平成２７年度卒業研究概要

メルセンヌ数の素数判定について

中等教育教員養成課程　数学専攻　吉田 紗季

本論文では, メルセンヌ数の素数判定を可能にしているリュカ・テストという定理を証明することを目標としている. メルセンヌ数とは $M_n = 2^n - 1$ の形で表される数である. 特に, これが素数となるときメルセンヌ素数と呼ばれる. リュカ・テストは次のような定理である.

定理 (リュカ・テスト). p を $p \equiv 3 \pmod 4$ を満たす素数とする. このとき, メルセンヌ数 M_p に対して, 次が成り立つ:

$$M_p \nmid S_k \ (1 \leq {}^{\forall}k \leq p-1) \Rightarrow M_p\text{は合成数},$$
$$M_p \mid S_{p-1} \Rightarrow M_p\text{は素数}.$$

ただし, $\{S_n\}$ は $S_1 = 3,\ S_{n+1} = S_n^2 - 2\ (n \geq 1)$ で定められる数列とする.

リュカ・テストの証明には, フィボナッチ数とフィボナッチ数に似たリュカ数という数が使われるが, 本論文では, フィボナッチ数, リュカ数の性質は証明なしに用いることとした.

更にリュカ・テストの証明には, 次の命題を必要とする.

命題 18. 奇素数 $p\ (\neq 5)$ に対して次が成り立つ:

$$5^{\frac{p-1}{2}} \equiv 1 \pmod p \Leftrightarrow p \equiv \pm 1 \pmod 5,$$
$$5^{\frac{p-1}{2}} \equiv -1 \pmod p \Leftrightarrow p \equiv \pm 2 \pmod 5.$$

この整数論の命題は平方剰余の相互法則を用いて示される. 本論文では, ガウス和を用いる方法で平方剰余の相互法則を証明した後, 上記命題を示し, 最後にリュカ・テストの証明を行う.

尚, リュカが 1878 年に証明を与えた上記リュカ・テストは p を $p \equiv 3 \pmod 4$ を満たす素数に限定しているが, その後何人もの人によって手が加えられ, 現在では次のような定理に整理されている.

定理. p が素数のとき,

$$M_p \mid S'_{p-1} \Leftrightarrow M_p\text{は素数}.$$

ただし, $\{S'_n\}$ は $S'_1 = 4,\ S'_{n+1} = {S'_n}^2 - 2\ (n \geq 1)$ で定められる数列とする.