

DSE-1(ii): Elements of Number Theory

Weeks 1 and 2: Revisiting: The division algorithm, divisibility and the greatest common divisor. Euclid's lemma; The Euclidean algorithm, Linear Diophantine equations.

[1]: Chapter 2 (Sections 2.2, 2.3, 2.4 [up to page 28], and 2.5. All Theorems without proofs).

Weeks 3 and 4: The Fundamental theorem of arithmetic, The sieve of Eratosthenes, Euclid's theorem and the Goldbach conjecture; The Fibonacci sequence and its nature.

[1]: Chapter 3 (Sections 3.1 [Theorem 3.2 without proof], 3.2 [Theorem 3.4], and 3.3 [up to p 53]).

[1]: Chapter 14 (Sections 14.1, and 14.2 [All results without proofs]).

Week 5: Congruence relation and its basic properties.

[1]: Chapter 4 (Section 4.2).

Weeks 6 and 7: Linear congruences and the Chinese remainder theorem, System of linear congruences in two variables.

[1]: Chapter 4 (Section 4.4, Theorems 4.8, and 4.9 without proofs).

Weeks 8 and 9: Fermat's little theorem and its generalization, Wilson's theorem and its converse.

[1]: Chapter 5 (Section 5.2 up to before pseudo-prime at Page 90, Section 5.3 before Theorem 5.5).

Week 10: Number-theoretic functions for sum and the number of divisors of a positive integer, Multiplicative functions.

[1]: Chapter 6 (Section 6.1, All Theorems without proofs).

Week 11: The greatest integer function; Euler's phi-function and its properties.

[1]: Chapter 6 (Section 6.3 up to page 118)

[1]: Chapter 7 (Section 7.2, Theorem 7.2 without proof).

Weeks 12 and 13: Basics of cryptography, Hill's cipher, Public-key cryptosystems and RSA encryption and decryption technique.

[1]: Chapter 10 (Section 10.1).

Weeks 14 and 15: Introduction to perfect numbers, Mersenne numbers and Fermat numbers.

[1]: Chapter 11 (Sections 11.2 [up to page 223], 11.3 [before Theorem 11.4], and 11.4 [before Theorem 11.10]).

Essential Reading

1. Burton, David M. (2011). Elementary Number Theory (7th ed.). McGraw-Hill Education Pvt. Ltd. Indian Reprint 2017.