Math 127, Spring 2020 **Name:** _____
Makeup Exam 2, Version A

This test consists of 7 questions on 3 pages, totalling 100 points. You are allowed to use **ONE** handwritten page of notes (both sides), but you are otherwise not allowed to use books, notes, or calculators. Unless otherwise stated, you may take as given anything that has been proven in class, in the homework, or in the reading.

Submission tips:

- Make sure you put your name at the beginning of the exam.
- If possible, please write each problem on a separate sheet of paper, and submit them in order. If that is not possible, please try not to start a problem on one sheet of paper and finish it on another.

1. (14 points) Note that in $\mathbf{F}_2[x]$, we have

$$x^4 + x^3 + 1 = (x+1)(x^3+1) + x,$$
$$x^3 + 1 = (x^2)(x) + 1.$$

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

Let $\mathbf{F}_{16} = \mathbf{F}_2[\alpha]$, where α is a root of x^4+x^3+1. Find the multiplicative inverse of $\alpha^3 + 1$. Show all your work.

2. (14 points) Let $\mathbf{F}_{64}$ be the field with 64 elements, and

(a) Suppose $a \in \mathbf{F}_{64}^{\times}$. What are all of the possible orders of a?

(b) Now suppose $a \in \mathbf{F}_{64}^{\times}$ is a **primitive** element (i.e., the cyclic subgroup generated by a is equal to all of $\mathbf{F}_{64}^{\times}$). Is it possible to find some a^k such that the order of a^k is equal to 9? If so, give an example of one value of k such that the order of a^k is 9, and briefly **EXPLAIN** how you know that the order of a^k is 9; if not, briefly **EXPLAIN** why this is not possible.

3. (14 points) Let $\mathcal{C}$ be the binary linear code of length 7 with parity check matrix

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

Find a generator matrix for $\mathcal{C}$. Show your work.

4. (14 points) Let A be a matrix with entries in $\mathbf{F}_7$ such that

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

Find bases for $\mathrm{Col}(A)$ and $\mathrm{Null}(A)$. Show 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 $\mathbf{y} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$. 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.

6. (14 points) Suppose $\mathbf{x}, \mathbf{y}, \mathbf{z} \in F_{13}^3$.

(a) Write down the definition of what it means for $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ to be linearly independent.

(b) Now suppose also that

$$\mathbf{x} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \qquad \mathbf{y} = \begin{bmatrix} 0 \\ 1 \\ r \end{bmatrix} \qquad \mathbf{z} = \begin{bmatrix} 1 \\ s \\ t \end{bmatrix},$$

where $r, s, t \in \mathbf{F}_{13}$ are unspecified constants. Use the **definition** of linear independence to prove that $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ is linearly independent.

7. (16 points) **PROOF QUESTION.** Let R be a ring, and let a be a fixed element of R. Define

$$I = \{x \in R \mid ax = 0\}.$$

(a) Prove that I is closed under addition. (Suggestion: What do two random elements $x, y \in I$ look like?)

(b) Prove that I is closed under multiplication by $r \in R$.