MAT 312 / AMS 351 – APPLIED ALGEBRA – FALL 2016

Class webpage: `http://www.math.stonybrook.edu/~jstarr/mat312fall2016/index.html`
Lectures: Tuesday and Thursday 11:30am-12:50pm, in Math Tower P-131.
Course Description: The description in the undergraduate bulletin: Topics in algebra: groups, informal set theory, relations, homomorphisms. Applications: error correcting codes, Burnside's theorem, computational complexity, Chinese remainder theorem. This course is offered as both AMS 351 and MAT 312.

Prerequisites: C or higher in AMS 210 or MAT 211. **Advisory Prerequisite**: MAT 200 or CSE 113.

Text: J. F. Humphreys and M. Y. Prest, *Numbers, Groups and Codes, Second Edition*, available at University Bookstore @ Stony Brook.

Course Learning Objectives: The course learning objectives include the following. Each of these is an important learning objective for *all* advanced mathematics and applied mathematics courses. Each is amplified with specific examples.

• **Acclimate to New Mathematics.** Gain familiarity with a new mathematical idea (be it a definition, a result, an algorithm, etc.) through examples, through basic results that involve that idea, and through deeper results that reflect the significance of the idea. **Example.** Cyclic groups and permutation groups are examples of abstract groups. Lagrange's Theorem relates orders of elements in a group to the order of the group. Burnside's Theorem relates the number of orbits of an action of a group to the cardinalities of the fixed sets of group elements.

• **Apply and Model.** Understand how an abstract notion or result can lead to an algorithm or computation arising in a context different from the original notion or result. Understand the necessary hypotheses and limitations of that model. **Example.** Euler's Totient Theorem leads to a Public Key encryption scheme. The most common version of that scheme requires as input an integer that is product of two distinct primes. The security of the scheme depends on the computational difficulty of discovering those two primes from the given integer (which is sometimes quite easy for poor choices of the integer).

• **Specialize.** Pass from general theorems, definitions, and methods to specific examples. Be able to compute with those examples. **Example.** The Chinese Remainder Theorem allows to compute the congruence class of an integer modulo a composite from the congruence classes of that integer modulo factors of the composite. Specialize this to find the least nonnegative integer whose congruence class modulo 17 equals 3 and whose congruence class modulo 7 equals 6.

• **Generalize.** Understand examples of ideas, constructions and arguments originally developed in one context yet that extend to another context. **Example.** The arithmetic theory of the division algorithm, unique factorization, the Chinese Remainder Theorem, etc., also applies to polynomial with real coefficients.

• **Prove.** For a conjectured result, often expected from examples, heuristics and other indirect evidence, rigorously prove the result using techniques such as proof by induction, proof by contradiction, proof by cases, and more advanced proof techniques. **Example.** Prove that every finite group of even order contains an element of order 2 (one proof uses Burnside's Theorem).

Course Outcomes / Key Skills: The course outcomes / key skills include 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.

Date: Fall 2016.

• 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 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.

• 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.

• Understand homomorphisms between specified groups. Know when a homomorphism is an isomorphism of groups. 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.

• 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 additional, subtraction, scaling, and product for polynomials in one variable with real coefficients.

• 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 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.

Lecturer: The lecturer is Jason Starr, Math Tower 4-108, E-mail: jstarr@math.stonybrook.edu

Recitations: Please register for and regularly attend one of the recitations. Your recitation instructor is the instructor who knows you best and who answers any questions about grading on problem sets. Your recitation instructor will have input in the assignment of final letter grades. The recitation instructor is Harrison Pugh.

• Recitation 1 meets on Tuesdays, 1 – 1:53PM, in Frey Hall 224.

• Recitation 2 meets on Wednesdays, 11 – 11:53 AM, in Frey Hall 224.

Office Hours: Office hours for Jason Starr are tentatively scheduled as follows.

• Tuesdays 10 – 11AM, Math Tower P–143 (advising).

• Tuesdays 1:15 – 2:15PM, Math Tower 4–108.

• Thursdays 10 – 11AM, Math Tower 4–108.

Office hours for the recitation instructor Harrison Pugh will be posted as well.

Required reading: For each date there is required reading from sections in the textbook and sections in the course reader. You are to read the material *before* the lecture.

Grading: Problem Sets count for 20 percent of total class points. Recitation participation counts for 5 percent of total class points. Each in-class Midterm counts for 15 percent of total class points. The Final Exam counts for 30 percent of total class points.

Grading: Graded problem sets and exams will be handed back in recitation. If you cannot attend the recitation in which a problem set or exam is handed back, it is your responsibility to contact the instructor and arrange a time to pick up the work (typically in office hours).

Students are responsible for collecting any graded work by the end of the semester.

Academic Resources: There are a number of organizations on campus offering tutoring and other academic resources in various locations. One such organization is the Academic Success and Tutoring Center. The mathematics department offers drop-in tutoring in the Math Learning Center. You are strongly encouraged to talk to a tutor in the MLC if you have an issue and are unable to attend your lecturer's office hours.

