令和 7 年度卒業研究概要

ガウスの補題とその応用

学校教員養成課程　義務教育専攻　算数・数学専修　馬場 悠輔

本論文では, 奇素数 p に関する平方剰余と平方非剰余について扱う. 平方剰余とは, ある整数が「平方の形」で表されるかどうかを表す概念であり, 整数の性質を調べる上で重要な役割をもつ.

定義 2 (**平方剰余, 平方非剰余**)**.** p を奇素数とする. $a \in \mathbb{Z},\ p \nmid a$ に対して,

$$x^2 \equiv a \pmod{p}$$

が解をもつとき a を p の平方剰余といい, 解をもたないとき a を p の平方非剰余という.

ある整数 a が奇素数 p の平方剰余かどうかを判断する方法の 1 つにガウスの補題がある.

定理 1 (**ガウスの補題**)**.** p を奇素数とする. $m \in \mathbb{Z},\ p \nmid m$ に対し,

$$m, 2m, 3m, \ldots, (p-1)m/2$$

の中で p を法とする最小の正の剰余が $p/2$ より大きい数の個数を μ とする. このとき,

$$\left(\frac{m}{p}\right) = (-1)^{\mu}$$

が成り立つ.

ここで, (m/p) は次で定義されるルジャンドル記号である.

定義 3 (**ルジャンドル記号**)**.** p を奇素数とする. $a \in \mathbb{Z},\ p \nmid a$ に対して, ルジャンドル記号 (a/p) を

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ は } p \text{ の平方剰余}) \\ -1 & (a \text{ は } p \text{ の平方非剰余}) \end{cases}$$

と定める.

ガウスの補題により, μ の値が偶数か奇数かによって, ある整数が奇素数 p の平方剰余か平方非剰余かを判定することができる.

本論文の前半はガウスの補題を証明し, 具体的に $2, -3, 5$ がどのような素数の平方剰余または平方非剰余になるかを調べる. 後半では, これらの結果から得られる規則性に着目し, それを一般化した定理を与える.