令和元年度卒業研究概要

ガウスを魅了した定理

中等教育教員養成課程　数学専攻　銭上 昂汰

私たちのゼミでは, 栗原将人著『ガウスの数論世界をゆく』という本を用いて学習を進めた. この本の中でガウスを魅了した定理として紹介されている定理があった. その定理が次の定理である.

定理 1. 奇素数 p に対し, $p \equiv 1 \pmod 4$ ならば -1 は p の平方剰余であり, $p \equiv 3 \pmod 4$ ならば -1 は p の平方非剰余である.

本論文では, 定理 1 を主定理とし, 前半でその 2 通りの証明を与える. そのうちの 1 つにおいて, 次の定理を用いる.

定理 2 (オイラーの基準). $a \in \mathbb{Z}$ $(p \nmid a)$ に対し,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

が成り立つ.

ここで, $\left(\frac{a}{p}\right)$ は, 次で定めるルジャンドル記号である.

定義 8. $a \in \mathbb{Z}$ $(p \nmid a)$ に対し,

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

と定める.

また後半では, -1 以外の元がどのような場合に平方剰余となるか研究することとした. その研究で見つけた定理が次の 2 つである.

定理 4. 奇素数 p に対し, $p \equiv 1 \pmod 8$ または $p \equiv 7 \pmod 8$ ならば 2 は p の平方剰余であり, $p \equiv 3 \pmod 8$ または $p \equiv 5 \pmod 8$ ならば 2 は p の平方非剰余である.

定理 5. 奇素数 p に対し, $p \equiv 1 \pmod 8$ または $p \equiv 3 \pmod 8$ ならば $(p-1)/2$ は p の平方剰余であり, $p \equiv 5 \pmod 8$ または $p \equiv 7 \pmod 8$ ならば $(p-1)/2$ は p の平方非剰余である.

定理 4 の証明においても, 定理 2 は重要な役割を果たしている. また, 定理 5 は定理 1 と定理 4 を合わせて得られる.