Please be aware that tutors in the MLC deal with students on a first-come, first-served basis. Thus it is usually preferrable to speak with your instructor in their office hours. (Even if you find your instructor in the MLC, the instructor may be obliged to speak to other students before speaking with you.)

Problem Sets: There will be 11 Problem Sets, due at the beginning of lecture on Thursday. The lowest problem set score is dropped in computing final class points.

Exams: There will be three in-class exams during the lecture hour on the dates listed below, Thursday, September 29, Thursday, October 27th, and Tuesday, November 22nd. There will also be a final exam on Wednesday, December 14th, 5:30pm – 8pm. The in-class exams and the final exam are closed book and closed

notes. Calculators and other electronic devices are not allowed, except as indicated by the DSS office. Please bring your Stony Brook ID to all exams to be checked agains photo sheets.

Absences and Other Accommodations: All excused absences from exams or other class assignments must be brought to the attention of the instructor as soon as possible. All DSS accommodations must be pursued through the DSS office. In case of an excused absence from an in-class exam, typically the exam will simply not be counted towards total class points, with remaining exams weighted proportionately more. In some cases, and in all cases of a missed final exam, a make-up exam will be scheduled.

Schedule of Topics and Assignments

• Tuesday, August 30
Section 1.1 The division algorithm and greatest common divisors.

• Thursday, September 1
Section 1.2 Mathematical induction.
In-class Diagnostic Quiz.

• Tuesday, September 6
LABOR DAY. NO CLASS.

• Thursday, September 8
Section 1.3 Primes and the Unique Factorization Theorem.
Problem Set 1 due in lecture.

• Tuesday, September 13
Section 1.4 Congruence classes.

• Thursday, September 15
Section 1.5 Solving linear congruences.
Problem Set 2 due in lecture.

• Tuesday, September 20
Section 1.6 Euler's Theorem and public key codes.

• Thursday, September 22
Section 1.6 Euler's Theorem and public key codes.
Problem Set 3 due in lecture.

• Tuesday, September 27
REVIEW FOR MIDTERM 1

• Thursday, September 29
MIDTERM 1

• Tuesday, October 4
Section 4.1 Permutations.

• Thursday, October 6
Section 4.3 Definition and examples of groups.
Problem Set 4 due in lecture.

• Tuesday, October 11
Section 4.3 Definition and examples of groups.

• Thursday, October 13
Section 4.2 The order and sign of a permutation.
Problem Set 5 due in lecture.

• Tuesday, October 18
Section 5.1 Preliminaries on group theory.

• Thursday, October 20
REVIEW FOR MIDTERM 2
Problem Set 6 due in lecture.

• Tuesday, October 25
Section 5.2 Cosets and Lagrange's Theorem.

• Thursday, October 27
MIDTERM 2

• Tuesday, November 1
Section 5.3 Groups of small order.

• Thursday, November 3
Section 5.4 Error-detecting and error-correcting codes.
Problem Set 7 due in lecture.

• Tuesday, November 8
Binary Codes.

• Thursday, November 10
Section 6.1 Introduction to polynomials.
Problem Set 8 due in lecture.

• Tuesday, November 15
Section 6.2 The division algorithm for polynomials.

• Thursday, November 17
REVIEW FOR MIDTERM 3
Problem Set 9 due in lecture.

• Tuesday, November 22
MIDTERM 3

• Thursday, November 24
THANKSGIVING. NO CLASS.

• Tuesday, November 29
Section 6.3 Factorisation.

• Thursday, December 1
Section 6.4 Polynomial congruence classes.
Problem Set 10 due in lecture.

• Tuesday, December 6
Section 6.5 Cyclic codes.

• Thursday, December 8
FINAL REVIEW
Problem Set 11 due in lecture.

Required Syllabi Statements: The University Senate Undergraduate and Graduate Councils have authorized that the following required statements appear in all teaching syllabi (graduate and undergraduate courses) on the Stony Brook Campus.

Americans with Disabilities Act: If you have a physical, psychological, medical or learning disability that may impact your course work, please contact Disability Support Services, ECC (Educational Communications Center) Building, Room 128, (631) 632-6748. They will determine with you what accommodations, if any, are necessary and appropriate. All information and documentation is confidential.

Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and Disability Support Services. For procedures and information go to the following website: http://www.stonybrook.edu/ehs/fire/disabilities.

Academic Integrity: Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty is required to report any suspected instances of academic dishonesty to the Academic Judiciary. Faculty in the Health Sciences Center (School of Health Technology Management, Nursing, Social Welfare, Dental Medicine) and School of Medicine are required to follow their school-specific procedures. For more comprehensive information on academic integrity, including categories of academic dishonesty please refer to the academic judiciary website at http://www.stonybrook.edu/commcms/academic_integrity/index.html.

Critical Incident Management: Stony Brook University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to the Office of University Community Standards any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn. Faculty in the HSC Schools and the School of Medicine are required to follow their school-specific procedures.