

Schedule

A week-by-week breakdown of the material.

Week 1 (01/05-01/09)

- Day 1
 - Numbers: Rationals, Reals, Complex¹
 - Basic proof techniques: Direct²
 - Assignment 1³
- Day 2
 - Basic proof techniques: Indirect⁴
 - Square root of 2 is irrational⁵
- Day 3
 - Quantifiers⁶
 - Principle of Mathematical Induction⁷
 - Assignment 2⁸
- Day 4
 - Strong induction and Well-Ordering Principle⁹
 - Fibonacci Numbers¹⁰

Week 2 (01/12-01/16)

- Day 1
 - Divisibility¹¹
- Day 2
 - Prime and Composite Numbers¹²

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[assignments/2.html](#)

⁹[notes/proofs_induction_other.html](#)

¹⁰[notes/numbers_fibonacci.html](#)

¹¹[notes/numbers_divisibility.html](#)

¹²[notes/primes_intro.html](#)

- Assignment 3¹³
- Day 3
 - Patterns in the Primes¹⁴
 - Common Divisors¹⁵
- Day 4
 - The Division Theorem¹⁶

Week 3 (01/19-01/23)

- Day 1
 - A weird number system¹⁷
 - The Division Theorem (cont)¹⁸
 - Assignment 4¹⁹
- Day 2
 - The Euclidean Algorithm²⁰
- Day 3
 - Diophantine Equations²¹
 - Euclidean Division and Diophantine Equations²²
- Day 4
 - Finding all Solutions²³
 - Assignment 5²⁴

Week 4 (01/26-01/30)

- Day 1
 - Finding all Solutions (cont)²⁵

¹³[assignments/3.html](#)

¹⁴[notes/primes_patterns.html](#)

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](#)

- Fundamental Theorem of Arithmetic²⁶
- Day 2
 - Consequences of Fundamental Theorem²⁷
- Day 3
 - Modular Arithmetic and Congruences²⁸
- Day 4
 - Arithmetic with Congruences²⁹

Week 5 (02/02-02/06)

- Day 1
 - Review
- Day 2
 - MIDTERM (Study guide³⁰)
- Day 3
 - Chinese Remainder Theorem³¹
 - Assignment 6³²
- Day 4
 - Congruence Classes as a Number System³³

Week 6 (02/09-02/13)

- Day 1
 - Multiplicative Inverses³⁴
- Day 2
 - Multiplicative Inverses (cont)³⁵
- Day 3

²⁶[notes/numbers_fundamental_theorem.html](#)

²⁷[notes/numbers_fta_consequences.html](#)

²⁸[notes/congruence_intro.html](#)

²⁹[notes/congruence_arithmetic.html](#)

³⁰[studyGuide1.html](#)

³¹[notes/congruence_chinese_remainder.html](#)

³²[assignments/6.html](#)

³³[notes/congruence_system.html](#)

³⁴[notes/congruence_multiplicative_inverses.html](#)

³⁵[notes/congruence_multiplicative_inverses.html](#)

- Basics of Encryption³⁶
- Encryption via Multiplication³⁷
- Day 4
 - Fermat's Little Theorem³⁸
 - Assignment 7³⁹

Week 7 (02/16-02/20)

- Day 1
- Day 2
 - Reduced Residues and ϕ ⁴⁰
- Day 3
 - Reduced Residues and ϕ (cont)⁴¹
- Day 4
 - Reduced Residues and ϕ (cont)⁴²

Week 8 (02/23-02/27)

BREAK

Week 9 (03/02-03/06)

- Day 1
 - Euler's Theorem⁴³
 - Assignment 8⁴⁴
- Day 2
 - Encryption via Exponentiation⁴⁵
- Day 3

³⁶[notes/encryption_basic.html](#)

³⁷[notes/encryption_mult.html](#)

³⁸[notes/congruence_fermats.html](#)

³⁹[assignments/7.html](#)

⁴⁰[notes/residues_basic.html](#)

⁴¹[notes/residues_basic.html](#)

⁴²[notes/residues_basic.html](#)

⁴³[notes/residues_eulers_theorem.html](#)

⁴⁴[assignments/8.html](#)

⁴⁵[notes/encryption_exponentiation.html](#)

- Snow Day
- Day 4
 - Public Key Cryprography and RSA⁴⁶

Week 10 (03/09-03/13)

- Day 1
 - Public Key Cryprography and RSA (cont)⁴⁷
- Day 2
 - Public Key Cryprography and RSA (cont)⁴⁸
- Day 3
 - Order of Elements in \mathbb{Z}_n ⁴⁹
- Day 4
 - Polynomials over \mathbb{Z}_n ⁵⁰

Week 11 (03/16-03/20)

- Day 1
 - Review
- Day 2
 - MIDTERM (Study guide⁵¹)
- Day 3
 - Everything below is work in progress.
 - Primitive Roots⁵²
- Day 4
 - Primitive Root Theorem⁵³

⁴⁶[notes/encryption_rsa.html](#)

⁴⁷[notes/encryption_rsa.html](#)

⁴⁸[notes/encryption_rsa.html](#)

⁴⁹[notes/residues_order.html](#)

⁵⁰[notes/residues_polynomials.html](#)

⁵¹[studyGuide2.html](#)

⁵²[notes/residues_primitive_roots.html](#)

⁵³[notes/residues_primitive_root_theorem.html](#)

Week 12 (03/23-03/27)

- Day 1
 - Applications of Primitive Roots: Diffie-Hellman protocol⁵⁴
- Day 2
 - Congruential Random Number Generators⁵⁵
- Day 3
 - Quadratic Residues⁵⁶
- Day 4
 - The Legendre Symbol⁵⁷
 - Euler's Identity⁵⁸

Week 13 (03/30-04/03)

- Day 1
 - Properties of Legendre symbol⁵⁹
- Day 2
 - Law of Quadratic Reciprocity⁶⁰
- Day 3
 - Gauss's Lemma⁶¹
- Day 4

Week 14 (04/06-04/10)

- Day 1
- Day 2
- Day 3
- Day 4

⁵⁴[notes/encryption_diffie_hellman.html](#)

⁵⁵[notes/numbers_random.html](#)

⁵⁶[notes/residues_quadratic.html](#)

⁵⁷[notes/residues_legendre.html](#)

⁵⁸[notes/residues_eulers_identity.html](#)

⁵⁹[notes/residues_legendre_properties.html](#)

⁶⁰[notes/residues_reciprocity.html](#)

⁶¹[notes/residues_gauss_lemma.html](#)