平成２９年度卒業研究概要

平方剰余の相互法則と素数判定

中等教育教員養成課程　数学専攻　宮木 克大

本論文では, 次の定理を証明することが目標である.

定理 1 (**平方剰余の相互法則**)**.** p と q を相異なる素数とする. このとき, 次が成り立つ:

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

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

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\dfrac{p}{q}\right), & p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4, \\ -\left(\dfrac{p}{q}\right), & p \equiv 3 \pmod 4 \text{ かつ } q \equiv 3 \pmod 4. \end{cases}$$

定理 1 の証明には, 次の命題を用いた.

命題 10. p を奇素数とする. このとき, p と互いに素な整数 a に対し, 次が成り立つ:

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

この命題の対偶は次のように述べられる.

定理 3. p を奇数とする. このとき,

$$a^{(p-1)/2} \not\equiv \left(\frac{a}{p}\right) \pmod p \tag{1}$$

となる p と互いに素な整数 a が存在するならば, p は合成数である.

これは一つの素数判定を与えている. 本論文の後半では, カーマイケル数と呼ばれる合成数 p に対して, 式 (1) が成り立つような p と互いに素な整数 a が存在するかどうかを確かめた. その結果, 次を予想した.

予想 1. すべてのカーマイケル数 p に対し,

$$^{\exists}a : \text{素数} \ \text{ s.t. } \ a \text{ が式 (1) を満たす}, (a, p) = 1.$$

さらに, a に条件をつけた次を予想した.

予想 2. カーマイケル数 p に対し,

$$^{\exists}a : \text{素数} \ \text{ s.t. } \ a \text{ が式 (1) を満たす}, p \equiv 1 \pmod{a+1}.$$

これらの予想は, 10^7 以下のすべてのカーマイケル数で成立している.