

**Sample Final Exam**  
**Math 127, Spring 2022**

1. (14 points) Let  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$  be vectors in  $\mathbf{F}_7^{11}$ , and let

$$W = \text{span} \{ \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \}.$$

Suppose that the only time we have that  $a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3 = \mathbf{0}$  is when  $a = b = c = 0$ . How many vectors are there in  $W$ ? Briefly **EXPLAIN** your answer.

2. (14 points) Consider  $a(x) = x^4 + x^2$  and  $b(x) = x^3 + 1$  in  $\mathbf{F}_2[x]$ . Use the Euclidean Algorithm to find  $d = \gcd(a(x), b(x))$ . Show all your work.

3. (14 points) Let  $\omega = e^{2\pi i/6}$  and let

$$f(x) = x^6 - 1, \quad g(x) = x^5 + x^4 + x^3 + x^2 + x + 1.$$

You may take it as given that

$$f(x) = (x - 1)g(x).$$

(I.e., you may use that fact without having to prove it.)

- (a) Explain why  $f(\omega) = 0$ .
- (b) Explain why  $g(\omega) = 0$ .

4. (14 points) Note that in  $\mathbf{F}_2[x]$ , we have

$$\begin{aligned} x^5 + x^3 + 1 &= (x^3 + x^2 + x)(x^2 + x + 1) + (x + 1), \\ x^2 + x + 1 &= (x)(x + 1) + 1. \end{aligned}$$

(I.e., you are given the above facts and do not need to check them yourself.)

Let  $\mathbf{F}_{32} = \mathbf{F}_2[\alpha]$ , where  $\alpha$  is a root of  $x^5 + x^3 + 1$ . Find the multiplicative inverse of  $\alpha^2 + \alpha + 1$ . Show all your work.

5. (14 points) Recall that the parity check matrix of the Hamming 7-code  $\mathcal{H}_7$  is

$$H_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Suppose Yolanda is receiving transmissions sent using the Hamming 7-code, and she receives

$$\mathbf{y} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Correct  $\mathbf{y}$  to a codeword  $\mathbf{y}'$ , if necessary, and read off the message bits 3, 5, 6,

and 7 to find the intended message  $\mathbf{m}'$ . Show all your work.

6. (14 points) Let  $\mathcal{C}$  be the binary linear code of length 5 with parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

In other words,  $\mathcal{C}$  is the nullspace of  $H$ .

- Find a basis for  $\mathcal{C}$ . Show your work.
- Find the dimension of  $\mathcal{C}$ . **JUSTIFY** your answer.

7. (14 points) Let  $\mathbf{F}_{256}^\times$  be the multiplicative group of the finite field of order 256.

- Is it possible that the order of every element of  $\mathbf{F}_{256}^\times$  is  $< 100$ ? Briefly **JUSTIFY** your answer.
- Exactly one of the following statements is **FALSE**:
  - There exists an element  $\alpha \in \mathbf{F}_{256}^\times$  of order 51.
  - There exists an element  $\alpha \in \mathbf{F}_{256}^\times$  of order 7.

Indicate which of those statements is false, and briefly **EXPLAIN** how you know that statement is false.

8. (14 points) Recall that the various forms of the Division Theorem for a ring  $R$  all say that when we divide  $a \in R$  by some nonzero divisor  $d \in R$ , we get

$$a = qd + r.$$

- Suppose  $R = \mathbf{Z}$  and the divisor  $d = 10$ . What conditions must be satisfied by the remainder  $r$  in that case? Be as precise as possible.
- Suppose  $R = \mathbf{F}_5[x]$  and the divisor  $d(x) = x^4 + 2x + 3$ . What conditions must be satisfied by the remainder  $r(x)$  in that case? Be as precise as possible.

9. (17 points) **PROOF QUESTION.** Let  $R$  be a ring, and suppose that  $I$  is an ideal of  $R$  and  $c$  is a fixed element of  $R$ . Define

$$J = \{ca \mid a \in I\}. \tag{1}$$

In other words,  $J$  is the set of all multiples of elements of  $I$  by the fixed element  $c$ .

- What properties must  $I$  have, given that  $I$  is an ideal of  $R$ ? In other words, what does it mean for  $I$  to be an ideal of  $R$ , by definition? (You can just copy this from your notes.)
- Prove that  $J$  is closed under addition. (Suggestion: What does it mean to say that  $x, y$  are in  $J$ ?)
- Prove that  $J$  is closed under multiplication by  $r \in R$ .

- 10.** (17 points) Let  $m(x) = x^4 + x + 1$ , and let  $F = \mathbf{F}_2[x]/(m(x))$ .
- (a) It is a fact that  $F$  is a field. What is the **ONE** key property of the polynomial  $m(x)$  that ensure that  $R$  is a field?
- (b) Let  $\alpha$  be a root of  $m(x)$  in  $F$ . Fill in the blank: Every element of  $F$  can be represented as a polynomial in  $\alpha$  of degree at most .
- (c) Let  $\beta = \alpha^3 + 1$  and  $\gamma = \alpha^2 + \alpha$ . Calculate the product  $\beta\gamma$ , and put your final answer in the form described in part (b).
- 11.** (17 points) Let  $\omega = e^{2\pi i/15}$ , let  $G = \langle \omega \rangle = C_{15}$ , and let  $H = \langle \omega^3 \rangle$ , the cyclic subgroup of  $G$  generated by  $\omega^3$ .
- (a) Write out all of the elements of  $H$ . How many elements does  $H$  have?
- (b) Write  $G = C_{15}$  as a disjoint union of cosets of  $H$ .
- 12.** (17 points) Find  $d = \gcd(162, 88)$ , and find  $x, y \in \mathbf{Z}$  such that  $162x + 88y = d$ . Show all your work.
- 13.** (20 points) Let  $E = \mathbf{F}_{256}$ , and let  $\alpha$  be a primitive root of unity of  $E$ . Let  $\mathcal{C}$  be the corresponding BCH code of designed distance  $\delta = 5$  over  $\mathbf{F}_2$ .
- (a) Find the Frobenius orbits needed to construct the BCH code  $\mathcal{C}$ . Show all your work.
- (b) Express  $m_3(x)$  as a product of terms of the form  $(x - \alpha^i)$ .
- (c) Express the generating polynomial  $g(x)$  of  $\mathcal{C}$  as a product of minimal polynomials  $m_i(x)$ . (You do not need to expand those  $m_i(x)$ .)
- (d) Find  $k = \dim \mathcal{C}$ .