Final Exam (Post-Midterm 2) Conceptual Review

MATH 558, Fall 2020

Introductory Modern Algebra

Our Final Exam times are as follows:
11 am section: Wednesday, December 9, 10:30 am – 1 pm
1 pm section: Tuesday, December 8, 1:30 – 4 pm

The format of the Final Exam is the same as for the midterms.

Our exam is cumulative, but will focus more on the material covered after Midterm 2:
Sections 7C, 9A–9C, 12A, 12C, 13A–13B, 14A–14C, 15E–15F

Please refer to the previous review sheets to study material from before Midterm 2.

You may use a scientific calculator, but it should only be used to check arithmetic. In particular, you must use methods from class wherever applicable, and show your work.

The best preparation is to *practice, practice, practice* working, and re-working problems. This includes homework, quiz, and investigation module problems.

As usual, late exams will not receive credit, with no exceptions.

Zero divisors, units and orders of elements in $\mathbb{Z}/m\mathbb{Z}$

Concepts: Zero divisors and complementary zero divisors modulo m/in $\mathbb{Z}/m\mathbb{Z}$, units and their inverses modulo m/in $\mathbb{Z}/m\mathbb{Z}$, the order of a unit in a finite ring, Euler phi function, Fermat's little theorem, Euler's theorem, RSA Cryptosystem, encryption modulus.

Goals: Determine the (number of) zero divisors/units modulo m/in $\mathbb{Z}/m\mathbb{Z}$, find inverses of units in and find complementary zero divisors of zero divisors modulo m/in $\mathbb{Z}/m\mathbb{Z}$, decide whether $\mathbb{Z}/m\mathbb{Z}$ is a field, apply Fermat's little theorem and Euler's theorem, find orders of units mofulo m/in $\mathbb{Z}/m\mathbb{Z}$, prove properties of orders, study and use the RSA Cryptosystem.

Assignments: Chapter 7, #24–34; Chapter 9, #18–22, 27–29, 42–44, 46, 49, 52; Problems 1–3 in Section 10 of Savin text; Quiz 9, Quiz 10

Videos:
- Units in $\mathbb{Z}/m\mathbb{Z}$
- Zero divisors, units, and orders of units
- Fermat's Little Theorem
- Euler's Theorem

Additional practice problems:

(1) Determine the number of units and zero divisors in $\mathbb{Z}/36\mathbb{Z}$. *After* this, find them all. Finally, find the inverse of each unit, and the complementary zero divisors of each zero divisor.

(2) Prove, from scratch that $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

(3) Prove that every unit of a finite ring has a well-defined order.

(4) Find the order each unit mod 13.

(5) Determine whether there is an element of order 15 in $\mathbb{Z}/97\mathbb{Z}$? If so, find one.

(6) Find the least nonnegative residue of 2^{47} modulo 23.

(7) Prove that if p is prime, then $a^p \equiv a \bmod p$ no matter whether or not an integer a is divisible by p.

(8) Verify that 5^{11} is an inverse of 5 modulo 26 without calculating its least nonnegative residue modulo 26. Then find its least nonnegative residue.

Chinese remainder theorem

Concepts: Chinese remainder theorem (CRT), existence and uniqueness of solutions to CRT.

Goals: Find all solutions to a system of congruences of two or more equations, or determine that no solution exists, set up a system of congruences from a word problem, and find all solutions.

Assignments: Chapter 12, #3, 10, 11, 12; Investigation module on CRT

Additional practice problems:

(1) Find all integer solutions x to both $36x \equiv 29 \bmod 5$ and $36x \equiv 29 \bmod 17$. Then use your answer to find all solutions to $36x \equiv 29 \bmod 85$.

(2) Our class of 13 students starts a fund raiser by selling RSA encryption keys, at a price of $1 per key, shared equally among everyone. I collect the money (in one-dollar bills) to distribute equally among you all, and find that after dividing the dollar bills into 13 piles, there was $4 remaining. Then I hear that one student had dropped the class, so I divided the money into 12 piles, and find 10 bills remain. If nobody took in more than $100 in sales, how much money did the class make, in total?

(3) Find the largest solution less than 1000 to the following system of congruences:

$$x \equiv 0 \bmod 7,\ x \equiv 11 \bmod 12,\ x \equiv 18 \bmod 19$$

Polynomial rings

Concepts: Polynomial with coefficients in a commutative ring, polynomial ring, degree of a polynomial, evaluation of a polynomial, Degree Proposition, roots of a polynomial, Root theorem, Remainder theorem, D'Alembert's theorem, associate polynomials, divisor of a polynomial, irreducible/reducible polynomial, unique factorization of polynomials, GCD of two polynomials, Division Algorithm/Euclidean Algorithm for polynomials, Bézout's theorem for polynomials, field of complex numbers, complex conjugate, Fundamental Theorem of Algebra.

Goals: Prove properties about polynomials, factor polynomials over a field (including the field of complex numbers using ideas from the Fundamental Theorem of Algebra), apply the Division algorithm for polynomials, use the Euclidean Algorithm to find GCDs of pairs of polynomials, show properties about the degree of polynomials.

Assignments: Chapter 13, #1, 2, 4, 5; Chapter 14, #1, 2, 4, 5, 7, 8, 10(i), 15, 16, 24, 27, 34, 37, 41, 42, 45, 46; Chapter 15, #8, 9; Problems 1–3 in 11/24 Course Digest entry; Investigation module on Divisibility in Polynomial Rings

Videos:

- Introduction to polynomial rings
- Division algorithm for polynomials
- Roots of polynomials
- Unique factorization of polynomials
- The field of complex numbers

Additional practice problems:

(1) Prove the Degree Proposition for polynomials over a fields: If f, g are polynomials over a field, then $\deg(fg) = \deg f + \deg g$.

(2) Find a polynomial f in $\mathbb{Z}/8\mathbb{Z}[x]$ for which the quotient and remainder in the Division Algorithm are not unique. (Notice that $\mathbb{Z}/8\mathbb{Z}$ is not a field; try finding a polynomial whose leading coefficient that is a zero divisor!)

(3) Find all integers m for which $(x^3 + [3]) \mid (x^5 + x^3 + x^2 - [9])$ in $\mathbb{Z}/m\mathbb{Z}$.

(4) In $\mathbb{Z}/2\mathbb{Z}[x]$, find the unique monic GCD $d(x)$ of $f(x) = x^6 + x^5 + x^3 + x$ and $g(x) = x^8+x^7+x^6+x^4+x^3+x^2+x+1$. Then find $r(x), s(x)$ for which $r(x)f(x)+s(x)g(x) = d(x)$.

(5) Show that in $\mathbb{R}[x]$, $x^4+x^2+a^2$ and x^2-x+a are relatively prime for all integers $a \neq 0, 1$.

(6) Factor $f(x) = x^2 + bx + 4 \in \mathbb{R}[x]$ into irreducible monic polynomials, for every $b \in \mathbb{R}$.

(7) For every prime p, show that $x^p - x$ factors as $x(x-1)(x-2)\cdots(x-(p-1))$ in $\mathbb{Z}/p\mathbb{Z}$.

(8) Show that $2i$ is a root of $p(x) = x^3 - 5x^2 + 4x - 20$. Then use this fact to factor $p(x)$ into irreducible polynomials in $\mathbb{C}[x]$, and in $\mathbb{R}[x]$.

(9) Show that $i + 1$ is a root of $q(x) = x^4 - 2x^3 - x^2 + 6x - 6$. Then use this fact to factor $q(x)$ into irreducible polynomials in $\mathbb{C}[x]$, and in $\mathbb{R}[x]$.