

ガウス整数におけるフェルマーの小定理

定理 1 μ を素数, $N(\mu) = m$ とする. $(\alpha, \mu) = 1$ ならば

$$\alpha^{m-1} \equiv 1 \pmod{\mu}$$

[証明]

$$\beta_1, \beta_2, \beta_3, \dots, \beta_{m-1}$$

を μ を法とする既約剰余類の完全代表系とする. $(\alpha, \mu) = 1$ のとき,

$$\beta_1\alpha, \beta_2\alpha, \beta_3\alpha, \dots, \beta_{m-1}\alpha$$

も既約剰余系を作るので, 全体としては一致し,

$$\beta_1\beta_2\beta_3 \cdots \beta_{m-1} \equiv \beta_1\alpha\beta_2\alpha\beta_3\alpha \cdots \beta_{m-1}\alpha$$

$(\beta_1\beta_2\beta_3 \cdots \beta_{m-1}, \mu) = 1$ なので

$$\alpha^{m-1} \equiv 1 \pmod{\mu}$$

[証明おわり]

参考文献

- [1] 高木貞治 『初等整数論講義第 2 版』(共立出版社, 1997 年)
- [2] 芹沢正三 『数論入門』(講談社ブルーバックス, 2008 年)