Sample Exam 3
Math 127, Fall 2023

1. (10 points) Let $I = (x^2 + 1)$ be the principal ideal of $R = \mathbf{F}_2[x]$ generated by $x^2 + 1$. Find some $f(x) \in I$ such that $\deg f(x) \geq 3$, and briefly **EXPLAIN** how you know that $f(x) \in I$. (If you don't know how to find $f(x)$, you may recite the definition of ideal for partial credit.)

2. (10 points) Let $\mathbf{F}_{128} = \mathbf{F}_2[\alpha]$, where α is a root of $x^7 + x^3 + 1$. Let $\beta = \alpha^3 + \alpha^2 + 1$ and $\gamma = \alpha^4 + \alpha$.

(a) Fill in the blanks: An element of $\mathbf{F}_{128}$ in reduced form is a polynomial in the variable [ ] of degree at most [ ].

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

3. (10 points) Let $\mathbf{F}_{16}$ be a field of order 16. Give an example of a ring of order 16 that is **not** isomorphic to $\mathbf{F}_{16}$. Briefly **JUSTIFY** your answer.

4. (12 points) Let $\mathbf{F}_{2048}$ be the field of order 2048, and let $\mathbf{F}_{2048}^\times$ be the multiplicative group of $\mathbf{F}_{2048}$. Note the prime factorizations $2048 = 2^{11}$ and $2047 = 23 \cdot 89$.

(a) What are the possible orders of elements of $\mathbf{F}_{2048}^\times$?

(b) For a given $\alpha \in \mathbf{F}_{2048}^\times$, what is the **smallest** set of powers of α that we need to compute to see if α is primitive? Briefly **EXPLAIN** your answer, referring to part (a).

5. (12 points) Let $\mathbf{F}_{64}$ be the field of order $64 = 2^6$, and let $\mathbf{F}_{64}^\times$ be the multiplicative group of $\mathbf{F}_{64}$.

(a) Let α be a primitive element of $\mathbf{F}_{64}$. What is the order of α? Briefly **EXPLAIN** your answer.

(b) Exactly one of the following is true.

- There exists an element $\beta \in \mathbf{F}_{64}^\times$ of order 3.
- There exists an element $\beta \in \mathbf{F}_{64}^\times$ of order 4.

Circle the true statement and explain how to find such an element β in terms of the primitive element α.

6. (14 points) Let α be a primitive element of $\mathbf{F}_{256}$. 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.

7. (14 points) Note that in $\mathbf{F}_2[x]$, we have

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

(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 $x^5 + x^2 + 1$. Find the multiplicative inverse of $\beta = \alpha^3 + \alpha$. Show all your work.

8. (18 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 given by E, α, and $\delta = 5$ 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 $k = \dim \mathcal{C}$.