平成２９年度卒業研究概要

ウィルソンの定理とその拡張

初等教育教員養成課程　数学選修　平子 航

本論文の目標は, 次に述べる素数に対するウィルソンの定理を自然数へ拡張することである.

定理 1 (**ウィルソンの定理**)**.** 素数 p に対して,

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

が成り立つ.

ウィルソンの定理は素数判定法の一つとして知られている定理である. その証明は複数存在しており, 最初の証明は 1773 年に, ラグランジュによって示された. 本論文では, ラグランジュの証明と同じ方法である 1 次合同式 $ax \equiv 1 \pmod{p}$ の解の性質と, $x^2 \equiv 1 \pmod{p}$ の解が $x \equiv \pm 1 \pmod{p}$ のみであることを用いた証明を行った.

また, ウィルソンの定理の拡張のために, 次を定義した.

定義. $m \in \mathbb{N},\ m \geq 3$ に対し, 集合 U_m を

$$U_m := \{a \in \mathbb{N} \,|\, 1 \leq a < m,\ (a, m) = 1\}$$

と定義する. また, $\varphi(m) := |U_m|$ とおき, U_m の元を $b_1, \ldots, b_{\varphi(m)}$ $(1 \leq b_1 < \cdots < b_{\varphi(m)} < m)$ と表す. さらに, U_m の部分集合 A_m を

$$A_m := \{a \in U_m \,|\, a^2 \equiv 1 \pmod{m}\}$$

と定義する.

このとき, 次が成り立つ.

定理 2. 上記の記号の下,

$$b_1 \cdots b_{\varphi(m)} \equiv \begin{cases} -1 \pmod{m} & (|A_m| \equiv 2 \pmod{4}), \\ 1 \pmod{m} & (|A_m| \equiv 0 \pmod{4}). \end{cases}$$

さらに, 本論文では集合 A_m の性質を考察することで, 定理 2 を次のように書きかえることができた.

主定理. 上記の記号の下,

$$b_1 \cdots b_{\varphi(m)} \equiv \begin{cases} -1 \pmod{m} & (m = 4, p^r, 2p^r\ (p : \text{奇素数},\ r \geq 1) \text{ の形}), \\ 1 \pmod{m} & (\text{それ以外}). \end{cases}$$