

情報代数 昨年度の問題

(A. 中間試験)

[1] $a, b, c \in \mathbb{N}$, $\ell = \text{lcm}(a, b)$ とし、 $a|c$ かつ $b|c$ ならば $\ell|c$ であることを示したい。次の (1) ~ (8) を埋めて証明を完成させなさい。

c を ℓ で割った商と余りをそれぞれ q と r とすると $c = \underline{\hspace{1cm}} (1) \underline{\hspace{1cm}} \quad ((2) \leq r \leq (3))$
 よって、 $a|c$ と $a|(4)$ より $a|(5)$ が成り立ち、 $b|c$ と $b|(4)$ より $b|(5)$ が成り立つので、(5) は a と b の
 (6) である。もし $r > 0$ ならば、(7) なので (8) に反する。
 故に $r = 0$ であり、 $\ell|c$ が成り立つ。

[2] 0 から 6 までの数字からなる 6 桁の番号 $a_1a_2a_3a_4a_5a_6$ ($a_1, \dots, a_6 \in \mathbb{Z}_7$) で商品を管理する。但し、 $a_1a_2a_3a_4a_5$ は商品番号、 a_6 は $a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5$ を 7 で割った余りと定める。

- (1) $\sum_{i=1}^6 ia_i \equiv 0 \pmod{7}$ が成り立つことを示せ。
 (2) $a_1 \neq a_2$ とする。 $a_1a_2a_3a_4a_5a_6$ を誤って $a_2a_1a_3a_4a_5a_6$ と入力したとき、誤り検出ができることを示せ。

[3] p は素数、 $G = \{(a, x) \mid a \in \mathbb{Z}_p, x \in \mathbb{Z}_p^*\}$ とし、 $(a, x), (b, y) \in G$ の積を $(a, x) \cdot (b, y) = (ay + bx, xy)$ と定義する。このとき、 $(G, \cdot)$ は群になることを示せ。

[4] $p = 5, q = 11, L = (p-1)(q-1), e = 7, n = pq$ とする。

- (1) $se + tL = \text{gcd}(e, L)$ をみたす整数の組 (s, t) を 1 組求めよ。
 (2) $ed \equiv 1 \pmod{L}$ をみたす $d \in \mathbb{Z}_L$ を求めよ。
 (3) n と e を公開し、送信メッセージ $x \in \mathbb{Z}_n$ を $c = x^e \in \mathbb{Z}_n$ に変換して送信する暗号化通信では、 c^d から x が求まることをオイラーの定理を使って説明せよ。

(B. 定期試験)

[1] 6 つの行列 $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A_1 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, A_2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, A_3 = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix},$

$A_4 = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, A_5 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ からなる集合を G とし、演算は乗算のみを考える。

- (1) G の乗算表を作り、 G は群であることを示せ。
 (条件 (G2), (G3) については、 G の単位元はどれか、各 A_i の逆元はどれか明示すること)
 (2) G は可換群ではないことを示せ。
 (3) G の部分群 H の位数 $|H|$ の取り得る値を全て求めよ。
 (4) G の全ての部分群を求めよ。

[2] $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x], f(\alpha) = 0$ とする。

- (1) $f(x)$ は $\mathbb{F}_2$ 上既約であることを示せ。
 (ヒント: $\mathbb{F}_2$ 上の 2 次の既約多項式は $x^2 + x + 1$ のみ)
 (2) α は $\mathbb{F}_{16}$ の原始元であることを示せ。
 (3) $\alpha + \alpha^2 + \alpha^4 + \alpha^8$ は $\mathbb{F}_2$ の元であることを示せ。

[3] C は、次の G を生成行列とする 2 元線形符号とする：

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- (1) C のパラメータ $[n, k, d]_q$ と重み分布を求めよ。