

Schedule

A week-by-week breakdown of the material.

Week 1 (09/05-09/09)

- Day 1
 - Numbers: Rationals, Reals, Complex¹
 - Basic proof techniques: Direct²
 - Assignment 1³
- Day 2
 - Basic proof techniques: Indirect⁴
 - Square root of 2 is irrational⁵
 - Quantifiers⁶
- Day 3
 - Principle of Mathematical Induction⁷
 - Strong induction and Well-Ordering Principle⁸
 - Fibonacci Numbers⁹
 - Assignment 2¹⁰

Week 2 (09/12-09/16)

- Day 1
 - Divisibility¹¹
 - Prime and Composite Numbers¹²
 - Assignment 3¹³
- Day 2
 - Patterns in the Primes¹⁴

¹[notes/numbers_intro.html](#)

²[notes/proofs_basic.html](#)

³[assignments/1.html](#)

⁴[notes/proofs_basic.html](#)

⁵[notes/irrationality_of_sqrt2.html](#)

⁶[notes/proofs_quantifiers.html](#)

⁷[notes/proofs_induction.html](#)

⁸[notes/proofs_induction_other.html](#)

⁹[notes/numbers_fibonacci.html](#)

¹⁰[assignments/2.html](#)

¹¹[notes/numbers_divisibility.html](#)

¹²[notes/primes_intro.html](#)

¹³[assignments/3.html](#)

¹⁴[notes/primes_patterns.html](#)

- Common Divisors¹⁵
- Day 3
 - The Division Theorem¹⁶

Week 3 (09/19-09/23)

- Day 1
 - A weird number system¹⁷
 - The Division Theorem (cont)¹⁸
 - Assignment 4¹⁹
- Day 2
 - The Euclidean Algorithm²⁰
 - Diophantine Equations²¹
- Day 3
 - Euclidean Division and Diophantine Equations²²
 - Finding all Solutions²³
 - Assignment 5²⁴

Week 4 (09/26-09/30)

- Day 1
 - Finding all Solutions (cont)²⁵
 - Fundamental Theorem of Arithmetic²⁶
- Day 2
 - Consequences of Fundamental Theorem²⁷
- Day 3
 - Modular Arithmetic and Congruences²⁸
 - Arithmetic with Congruences²⁹

¹⁵[notes/numbers_gcd.html](#)

¹⁶[notes/numbers_division_theorem.html](#)

¹⁷[notes/weird_number_system.html](#)

¹⁸[notes/numbers_division_theorem.html](#)

¹⁹[assignments/4.html](#)

²⁰[notes/numbers_euclidean_algorithm.html](#)

²¹[notes/equations_diophantine_intro.html](#)

²²[notes/equations_diophantine_and_euclidean.html](#)

²³[notes/equations_diophantine_all_solutions.html](#)

²⁴[assignments/5.html](#)

²⁵[notes/equations_diophantine_all_solutions.html](#)

²⁶[notes/numbers_fundamental_theorem.html](#)

²⁷[notes/numbers_fta_consequences.html](#)

²⁸[notes/congruence_intro.html](#)

²⁹[notes/congruence_arithmetic.html](#)

Week 5 (10/03-10/07)

- Day 1
 - Chinese Remainder Theorem³⁰
 - Assignment 6³¹
- Day 2
 - Congruence Classes as a Number System³²
- Day 3
 - MIDTERM (Study guide³³)

Week 6 (10/10-10/14)

- Day 1
 - Multiplicative Inverses³⁴
- Day 2
 - Basics of Encryption³⁵
 - Encryption via Multiplication³⁶
- Day 3
 - Fermat's Little Theorem³⁷
 - Assignment 7³⁸

Week 7 (10/17-10/21)

- Day 1
 - Fall Break
- Day 2
 - Reduced Residues and ϕ ³⁹
- Day 3
 - Reduced Residues and ϕ (cont)⁴⁰

³⁰[notes/congruence_chinese_remainder.html](#)

³¹[assignments/6.html](#)

³²[notes/congruence_system.html](#)

³³[notes/studyGuide1.html](#)

³⁴[notes/congruence_multiplicative_inverses.html](#)

³⁵[notes/encryption_basic.html](#)

³⁶[notes/encryption_mult.html](#)

³⁷[notes/congruence_fermats.html](#)

³⁸[assignments/7.html](#)

³⁹[notes/residues_basic.html](#)

⁴⁰[notes/residues_basic.html](#)

Week 8 (10/24-10/28)

- Day 1
 - Reduced Residues and ϕ (cont)⁴¹
 - Euler's Theorem⁴²
 - Assignment 8⁴³
- Day 2
 - Encryption via Exponentiation⁴⁴
- Day 3
 - Public Key Cryptography and RSA⁴⁵

Week 9 (10/31-11/04)

- Day 1
 - Public Key Cryptography and RSA (cont)⁴⁶
- Day 2
 - Order of Elements in \mathbb{Z}_n ⁴⁷
- Day 3
 - Polynomials over \mathbb{Z}_n ⁴⁸

Week 10 (11/07-11/11)

- Day 1
 - Primitive Roots⁴⁹
- Day 2
 - Primitive Roots (cont)⁵⁰
- Day 3
 - MIDTERM (Study guide⁵¹)

⁴¹[notes/residues_basic.html](#)

⁴²[notes/residues_eulers_theorem.html](#)

⁴³[assignments/8.html](#)

⁴⁴[notes/encryption_exponentiation.html](#)

⁴⁵[notes/encryption_rsa.html](#)

⁴⁶[notes/encryption_rsa.html](#)

⁴⁷[notes/residues_order.html](#)

⁴⁸[notes/residues_polynomials.html](#)

⁴⁹[notes/residues_primitive_roots.html](#)

⁵⁰[notes/residues_primitive_roots.html](#)

⁵¹[notes/studyGuide2.html](#)

Week 11 (11/14-11/18)

- Day 1
 - Applications of Primitive Roots: Diffie-Hellman protocol⁵²
- Day 2
 - Applications of Primitive Roots: Diffie-Hellman protocol (cont)⁵³
 - Quadratic Residues⁵⁴
 - Assignment 9⁵⁵
- Day 3
 - Quadratic Residues (cont)⁵⁶

Week 12 (11/21-11/25)

- Day 1
 - Law of Quadratic Reciprocity⁵⁷
- Day 2
 - Thanksgiving
- Day 3
 - Thanksgiving

Week 13 (11/28-12/02)

- Day 1
 - Gauss's Lemma⁵⁸
- Day 2
 - Proof of Quadratic Reciprocity⁵⁹
 - Assignment 10⁶⁰
- Day 3
 - Primality Tests⁶¹

⁵²[notes/encryption_diffie_hellman.html](#)

⁵³[notes/encryption_diffie_hellman.html](#)

⁵⁴[notes/residues_quadratic.html](#)

⁵⁵[assignments/9.html](#)

⁵⁶[notes/residues_quadratic.html](#)

⁵⁷[notes/residues_reciprocity.html](#)

⁵⁸[notes/residues_reciprocity.html](#)

⁵⁹[notes/residues_reciprocity_proof.html](#)

⁶⁰[assignments/10.html](#)

⁶¹[notes/primes_testing.html](#)

Week 14 (12/05-12/09)

- Day 1
 - Primality Tests (cont)⁶²
- Day 2
 - TBA
- Day 3
 - TBA

⁶²[notes/primes_testing.html](#)