MAT 312 APPLIED ALGEBRA

FALL 2021

Course Instructor: Lisa Berger
Office: Math 4-100A
Email: lisa.berger@stonybrook.edu
Web page: `http://www.math.sunysb.edu/~lbrgr/`
Current Office Hours:

Tuesdays and Thursdays: 3:00-4:00 in 4-100A
Mondays: 2:00-3:00 On-line Via Zoom
By appointment. Please send email to schedule.

Office hours may be adjusted to accommodate the instructor's schedule and/or student needs. Students unable to meet during scheduled office hours are encouraged to schedule an appointment with the instructor.

Recitation Instructor: Owen Mireles Briones-R01 and R02
Email: Owen.MirelesBriones@stonybrook.edu
Current Office Hours:

Tuesday 12-1 in Math 3-106
Tuesday 4-6 via Zoom in virtual MLC

Recitation Instructor: Jiahao Hu-R03
Email: Jiahao.Hu@stonybrook.edu
Current Office Hours:

Tuesday 8:30-9:30 in Math 3-105
Tuesday 3:30-5:30 via Zoom in virtual MLC

The exam day (below) was corrected from Tuesday to Wednesday.

General Information. This is an introductory course in abstract algebra with some emphasis on its practical applications. Abstract algebra is a critical tool in many fields of advanced mathematics and a beautiful theory of its own. We will cover chapters 1, 4, 5, and 6 of the textbook. Time permitting, we'll look at some applications beyond the scope of the book. You should leave this course with the beginnings of an understanding of the power of abstraction in mathematics and some ideas about how this abstraction is applied to cryptography and coding. This course will involve both computational and theoretical work, and the course MAT 200, an introduction to mathematical proof, is a recommended pre-requisite. You should be prepared to work through a lot of problems, prove your results and write your work clearly and accurately. Course information will be posted regularly to the course web page:

`http://www.math.sunysb.edu/~lbrgr/MAT312Fall2021.html`.

Students are expected to attend class regularly and are responsible for all announcements made in class or posted to the course page.

Pre-requisites. A *minimum* pre-requisite for this course is completion of linear algebra, MAT 211 or AMS 201; MAT 200 or CSE 250 is recommended.

0.1. Textbook.

We will be using the second edition of *Numbers, Groups and Codes* by J.F. Humphreys and M.Y. Prest

Homework/Class Work/Quizzes.

Homework is an essential component of the course. Homework will be assigned and collected regularly, and selected problems will be graded. Homework is due at the beginning of the recitation period for the week it is due, and late homework will not be accepted. Announced and/or unannounced quizzes may be given, and there may be assignments completed and collected during lecture or recitation. Students are expected to be present for all course meetings, and missed quizzes or classwork may not be completed for credit. The lowest 2 scores in the homework/classwork/quiz category will be dropped.

Homework is due at the beginning of the scheduled recitation and is to be submitted to the recitation instructor.

A significant part of doing mathematics is *communicating* mathematics. Homework is expected to be clear and grammatically correct, in addition to mathematically accurate. Homework not meeting this criteria may be returned ungraded.

You are encouraged to work together, but submitted written assignments must be your own work and represent your own understanding. If you consult any outside sources, these must be cited. If you need clarification on these statements, please ask.

Exams.

There will be two midterms exams and a final exam. Exam 1 is *tentatively* scheduled for Tuesday, September 28. Exam 2 is *tentatively* scheduled for Tuesday, November 9. The **final exam** is as scheduled by the University: Wednesday, December 15, 11:15 - 1:45 p.m.

Final Grades. Your final grades will be based on the following:

(1) Exam 1: 20%
(2) Exam 2: 20%
(3) Homework/Quizzes/Classwork: 30%
(4) Final Exam: 30%

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 are 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`.

If you do not understand the policy on academic integrity, please ask for clarification.

Disability Support Services. If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact the Student Accessibility Support Center, Stony Brook Union Suite 107, (631) 632 − 6748 or `http://studentaffairs.stonybrook.edu/dss/` or at sasc@stonybrook.edu. They will determine with you what accommodations 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 the Student Accessibility Support Center. For procedures and information go the the following website: `https://ehs.stonybrook.edu//programs/fire-safety/emergency-evacuation/evacuation-guide-disabilities`, and search Fire Safety and Evacuation Disabilities.

