv 1 \pmod{p}$
となる $x \in \mathbf{N}$ が存在する．

ことが分かる。これより

定義 1

p を素数として，$(a,p)=1$ の場合，
$a^e \equiv 1 \pmod{p}$
となる最小の $e \in \mathbf{N}$ を mod p に関する a の位数 (ベキ数) と云う．

定義 2

p を素数として，$(a,p)=1$ の場合，a の位数 (ベキ数) が $p-1$ となる a を素数 p の原始根 **primitive root** と云う．

注 mod p (p は素数) に関する相異なる原始根は全部で $\varphi(p-1)$ 個存在する。

注 a^n，$(n \geq 2)$ は $p \equiv 1 (\mathrm{mod}\ n)$ なる素数 p の原始根には成り得ない。
これより，(完全) 平方数は原始根に成り得ない。

定義 3

p を素数として，$(a,p)=1$ の場合，g を素数 p の原始根とするとき，
$g^x \equiv a \pmod{p}$ となる x を原始根 g を底とする a の標数 **index** と云って $\mathrm{Ind}_g a$ 又は $\mathrm{Ind}\ a$ と表わす。

注 任意の a に対して $\mathrm{Ind}_g a$ は存在する。

補題 1

mod p に関して a の位数 (ベキ数) が $e \Longleftrightarrow e = \dfrac{p-1}{(\mathrm{Ind}\ a, p-1)}$

証明省略.

補題 2

$$\sum_{x<n;(x,n)=d} x = \frac{n}{2}\varphi(\frac{n}{d}).$$

証明　$(x,n)=d \Longleftrightarrow (n-x,n)=d$ と

$$\sum_{x<n;(x,n)=d} 1 = \varphi(\frac{n}{d})$$

に注意すると

$$2\sum_{x<n;(x,n)=d} x = \sum_{x<n;(x,n)=d} \{x+(n-x)\} = n\sum_{x<n;(x,n)=d} 1 = n\varphi(\frac{n}{d})$$

を得る。□

定理 1

p が素数として，位数 e に関する自然数 a の Ind a の総和は

$$\sum_{a;\ (\mathrm{Ind}\ a,\ p-1)=(p-1)/e} \mathrm{Ind}\ a = \frac{(p-1)\varphi(e)}{2}.$$

証明

補題 1 より $(\mathrm{Ind}\ a,\ p-1)=(p-1)/e$。故に補題 2 を使って

$$\sum_{a;\ (\mathrm{Ind}\ a,\ p-1)=(p-1)/e} \mathrm{Ind}\ a = \sum_{x;\ (x,\ p-1)=(p-1)/e} x = \frac{(p-1)\varphi(e)}{2}.\quad \square$$

補題 3

g が素数 $p\equiv 1 \pmod 4$ の原始根ならば，$-g \equiv p-g \pmod p$ も原始根である.

証明省略.

補題 4

$p\equiv 1 \pmod 4$ の最小原始根を g_0，最大原始根を G_0 とすると，

$$g_0 \le \frac{p-1}{2} - \frac{\varphi(p-1)}{2} + 1,\ G_0 \ge \frac{p-1}{2} + \frac{\varphi(p-1)}{2}.$$

証明

pの原始根は全部で$\varphi(p-1)$個あり，補題4から1から$p-1$の間に$\dfrac{p-1}{2}$に関して対称に分布する事から従う。□

定理2

素数pの相異なる原始根を$g_1, g_2, \cdots, g_{\varphi(p-1)}$とすると，
任意の自然数$a \neq 1$に対して
$$\sum_{k=1}^{\varphi(p-1)} \mathrm{Ind}_{g_k} a = \frac{(p-1)\varphi(p-1)}{2}$$
が成り立つ。

証明 定理2の証明として後に行う。

定理3

素数pの相異なる原始根を$g_1, g_2, \cdots, g_{\varphi(p-1)}$とすると$(p \neq 2, 3)$，
$g_1 g_2 \cdots g_{\varphi(p-1)} \equiv 1 \pmod{p}$

