令和４年度卒業研究概要

平方剰余と平方非剰余の和および個数についての考察

中等教育教員養成課程　数学専攻　岩月 陸

本論文では, 平方剰余 (QR) と平方非剰余 (NR) の定義を用いて, 下記のように定義される α, β, α', β' に関する 2 つの定理を示すことを目的としている.

奇素数 p に対し, 集合 A, B, A', B' を

$$A := \{q \,|\, 0 < q \leq p-1,\ q : \mathrm{QR}\},\ B := \{q \,|\, 0 < q \leq p-1,\ q : \mathrm{NR}\},$$
$$A' := \{q \,|\, 0 < q \leq (p-1)/2,\ q : \mathrm{QR}\},\ B' := \{q \,|\, 0 < q \leq (p-1)/2,\ q : \mathrm{NR}\}$$

で定め, α, β, α', $\beta' \in \mathbb{Z}$ を

$$\alpha := \sum_{a \in A} a,\ \beta := \sum_{a \in B} a,$$
$$\alpha' := \sum_{a \in A'} a,\ \beta' := \sum_{a \in B'} a$$

で定義する. また, 簡単のため, $\#A' = t$, $\#B' = u$ とおく.

定理 1. α, β について,

$$\beta - \alpha \geq 0$$

が成り立ち, さらに

$$\beta - \alpha = \begin{cases} 0 & (p \equiv 1 \pmod 4) \\ \frac{1}{3}(t-u)p & (p \equiv 3 \pmod 8) \\ (t-u)p & (p \equiv 7 \pmod 8) \end{cases}$$

が成り立つ.

定理 2. $p \equiv 3 \pmod 4$ のとき, α', β' について,

$$\alpha' - \beta' \geq 0$$

が成り立ち, さらに

$$\alpha' - \beta' = \begin{cases} \frac{1}{3}(t-u)p & (p \equiv 3 \pmod 8) \\ 0 & (p \equiv 7 \pmod 8) \end{cases}$$

が成り立つ.

これらの定理は, 平方剰余の補充法則やディリクレの L 関数などを用いて示される.

さらに本論文内では, 定理 2 で示すことができなかった $p \equiv 1 \pmod 4$ のときの $\alpha' - \beta'$ についての予想を与えている.