# 代数入門 試験問題 July 26, 2019 (中野 伸)

**注意:** 数値等を求める問題についても，結果に至る考え方を書くこと

[1] 以下の問に答えよ．

(1) 26 を法とする 7 の逆元を求めよ．

(2) 自然な写像

$$f : \boldsymbol{Z}/182\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/7\boldsymbol{Z}) \times (\boldsymbol{Z}/26\boldsymbol{Z})$$

について，$f(\overline{a}) = (\overline{20},\ \overline{19})$ をみたす最小の自然数 $a$ を求めよ．

(3) 26 を法とする 3 の位数，5 の位数，15 の位数をそれぞれ求めよ．

[2] $m = 115 = 5 \cdot 23$ について，以下の問に答えよ．

(1) オイラー関数の値 $\varphi(m)$ を計算せよ．

(2) $8^{267}$ を $m$ で割った余りを求めよ．

(3) $41^{231}$ を $m$ で割った余りは 1 であることがわかっている． $m$ を法とする 41 の位数を求めよ．

[3] 素数 101 に関する以下のそれぞれの命題を証明せよ（ヒント： (1) はフェルマーの定理，(2) はオイラーの規準が使えるかも，(3) は平方剰余を考えると…）．

(1) 自然数 $n$ が 202 と互いに素ならば，$100^n + n^{100}$ は 101 の倍数である．

(2) $26^{50} + 1$ は 101 の倍数である．

(3) $(-5)^n \equiv 26 \pmod{101}$ をみたす自然数 $n$ は存在しない．

[4] $N = pq$ （ただし $p, q$ は相異なる二つの素数）であるとき，以下の問に答えよ．

(1) $p^{q-1} + q^{p-1} \equiv 1 \pmod{N}$ が成り立つことを示せ．

(2) $N = 360301$，かつ，オイラー関数の値が $\varphi(N) = 359100$ であるとき，$N$ の二つの素因数 $p, q$ （ただし，$p < q$）を求めよ．

(3) $p, q$ を前問で求めた素因数とする． $p < q$ に注意して，$q$ を法として $p$ が平方剰余かどうか判定せよ．