General information.

- Semester: Fall, 2018.
- Lecture Time: Tuesday & Thursday 12:30PM – 01:50PM
- Lecture Venue: ED 111 (College of Education)
- Instructor: Shi Bai, SE230, `sbai@fau.edu`

Description. Computer algebra systems are now ubiquitous in all areas of science and engineering. In this course, we shall cover standard techniques from modern computer algebra.

We will start with basic techniques for manipulating large integers, matrices, and polynomials. Equipped with these, we will look at algorithms for fast multiplication and fast linear algebra and their applications for practical problems such as cryptography. We will also learn some topics in symbolic computation and numerical analysis. The goal of this course is to investigate the relationship between algebra/analysis and computation. After completion of the course, you should be able to analyze and compare the complexity of fundamental algorithms including arithmetics, effective linear algebra, polynomial system solving. We will use the computer algebra systems *SageMath* (`http://www.sagemath.org/`) throughout the course. This includes the use of SageMath to assist in the development of mathematical ideas and concepts, as well as a tool for analysis, problem-solving and modelling work. The course modules include:

- Fundamental Algorithms: representation of numbers and polynomial.
- Euclidean Algorithm
- Resultants and GCD Computation
- Fast Multiplication
- Fast Linear Algebra and application to factoring.
- Short Vectors in Lattice and application in cryptography.
- Factoring polynomials over Finite Fields

Textbook. We will mainly follow the textbook,

- J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press; 3 edition (June 28, 2013).

Supplementary reading. For additional reading,

- P. Zimmermann, A. Casamayou, N. Cohen and et al. *Computational Mathematics with SageMath*, Creative Commons, Free license: Attribution-ShareAlike 4.0 International. `http://sagebook.gforge.inria.fr/english.html`

Evaluation

The grade for the course will be determined by:

Homework (10% x 5), Midterm exams (15% x 2), Group project (20%).

Homework. Every two week there will be some homework assignments posted online. All these homework assignments contribute 50% to your overall score. There will be no assignments for the first week, the mid-exam weeks and the last week before the group project presentation. Assignments should be clearly handwritten or printed on paper or sent by email in PDF formats. Collaboration is allowed for the homework. But you must turn in your OWN write ups of all problems, and, if you do collaborate, you must write on your solution paper the names of the students you worked with. Failure to do so constitutes plagiarism.

Mid-exams. There will be two midterm exams, which counts for 30% of your overall grade. The tentative date of the midterm exams are Sep and Oct. The midterm exam will cover the lectures and topics taught during the first 2/3 semester.

Group project. A small research project (group project) on the applications of computer algebra will be given during the semester, which counts for 20% of the grade. The evaluation will be a group presentation, report and coding (if applicable).

Grading scale. At the end of the semester, the following scale for FAU grade will be used.

%	92-100	89-91	86-88	83-85	80-82	75-79	70-74	60-69	0-59
Grade	A	A-	B+	B	B-	C+	C	D	F

You should try to meet the above scale to be assured of the grade you want. A grade of I (incomplete) will only be given for circumstances specified in the FAU Catalog. This rarely happens.

Course Policies

Attendance. Attendance is required. Students are expected to be regular in class attendance and to fully participate in the course. Grade penalties will be imposed for unexcused absences.

Exam policies. No calculator, books, notes will be allowed at any time during exams. All exams will be taken as scheduled. Make-up examinations will not be given for missed tests, unless prior arrangements have been made under exceptional circumstances with advance notice. In the case of a valid excuse, it is the students responsibility to establish with documentation that the exam was missed for a solid reason. The student cannot make up a missed midterm or final exam without such documentation.

Counseling and Psychological Services (CAPS) Center: Life as a university student can be challenging physically, mentally and emotionally. Students who find stress negatively affecting their ability to achieve academic or personal goals may wish to consider utilizing FAU's Counseling and Psychological Services (CAPS) Center. CAPS provides FAU students a range of services – individual counseling, support meetings, and psychiatric services, to name a few – offered to help improve and maintain emotional well-being. For more information, go to http://www.fau,edu/counseling/.

Disclaimer. This syllabus is subject to reasonable changes/updates..