

原始根について

中等教育教員養成課程 数学専攻 齋藤 宏紀

本論文の目標は原始根定理の証明, 及び, 原始根の性質を見つけその証明をすること. また, 見つけた性質を基にある素数に対する原始根すべてを簡単に求める方法を見つけることにある. 原始根とは以下で定義されるものである.

定義 3.  $p$  を素数とし,  $g < p, g \in \mathbb{N}$  とする. このとき,  $p$  を法とした  $g$  の位数が  $p-1$  であれば,  $g$  を  $p$  を法とした原始根と言う.

また, 原始根定理とは次のものである.

定理 1 (原始根定理). 任意の素数  $p$  は原始根をもつ. さらに,  $p$  を法とした原始根は  $\varphi(p-1)$  個ある. 但し,  $\varphi$  はオイラー関数を表す.

1 節では原始根について考える上で必要となるオイラー関数についての定義, 命題を紹介し証明する. そして, 2 節では原始根, 及び, 原始根定理の紹介と, 原始根定理を証明する上で必要となる命題, 補題の証明を行う. これらを基にして 3 節に原始根定理の証明を行う. 4 章では, 原始根の性質を見つけそれを証明することと, 見つけた性質を基に原始根を求める時間を短縮する方法の考察を行う. 原始根の性質については, 原始根の表から法則性を見出し, 群論を利用して証明した. また, コンピュータを用いて素数  $p$  に対し 1 から  $p-1$  までの位数を調べ原始根を求める方法と, 4 節で証明した原始根の性質を基に原始根を求める方法をプログラミングし, それぞれで原始根を計算するのにかかる時間を計り表にした. その結果を基に, それぞれのプログラムの計算量が何に依存するかについての考察をした. なお, プログラムは計算ソフト BASIC.Ink によって作成した.

今後の課題は, ある素数に対してその原始根 1 つを特定することである. 1 つの原始根を特定することができれば, 4 節で使った方法を用いることにより, ある素数に対してその原始根すべてを求める時間を大幅に短縮することができるからである. また, これに関連して有名な未解決問題がある.

問題. 2 を原始根にもつ素数には, どのような法則があるか.

この問題に向けて研究していきたいと考える.