Math 127, Spring 2020 **TYPOS CORRECTED**
Makeup Exam 2, Version B

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

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

(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+1. Find the multiplicative inverse of $\alpha^3 + \alpha + 1$. Show all your work.

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

(a) Define the **order** of an element $a \in \mathbf{F}_{64}^{\times}$. (You can just copy this from your notes.)

(b) Now suppose you want to know if $a \in \mathbf{F}_{64}^{\times}$ is a **primitive** element (i.e., if the cyclic subgroup generated by a is equal to all of $\mathbf{F}_{64}^{\times}$). Exactly which powers of a do you need to compute to determine if a is primitive? Briefly **EXPLAIN** your answer in terms of the **DEFINITION** of the order of a.

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

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

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

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

(a) What is the *dimension* of $\mathrm{Col}(A)$? Briefly **justify** your answer.

(b) Find a basis for $\mathrm{Null}(A)$.

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

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

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 F be a field, and define

$$I = \{f(x) \in F[x] \mid f(1) = 0\}.$$

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

(b) Prove that I is closed under multiplication by $h(x) \in F[x]$.