令和２年度卒業研究概要

フェルマー数の性質とその素数判定法

中等教育教員養成課程　数学専攻　葛島 昌利

本論文では, フェルマー数と呼ばれる数に対して, その性質と素数性について考察することを目的としている. フェルマー数およびフェルマー素数は次のように定義される数である.

定義 1. $m \in \mathbb{Z}_{\geq 0}$ に対し, $F_m = 2^{2^m} + 1$ をフェルマー数という.

定義 2. $m \in \mathbb{Z}_{\geq 0}$ に対し, $F_m = 2^{2^m} + 1$ が素数となるとき, F_m をフェルマー素数という.

フェルマー数の性質として, 次を示した.

命題 1. フェルマー数は以下の漸化式で表すことができる:

$$F_0 = 3,$$
$$F_m = F_0F_1F_2 \cdots F_{m-1} + 2 \ (m \geq 1).$$

命題 2. 相異なる $m,\ n \in \mathbb{Z}_{\geq 0}$ に対し, F_m と F_n は互いに素である.

定理 2. p を素数としたとき, $p \mid F_m$ ならば, $p \equiv 1 \pmod{2^{m+1}}$ が成り立つ.

命題 1, 命題 2 を用いて, 素数の無限性を導くことができる. また, 定理 2 を用いて, F_m の素数性が判定できる. 具体的には, 定理 2 により, F_m の素因数の候補 $p_1, p_2, \ldots, p_n$ をリストアップすることができる. その中の 1 つ p_k が F_m を割り切るならば, F_m は合成数となり, 当然 p_k が F_m の素因数となる. また, $p_1, p_2, \ldots, p_n$ のすべてが F_m を割り切らないならば, F_m が素数であるということが断定できる.

さらに, 定理 2 に基づいたプログラムを組み, PARI/GP という計算機を用いて, 実際に $5 \leq m \leq 10$ における F_m に対して, それら素数となるかどうか, またどのように素因数分解されるのかを調べた. そして, 何度かプログラムを変えて実験していく中で, 定理 2 を改良した次の定理を発見した.

定理 3. $m \in \mathbb{Z}_{\geq 2}$ とする. p を素数としたとき, $p \mid F_m$ ならば, $p \equiv 1 \pmod{2^{m+2}}$ が成り立つ.

残念ながら, F_7, F_8, F_9, F_{10} の素因数分解はできなかった. 定理 2, 定理 3 のさらなる改良, および新たなプログラムの作成は, 今後の研究の課題としたい.