証明

gをpの原始根の一つとすると
$g_1 g_2 \cdots g_{\varphi(p-1)} \equiv g^{\mathrm{Ind}(g_1 g_2 \cdots g_{\varphi(p-1)})} \pmod{p} \cdots (*)$
が成り立つ。
一方，
$\mathrm{Ind}(g_1 g_2 \cdots g_{\varphi(p-1)}) \equiv \mathrm{Ind} g_1 + \mathrm{Ind} g_2 + \cdots + \mathrm{Ind} g_{\varphi(p-1)} \pmod{p-1}$
$= \dfrac{(p-1)\varphi(p-1)}{2}$（$g_k$の位数は$p-1$として定理1を使った。）
$\equiv 0 \pmod{p-1}$（$\varphi(p-1)$は偶数である事を使った。）
従って，$n_0 \in \mathbf{N}$が存在して
$(*) \equiv g^{n_0(p-1)} \equiv 1 \pmod{p}$. □

定理2の証明

次の事を証明すれば十分である。

補題5

(i) 自然数 a が位数 e に属すと，$\mathrm{Ind}_{g_k}a$ は g_k が p の全原始根を動くとともに，位数 e に属す自然数 a の標数 Ind 全ての値を取る事が出来る。即ち，位数 e に属す自然数を，(a も含めて)$a_1, a_2, \cdots, a_{\varphi(e)}$ とすると，原始根 g を固定した集合 $S = \{\mathrm{Ind}_g a_1, \mathrm{Ind}_g a_2, \cdots, \mathrm{Ind}_g a_{\varphi(e)}\}$ と a を固定した集合 $S' = \{\mathrm{Ind}_{g_1} a, \mathrm{Ind}_{g_2} a, \cdots, \mathrm{Ind}_{g_{\varphi(p-1)}} a_{\varphi(e)}\}$ に対して $S = S'$ が成立する。但し，$\{1,3,2,1,1,3\} = \{1,2,3\}$ 等とする。
(ii) $\mathrm{Ind}_{g_k}a$ $(k = 1, 2, \cdots, \varphi(p-1))$ が取る値は $\mathrm{Ind}_g a_1, \mathrm{Ind}_g a_2, \cdots, \mathrm{Ind}_g a_{\varphi(e)}$ だが，それらは同数個現れる。(勿論，(i) と同様に $a_1, a_2, \cdots, a_{\varphi(e)}$ は位数 e に属し，a は $a_1, a_2, \cdots, a_{\varphi(e)}$ のどれかである。)即ち，$\mathrm{Ind}_{g_k}a = \mathrm{Ind}_g a_i$ $(i = 1, 2, \cdots, \varphi(e))$ なるが g_k は，$\frac{\varphi(p-1)}{\varphi(e)}$ 個ある。但し，$a_i \not\equiv a \pmod p$ である。

例：定理 2 と補題 5　$p = 13$ とすると，原始根は $2, 6, 7, 11$ の $4 = \varphi(12)$ 個である。

g_k \ a	1	2	3	4	5	6	7	8	9	10	11	12
2	0	1	4	2	9	5	11	3	8	10	7	6
6	0	5	8	10	9	1	7	3	4	2	11	6
7	0	11	8	10	3	7	1	9	4	2	5	6
11	0	7	4	2	3	11	5	9	8	10	1	6
$\sum_{k=1}^{4} \mathrm{Ind}_{g_k}a$	0	24	24	24	24	24	24	24	24	24	24	24
a の位数 e	/	12	3	6	4	12	12	4	3	6	12	2

証明　$a = 3$ を例に取ると，定理 2 の式は表 table を縦に加えて和 24 を出すものであるが，補題 5 を使えば，$a = 3$ と同じ位数を持つ $a = 9$ を考えて横に加え，その重複度 (補題 5,(ii)) を適用すれば，同様に和 24 を出す事が出来る。補題 5 を証明すれば補題 2 により，

$$\sum_{k=1}^{\varphi(p-1)} \mathrm{Ind}_{g_k}a = \frac{\varphi(p-1)}{\varphi(e)} \sum_{(\mathrm{Ind}a, p-1) = \frac{p-1}{e}} \mathrm{Ind}a = \frac{\varphi(p-1)}{\varphi(e)} \frac{p-1}{2} \varphi(e)$$

