Midterm 2 Conceptual Review

MATH 558, Fall 2020

Introductory Modern Algebra

- Midterm 2 will be taken online during our class period on **Tuesday, October 27**.
- Please note that **late exams will not receive credit**, with no exceptions.
- Our exam is cumulative, but focuses on the course material not covered in Midterm 1: Sections 4A–4C and Chapter 1, and Sections 5A–5B, 6A–6F, and 7A.
- 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.

Prime factorizations

Concepts: Unique prime factorization, Fundamental Theorem of Arithmetic (FTA), special property of primes, notion of divides in terms of prime factorizations, prime factorizations of GCD and LCM, the infinitude of primes.

Goals: Apply the FTA to prove statements about integers, including about divisibility, find GCDs and LCMs using prime factoizations, prove that certain numbers are irrational, prove that there are infinitely many primes.

Assignments: Chapter 4, #4, 10, 13, 14, 16, 17, 19–21, 30, 37, 43; Quiz 5, Quiz 6

Videos:
- The utility of prime factorizations
- Divisibility in terms of prime factorizations
- Existence of infinitely many primes
- $\sqrt{2}$ is irrational

Additional practice problems:

(1) Prove that if a prime p divides a product of integers $a_1 a_2 \cdots a_n$, then p must divide (at least) one of the a_i.

(2) If $a, b > 1$ are integers, prove that a and b are relatively prime if and only if a and b^k are relatively prime for all $k > 0$.

(3) Prove that if $a \mid bc$ and$(a, b) = 1$, then $a \mid c$.

(4) Prove that $\sqrt{15}$ and $\sqrt[3]{24}$ are irrational.

(5) Show that if $a \mid bc$ and $(a, b)|c$, then $a|c^2$.

Congruence modulo m

Concepts: Congruence modulo m, least nonnegative residue of an integer modulo m.

Goals: Prove properties of congruence modulo m, determine whether or not who integers are congruence modulo m, find the least nonnegative residue of an integer modulo m.

Assignments: Chapter 5, #1, 3, 4, 6, 7, 9, 11, 12, 15–17, 22; Quiz 6, Quiz 7

Videos:
- Introduction to congruence modulo m
- Least nonnegative residues modulo m
- Basic properties of congruence modulo m
- Calculations modulo m
- More practice on computations modulo m
- Congruence modulo m is an equivalence relation

Additional practice problems:

(1) Prove the reflexive, symmetric, and transitive properties of congruence modulo m.

(2) Find the least nonnegative residue of 4^n modulo 9 for all positive integers n. Then prove that $6 \cdot 4^n \equiv 6 \bmod 9$ for all $n > 0$.

(3) Show that $5^n + 6^n$ is a multiple of 11 for all odd integers $n > 0$, but for no even integers $n > 0$.

(4) Find the least nonnegative residue of 12^{39} and 6^{37} modulo 13, 85^{35} modulo 20, and 9^{100} modulo 24.

(5) Find the last digit of $11111^{555} \cdot 99999^{777}$.

Equivalence relations

Concepts: Equivalence relation, binary relation, reflexive property, symmetric property, transitive property, equivalence class, set is split up into equivalence classes that don't overlap, representative of an equivalence class.

Goals: Determine whether a given binary relation on a set is an equivalence relation, describe the equivalence classes associated to an equivalence relation.

Assignments: Chapter 1: #2, 3

Videos:
- Equivalence relations
- Congruence modulo m is an equivalence relation

Additional practice problems:

(1) Let A and B be sets, and fix a function $f : A \to B$ that is onto. Prove that the relation on A given by $x \sim y$ if $f(x) = f(y)$ is an equivalence relation, and carefully describe the equivalence classes.

$\mathbb{Z}/m\mathbb{Z}$

Concepts: $\mathbb{Z}/m\mathbb{Z}$, congruence class, addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$, representative of a congruence class, complete set of representatives modulo m, primitive root modulo m, units in $\mathbb{Z}/m\mathbb{Z}$.

Goals: Perform arithmetic in $\mathbb{Z}/m\mathbb{Z}$, solve equations in $\mathbb{Z}/m\mathbb{Z}$, study and prove properties about complete sets of representatives and primitive roots modulo m, determine units in $\mathbb{Z}/m\mathbb{Z}$ and their inverses.

Assignments: Chapter 6, #5–8, 42, 44, 47, 48, 61, 62; Quiz 7; Investigation Module on Arithmetic in $\mathbb{Z}/m\mathbb{Z}$

Videos:
- Intro to $\mathbb{Z}/m\mathbb{Z}$
- Review of $\mathbb{Z}/m\mathbb{Z}$
- Units in $\mathbb{Z}/m\mathbb{Z}$
- Solving equations in $\mathbb{Z}/m\mathbb{Z}$

Additional practice problems:

(1) Find a primitive root of 17 other than $3, 5, 6$, or 7.

(2) If $\{a_1, a_2, \ldots, a_m\}$ is a complete set of representatives for $\mathbb{Z}/m\mathbb{Z}$ and b is any integer, prove that $\{a_1 + b, a_2 + b, \ldots, a_m + b\}$ is also a CSR.

(3) Find all units, and determine each inverse: $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/20\mathbb{Z}$

(4) Prove that if $[a]_m = [b]_m$ in $\mathbb{Z}/m\mathbb{Z}$ and $(a, m) = 1$, then $(b, m) = 1$ as well.

(5) Find all solutions to $[14]X = [18]$ in $\mathbb{Z}/12\mathbb{Z}$.

(6) Explain why $[36]X = [6]$ has no solution in $\mathbb{Z}/45\mathbb{Z}$.

Groups and rings

Concepts: Binary operation, group, ring, identity, inverse, additive inverse/negative, multiplicative inverse, associative and distributive properties, units of a ring.

Goals: Give the precise definition of a group and of a ring, determine if a given set with given binary operation(s) is a group or ring, prove properties of groups and rings.

Assignments: Chapter 7, #1, 3, 5–9, 12, 15

Videos:
- Intro to groups
- Examples of groups
- Proofs of properties of groups
- More on groups
- Intro to rings

Additional practice problems:

(1) Determine which of these sets are groups under addition:
   (a) The set of rational numbers (in lowest terms) with even denominator.
   (b) The set of rational numbers (in lowest terms) with even denominator.
   (c) The set of all real numbers with absolute value < 1.
   (d) The set of all real numbers with absolute value ≥ 1, along with 0.
   (e) The set of rational numbers with denominator 1 or 2.
   (f) The set of rational numbers with denominator $1, 2$, or 3.

(2) Prove that for an element a of a ring R, $-(-a) = a$, and if a is a unit, then so is a^{-1}, and $(a^{-1})^{-1} = a$.

(3) Show that in a ring R, if $ab = ba = 1$ and $ac = 1$, then $b = c$.

(4) Prove the Distributive Law for $\mathbb{Z}/m\mathbb{Z}$.

(5) Explain why -1 is an element of any ring. Then re-prove that in a ring R with element a, $(-1)(-1) = 1$ and $(-1)a = -a$.