平成２４年度卒業研究概要

二つの平方数の和で表される数

中等教育教員養成課程　数学専攻　植田 史郎

本論文の目標は, 二つの平方数の和で表される数が, どのような数であるかを与えることである. 二つの平方数の和で表される数とは, 整数 a, b に対し, $m = a^2 + b^2$ の形で表される自然数 m のことである. この問題を, まず m が素数の場合について, 次に m が正の整数の場合について考察する. 具体的には, 以下の二つの定理を証明する.

定理 1. 素数 p に対し,

$$p \text{ が二つの平方数の和で表される} \iff p \equiv 1 \pmod 4 \text{ または } p = 2.$$

定理 2. 平方数でない自然数 m に対し, $m = p_1 p_2 p_3 \cdots p_r M^2$ (p_i : 異なる素数, $M \in \mathbb{N}$) と分解したとする. このとき,

$$m \text{ が二つの平方数の和で表される} \iff \text{各 } p_i \text{ は } p_i = 2 \text{ または } p_i \equiv 1 \pmod 4.$$

これらの定理は, 主に平方剰余を用いて証明される.

主定理の証明の準備として, まず 1 節では, 原始根の定義をし, 原始根についての性質を述べる. 次に 2 節では, 平方剰余の定義及び, 平方剰余に関する性質, 定理について述べる. そして, 3 節では定理 1 の, 4 節では定理 2 の証明を行う.

また, 本論文の最後に, 二つの平方数で表される数の, 表し方の個数について考察をした. いくつかの計算により, 次の予想を得た.

予想. 平方数でない自然数 m の二つの平方数の和での表し方の個数を $\psi(m)$ とする. また, p_i, q を $p_i \equiv q \equiv 1 \pmod 4$ を満たす相異なる素数とし, M を 4 を法として 1 と合同な素数を含まない自然数, a を $a \notin \mathbb{Z}^2 \cup 2\mathbb{Z}^2$ を満たす自然数とする. このとき次が成り立つ:

$$\begin{aligned}
\psi(a) = \psi(2a) &= \psi(aM^2), \\
\psi(2) = \psi(2M^2) &= 1, \\
\psi(p_1 p_2 \cdots p_r) &= 2^{r-1}, \\
\psi(p_1 p_2 \cdots p_r p_i^2) &= 2^r, \\
\psi(p_1 p_2 \cdots p_r q^2) &= 3 \cdot 2^{r-1}.
\end{aligned}$$

今回の卒業論文では, この予想を証明することはできなかったが, 今後の課題として取り組んでいきたい.