Math 127, Spring 2022 **Name:** ______________________

Exam 3

This test consists of 8 questions on 6 pages, totalling 100 points. You are 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.

1. (10 points) Let I be a subset of a ring R. Define what it means for I to be an ideal of R.

2. (10 points) Let $\mathbf{F}_{32} = \mathbf{F}_2[\alpha]$, where α is a root of $x^5 + x^2 + 1$. Let $\beta = \alpha^4 + \alpha^2 + \alpha$ and $\gamma = \alpha^2 + 1$.

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

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

3. (10 points) Let $\mathbf{F}_{32}$ be a field of order 32. Is $\mathbf{F}_{32}$ isomorphic to $\mathbf{Z}/(32)$? Briefly **JUSTIFY** your answer.

4. (10 points) Suppose a is a nonzero element of $\mathbf{F}_{11}$ such that $a \neq 1$, $a^2 \neq 1$ and $a^5 \neq 1$. Briefly **EXPLAIN** why a must be a primitive element of $\mathbf{F}_{11}$.

5. (14 points) Let $\mathbf{F}_{4096}$ be the field of order $4096 = 2^{12}$, and let $\mathbf{F}_{4096}^{\times}$ be the multiplicative group of $\mathbf{F}_{4096}$.

(a) Does $\mathbf{F}_{4096}^{\times}$ contain an element of order 2? Briefly **EXPLAIN** your answer.

(b) What is the largest possible order of an element of $\mathbf{F}_{4096}^{\times}$? Briefly **EXPLAIN** your answer.

6. (14 points) Let α be a primitive element of $\mathbf{F}_{64}$. Find the minimal polynomial $m(x)$ of α^7 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

$$\begin{aligned} x^6 + x + 1 &= (x^2+1)(x^4+x^2+1) + (x), \\ x^4 + x^2 + 1 &= (x^3+x)(x) + 1. \end{aligned}$$

(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 $\alpha^4+\alpha^2+1$. Show all your work.

8. (18 points) Let $E = \mathbf{F}_{1024}$, let β be a primitive element of E, and let $\alpha = \beta^{31}$. Note that the order of α is 33 (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 $\delta = 5$ 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 $k = \dim \mathcal{C}$.

(This page intentionally left blank for scratchwork or extra space.)