MATH 320 Unit 4 Exam Name:

Instructions:

Please write your answers on separate paper. Please write clearly and legibly, using a large font and plenty of white space (I need room to put my comments). Staple all your pages together, with your problems in order, when you turn in your exam. Make clear what work goes with which problem. Put your name on every page. To get credit, you must show adequate work to justify your answers. If unsure, show the work. No outside materials are permitted on this exam – no notes, papers, books, calculators, phones, smartwatches, or computers – only pens and pencils. You may freely use the contents of the box on the reverse side, but not any other results we may have proved. Each problem is out of 10 points, 40 points maximum. You have 30 minutes.

1. Prove that $x^3 + x + [1]$ is irreducible in $\mathbb{Z}_5[x]$.
2. Prove the Remainder Theorem.
3. Find all monic irreducible polynomials of degree at most 3 in $\mathbb{Z}_2[x]$.
4. Express $x^4 - [4]$ as a product of irreducibles in $\mathbb{Z}_7[x]$.

For any ring R, we define $R[x] = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in R, n \geq 0\}$, where x is a new element, that was not in R, which commutes with each element of R. We call n the *degree*[a] of the polynomial, writing $deg(f)$ or $deg(f(x))$, and a_n the *leading coefficient*, provided $a_n \neq 0_R$. $R[x]$ is called the *polynomial ring* with coefficients from R. Two polynomials are equal if their degrees are equal and all coefficients are equal. We call the polynomial *monic* if its leading coefficient $a_n = 1_R$.

Degree Sum Theorem: Let R be an integral domain, and $f(x), g(x)$ nonzero polynomials in $R[x]$. Then $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$.

$\mathbb{F}[x]$ Division Algorithm Theorem: Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ with $f(x) = g(x)q(x)+r(x)$ and either $r(x) = 0_{\mathbb{F}}$ or $deg(r(x)) < deg(g(x))$. We write $(f(x), g(x)) \to DA \to (q(x), r(x))$ or $(f, g) \to DA \to (q, r)$.

Let R be a commutative ring with identity, and let $a, b \in R$. We say that a is an *associate* of b if there is some unit $u \in R$ with $a = ub$. If $a \in R$ is not a unit and not 0_R, we call a *irreducible* if all of its divisors are units and associates (otherwise we call a *reducible*). We call nonzero nonunit $a \in R$ *prime* if it satisfies $\forall b, c \in R,$ if $a|bc$ then $\big(a|b$ or $a|c\big)$.

Unique Factorization Theorem: Let $R \in \{\mathbb{Z}, \mathbb{F}[x]\}$, and let $n \in R$ where $n \neq 0_R$ and n is not a unit in R. Then n has a factorization into primes, which is unique up to order and up to associates.

Let R be a commutative ring, and $f(x) \in R[x]$. Then $f(x) = a_nx^n + \cdots + a_1x + a_0$ *induces* a function $f : R \to R$ via $f(r) = a_nr^n + \cdots + a_1r + a_0$. We call $a \in R$ a *root* of $f(x)$ if $f(a) = 0_R$, that is if the induced function maps a to 0_R.

Remainder Theorem: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, and $a \in \mathbb{F}$. The remainder when $f(x)$ is divided by the polynomial $x - a$ is the constant polynomial $f(a)$. That is, $(f(x), x - a) \to DA \to (q(x), f(a))$.

Factor Theorem: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, and $a \in F$. Then a is a root of $f(x)$ if and only if $x - a$ is a factor of $f(x)$ (in $\mathbb{F}[x]$).

Max Root Theorem: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$ with[b] $deg(f(x)) = n$. Then $f(x)$ has at most n roots in $\mathbb{F}$.

---

[a] 0_R has no degree, while all other elements of R have degree 0.

[b] In particular, $f(x) \neq 0_{\mathbb{F}}$, since its degree exists.