MATH 320 Unit 3 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. Use the Euclidean algorithm to find $[5]^{-1}$ in $\mathbb{Z}_{13}$.
2. We work in $\mathbb{Q}[x]$. Take $f(x) = x^2 + 2x - 1$ and $g(x) = x^3 - 3x - 1$. Use the $\mathbb{F}[x]$ Euclidean algorithm to find $\gcd(f(x), g(x))$ and also find $u(x), v(x) \in \mathbb{Q}[x]$ satisfying $f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$.
3. Let R be a commutative ring with identity. Let $a \in R$ satisfy $a^4 = 0_R$. Prove that $1_R + ax$ is a unit in $R[x]$.
4. Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $[a] \in \mathbb{Z}_n$ with $[a] \neq [0]$. Prove that $[a]$ is a unit, if and only if $[a]$ is not a zero divisor.

We call $a \in R$ a *unit* if there is some $x \in R$ with $ax = xa = 1_R$ (1_R must exist). We write $x = a^{-1}$. We call $a \in R$ a *zero divisor* if $a \neq 0_R$ and there is some nonzero $x \in R$ with $ax = 0_R$ or $xa = 0_R$. A commutative ring R is an *integral domain* if it has identity 1_R and there are no zero divisors. A nontrivial[a] commutative integral domain R is a *field* if every nonzero $a \in R$ is a unit.

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*[b] 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 $a_n = 1_R$.

$\mathbb{Z}_p$ Theorem: Let $p \in \mathbb{Z}$ with $p \geq 2$. The following are equivalent: (i) p is prime; (ii) $\mathbb{Z}_p$ is an integral domain; (iii) $\mathbb{Z}_p$ is a field.

$\mathbb{F}[x]$ 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 $(f(x), g(x)) \rightarrow DA \rightarrow (q(x), r(x))$ or $(f, g) \rightarrow DA \rightarrow (q, r)$.

Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$, not both zero. We define their *greatest common divisor* $\gcd(f(x), g(x))$ or $\gcd(f, g)$ as their monic common divisor of greatest degree. (this must exist since $1_{\mathbb{F}}$, of degree 0, is always a monic common divisor)

Let $\mathbb{F}$ be a field, and let $a_1(x), a_2(x) \in \mathbb{F}[x]$ with $a_2(x) \neq 0$. We define the $\mathbb{F}[x]$ *Euclidean algorithm* as $(a_1, a_2) \rightarrow DA \rightarrow (q_1, a_3)$, then $(a_2, a_3) \rightarrow DA \rightarrow (q_2, a_4)$, and so on until $(a_k, a_{k+1}) \rightarrow DA \rightarrow (q_k, 0)$.

Bézout's Lemma: Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $u, v \in \mathbb{Z}$ with $au + bv = \gcd(a, b)$. Conversely, for any $x, y \in \mathbb{Z}$, we must have $\gcd(a, b)|(ax + by)$.

Bézout's $\mathbb{F}[x]$ Lemma: Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$, not both zero. Then there exist $u(x), v(x) \in \mathbb{F}[x]$ with $f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$. Conversely, for any $a(x), b(x) \in \mathbb{F}[x]$, we must have $\gcd(f(x), g(x))\big|\big(f(x)a(x) + g(x)b(x)\big)$.

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

$$\forall b, c \in R, \text{ if } a|bc \text{ then } \big(a|b \text{ or } a|c\big).$$

[a] A ring R is trivial if $R = \{0_R\}$, i.e. $|R| = 1$.

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