

情報代数 問題 (2009.2.9)

[1]₂₄ (1) $a = 1517, b = 2173$ に対して、 $\gcd(a, b) = ax + by$ をみたす整数の組 (x, y) をユークリッド互除法を用いて 1 組求めよ。

(2) 次の (a)~(h) に当てはまる適切な単語を選択肢から選び、文章を完成させなさい。

2 以上の整数 n に対して、 $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ は、 n を法とする加法と乗法に関して [(a)] になる。[(b)] に関しては常に [(c)] になるが、 n が [(d)] のときは、[(e)] に関して [(c)] にならない。 n が [(f)] のときは、 $\mathbb{Z}_n$ の任意の 0 でない元に対して [(g)] が存在するので、[(e)] に関しても [(c)] になり、 $\mathbb{Z}_n$ は [(h)] になる。

【選択肢： 群, 環, 体, 乗法, 加法, 素数, 合成数, 単位元, 逆元】

(3) 整数 a, b に対して $\gcd(a, b) = ax + by$ をみたす整数の組 (x, y) が存在することを用いて、(2) の「 n が [(f)] のときは、 $\mathbb{Z}_n$ の任意の 0 でない元に対して [(g)] が存在する」が成り立つことを示せ。

[2]₄₆ $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x], f(\alpha) = 0, G = \{\alpha, \alpha^2, \dots, \alpha^r = 1\}$ (r は α の乗法位数 $|\alpha|$) とする。

(1) $f(x)$ は $\mathbb{F}_3$ 上既約であることを示せ。

(2) $r = |\alpha|$ を求めよ。

(3) G は、乗法に関して群になる。単位元と各元の逆元を示せ。

(4) G の乗法に関する部分群を H とする。 H の位数 $|H|$ として取り得る値を全て求めよ。

(5) (4) の H として、巡回群でないものは存在しないことを示せ。

(6) (4) の H を全て求めよ。

[3]₃₀ 次の (1)~(5) から 3 問選んで答えなさい。(途中の計算も書くこと)

(1) 整数 1234^{209} の 1 桁目 (一の位) を合同式の計算を使って求めよ。

(2) 連立合同式 $x \equiv 2 \pmod{4}, x \equiv 3 \pmod{5}, x \equiv 4 \pmod{6}$ を解け。

(3) $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ を考える。次の値はそれぞれ $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ のどれと一致するか?

$$\overline{-123} + \overline{-32}, \quad \overline{-2} + \overline{13}, \quad \overline{7} \cdot \overline{134}, \quad \overline{32}^{-1}$$

(4) $a \equiv \alpha \pmod{n}, b \equiv \beta \pmod{n}$ のとき、 $ab \equiv \alpha\beta \pmod{n}$ が成り立つことを示せ。

(5) 次の G を生成行列とする 2 元線形符号 C の重み分布とパラメータ $[n, k, d]_q$ を求めよ。

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

$$\overline{32}^{-1} = \overline{x}$$

$$\overline{32} \cdot \overline{x} = \overline{1}$$

$$\overline{2} = 2 + 5t$$

$$(2+5t)(x+5t) = 1$$

$$2x + 10t + 5xt + 25t^2$$

$$x(2+5t) + 10t + 25t^2$$

$$x = \frac{1 - 10t - 25t^2}{2+5t}$$

$$= \frac{(1-5t)^2}{2+5t}$$

$$x = \frac{(1-5)^2}{2+5} = \frac{16}{7}$$