

Lecture: 1:40–2:55p.m. Monday, Wednesday, Room: Engr 107.

Instructor: Dr. Seung H. Son www.uccs.edu/sson E-mail: sson@uccs.edu

Office: Engr 282 Phone: [719] 255–3515 Fax: [719] 255–3605

1420 Austin Bluffs Parkway, Colorado Springs, Colorado 80918.

Office hours : 3-4pm Mon., 12:20-1:20pm Wed., or by appointment

Prerequisite: Math 136 (Calculus II) and Math 215 (Discrete Math)

Text: *Elementary Number Theory*, 6th edition, David M. Burton, 2007, McGraw-Hill, ISBN: 0-07-305188-8

Description: A careful study, with emphasis on **proofs**, of the following topics associated with the set of integers; divisibility, congruences, arithmetic functions, sums of squares, quadratic residues and reciprocity, and elementary results on distributions of primes.

Important Dates:

Jan. 20 First day of lectures

Feb. 3 Last day to register/Final day for 100% Drop Refund

March 22–28 Spring Break: No classes

May 5 Last day of lectures

Exams: There will be two 75-minute exams, and the Final Exam.

Exam 1 1:40–2:55p.m., March 3 (Wed.)

Exam 2 1:40–2:55p.m., April 21 (Wed.)

Final 1:40–4:10p.m., May 10 (Mon.)

There will be NO makeup exams unless arrangements have been made prior to Feb. 4th. A missed exam will count as a **zero** toward your course grade. Online (or online-equivalent) students have different sets of rules, dates, exam-problem sets, exam types, grading policy, and curving. I will personally contact online students to explain the details after their official registration records are passed to me.

Grade : 100 points (50 pts: Exams 1, 2) plus extra-credit (EC) points (0 pts.: Homework, 0 pts.: Final)

A: 93–100 A–: 90–92.9 B+: 87–89.9 B: 83–86.9 B–: 80–82.9 C+: 77–79.9

C: 73–76.9 C–: 70–72.9 D+: 67–69.9 D: 63–66.9 D–: 60–62.9 F: below 60%

If the mean/median/average is abnormally low, I may curve the grade.

Classroom Behavior and Conduct: Students and faculty both share responsibility for maintaining a positive educational environment. Faculty have a responsibility to treat students with understanding, dignity and respect. Faculty also have the right and the authority to guide classroom discussion and to set reasonable limits on the manner in which students express opinions. Disruptive students in the academic setting hinder the educational environment. Students who fail to adhere to such reasonable limits shall be subject to disciplinary action(s) in addition to a mandatory “F” for the course grade.

Disruption, as applied to the academic setting, means verbal and other behavior in the classroom that a faculty member judges as interfering with normal academic functions. Disruptive student conduct is prohibited by Regent Laws, the UCCS Student Code of Conduct and the Student Classroom/Course-Related Behavior Policy. For more information go to the Office of the Dean of Students website at www.uccs.edu/dos/studentconduct/index.html.

Electronic devices: I will allow **NO electronic devices such as calculators, cell phones, or mp3 players** for any exam. You must turn off your devices before the exam begins.

Extra Credit: I may use in-class pop-Quizzes to give EC points at any “class/exam”-day (after Feb. 3rd) during this semester. More precisely, it is your responsibility to attend official classes and exams to obtain your extra credit. If you cannot attend some classes because of bona fide official reasons, you may request “No Extra Credit Day”. Last-minute e-mail request may not even be read by me. Only when I confirm that I will not give any extra credit, your request will be honored.

Drop : Please seek counseling from the Dean's office before dropping *any* course.

April 2: Last day to drop without special permission from your Dean.

Disability Statement: If you have a disability for which you are requesting an accommodation, you are encouraged to contact the Disability Services Office within the first week of classes. The Disability Services Office is located in Main Hall #105. (Phone number is 255-3354)

Outline:

Sec.	Subject	Practice problems	Homework
1.1	Mathematical Induction	9, 11, 13	1a, b, c, d, e, 3, 7
1.2	The Binomial Theorem	1a, b, 3c-f, 5a, c, 7, 9	3a, b, 5b
2.1	Early Number Theory	1b-d, 3, 7, 9, 11a, b	1a, 7
2.2	The Division Algorithm	3b, c, 5, 9, 11	1, 3a
2.3	The Greatest Common Divisor	15, 17, 19a-e, 21a, b, 23	1, 5, 7, 9, 13a, b
2.4	The Euclidean Algorithm	11	1, 5a, b, 9
2.5	The Diophantine Equation $ax + by = c$	3b-d, 5b, c	3a, 5a, 7
3.1	The Fundamental Theorem of Arithmetic	3b-e, 13, 15, 17, 19	3a, 5a, 11b
3.2	The Sieve of Eratosthenes	3, 9a, b, 13b, c	5, 7, 13a
3.3	The Goldbach Conjecture	23a, b, 25, 27	3, 9a, 13, 21a
4.2	Basic Properties of Congruence	5a, b, 7, 9, 11, 13, 15, 17	1a-c, 3, 5a-b
4.3	Binary and Decimal Representations of Integers	5a-c, 13, 15, 25, 27a-c	1, 3, 7a, b, c, d, 9, 11, 21, 23
4.4	Linear Congruences and the Chinese Remainder Theorem	7a, b, 911, 13, 15a-c, 17, 19	1a-c, d-f, 5, 9
5.2	Fermat's Little Theorem and Pseudoprimes	11a, b, 13, 15, 17, 19, 21	1, 3, 5, 7, 9a, b
5.3	Wilson's Theorem	13, 15, 17	1a-b, 5a-b, 7, 9
6.1	The Sum and Number of Divisors	13, 15, 17, 19, 21, 23a, b	1, 3, 5a-b, 7a-b, 9, 11
6.2	The Möbius Inversion Formula	3	1a-b, 5, 7a-b
6.3	The Greatest Integer Function	7, 9, 13a-b	1, 3, 5a-b
7.2	Euler's Phi-Function	9a, b, 11a, b, 13, 21	1, 3, 5, 7a-c
7.3	Euler's Theorem	5, 7	1a, b, c, 3, 9, 11, 13
7.4	Some Properties of the Phi-Function	3, 5a-c, 7, 9, 11, 13, 15	1, 3, 7
8.1	The Order of an Integer Modulo n	11, 13a, b	1a, b, c, 3, 5, 7, 9
8.2	Primitive Roots for Primes	7, 9, 11	1a-b, 3, 5
9.1	Euler's Criterion	9a, b, 11a, b, 13	1a-c, 3a-b, 5a-c, 7
9.2	The Legendre Symbol and Its Properties	7, 9, 11a, b, 13, 15, 17	1a-e, 3
9.3	Quadratic Reciprocity	9, 11, 13a, b, 15, 17, 19	1a-e, 3a-c, 5a-b, 7
12.2	Fermat's Last Theorem		
13.2	Sums of Two Squares	9a, b, 11a, b, 13a, b, 15, 17	3a-e, 5a, b, 7
13.3	Sums of More Than Two Squares	11, 15, 17	1a-d, 3, 5, 9a, b, c
15.2	Finite Continued Fractions		
15.3	Infinite Continued Fractions		
15.4	Pell's Equation		
16.4	The Prime Number Theorem and Zeta Function		