Jason Starr
Fall 2016

MAT 312 / AMS 351 Review Topics

Exam Policy. The final exam is closed book, closed notes, no electronic devices are allowed, and you need only bring a writing implement. You will write directly on the exam booklet. Scratch paper and a stapler will be provided.

Review Topics. Please be familiar with all of the following.

• Understand the division algorithm, particularly uniqueness of the quotient and the remainder.

• Understand the definition of the greatest common divisor of two integers, and be able to express the greatest common divisor as an integer linear combination of the two input integers using repeated application of the division algorithm (the Euclidean algorithm).

• Understand how to use recursion to define a mathematical object with dependence on a positive integer, such as factorials and binomial coefficients.

• Understand how to use induction to verify for all positive integers a proposition that depends on a positive integer, such as the Binomial Theorem.

• Understand prime and irreducible integers, and understand the relation between these.

• Understand unique factorization of integers and the Fundamental Theorem of Arithmetic. Be prepared to factor any specified integer less than 1000.

• For a specified positive integer n, understand the arithmetic system of congruence classes modulo n, i.e., modular arithmetic. Understand what it means for a congruence class to be invertible. Understand the special properties of the arithmetic system of congruence classes modulo a prime integer p.

• Know a necessary and sufficient condition for solving a single linear congruence. Understand the Chinese Remainder Theorem that reduces the solution of a linear congruence modulo a composite to simultaneous solutions of linear congruences modulo factors of the composite.

• Understand the totient function of Euler. Be able to compute the totient function for powers of primes. Reduce computation of the totient function for all integers to computation for powers of primes.

• Understand the statements and proofs of both Fermat's Little Theorem and Euler's Theorem. Use this to simplify exponentiation in modular arithmetic.

• Understand the basic Public Key encryption scheme. Understand what are the inputs of this scheme, and what are the challenges in implementing this scheme.

• Understand the statements and proofs of both Fermat's Little Theorem and Euler's Theorem. Use this to simplify exponentiation in modular arithmetic.

• Understand the basic Public Key encryption scheme. Understand what are the inputs of this scheme, and what are the challenges in implementing this scheme.

• Understand permutations of a finite set. Understand the identity permutation, understand the (non-commutative) composition of permutations, and understand inverses of permutations. Understand both "two-row" and disjoint cycle notation for permutations.

• Understand exponentiation of a single permutation. Understand the order of a permutation. Know how to compute the order of a permutation quickly from its disjoint cycle notation.

• Know what is a transposition. Understand the definition of the sign of a permutation. Know identities involving the sign. Know methods for computing the sign.

• Understand the group of permutations of a fixed finite set. Understand what is a subgroup, particularly in the context of the group of permutations of a fixed finite set.

• Know other examples of groups, such as the (non-commutative) group of invertible 2 by 2 matrices. Understand the special properties of the determinant with respect to the group operations on this group.

• Understand how to iteratively take a product of many copies of a group element with respect to the group composition, i.e., group exponentiation. Understand the meaning of order of a group element.

• Understand the notion of subgroup of a group. Understand the meaning of order of a subgroup. Understand the cyclic subgroup generated by an element and the relation between the order of the element and the order of the cyclic subgroup. Know that the intersection of subgroups is again a subgroup.

• Understand homomorphisms between specified groups. In particular, understand the determinant homomorphism defined on the group of invertible matrices, understand the "standard representation" homomorphism from the symmetric group to the group of invertible matrices, and understand the sign homomorphism on the group of invertible matrices. Know when a homomorphism is an isomorphism of groups.

• For a specified subgroup of a group, understand what are left cosets, respectively right cosets. Understand why the left cosets, resp. right cosets, form a partition of the group. Know the associated coset space. Understand Lagrange's Theorem and the notion of index of a subgroup of a group.

• Know what is conjugation in a group. Know the special properties satisfied by the conjugation maps $c_g : G \to G$, $c_g(h) = ghg^{-1}$.

• Know when a homomorphism is an isomorphism of groups. Know what is a normal subgroup, and understand the special properties of the left and right cosets of a normal subgroup. Understand the direct product of two specified groups.

• Understand when a product of cyclic groups is again a cyclic group. Know unique factorization of cyclic groups. Understand some simple results using counting of elements of specified orders to characterize certain groups, i.e., every finite group of prime order is cyclic.

• Understand the statement of Burnside's Lemma. In particular, for a subgroup of a symmetric group, know what are the fixed sets of each permutation in the subgroup.

• Know what are binary codes. Understand the basic scheme of error detection in binary codes. Know about word distance in binary codes, and the relation of distance to error corrections.

• Understand generator matrices and parity-check matrices. Using these, be able to compute the minimal distance between words.

• Understand addition, subtraction, scaling, and product for polynomials in one variable with coefficients in a specified field, e.g., the field of real numbers, the field of fractions, or a field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

• For polynomials, understand the division algorithm. Understand the notion of greatest common divisor of two nonconstant polynomials. Understand the Euclidean algorithm for polynomials.

• Understand prime and irreducible polynomials. Understand the unique factorization theorem for polynomials of one variable with real coefficients.

• Know the Fundamental Theorem of Algebra: every complex polynomial of positive degree has at least one complex zero.

• Understand polynomial congruences. Understand how the coset space for a polynomial is a real vector space with a distinguished real linear self-map. Understand how this defines a commutative product operation on the coset space.

• Know what is a field. Understand when the coset space for a polynomial is a field.

• Know how to compute arithmetic in a field arising as the coset space of a polynomial.

• Understand what it means for a binary linear code to be cyclic. Know what is a generator polynomial and parity polynomial for such a code. Be able to compute the syndrome of a word, and use this to find the codeword nearest to the given word.