Notes, Assignments and Study Guides

Notes

- Numbers: Rationals, Reals, Complex[1]
- Basic proof techniques: Direct[2]
- Square root of 2 is irrational[3]
- Quantifiers[4]
- Principle of Mathematical Induction[5]
- Strong induction and Well-Ordering Principle[6]
- Fibonnaci Numbers[7]
- Divisibility[8]
- Prime and Composite Numbers[9]
- Patterns in the Primes[10]
- Common Divisors[11]
- The Division Theorem[12]
- A weird number system[13]
- The Division Theorem (cont)[14]
- The Euclidean Algorithm[15]
- Diophantine Equations[16]
- Euclidean Division and Diophantine Equations[17]
- Finding all Solutions[18]
- Finding all Solutions (cont)[19]
- Fundamental Theorem of Arithmetic[20]
- Consequences of Fundamental Theorem[21]
- Modular Arithmetic and Congruences[22]

[1] notes/numbers_intro.html

[2] notes/proofs_basic.html

[3] notes/irrationality_of_sqrt2.html

[4] notes/proofs_quantifiers.html

[5] notes/proofs_induction.html

[6] notes/proofs_induction_other.html

[7] notes/numbers_fibonacci.html

[8] notes/numbers_divisibility.html

[9] notes/primes_intro.html

[10] notes/primes_patterns.html

[11] notes/numbers_gcd.html

[12] notes/numbers_division_theorem.html

[13] notes/weird_number_system.html

[14] notes/numbers_division_theorem.html

[15] notes/numbers_euclidean_algorithm.html

[16] notes/equations_diophantine_intro.html

[17] notes/equations_diophantine_and_euclidean.html

[18] notes/equations_diophantine_all_solutions.html

[19] notes/equations_diophantine_all_solutions.html

[20] notes/numbers_fundamental_theorem.html

[21] notes/numbers_fta_consequences.html

[22] notes/congruence_intro.html

- Arithmetic with Congruences[23]
- Chinese Remainder Theorem[24]
- Congruence Classes as a Number System[25]
- Multiplicative Inverses[26]
- Basics of Encryption[27]
- Encryption via Multiplication[28]
- Fermat's Little Theorem[29]
- Reduced Residues and phi[30]
- Euler's Theorem[31]
- Encryption via Exponentiation[32]
- Public Key Cryprography and RSA[33]
- Order of Elements in Zn[34]
- Polynomials over Zn[35]
- Primitive Roots[36]
- Applications of Primitive Roots: Diffie-Hellman protocol[37]
- Quadratic Residues[38]
- Law of Quadratic Reciprocity, Gauss's Lemma[39]
- Proof of Quadratic Reciprocity[40]
- Primality Tests[41]

Assignments

- Assignment 1[42]
- Assignment 2[43]
- Assignment 3[44]
- Assignment 4[45]

[23] notes/congruence_arithmetic.html
[24] notes/congruence_chinese_remainder.html
[25] notes/congruence_system.html
[26] notes/congruence_multiplicative_inverses.html
[27] notes/encryption_basic.html
[28] notes/encryption_mult.html
[29] notes/congruence_fermats.html
[30] notes/residues_basic.html
[31] notes/residues_eulers_theorem.html
[32] notes/encryption_exponentiation.html
[33] notes/encryption_rsa.html
[34] notes/residues_order.html
[35] notes/residues_polynomials.html
[36] notes/residues_primitive_roots.html
[37] notes/encryption_diffie_hellman.html
[38] notes/residues_quadratic.html
[39] notes/residues_reciprocity.html
[40] notes/residues_reciprocity_proof.html
[41] notes/primes_testing.html
[42] assignments/1.html
[43] assignments/2.html
[44] assignments/3.html
[45] assignments/4.html

- Assignment 5[46]
- Assignment 6[47]
- Assignment 7[48]
- Assignment 8[49]
- Assignment 9[50]
- Assignment 10[51]

Study Guides

- Midterm 1 Study Guide[52]
- Midterm 2 Study Guide[53]
- Midterm 3 Study Guide[54]

[46] assignments/5.html
[47] assignments/6.html
[48] assignments/7.html
[49] assignments/8.html
[50] assignments/9.html
[51] assignments/10.html
[52] notes/studyGuide1.html
[53] notes/studyGuide2.html
[54] notes/studyGuide3.html