

(2) C のパリティ検査行列 H を求めよ。

(3) 受信ベクトル $x = 100010$ と $y = 111000$ を復号せよ。

【略解 (A)】

[1] (1) $\ell q + r$ (2) 0 (3) $\ell - 1$ (4) ℓ (5) r (6) 公倍数 (7) $r < \ell$ (8) ℓ が a と b の最小公倍数であること

[2] (1) ヒント：題意より、 $a_6 \equiv a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 \pmod{7}$ が成り立つことを使う。

(2) ヒント：問題のように入力を誤ると、(1) の合同式が成り立たなくなることを示せばよい。

[4] (1) $(s, t) = (-17, 3)$ (2) $d = e^{-1} = 23$

【略解 (B)】

$\times$	A_0	A_1	A_2	A_3	A_4	A_5
A_0	A_0	A_1	A_2	A_3	A_4	A_5
A_1	A_1	A_2	A_0	A_4	A_5	A_3
[1] (1) A_2	A_2	A_0	A_1	A_5	A_3	A_4
A_3	A_3	A_5	A_4	A_0	A_2	A_1
A_4	A_4	A_3	A_5	A_1	A_0	A_2
A_5	A_5	A_4	A_3	A_2	A_1	A_0

(2) 例えば、(1) の表より $A_1 A_3 \neq A_3 A_1$

(3) Lagrange の定理より $|H|$ は $|G| = 6$ の約数なので、 $|H|$ の取り得る値は 1, 2, 3, 6

(4) $\{A_0\}, \{A_0, A_3\}, \{A_0, A_4\}, \{A_0, A_5\}, \{A_0, A_1, A_2\}, G$

[2] (1) $f(0) = f(1) = 1$ なので、因数定理より $f(x)$ は 1 次因子をもたない。

また、 $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x)$ なので、既約 2 次因子をもたない。

(2) ヒント： $|\alpha| = 15$ を示せばよい

(3) $\alpha^{15} = 1$ を使って計算すると、 $(\alpha + \alpha^2 + \alpha^4 + \alpha^8)^2 = \alpha + \alpha^2 + \alpha^4 + \alpha^8$ となる。

よって「 $a \in \mathbb{F}_q \Leftrightarrow a^q = a$ 」より、 $\alpha + \alpha^2 + \alpha^4 + \alpha^8 \in \mathbb{F}_2$ が成り立つ

[3] (1) $[6, 3, 3]_2$ (2) $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ (3) 100110, 111000