令和元年度卒業研究概要

原始根の存在と考察

中等教育教員養成課程　数学専攻　榊原 康太朗

本論文では, 原始根についての研究を行った. 原始根とは, 素数 p に対し, 次で定義される整数である.

定義 4. $g \in \mathbb{Z}\,(1 \leq g \leq p-1)$ に対し, $\overline{g}$ が $\mathbb{F}_p^{\times}$ の位数 $p-1$ の元であるとき, g を p の原始根という.

原始根を用いることで, $\mathbb{F}_p^{\times}$ の元を 1 つの数字のみを使って表すことができる. 例えば, $\mathbb{F}_5^{\times}$ は原始根として $g=2$ とすれば,

$$\mathbb{F}_5^{\times} = \{\overline{2}, \overline{2}^2, \overline{2}^3, \overline{2}^4\}$$

と表される.

本論文の主結果は次である.

定理 1. 任意の素数 p に対して, $\mathbb{F}_p^{\times}$ には原始根が存在する.

定理 1 から, 原始根の存在が示される. この定理を基にして, 1 つ原始根が見つかっているときのその他の原始根の見つけ方に関する次の定理を発見し, 証明した.

定理 2. g を p の原始根とする. このとき, $\overline{g}^{-1} = \overline{t}$ となる $t \in \mathbb{Z}\,(1 \leq t \leq p-1)$ に対し, t は p の原始根となる.

定理 3. g を p の原始根とし, $m \in \mathbb{Z}$ とする. このとき, $\overline{g}^m = \overline{t}$ となる $t \in \mathbb{Z}\,(1 \leq t \leq p-1)$ に対し,

$$t : p \text{の原始根} \iff (m, p-1) = 1.$$

定理 2, 定理 3 から, 原始根の個数に関する次の定理を得る.

定理 4. p の原始根の個数は, $p-1$ と互いに素な $p-1$ 以下の整数の個数と等しい.

また, 2 に注目して, 2 が原始根にならないための 1 つの十分条件を与える.

定理 5. 素数 p が $p \equiv \pm 1 \pmod 8$ をみたすとき, 2 は p の原始根とならない.

本論文の最後に, 2 つの表を与える. 1 つ目は, $2 \leq p \leq 31$ をみたす素数 p の原始根をすべて挙げたものである. この表から定理 2, 定理 3 を発見した. 2 つ目は, $37 \leq p \leq 211$ をみたす素数 p の原始根の小さいほうから 3 つを挙げたものである. この表から 2 が原始根となる場合とならない場合を整理することで規則性を見つけ, 定理 5 を発見した.