

本論文の目標は, ルジャンドル記号 $\left(\frac{a}{p}\right)$ の値を考察することである.
本論文では, まず次の2つの定理を示す.

定理 1 (平方剰余の第1法則). 奇素数 p に対し,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4}. \end{cases}$$

定理 2 (平方剰余の第2法則). 奇素数 p に対し,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ または } 7 \pmod{8} \\ -1 & p \equiv 3 \text{ または } 5 \pmod{8}. \end{cases}$$

本論文では, 上記2つの定理を主定理と呼ぶ. 主定理の証明の鍵となるのは, 次に述べるオイラー基準である.

命題 7 (オイラー基準). p を奇素数とする. $p \nmid a$ を満たす $a \in \mathbb{Z}$ に対し,

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

が成り立つ.

さらに本論文では, $3^{\frac{p-1}{2}} \pmod{p}$ を計算した次の命題を与える.

命題 8. 5以上の素数 p に対して, $3^{\frac{p-1}{2}} \pmod{p}$ の値は次のように求められる:

$$3^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{p-1}{6}} \pmod{p} & \frac{p-1}{2} \equiv 0 \pmod{3} \\ (-1)^{\frac{p+1}{6}} \pmod{p} & \frac{p-1}{2} \equiv 2 \pmod{3}. \end{cases}$$

オイラー基準と命題8を組み合わせることで, 主定理の類似となる次の定理を示すことができる.

定理 3. 5以上の素数 p に対し,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ または } 11 \pmod{12} \\ -1 & p \equiv 5 \text{ または } 7 \pmod{12}. \end{cases}$$