目 次

卒業論文

1　第2の証明

　ガウスの補題を使用せず、有限体で **ガウス和** と呼ばれるものを使用する。

まず、有限体に関して以下のこと A, B を示す。

A. p と q を異なる奇素数とする。q^{p-1} 個の要素を持つ有限体 F について考える。素体は $\mathbb{Z}_q$ であり、$\forall a \in F$ について $qa = 0$ が成り立つ。

ここで

$$(a+b)^q = a^q +_q C_{q-1} a^{q-1} b^1 +_q C_{q-2} a^{q-2} b^2 + \cdots + b^q$$

となるが、任意の二項係数 $\binom{q}{i}$ は $0 < i < q$ で q の倍数であるため $qa = 0$ より、

$$(a+b)^q = a^q + b^q \tag{1}$$

が成り立つ。ここで、オイラーの規準は、素体 $\mathbb{Z}_q$ 上で

$$\frac{p}{q} = p^q - \frac{1}{2}$$

となることに注意する。

B. 乗法群 $F^* = F \backslash \{0\}$ は大きさ $q^{p-1}-1$ の巡回群である。フェルマーの小定理によると p は $q^{p-1}-1$ の約数であるため、位数 p の元 $\zeta \in F(\zeta^p = 1)$ が存在し、F^* の部分群 $\{\zeta, \zeta^2, \ldots, \zeta^p = 1\}$ を生成する。$\forall \zeta^i (i \neq p)$ もまた生成元であることに注意する。

したがって $x^p - 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^p)$ と多項式分解を得る。

ここでガウス和について考える。ガウス和を以下とする。

$$G := \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^i \in F, \tag{2}$$

ここで $(\frac{i}{p})$ はルジャンドル記号である。ここで証明のために、G^q に関する2つの説明を提示しそれらが等しいことを示す。

1. 式 (1) より

$$G^q = \sum_{i=1}^{p-1} (\frac{i}{p})^q \zeta^{iq}$$

を得る。また、q は奇数なので $(\frac{i}{p})^q = (\frac{i}{p})$ となるため

$$G^q = \sum_{i=1}^{p-1} (\frac{i}{p})^q \zeta^{iq} = \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{iq}$$

を得る。さらに、$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ より $(\frac{i}{p}) = (\frac{q}{p})(\frac{iq}{p})$ が得られるため

$$G^q = \sum_{i=1}^{p-1} (\frac{i}{p})^q \zeta^{iq} = \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{iq} = (\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{iq}{p}) \zeta^{iq}$$

が成り立つ。ここで、iq について p で割った余りを考えると i になるので以下が成り立つ。

$$(\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{iq}{p}) \zeta^{iq} = (\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{i} = (\frac{q}{p}) G$$

つまり

$$G^q = \sum_{i=1}^{p-1} (\frac{i}{p})^q \zeta^{iq} = \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{iq} = (\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{iq}{p}) \zeta^{iq} = (\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{i} = (\frac{q}{p}) G \tag{3}$$

を得る。

2.

$$G^2 = (-1)^{\frac{p-1}{2}} p \tag{4}$$

$$G^q = G(G^2)^{\frac{q-1}{2}} = G(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} = G(\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{5}$$

式 (3) = 式 (5) より

$$(\frac{q}{p}) G = G(\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{6}$$

となり、式 (4) より $G \neq 0$ なので両辺を G で割ると

$$(\frac{q}{p}) = (\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{7}$$

となる。両辺に $(\frac{p}{q})$ を掛けると

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{8}$$

が得られる。