Sample Final Exam
Math 127, Fall 2023

1. (12 points) Describe how to construct a field of order $8 = 2^3$ as a quotient ring R/I (i.e., state what the appropriate ring R and ideal I are). In particular, describe what the elements of the ring R/I are for your chosen R and I.

2. (12 points) Let C be the set of solutions $z \in \mathbf{C}$ to the equation $z^8 = 1$.

(a) Describe the elements of C as powers of a single complex number ω. (What is ω? Which powers? You may also find it helpful to draw the elements of C in the complex plane.)

(b) What is the sum of the elements of C? (No explanation necessary.)

3. (12 points) Let a and d be positive integers. State what the Division Theorem says about dividing a by d.

4. (14 points) Solve $87x = 3$ in $\mathbf{Z}/(156)$, or explain why no solution is possible. Show all your work and **JUSTIFY** your answer.

5. (14 points) Let $\mathbf{F}_{64}$ be the field of order 64, and let α be a primitive element of $\mathbf{F}_{64}$.

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

(b) What is the order of $\beta = \alpha^6$? Briefly **EXPLAIN**.

(c) Find a different element of $\mathbf{F}_{64}$ that has the same order as $\beta = \alpha^6$. Express your answer as a power of α, and briefly **JUSTIFY** your answer.

6. (14 points) Let $\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 3 \end{bmatrix}$, and $\mathbf{v}_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 4 \end{bmatrix}$ be vectors in $\mathbf{F}_{17}^4$ and let $W = \operatorname{span}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$.

(a) Use the **definition** of linear independence to prove that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is linearly independent.

(b) How many vectors are there in W? **JUSTIFY** your answer. (You can just express your answer as a power of some number; you don't have to multiply out that power.)

7. (14 points) Consider the subgroup $H = \langle 7 \rangle$ in $\mathbf{F}_{19}^\times$.

(a) List all of the elements of H (the powers of 7 (mod 19)).

(b) Write $\mathbf{F}_{19}^\times$ as a disjoint union of cosets of H.

8. (14 points) Let W be the subset of $\mathbf{F}_{13}^3$ defined by

$$W = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbf{F}_{13}^3 \middle| \, x_1 + x_2 = 0 \right\}.$$

Give **part of** the proof that W is a subspace of $\mathbf{F}_{17}^3$, in the following steps:

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

(b) Suppose $\mathbf{x}, \mathbf{y} \in W$. Explain why $\mathbf{x} + \mathbf{y} \in W$.

9. (14 points) Use the Euclidean Algorithm to find

$$\gcd(x^6 + x^5 + x^3 + 1, x^4 + x^2 + x + 1)$$

in $\mathbf{F}_2[x]$, given the following first step:

$$x^6 + x^5 + x^3 + 1 = (x^2 + x + 1)(x^4 + x^2 + x + 1) + (x^3 + x^2)$$

In other words, the first step of the Euclidean Algorithm is done for you, above, and you do not need to check it. Otherwise, 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 $\mathbf{y} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$. 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

$$x^6 + x + 1 = (x^3 + x^2)(x^3 + x^2 + x + 1) + (x^2 + x + 1)$$
$$x^3 + x^2 + x + 1 = (x)(x^2 + x + 1) + 1$$

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

Let $\mathbf{F}_{64} = \mathbf{F}_2[\alpha]$, where α is a root of $x^6 + x + 1$. Find the multiplicative inverse of $\alpha^3 + \alpha^2 + \alpha + 1$. Show all your work.

12. (14 points) Let A be a matrix with entries in $\mathbf{F}_5$ such that

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

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

13. (14 points) Let $E = \mathbf{F}_{256}$, let β be a primitive element of E, and let $\alpha = \beta^5$. Note that the order of α is 51 (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 $\delta = 5$ 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 $N = 36$ and $\omega = e^{2\pi i/36}$. Let $H_0 = C_1$, $H_1 = C_2$, $H_2 = C_6$, $H_3 = C_{12}$, and $H_4 = C_{36}$. Recall that the main loop of the FFT based on $C_1 \le C_2 \le C_6 \le C_{12} \le C_{36}$, 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 ($i = 3$).