Sample Final Exam
Math 127, Fall 2024

1. (12 points) In the following, if you discuss an object, make sure to be clear what ring that object belongs to.

(a) Let a and d be nonzero integers. Define what it means for d to divide a.

(b) Let F be a field and let $a(x)$ and $d(x)$ be nonzero polynomials in $F[x]$. Define what it means for $d(x)$ to divide $a(x)$.

2. (12 points) Let $\omega = e^{2\pi i/9}$.

(a) Fill in the blank, no explanation necessary: For $k =$ ____, we have that

$$1 + \omega + \omega^2 + \cdots + \omega^k = 0.$$

(b) For the same value of k you used in part (a), what is the value of

$$1 + \omega^3 + \omega^6 + \cdots + \omega^{3k}?$$

Briefly **EXPLAIN** your answer. (Try writing out the full sum and simplifying the exponents on the powers of ω.)

3. (12 points) Note that $16384 = 2^{14}$ (i.e., you are given this fact and do not need to check it). Fill in the blanks, no explanation necessary:

The field of order 16384 is constructed as $\mathbf{F}_2[x]$ mod $m(x)$, where $m(x)$ is a/an ____ polynomial of degree ____ in $\mathbf{F}_2[x]$.

4. (14 points) Let W be the subset of $\mathbf{F}_{31}^4$ defined by

$$W = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \in \mathbf{F}_{31}^4 \;\middle|\; x_3 = 7x_1 \right\}.$$

Give **part of** the proof that W is a subspace of $\mathbf{F}_{31}^4$, in the following steps:

(a) Explain why $\mathbf{0} \in W$.

(b) Suppose $a \in \mathbf{F}_{31}$ and $\mathbf{x} \in W$. Explain why $a\mathbf{x} \in W$.

5. (14 points) Let $\mathbf{F}_{256}$ be the field of order 256, and let α be a primitive element of $\mathbf{F}_{256}$.

(a) What is the order of α? (No explanation necessary.)

(b) What is the order of $\beta = \alpha^5$? Briefly **JUSTIFY** your answer.

6. (14 points) Suppose $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{F}_5^4$, and let $W = \operatorname{span}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$.

(a) What is the **largest** number of vectors that could be in W, and what condition must $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ satisfy for W to contain that largest number of vectors?

(b) Give one example of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{F}_5^4$ that satisfy the condition in part (a). No explanation necessary.

7. (14 points) Consider the subgroup $H = \langle 4 \rangle$ in $\mathbf{F}_{17}^{\times}$. In the following, show all your work.

(a) List all of the elements of H (the powers of 4 (mod 17)).

(b) Write $\mathbf{F}_{17}^{\times}$ as a disjoint union of cosets of H.

(c) Find a transversal for H in $\mathbf{F}_{17}^{\times}$.

8. (14 points) Solve $115x = 2$ in $\mathbf{Z}/(142)$, or explain why no solution is possible. Show all your work and **JUSTIFY** your answer.

9. (14 points) Let $a = 108$ and $b = 75$. Find $x, y \in \mathbf{Z}$ such that $ax + by = \gcd(a, b)$. Show all your work.

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

11. (14 points) Note that in $\mathbf{F}_2[x]$, we have

$$\begin{aligned} x^5 + x^3 + 1 &= (x)(x^4 + x + 1) + (x^3 + x^2 + x + 1) \\ x^4 + x + 1 &= (x + 1)(x^3 + x^2 + x + 1) + x \\ x^3 + x^2 + x + 1 &= (x^2 + x + 1)(x) + 1 \end{aligned}$$

(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 α is a root of $x^5 + x^3 + 1$. Find the multiplicative inverse of $\beta = \alpha^4 + \alpha + 1$. Show all your work.

12. (14 points) Let A be a matrix with entries in $\mathbf{F}_7$ such that

$$A = \begin{bmatrix} 4 & 2 & 2 & 6 & 5 & 3 & 2 \\ 4 & 2 & 3 & 5 & 1 & 4 & 2 \\ 5 & 6 & 4 & 4 & 0 & 2 & 0 \\ 1 & 4 & 6 & 2 & 1 & 0 & 4 \\ 1 & 4 & 3 & 3 & 4 & 1 & 2 \end{bmatrix}, \qquad RREF(A) = \begin{bmatrix} 1 & 4 & 0 & 0 & 3 & 0 & 4 \\ 0 & 0 & 1 & 0 & 4 & 0 & 3 \\ 0 & 0 & 0 & 1 & 1 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Find bases for $\text{Col}(A)$ and $\text{Null}(A)$. Show your work.

13. (14 points) Let $E = \mathbf{F}_{512}$, let β be a primitive element of E, and let $\alpha = \beta^7$. Note that the order of α is 73 (i.e., you are given this fact and do not need to check it or justify it). Let $\mathcal{C}$ be the BCH code based on α with designed distance $\delta = 9$ over $\mathbf{F}_2$. In the following, show all your work, especially your orbit calculations.

(a) Recall that $m_i(x)$ is the minimal polynomial of α^i. Express $m_1(x)$ as a product of terms of the form $(x - \alpha^j)$.

(b) Find the generating polynomial $g(x)$ of $\mathcal{C}$, expressed as a product of minimal polynomials $m_i(x)$. (You do not need to expand each $m_i(x)$ as a product of terms of the form $(x - \alpha^j)$, other than the expansion of $m_1(x)$ that you have already done in part (a).)

(c) Find $k = \dim \mathcal{C}$.

14. (24 points) Fix $N = 24$ and $\omega = e^{2\pi i/24}$. Let $H_0 = C_1$, $H_1 = C_2$, $H_2 = C_4$, $H_3 = C_{12}$, and $H_4 = C_{24}$. Recall that the main loop of the FFT based on $C_1 \leq C_2 \leq C_4 \leq C_{12} \leq C_{24}$, applied to the initial input $\mathbf{x} = \begin{bmatrix} f(0) \\ \vdots \\ f(N-1) \end{bmatrix}$, can be described as follows. For $i = 1$ to 4:

- Set $H_{i-1} = \langle \omega^m \rangle$, $H_i = \langle \omega^k \rangle$, and $d = m/k$.
- *Subgroup fill:* For $j = 0$ to $(N/k) - 1$, set $y(jk) = \sum_{r=0}^{d-1} x(jm + kr)\omega^{-rkj}$.
- Translate the subgroup fill to cosets of H_i, set $\mathbf{x} = \mathbf{y}$, and loop.

(a) Working in terms of ω, write out the elements of H_2 and H_3 and write out the elements of the standard transversal $T_{2,3}$ for H_2 in H_3.

(b) Write out the results of the "subgroup fill" part of step 3 ($i = 3$). That is, for all t corresponding to the elements of H_3, write out the formula for $y(t)$ in terms of the inputs $\mathbf{x}$ (the output of step 2, $i = 2$).

(c) Draw the corresponding subgroup subdiagram for step 3 ($i = 3$).