Schedule

A week-by-week breakdown of the material.

Week 1 (01/05-01/09)

- Day 1
  - Numbers: Rationals, Reals, Complex[1]
  - Basic proof techniques: Direct[2]
  - Assignment 1[3]
- Day 2
  - Basic proof techniques: Indirect[4]
  - Square root of 2 is irrational[5]
- Day 3
  - Quantifiers[6]
  - Principle of Mathematical Induction[7]
  - Assignment 2[8]
- Day 4
  - Strong induction and Well-Ordering Principle[9]
  - Fibonnaci Numbers[10]

Week 2 (01/12-01/16)

- Day 1
  - Divisibility[11]
- Day 2
  - Prime and Composite Numbers[12]

[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 3[13]

- Day 3
  - Patterns in the Primes[14]
  - Common Divisors[15]
- Day 4
  - The Division Theorem[16]

Week 3 (01/19-01/23)

- Day 1
  - A weird number system[17]
  - The Division Theorem (cont)[18]
  - Assignment 4[19]
- Day 2
  - The Euclidean Algorithm[20]
- Day 3
  - Diophantine Equations[21]
  - Euclidean Division and Diophantine Equations[22]
- Day 4
  - Finding all Solutions[23]
  - Assignment 5[24]

Week 4 (01/26-01/30)

- Day 1
- Day 2
- Day 3

[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

  - Other Diophantine Equations[25]
  - Diophantine Equations: Finding all solutions[26]
- Day 4
  - Fundamental Theorem of Arithmetic[27]

Week 5 (02/02-02/06)

- Day 1
  - Finding all Divisors[28]
- Day 2
  - MIDTERM
- Day 3
  - Modular Arithmetic and Congruences[29]
- Day 4
  - Arithmetic with Congruences[30]
  - Divisibility Tests[31]

Week 6 (02/09-02/13)

- Day 1
  - Chinese Remainder Theorem[32]
- Day 2
  - Congruence Classes as a Number System[33]
- Day 3
  - Zn as a Ring[34]
- Day 4
  - Multiplicative Inverses[35]
  - Multiplicative Cancellation[36]

[25] notes/equations_diophantine_other.html
[26] notes/equations_diophantine_all_solutions.html
[27] notes/numbers_fundamental_theorem.html
[28] notes/numbers_all_divisors.html
[29] notes/congruence_intro.html
[30] notes/congruence_arithmetic.html
[31] notes/numbers_divisibility_tests.html
[32] notes/congruence_chinese_remainder.html
[33] notes/congruence_system.html
[34] notes/congruence_ring.html
[35] notes/congruence_multiplicative_inverses.html
[36] notes/congruence_multiplicative_cancellation.html

Week 7 (02/16-02/20)

- Day 1
  - Wilson's Theorem[37]
- Day 2
  - Basics of Encryption[38]
- Day 3
  - Encryption via Multiplication[39]
- Day 4
  - Fermat's Little Theorem[40]

Week 8 (02/23-02/27)

BREAK

Week 9 (03/02-03/06)

- Day 1
  - Reduced Residues and Euler's phi[41]
- Day 2
  - Euler's Theorem[42]
- Day 3
  - Fast exponentiation[43]
- Day 4
  - Encryption via Exponentiation[44]

[37] notes/congruence_wilsons.html
[38] notes/encryption_basic.html
[39] notes/encryption_mult.html
[40] notes/congruence_fermats.html
[41] notes/residues_basics.html
[42] notes/residues_eulers_theorem.html
[43] notes/residues_exponentation.html
[44] notes/encryption_exp.html

Week 10 (03/09-03/13)

- Day 1
  - Public Keys and RSA[45]
- Day 2
  - Order of Elements in Zn[46]
- Day 3
  - Polynomials over Zn[47]
- Day 4
  - Primitive Roots[48]

Week 11 (03/16-03/20)

- Day 1
  - Primitive Root Theorem[49]
- Day 2
  - MIDTERM
  - Applications of Primitive Roots: Diffie-Hellman protocol[50]
- Day 3
  - Congruential Random Number Generators[51]
- Day 4

Week 12 (03/23-03/27)

- Day 1
  - Quadratic Residues[52]
- Day 2
  - The Legendre Symbol[53]

[45] notes/encryption_rsa.html
[46] notes/residues_order.html
[47] notes/residues_polynomials.html
[48] notes/residues_primitive_roots.html
[49] notes/residues_primitive_root_theorem.html
[50] notes/encryption_diffie_hellman.html
[51] notes/numbers_random.html
[52] notes/residues_quadratic.html
[53] notes/residues_legendre.html

- Day 3
  - Euler's Identity[54]
- Day 4
  - Properties of Legendre symbol[55]

Week 13 (03/30-04/03)

- Day 1
  - Law of Quadratic Reciprocity[56]
- Day 2
  - Gauss's Lemma[57]
- Day 3
  - []
- Day 4

Week 14 (04/06-04/10)

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

[54] notes/residues_eulers_identity.html
[55] notes/residues_legendre_properties.html
[56] notes/residues_reciprocity.html
[57] notes/residues_gauss_lemma.html