となり，定理 2 が証明される。従って補題 5 が証明されれば良い。□
補題 **5** $\Longleftrightarrow$ 次の補題 **6**　は明らかである。

補題 6
方程式

$$\mathrm{Ind}_{g_k}a = \mathrm{Ind}_g a_i \ (g_k \not\equiv g \pmod p, a \not\equiv a_i \pmod p)$$

の解 g_k は存在し，その個数は $\frac{\varphi(p-1)}{\varphi(e)}$ 個である。但し，e は a の位数である。

証明　標数の良く知られた性質により，

$$\mathrm{Ind}_g a \equiv \mathrm{Ind}_g a_i \mathrm{Ind}_g a_k (\mathrm{mod}\ p-1),$$
$$(\mathrm{Ind}_g a, p-1) = (\mathrm{Ind}_g a_i, p-1) = \frac{p-1}{e} = d,$$
$$(\mathrm{Ind}_g g_k, p-1) = 1$$

であるから，

$$\mathrm{Ind}_g a =: B,\quad \mathrm{Ind}_g a_i =: A,\quad \mathrm{Ind}_g g_k =: x,\quad p-1 =: m$$

と置けば**補題６**は次の**補題７**に帰着する。□

補題７

$$Ax \equiv B\ (\mathrm{mod}\ m),\ (A,m) = (B,m) = d\ \text{の}\ (x,m) = 1\ \text{なる解}\ x$$

の個数は

$$\frac{\varphi(m)}{\frac{\varphi(m}{d)}}$$

個である。**証明**　$A = da,\ B = db,\ m = dm_0$ とすると $(a, m_0) = (b, m_0) = 1$ で $ax \equiv b\ (\mathrm{mod}\ m_0)$ の解 x は唯１つしかなく，それを x_0 とすると $(x_0, m_0) = 1$ である。故に $Ax \equiv B\ (\mathrm{mod}\ m)$ の解は $x_0, x_0 + m_0, x_0 + 2m_0, \cdots, x_0 + (d-1)m_0$ である。$(x_0, m_0) = 1$ より $(x_0 + km_0, m_0) = 1$ である。故に $(x, m) = 1$ なる解を調べる事に帰着する。よって次の**定理４**が証明されれば、**定理２**の証明は完了する。□

定理４　[3]

$$\sharp\{k \mid (a+kd, t) = 1,\ (k = 1, 2, \cdots, t),\ (a, d) = 1\} = \frac{\varphi(td)}{\varphi(d)}$$

注 補題７の $x_0 \to a,\ m_0 \to d,\ d \to t$ と書き換えた。

証明　[3] を参照せよ。□

これで**定理２の証明は完了した。**□

幾つかの予想 Some Conjectures

予想 1Cojecture 1

任意の素数 $p(\geq 5)q(\geq 2)$ に対して

$$p = \frac{r-1}{\mathrm{Ind}q \cdot r - 1}$$

となる素数 r が存在する。但し Ind$q$ は r に関するものである。
注　これは、奇数の完全数 odd perfect number と関係する。
予想 2Cojecture 2
任意の素数 p の原始根のうち，半数は $\geq \frac{p-1}{2}+1$ である。
予想 3Cojecture 3
g, g' をある素数の二つの原始根とすると

$$\mathrm{Ind}_g g' = \mathrm{Ind}_{g'} g$$

となる。但し，g' は g のベキでないとする。

参考文献

[1] 北村泰一 Kitamura,T.『数論入門 (改訂版)』*Introduction to Number Theory,* (in Japanese), revised ed., 槇書店 Maki-Shoten, 1986(1965 1st ed.), (v+160)pp..

[2] Vinogradov,I.M.，三瓶与右衛門，山中健訳:『整数論入門』共立出版，1959, (iii+202)pp.. *Introduction to Number Theory* (Japanese translation)，Kyouritsu-Shuppan, Tokyo.

[3] 中嶋眞澄 Nakajima,M.: 等差数列上の Euler 関数，Euler's Totient Function $\varphi(n)$ on Arithmetical Progressins, 鹿児島経済論集，第 62 巻 1 号, 2021 年 7 月, 1-6, *The Kagoshima Journal of Economics,* **62**, July 2021, 1-6.

(received 26 January 2022.)