平成２５年度卒業研究概要

素数の判定法について

中等教育教員養成課程　数学専攻　田村 太志

素数はだれしも中学のときには勉強して知っているにもかかわらず, 多くの人はその知識を名前のみにとどめている. 素数に関する未解決問題として, 第 n 番目の素数を見つける関数や, 第 n 番目と第 $n+1$ 番目の素数の関係の漸化式のように素数を見つける簡単な手段はいまだに見つかっていない. 素数を見つけ出す手段がないことに私は興味深いと感じたため, 素数の判定法を本論文のテーマとした.

主定理は次である.

定理 1. p を奇素数, $h \in \mathbb{Z}_{>0},\ h < p,\ b = 1$ または $b = 2$ とし, $n = hp^b + 1$ とおく. このとき,

$$2^h \not\equiv 1 \pmod{n},\ 2^{n-1} \equiv 1 \pmod{n} \Longrightarrow n \text{ は素数.}$$

定理 2. $m \in \mathbb{Z},\ 2 \leq m,\ h < 2^m$ とし, $n = h2^m + 1$ とおく. また, n がある奇素数 p の平方非剰余であるとする. このとき,

$$n \text{ が素数} \Longleftrightarrow p^{(n-1)/2} \equiv -1 \pmod{n}.$$

定理 3. p を $p = 4k + 3\ (k \geq 0)$ の形の素数とする. このとき,

$$2p + 1 \text{ が素数} \Longleftrightarrow 2^p \equiv 1 \pmod{2p+1}.$$

よって, $2p + 1$ が素数ならば, $2^p - 1$ は $2p + 1$ を約数にもつ. 特に, $k \geq 1$ で $2p + 1$ が素数ならば $2^p - 1$ は合成数となる.

定理 3 の素数 p に関する条件である “$p = 4k + 3$ の形” を, “$p = 4k + 1$ の形” という条件に変えた場合について考えた結果, 次が得られた.

定理 4. p を $p = 4k + 1\ (k \geq 1)$ の形の素数とする. このとき,

$$2p + 1 \text{ が素数} \Longleftrightarrow 2^p \equiv -1 \pmod{2p+1}.$$

よって, $2p + 1$ が素数ならば, $2^p + 1$ は $2p + 1$ を約数にもつ.

この定理は, 定理 3 とほぼ同様の手順で証明される.

本論文の構成は次の通りである. 第 1 節ではこの論文のための基礎的な準備を行い, 第 2 節において平方剰余, 平方非剰余の定義およびルジャンドル記号の定義をする. 第 3 節では上記定理 1, 2, 3 を証明し, 第 4 節で定理 4 の証明を与える.