Syllabus for
BU-CAS-CS-235: Algebraic Algorithms

Basic concepts and algorithms for manipulation of algebraic objects, such as residues, matrices, polynomials, and applications to various CS areas, such as cryptography, fault-tolerance, etc. Emphases on rigorous reasoning and analysis. Coreq: CAS CS 232 and CAS MA 123 are recommended. (Counts as a CS Background course for the CS concentration.) 4 cr.

Text: Victor Shoup. A Computational Introduction to Number Theory and Algebra.
(2nd Edition) Cambridge University Press, ISBN-13:9780521516440
Free at http://www.shoup.net/ntb/ntb-v2.pdf Hardcopies (required!) also available at CS office.

Important Deadlines: Add class: M 1/30; **Drop: T 2/21; W grade: F 3/30; Final: M 5/7 9am**.

Room, Time: GCB-209 TR 9:30-11. Disc. Sec.: MCS-B23 F 10-11, CAS-229 F 2-3.

TF: Xianrui Meng (xmeng@cs.bu.edu) tel.: 857-540-0460; office: PSY 223, hours: M 3-4, W 11-12, TR 4-5, or by appointment

TF's Class Page: http://cs-people.bu.edu/xmeng/cs235

Instructor's office hours: T 11-1:50.

Instructor: Leonid Levin (Lnd@bu.edu); Office: MCS-273, tel.: 353-3649; home: 332-9492.

Grading: Midterm, Final, homework in roughly comparable weights.

Remarks

- You must register in a discussion section and attend **all** its meetings as well as my lectures.
- You are encouraged to cooperate in learning the lecture material, reading the book, notes, etc. However, **absolutely no** collaboration is permitted in doing the homeworks which are to be graded! The Dean's office will investigate any infractions of the CAS Academic Conduct Code which everyone must read thoroughly at: http://www.bu.edu/academics/files/2011/08/AcademicConductCode.pdf
- If your handwriting is hard to read, please type your homeworks. Start each problem on a new page (except really short ones); staple the pages. Include your name, class and homework number on the first page. Submit only one version of any material. Extra versions are not graded.
- Make answers short and to the point. Be as precise and specific as possible.
Make explicit your assumptions and goals (e.g., if showing partial work, clarify where exactly you could not complete the problem - otherwise the whole problem will be assumed wrong).
Sketch a proof for every un-obvious statement. Examples do **not** prove a general statement.
- Homeworks submitted within a week carry a premium; unless otherwise announced, no homeworks are accepted after the start of next class since the premium date.
All deadlines end at the **beginning** of class.
- No substitute exams are possible under **ANY** circumstances. If you think you will miss an exam, do not take the class. The exams are closed book. Only materials written with **your** own hand (not typed, printed, copied, or written by others) or your graded homeworks can be in the room.

I wish you enjoyment and success! -Leonid.