18.781 Theory of Numbers Spring Semester, 2019

Class meetings: Monday, Wednesday, and Friday 3:00–4:00, in 2-139.

Text: Niven, Zuckerman, and Montgomery, *An Introduction to the Theory of Numbers*. You should try to read the text *before* class as well as after. Both your own understanding and your chance of catching the lecturer in a *faux pas* will be greatly increased.

I have not yet made a detailed syllabus for the second half of the semester; that should be filled in during February.

Lecturer: David Vogan, 2-355. Telephone: 617-253-4991. E-mail: `dav@math.mit.edu`. My office hours are Thursday 3:30–4:30, Friday 4–5, or by appointment. (But in practice I'll be in my office most of the time 9–5 weekdays, and dropping in is fine.)

Homework will be assigned in most classes. Problems assigned during each week will be collected at the beginning of the first class of the following week. You are free to consult your friends and any other sources while working on the problems, but you should write up your solutions entirely on your own. This is a place to show your understanding without time pressure.

You may if you wish email solutions to me; they should arrive at least half an hour before the class in which they are due, so that I can forward them to the grader appropriately.

Solutions will usually be posted shortly after the class in which the problems are due. In part for that reason, *late homework will not be accepted*. The grading system is mostly interested in your *best* work, and a single problem set will not have a large effect on how that looks.

Exams: There will be two exams during the lecture hour, on March 8 and April 17. There will be a three-hour final exam, scheduled by the Registrar soon. The exams will all be closed book.

Grading: Each hour exam will be worth 100 points, the final exam will be worth 150 points, and the problem sets will be worth a total of 150 points.

You are welcome to talk with anyone about the problem sets. **What you write up and hand in needs to be done entirely by yourself.**

Schedule

W 2/6	Lec 1	1.1–2	Division with remainder	
F 2/8	Lec 2	1.2	Greatest common divisor	
M 2/11	Lec 3	1.2	The Euclidean algorithm	PS 1 due
W 2/13	Lec 4	1.3	Prime factorization	
F 2/15	Lec 5	1.4	Binomial theorem	
Tue 2/19	Lec 6	2.1	Congruences	PS 2 due
W 2/20	Lec 7	2.1	Fermat, Euler, Wilson	
F 2/22	Lec 8	2.2	Solutions of congruences	
M 2/25	Lec 9	2.5	RSA	PS 3 due
W 2/27	Lec 10	2.3	Chinese Remainder Theorem	
F 3/1	Lec 11	2.6	Prime power moduli	
M 3/4	Lec 12	2.7	Solving equations mod p	PS 4 due
W 3/6	Lec 13		Review	
F 3/8	Lec 14		**Exam 1 on Chapters 1–2**	
M 3/11	Lec 15	2.10–11	Number theory and algebra	
W 3/13	Lec 16	3.1	Quadratic residues	
F 3/15	Lec 17	3.2	Quadratic reciprocity	
M 3/18	Lec 18	3.4	Binary quadratic forms	PS 5 due

W 3/20	Lec 19	3.5	Equivalence and reduction	
F 3/22	Lec 20	3.6	Sums of two squares	
3/25–3/29			**Spring break**	
M 4/1	Lec 21			PS 6 due
W 4/3	Lec 22			
F 4/5	Lec 23			
M 4/8	Lec 24			PS 7 due
W 4/10	Lec 25			
F 4/12	Lec 26			
M 4/15			**Holiday**	
W 4/17	Lec 27			PS 8 due
F 4/19	Lec 28			
M 4/22	Lec 29			PS 9 due
W 4/24	Lec 30		Review	
F 4/26	Lec 31		**Exam 2 on Chapters 1–3, ??**	
M 4/29	Lec 32			
W 5/1	Lec 33			
F 5/3	Lec 34			
M 5/6	Lec 35			PS 10 due
W 5/8	Lec 36			
F 5/10	Lec 37			
M 5/13	Lec 38			
W 5/15	Lec 39			
week of 5/20–5/24			**Final Exam**	