Math 127, Spring 2021 **Exam 3**

This test consists of 7 questions on 2 pages, totalling 100 points. You are allowed to use one page of notes. Unless otherwise stated, you may take as given anything that has been proven in class, in the homework, or in the reading.

1. (12 points)

(a) List three nonzero elements of the principal ideal $(1+x^3)$ of $\mathbf{F}_2[x]$. No explanation necessary.

(b) Write out the elements of the coset $2+(5)$ of the ideal (5). (There are infinitely many elements of that coset, but they fall into a pattern you can indicate by ....)

2. (12 points) Note that in $\mathbf{F}_2[x]$, we have

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

(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^2+1. Find the multiplicative inverse of $\alpha^4+\alpha+1$. Show all your work.

3. (12 points) Let $\mathbf{F}_{64} = \mathbf{F}_2[\alpha]$, where α is a root of x^6+x+1. Let $\beta = \alpha^5+\alpha^3+1$ and $\gamma = \alpha^3+\alpha$.

(a) Find a reduced representative for $\beta+\gamma$. Show all your work.

(b) Find a reduced representative for $\beta\gamma$. Show all your work.

4. (14 points) Let $\mathbf{F}_4$ be the field of order 4.

(a) Find a nonzero element $a \in \mathbf{Z}/(4)$ such that a is not a unit. Justify your answer.

(b) Briefly **explain** how you know that $\mathbf{F}_4$ and $\mathbf{Z}/(4)$ are not isomorphic.

5. (14 points) Let α be a primitive element of $\mathbf{F}_{128}$. Find the minimal polynomial $m(x)$ of α^5 over $\mathbf{F}_2$, expressed as a product of terms of the form $(x-\alpha^i)$. Show all your work.

6. (18 points) Let $\mathbf{F}_{64}$ be the field of order 64.

(a) If $\mathbf{F}_{64} = \mathbf{F}_2[x]/(m(x))$ for some irreducible $m(x) \in \mathbf{F}_2[x]$, what is the degree of $m(x)$? Briefly **explain** your answer.

(b) Does $\mathbf{F}_{64}^{\times}$, the multiplicative group of $\mathbf{F}_{64}$, contain an element of order 11? Briefly **explain** your answer.

7. (18 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 corresponding BCH code of designed distance $\delta = 9$ over $\mathbf{F}_2$.

(a) Find the generating polynomial $g(x)$ of $\mathcal{C}$, expressed as a product of minimal polynomials $m_i(x)$, where $m_i(x)$ is the minimal polynomial of α^i. (You do not need to expand each $m_i(x)$ as a product of terms of the form $(x - \alpha^j)$.) Show all your work, especially your orbit calculations.

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