

MTWTh 1:00 – 3:00 pm, Physical Sciences 114

<http://people.ucsc.edu/~yorik/Math110>**Instructor:** Yonatan Katznelson**Office:** Baskin 361B**Phone:** 459 - 1046**Email:** yorik@ucsc.edu**Required text:** *Elementary Theory of Numbers*, by William J. LeVeque.

Course Description: Math 110 is an introduction to elementary number theory. Topics include divisibility and the primes, congruence arithmetic, quadratic reciprocity, the Gaussian integers, Diophantine approximation and Diophantine equations. We will also study (briefly) two simple applications of number theory to cryptography. See the lecture schedule for more details.

Reading: Students are expected to read the book, *early and often*. By this I mean that you should plan on reading the entire book at least twice before the end of the quarter and that you should stay ahead of the lectures (as described in the schedule that follows). There will also be supplements to the textbook (posted on the course website) that you should also read in detail two or three times. There will be a small collection of alternate texts covering much of the same material on reserve in the Science Library – you should take the time to explore these books as well. Bottom line — the more you read, the better you will understand the material.

Homework: Every reading assignment is accompanied by homework problems. Doing (or trying to do) the homework assignments is the best way to master the material. Homework will not be collected or graded.

Exams: There will be a quiz in class every Thursday and a comprehensive final (also on a Thursday). There will be no make-up quizzes, but your lowest quiz score will be dropped.

Course grade: Your three highest quiz scores contribute 20% each to your course grade and the final exam contributes 40%. Letter grades will correspond (approximately) to the following ranges:

Overall Score	Grade
90 – 100	A– to A+
80 – 89	B– to B+;
65 – 79	C to C+
60 – 64	C-
50 – 59	D
0 – 49	F

Key Summer Session dates:

Last day to enroll: Thursday, June 23

Last day to drop: Monday, June 27 (with refund)

Last day to withdraw: (no refund) Friday, July 8

Last day to change grade option: Friday, July 1

Students with disabilities: If you qualify for classroom/exam accommodations because of a disability, please submit your Accommodation Authorization Letter from the Disability Resource Center (DRC) to me as soon as possible, preferably within the first few days of the course. Contact DRC by phone at **831-459-2089** or by email at **drc@ucsc.edu** for more information.

TIPS FOR SUCCESS

1. Come to all the lectures, and come prepared — read the assigned sections at least once before the lecture, so you have an idea of what we will be discussing in the lecture. You don't have to read the material in depth the first time through. Have a look at the homework for the sections you have read — take note of the problems you find difficult or mysterious.
2. Read the material again after the lecture, this time in more depth. Read actively: take notes, try to work through the examples on your own.
3. Work in detail on the relevant homework problems after the second reading. Make a note of the problems that you don't understand so that you can ask about them.
4. **Ask questions** in class, during office hours and in section. Remember: the more specific your question, the better and more helpful the answer is likely to be.
5. Study with friends for a few hours a week. Technical skills can be practiced alone, but concepts should be *discussed*.
6. The standard for a 5-unit course at UCSC is 15 hours a week in a 10 week quarter, including lectures, sections and studying outside of class. In a 5-week summer session course, you should realistically expect to spend about 20-30 hours a week with the material in order to succeed.
7. If you feel that you are getting lost, take action. Don't wait and hope 'it goes away'. Come to office hours or ask questions in class to clear up any confusion.

CHEATING:

Cheating in any form (e.g., using notes on quizzes or exams, or copying from someone else) will not be tolerated. Any student caught cheating will be reported to the Math department and to his or her college provost. In most cases, students caught cheating will receive a failing grade. Students who help others cheat are also considered cheaters.

***Cheating devalues everyone's grades.
You should not tolerate it either.***

Lecture Schedule (subject to change)...
... with Quiz and Exam Dates (not subject to change).

Monday, 6-20: Introduction: a survey of classical problems in number theory, and a brief review of methods of proof.

Reading: Chapter 1

Homework: 1.3: 2, 4, 7; 1.4: 2; 1.5: 3, 4.

Tuesday, 6-21: Division with remainder and the GCD.

Reading: Sections 2.1 - 2.2.

Homework: 2.2: 1, 5, 6, 11.

Wednesday, 6-22: Unique factorization. The linear Diophantine equation.

Reading: Sections 2.3 and 2.4.

Homework: 2.3: 1, 3; 2.4: 1, 2, 6, 7.

Thursday, 6-23: Congruence I. **Quiz 1** (*chapters 1 and 2*).

Reading: Sections 3.1 and 3.2.

Homework: 3.1: 2, 3 ; 3.2: 1, 2, 5, 6, 10.

Monday, 6-27: Congruence II.

Reading: Sections 3.3 - 3.5.

Homework: 3.3: 1, 2; 3.4: 1, 2, 6, 7; 3.5: 2, 3, 8.

Tuesday, 6-28: Cryptographic interlude - Caesar, Vigenère and linear block ciphers.

Reading: Supplemental note on Cryptography I.

Homework:

Wednesday, 6-29: Polynomial congruences; quadratic residues.

Reading: Sections 3.6 and 3.7. Supplemental note on quadratic reciprocity.

Homework: 3.6: 1, 2, 4, 5; 3.7: 1, 2, 3, 4, 5.

Thursday, 6-30: Quadratic reciprocity. **Quiz 2.** (*chapter 3*).

Reading: Supplemental note on quadratic reciprocity.

Homework: Exercises 1 and 2 at the end of the supplemental note.

Monday, 7-4: *Holiday – no class.*

Tuesday, 7-5: Prime numbers and their distribution.

Reading: Supplemental note on prime numbers.

Homework: Exercises 1-3 in the Supplemental note on Primes.

Wednesday, 7-6: The order of an integer (mod m).

Reading: Section 4.1.

Homework: 4.1: 1, 2, 3, 4, 6, 7.

Thursday, 7-7: Cryptographic interlude — RSA. **Quiz 3.** (*Quadratic reciprocity and distribution of primes*).

Reading: Supplemental note on cryptography II.

Monday, 7-11: Diophantine Approximation.

Reading: Supplemental Note on Diophantine Approximation (and Section 5.6)

Tuesday, 7-12: Gaussian integers I

Reading: Sections 6.1 - 6.3

Homework: 6.2: 2, 3, 6; 6.3: 1, 2, 3, 4.

Wednesday, 7-13: Gaussian integers II

Reading: Sections 6.4 - 6.5

Homework: 6.4: 1, 2(a), 3; 6.5: 1, 2, 3.

Thursday, 7-14: Diophantine Equations I **Quiz 4.** (*Gaussian integers*).

Reading: Sections 7.1 - 7.2.

Homework: 7.2: 1, 2.

Monday, 7-18: Diophantine Equations II

Reading: Sections 7.3 - 7.4

Homework:

Tuesday, 7-19: Diophantine approximation III.

Reading: Section 7.5.

Wednesday, 7-19: Review

Reading: Review problems.

Thursday, 7-20: ***FINAL EXAM.***