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 $I = (x^2+1)$ 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.)

I is all poly mults of x^2+1
(defn of (x^2+1))

So $f(x) = x^2(x^2+1) \in I$

$f(x) = x^4 + x^2$

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 $\boxed{\alpha}$ of degree at most $\boxed{6}$.

$\alpha^7 = \alpha^3 + 1$

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

$$\beta\gamma = (\alpha^3+\alpha^2+1)(\alpha^4+\alpha)$$
$$= \alpha^7 + \cancel{\alpha^4} + \alpha^6 + \alpha^3 + \cancel{\alpha^4} + \alpha$$
$$= (\cancel{\alpha^3}+1) + \alpha^6 + \cancel{\alpha^3} + \alpha$$
$$= \alpha^6 + \alpha + 1$$

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.

$R = \mathbb{Z}/(16)$

$4(4) = 0$ in $\mathbb{Z}/(16)$

Field can't have zero divs

$\Rightarrow R$ not isom to $\mathbb{F}_{16}$.

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).

(a) Divisors of 2047: 1, 23, 89, 2047

(b) If $\alpha^1, \alpha^{23}, \alpha^{89} \neq 1$

then $\mathrm{ord}(\alpha) \neq 1, 23, 89$

$\Rightarrow \mathrm{ord}(\alpha) = 2047 \Rightarrow \alpha$ prim.

$\boxed{\alpha^1, \alpha^{23}, \alpha^{89}}$

NB: α^{2047} always $=1$, so no need

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.

False b/c 4 doesn't div 63

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

(a) $\text{ord}(\alpha) = 64 - 1 = 63$

(b) $\beta = \alpha^{21}$; $\text{ord}(\beta) = \dfrac{63}{\gcd(21, 63)} = 3$

2^8

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.

$\text{ord}(\alpha) = 255$, $\alpha^{255} = 1$

$O_5 = \{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{80}, \alpha^{160},$

$320 - 255$ $\alpha^{65}, \alpha^{130}\}$ $260 - 255 = 5$ ✓

$m(x) = (x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^{40})$
$(x-\alpha^{80})(x-\alpha^{160})(x-\alpha^{65})(x-\alpha^{130})$

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

$$\begin{aligned} x^5+\overset{m}{x^2}+1 &= (x^2+1)\overset{b}{(x^3+x)}+(x^2+x+1), && A_1 \\ b\quad x^3+x &= (x+1)(x^2+x+1)+(x+1), && A_2 \\ x^2+x+1 &= (x)(x+1)+1. && A_3 \end{aligned}$$

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

$m=0$

A_1 $\quad 0 = (\alpha^2+1)\beta + 1(\alpha^2+\alpha+1)$

$\alpha^2+\alpha+1 = (\alpha^2+1)\beta$

A_2 $\quad \alpha+1 = \beta + (\alpha+1)(\alpha^2+\alpha+1)$

$= \beta + (\alpha+1)(\alpha^2+1)\beta$

$= 1\beta + (\alpha^3+\alpha^2+\alpha+1)\beta$

$= (\alpha^3+\alpha^2+\alpha)\beta$

A_3 $\quad 1 = \alpha(\alpha+1) + (\alpha^2+\alpha+1)$

$= \alpha(\alpha^3+\alpha^2+\alpha)\beta + (\alpha^2+1)\beta$

$= (\alpha^4+\alpha^3+\alpha^2)\beta + (\alpha^2+1)\beta$

$1 = (\alpha^4+\alpha^3+1)\beta$

$\Rightarrow \beta^{-1} = \alpha^4+\alpha^3+1$

2^9

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 $k = \dim \mathcal{C}$.

$\alpha^{73} = 1$, $n = 73$ Want $d \geq \delta = 5$

$\delta - 1 = 4$

$128 - 73 = 55$

$110 - 73 = 37$

$\mathcal{O}_1 = [1, 2, 4, 8, 16, 32, 64, 55, 37]$

$74 - 73 = 1$ ✓

$96 - 73 = 23$

$92 - 73 = 19$

$\mathcal{O}_3 = [3, 6, 12, 24, 48, 23, 46, 19, 38]$

$76 - 73 = 3$ ✓

(a) $g(x) = m_1(x)\, m_3(x)$ $\deg g = 18$

(b) $k = n - \deg g = 73 - 18 = 55$

$\mathcal{C}$ is $[73, 55, d]$, $d \geq 5$

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