

本論文の前半の目標は、次の2つの定理を証明することである。

**定理 1.**  $f(X) = X^2 + 1$  とするとき、次は同値である：

- (i) 素数  $p$  はある整数  $n$  に対する  $f(n)$  の素因数となる。
- (ii)  $p = 2$  または  $p \equiv 1 \pmod{4}$ 。

**定理 2.**  $l$  を素数、 $f(X) = X^{l-1} + X^{l-2} + \cdots + 1$  とするとき、次は同値である：

- (i) 素数  $p$  はある整数  $n$  に対する  $f(n)$  の素因数となる。
- (ii)  $p = l$  または  $p \equiv 1 \pmod{l}$ 。

本論文の後半の目標は、上記定理2の  $l$  を合成数に拡張することである。定理2に現れる多項式が円分多項式であることを利用し、数多くの数値実験を行うことで、次の一般の円分多項式についての定理を得た。

**定理 3.**  $m$  を合成数、 $\phi_m(X)$  を  $m$  次の円分多項式とするとき、 $m$  と互いに素な素数  $p$  について次は同値である：

- (i) 素数  $p$  はある整数  $n$  に対する  $\phi_m(n)$  の素因数となる。
- (ii)  $p \equiv 1 \pmod{m}$ 。

さらに、定理3において  $m$  と互いに素でない素数が素因数としていつ現れるかを  $m$  の形によって場合分けをして調べ、次の結果を得た。

**定理 4.**  $m$  を合成数、 $\phi_m(X)$  を  $m$  次の円分多項式とするとき、次が成り立つ：

- (1)  $m = 2q$  ( $q$  : 奇素数) のとき、 $q$  はある整数  $n$  に対する  $\phi_m(n)$  の素因数に現れ、2は現れない。
- (2)  $m = q^r$  ( $q$  : 素数,  $r$  : 自然数) のとき、 $q$  はある整数  $n$  に対する  $\phi_m(n)$  の素因数に現れる。
- (3)  $m = 2q^r$  ( $q$  : 奇素数,  $r$  : 自然数) のとき、 $q$  はある整数  $n$  に対する  $\phi_m(n)$  の素因数に現れ、2は現れない。
- (4)  $m = 4q$  ( $q$  : 奇素数) のとき、2は素因数に現れない。また、 $q \equiv 1 \pmod{4}$  ならば、 $q$  はある整数  $n$  に対する  $\phi_m(n)$  の素因数に現れる。