

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
 - Prime and Composite Numbers¹²
- Day 2
 - Prime Factorization: Existence¹³

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](#)

¹³[notes/primes_factorization_existence.html](#)

- Day 3
 - Infinitude of Primes¹⁴
 - The Prime Number Theorem¹⁵
- Day 4

Week 3 (01/19-01/23)

- Day 1
 - Common Divisors¹⁶
- Day 2
 - The Division Theorem¹⁷
- Day 3
 - Euclidean Division Algorithm¹⁸
- Day 4
 - GCD via Euclidean Algorithm¹⁹

Week 4 (01/26-01/30)

- Day 1
 - Diophantine Equations²⁰
- Day 2
 - Euclidean Division and Diophantine Equations²¹
- Day 3
 - Other Diophantine Equations²²
 - Diophantine Equations: Finding all solutions²³
- Day 4
 - Fundamental Theorem of Arithmetic²⁴

¹⁴[notes/primes_infinitude.html](#)

¹⁵[notes/primes_theorem.html](#)

¹⁶[notes/numbers_gcd.html](#)

¹⁷[notes/numbers_division_theorem.html](#)

¹⁸[notes/numbers_euclidean.html](#)

¹⁹[notes/numbers_gcd_compute.html](#)

²⁰[notes/equations_diophantine_intro.html](#)

²¹[notes/equations_diophantine_and_euclidean.html](#)

²²[notes/equations_diophantine_other.html](#)

²³[notes/equations_diophantine_all_solutions.html](#)

²⁴[notes/numbers_fundamental_theorem.html](#)

Week 5 (02/02-02/06)

- Day 1
 - Finding all Divisors²⁵
- Day 2
 - MIDTERM
- Day 3
 - Modular Arithmetic and Congruences²⁶
- Day 4
 - Arithmetic with Congruences²⁷
 - Divisibility Tests²⁸

Week 6 (02/09-02/13)

- Day 1
 - Chinese Remainder Theorem²⁹
- Day 2
 - Congruence Classes as a Number System³⁰
- Day 3
 - \mathbb{Z}_n as a Ring³¹
- Day 4
 - Multiplicative Inverses³²
 - Multiplicative Cancellation³³

²⁵[notes/numbers_all_divisors.html](#)

²⁶[notes/congruence_intro.html](#)

²⁷[notes/congruence_arithmetic.html](#)

²⁸[notes/numbers_divisibility_tests.html](#)

²⁹[notes/congruence_chinese_remainder.html](#)

³⁰[notes/congruence_system.html](#)

³¹[notes/congruence_ring.html](#)

³²[notes/congruence_multiplicative_inverses.html](#)

³³[notes/congruence_multiplicative_cancellation.html](#)

Week 7 (02/16-02/20)

- Day 1
 - Wilson's Theorem³⁴
- Day 2
 - Basics of Encryption³⁵
- Day 3
 - Encryption via Multiplication³⁶
- Day 4
 - Fermat's Little Theorem³⁷

Week 8 (02/23-02/27)

BREAK

Week 9 (03/02-03/06)

- Day 1
 - Reduced Residues and Euler's ϕ ³⁸
- Day 2
 - Euler's Theorem³⁹
- Day 3
 - Fast exponentiation⁴⁰
- Day 4
 - Encryption via Exponentiation⁴¹

³⁴[notes/congruence_wilsons.html](#)

³⁵[notes/encryption_basic.html](#)

³⁶[notes/encryption_mult.html](#)

³⁷[notes/congruence_fermats.html](#)

³⁸[notes/residues_basics.html](#)

³⁹[notes/residues_eulers_theorem.html](#)

⁴⁰[notes/residues_exponentiation.html](#)

⁴¹[notes/encryption_exp.html](#)

Week 10 (03/09-03/13)

- Day 1
 - Public Keys and RSA⁴²
- Day 2
 - Order of Elements in \mathbb{Z}_n ⁴³
- Day 3
 - Polynomials over \mathbb{Z}_n ⁴⁴
- Day 4
 - Primitive Roots⁴⁵

Week 11 (03/16-03/20)

- Day 1
 - Primitive Root Theorem⁴⁶
- Day 2
 - MIDTERM
 - Applications of Primitive Roots: Diffie-Hellman protocol⁴⁷
- Day 3
 - Congruential Random Number Generators⁴⁸
- Day 4

Week 12 (03/23-03/27)

- Day 1
 - Quadratic Residues⁴⁹
- Day 2
 - The Legendre Symbol⁵⁰

⁴²[notes/encryption_rsa.html](#)

⁴³[notes/residues_order.html](#)

⁴⁴[notes/residues_polynomials.html](#)

⁴⁵[notes/residues_primitive_roots.html](#)

⁴⁶[notes/residues_primitive_root_theorem.html](#)

⁴⁷[notes/encryption_diffie_hellman.html](#)

⁴⁸[notes/numbers_random.html](#)

⁴⁹[notes/residues_quadratic.html](#)

⁵⁰[notes/residues_legendre.html](#)

- Day 3
 - Euler’s Identity⁵¹
- Day 4
 - Properties of Legendre symbol⁵²

Week 13 (03/30-04/03)

- Day 1
 - Law of Quadratic Reciprocity⁵³
- Day 2
 - Gauss’s Lemma⁵⁴
- Day 3
 - []
- Day 4

Week 14 (04/06-04/10)

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

⁵¹notes/residues_eulers_identity.html

⁵²notes/residues_legendre_properties.html

⁵³notes/residues_reciprocity.html

⁵⁴notes/residues_gauss_lemma.html