令和元年度卒業研究概要

フェルマ・オイラーの定理と 4 次のガウス周期について

中等教育教員養成課程　数学専攻　小島 史也

私は, ある整数を素数 p で割った余りが等しくなるものを 1 つの数として扱う有限体 $\mathbb{F}_p$ の世界で, 平方剰余やガウス周期について興味を持ち, 4 次ガウス周期の基本定理を卒業論文のテーマとした. 本論文では, 次の 2 つの定理を示すことを目的とする.

定理 1 (**フェルマ・オイラー**)**.** p を $p \equiv 1 \pmod 4$ をみたす素数とすると,

$$p = a^2 + b^2 \ (a, b \in \mathbb{Z})$$

という形で表せる. また, a を奇数, b を偶数と取ると, $|a|, |b|$ は p によって一意的に決まる.

定理 2 (**4 次ガウス周期の基本定理 1**)**.** p を $p \equiv 1 \pmod 4$ をみたす素数とし,

$$p = a^2 + b^2 \ (a \text{ は奇数}, b \text{ は偶数})$$

と表す. 但し, $p \equiv 1 \pmod 8$ のとき $a \equiv 1 \pmod 4$, $p \equiv 5 \pmod 8$ のとき $a \equiv 3 \pmod 4$ となるように a の符号を決める. さらに, g を p の原始根とする.

(1) $p \equiv 1 \pmod 8$ のとき,

$$[1]_4 + [g^2]_4 = \frac{-1 + \sqrt{p}}{2},$$
$$[1]_4 \cdot [g^2]_4 = -\frac{p-1}{16} + \frac{a-1}{8}\sqrt{p}$$

が成り立つ.

(2) $p \equiv 5 \pmod 8$ のとき,

$$[1]_4 + [g^2]_4 = \frac{-1 + \sqrt{p}}{2},$$
$$[1]_4 \cdot [g^2]_4 = \frac{3p+1}{16} - \frac{a+1}{8}\sqrt{p}$$

が成り立つ.

さらに, 定理 1 の a, b にどんな奇数, 偶数が現れるのかに興味を持ち, 卒業論文のもう 1 つのテーマとした. そして, 数多くの数値実験を経て, 次の結果を得ることができた.

定理 4. $p \equiv 1 \pmod 4$ をみたす素数 p を $p = a^2 + b^2$ (a は奇数, b は偶数) と表したとき,

$$b \equiv \begin{cases} 0 \pmod 4 & (p \equiv 1 \pmod 8 \text{ のとき}) \\ 2 \pmod 4 & (p \equiv 5 \pmod 8 \text{ のとき}) \end{cases}$$

が成り立つ.