

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

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

Office: Engr 282 Phone: [719] 262–3515 Fax: [719] 262–3605

1420 Austin Bluffs Parkway, Colorado Springs, Colorado 80933-7150.

Office hours : 3–4p.m. Mon., 12:30–1:30p.m. 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. 23	First day of lectures
Feb. 6	Last day to register/Final day for 100% Drop Refund
Mar. 24–Mar. 30	Spring Break: No classes
4/30 or 5/5	2:35–2:55 p.m.: Instructor Evaluation (FCQ)
May 12	Last day of lectures

Exams: There will be two 75-minute exams and a comprehensive final exam.

Exam 1 1:40–2:55p.m., Feb. 27 (Wed.)

Exam 2 1:40–2:55p.m., Apr. 23 (Wed.)

Final Exam 1:40–4:10p.m., May 19 (Mon.)

There will be NO makeup exams unless arrangements have been made prior to Feb. 8th. A missed exam will count as a **zero** toward your course grade. I cannot change the *Final Exam date/time* and I will give no makeup final exams under any circumstances. If you do not take the final exam on the above date/time, the course grade will be an “F” by default.

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.

Grade : $66\%+1\%+33\%= 100\%$

66%: 2 Midterm exams: 33%/each exam

1%: Homework

33%: Final Exam

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.

Options: If you submit over 70% of the correct answers to the assigned homework problems before the first exam, your second exam score can override the first exam score. If your homework score is over 80% for the semester, your final exam score can determine the course grade.

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

Important dates:

Feb. 6: Last day to drop and receive a 100% tuition refund.

Apr. 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 262-3354)

Outline:

Sec.	Subject	Practice problems	Homework
1.1	Mathematical Induction	1c, 7, 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–d, 9, 11, 21, 23
4.4	Linear Congruences and the Chinese Remainder Theorem	11, 13, 15a–c, 17, 19	1a–f, 5, 7a, b, 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	15, 17, 19, 21, 23a, b	1, 3, 5a, b, 7a, b, 9, 11, 13
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	1, 3, 5, 7a–c, 21
7.3	Euler’s Theorem	5, 7, 11, 13	1a–c, 3, 9
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–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	13a, b, 15, 17, 19	1a–e, 3a–c, 5a, b, 7, 9, 11
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–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		