Mathemtics UN3020
Number Theory and Cryptography
Spring 2023
Columbia University

Instructor: Daniele Alessandrini.
E-mail: daniele.alessandrini@gmail.com
Office: 624 Mathematics.
Office hours: Tentative schedule: Mo. 2pm-3pm, Room 528 Mathematics, We. 11:30am-12:30pm, Room 622 Mathematics.
Website of the course:
https://www.math.columbia.edu/~alessandrini/Courses/NumberTheory-s2023/NumberTheory.html

Classroom: Room 312 Mathematics.
Lectures: Mo., We. 10:10am-11:25am.

Required text: There is no required text. We will mainly follow the notes by Gordan Savin: Numbers, Groups and Cryptography. They are available online here: https://www.math.utah.edu/~savin/book18.pdf.

Prerequisite: One year of Calculus; some familiarity with proofs or a willingness to learn.

Course outline: This is a course in elementary number theory. We will present some applications to cryptography to motivate the theory. Main topics: Prime numbers and factorization, congruences and modular arithmetic, primitive roots, quadratic residues and quadratic reciprocity. Planned applications to cryptography include RSA encryption algorithm, Diffie-Hellmann key exchange, Miller-Rabin primality test.

Attendance: Attendance is NOT mandatory. Anyway, when skipping a lecture it is YOUR responsibility to figure out the exact content of the lecture and to stay up to date with the course and the information given in class. Usually, the best way to do this is to ask your classmates and possibly to borrow someone's notes. The approximate content of every lecture is given in the website of the course, with pointers to the relevant textbook sections.

Homework: Homework exercises will be published online every Wednesday night, and the solutions are due 6 days later, on the night between Tuesday and Wednesday. More precisely, the dead line for submitting will be on Wednesday early morning, at 5am. The solutions must be submitted electronically, via Courseworks, at the Gradescope tab. We *will* accept late assignment, but we deduct 10% of the points for every day of lateness.

Extensions: Understandably, there will be some weeks when a student doesn't manage to submit the homework on time. In order to cover for these special situations, there are three special policies.

1. If you are just a few days late, you can still submit, with a small penalty of 10% of the points for every day of lateness.
2. At the end of the semester, I will discard the two worst grades of the homework sheets.

3. If you are under severe circumstances due to your health or other factors, you can ask for an extension. In this case, please send me an email explaining your situation, and, if the request seems reasonable, you will be allowed two extra weeks to submit one particular homework sheet. The extra time is reduced to only one extra week for the last graded homework sheet at the end of the semester. Extensions can be granted only once or twice per student during the semester. Students registered with disability services may have right to additional extensions.

Midterm exam: There will be two midterm exams. The first will be on Wednesday February 15th, the second on Wednesday March 29th.

Final exam: Projected schedule for the final exam: Wednesday May 10th, 9am–Noon. The date will be confirmed by the University. The date of the final exam is not under the instructor's control, and cannot be moved.

Exam dates: You *must* plan to take the midterm and final exams at the scheduled time, so please make your travel plans accordingly. Besides students with disabilities having prior arrangements with DS or CARDS, the only exceptions will be for those with an incapacitating illness, a serious family emergency, or situations of comparable gravity. In this case you will need to ask your advising dean to send me a note to confirm your situation of need. In case of illness, your advising dean will need to see a doctor's note. If your motivation seems reasonable, I will use the grade of your final exam as grade for your midterm. For the final exam, we will organize a make-up exam. Incompletes can be granted only by your advising dean and only in the circumstances mentioned above.

Students with disabilities: Students with disabilities, who are regularly registered with Columbia Disability Services (DS) or Barnard CARDS, may be granted extra accommodations for homework or for the exams, as required by their situation.

Academic dishonesty Anyone guilty of academic dishonesty, such as cheating on an exam or helping someone else to cheat, will fail the course and faces further academic discipline.

Grading: I will first compute a numerical final score for every student. This will depend on the homework, the midterm and the final exam. Every week the homework will be graded from 0 to 60 points. Every midterm and the final exam is graded from 0 to 60 points. The numerical final score is computed in the following way:

Let H be the average of the homework grades (where the two worst grades are discarded). Let M_1 and M_2 be the grades of the two midterms. Let F be the grade of the final exam. The numerical final score S, also from 0 to 60 points, is given by

$$S = \frac{10H + 25M_1 + 25M_2 + 40F}{100}\,.$$

In other words, the formula is: Homework 10%, midtermS 25% each, final 40%.

After computing the numerical final score for every student, I will translate them into letter grades (A,B,C,D,F) using a curve. I will choose the curve after the final exam.