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 Student Conduct and Community Standards any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn. Until/unless the latest COVID guidance `https://www.stonybrook.edu/commcms/strongertogether/latest.php` is explicitly amended by SBU, during Fall 2021, "disruptive behavior" will include refusal to wear a mask during classes.

Further information about most academic matters can be found in the Undergraduate Bulletin, the Undergraduate Class Schedule, and the Faculty-Employee Handbook.

Student Learning Outcomes. Students should be able to do the following:

- Use the division algorithm in the integers and in a polynomial ring.
- State the definition of the greatest common divisor of two integers, and express the greatest common divisor as an integer linear combination of the two input integers using the Euclidean algorithm.
- Use recursion to define a mathematical object with dependence on a positive integer, such as factorials and binomial coefficients.
- Use induction to verify for all positive integers a proposition that depends on a positive integer.
- Define prime and irreducible integers, and describe the relation between these.
- State Fundamental Theorem of Arithmetic. Factor any specified integer less than 1000.
- Do modular arithmetic. Determine whether a congruence class is be invertible. Describe the special properties of the arithmetic system of congruence classes modulo a prime integer p.
- Describe a necessary and sufficient condition for solving a single linear congruence. Know the Chinese Remainder Theorem and use it to reduces the solution of a linear congruence modulo a composite to simultaneous solutions of linear congruences modulo factors of the composite.
- Compute the Euler totient function for powers of primes. Reduce computation of the totient function for all integers to computation for powers of primes.
- State and and prove Fermat's Little Theorem and Euler's Theorem. Use these theorems to simplify exponentiation in modular arithmetic.
- Describe the basic Public Key encryption scheme, including the inputs of this scheme. Discuss the challenges in implementing this scheme.
- Describe the permutations of a finite set, including the identity permutation; the (non-commutative) composition of permutations. Determine inverses of permutations. Use both "two-row" and disjoint cycle notation for permutations.
- Exponentiate a single permutation. Compute the order of a permutation quickly from its disjoint cycle notation.
- State what is a transposition and what is the sign of a permutation. State and use identities involving the sign. Use methods for computing the sign.
- Describe the group of permutations of a fixed finite set. State the definition of a subgroup, particularly in the context of the group of permutations of a fixed finite set.
- Provide other examples of groups, such as the (non-commutative) group of invertible 2 by 2 matrices. Explain 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.
- Define A subgroup of a group. Determine the of order of a subgroup. Describe the cyclic subgroup generated by an element and the relation between the order of the element and the order of the cyclic subgroup. Prove that the intersection of subgroups is again a subgroup.
- For a specified subgroup of a group, determine its left cosets, respectively right cosets. Prove that the left cosets, resp. right cosets, form a partition of the group. Describe the associated coset space. State and use Lagrange's Theorem about the index of a subgroup of a group.
- Define homomorphisms between specified groups. Prove when a homomorphism is an isomorphism of groups, and when it is not. Describe the direct product of two specified groups.
- Determine when a product of cyclic groups is again a cyclic group. Know unique factorization of cyclic groups. Prove some simple results using counting of elements of specified orders to characterize certain groups, e.g., that every finite group of prime order is cyclic.
- Explain what are binary codes. Describe the basic scheme of error detection in binary codes. Explain the concept of word distance in binary codes, and the relation of distance to error corrections.
- Use generator matrices and parity-check matrices to compute the minimal distance between words.
- Add, subtraction, multiply and scale, polynomials in one variable with real coefficients.

- Describe the analogous structures of the ring of integers and the ring of polynomials in one variable with real coefficients.
- Use the division algorithm for polynomials. Define the greatest common divisor of two non-constant polynomials. Use the Euclidean algorithm to determine a greatest common divisor of two polynomials.
- Define prime and irreducible polynomials. State the unique factorization theorem for polynomials of one variable with real coefficients.
- State and apply the Fundamental Theorem of Algebra.
- Determine polynomial congruences. Explain how the coset space for a polynomial is a real vector space with a distinguished real linear self-map. Describe how this defines a commutative product operation on the coset space.
- Define is a field. Determine when the coset space for a polynomial is a field.
- Do arithmetic in a field arising as the coset space of a polynomial.