

# 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. 4 cr. Recommended coreq: CAS CS-132, MA-123.

**Text:** Victor Shoup. A Computational Introduction to Number Theory and Algebra.  
(2nd Edition) Cambridge University Press. Free at <http://www.shoup.net/ntb>

**Deadlines: Add class: F 2/5; Drop: M 3/1; W grade: F 4/2; Final Exam: T 5/4-8.**

**Room, Time:** KCB-106 MW 4:30-5:45pm  
Disc. Sec.: CAS-B06B T 9:30-10:20am, KCB-106 T 11:15-12:05pm

**TF:** Ngu Si Dang: [ndang@bu.edu](mailto:ndang@bu.edu); cell: 802-777-7966;  
office hours: T 6-7pm, R 10-11am, F 5:30-6:30pm via Zoom: <https://zoom.us/j/5911998238>

**Instructor's office hours:** by email, any time MWR 8am-8pm.

**Instructor:** Leonid Levin ([Lnd@bu.edu](mailto:Lnd@bu.edu)); home tel.: 617-332-9492.  
No calls nights 9pm-8am, Fridays eves, or Saturdays; anonymous calls blocked.

**Grading:** Midterm, Final, homework (in roughly comparable weights).

Classes will not be recorded: you can discuss all matters freely without concerns that it may be recorded. Synchronous participation is required. Exam info is tentative, may change. Vedeo must be ON during any exams. While you are permitted to take the class remotely, I strongly recommend against it: intense interaction is essential for the mastery of the material.

## 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 material of lecture, 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:  
[www.bu.edu/cas/current-students/phd-mfa-students/academic-policies-and-conduct-code](http://www.bu.edu/cas/current-students/phd-mfa-students/academic-policies-and-conduct-code)  
[www.bu.edu/academics/policies/academic-conduct-code](http://www.bu.edu/academics/policies/academic-conduct-code)
- If your handwriting is hard to read, type your homeworks. Start each problem on a new page (except really short ones); staple the pages. Include your name, class, 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. No electronics. Those leaving the room during the exam cannot come back.

I wish you enjoyment and success! -Leonid.