

Unit 4 Plan

Mon	Wed	Fri
Mar 27, 2023	Mar 29, 2023	Mar 31, 2023
Exam 3 (4.1, Crypto thru 9.5)	Jacobi Symbol (Crypto, 12.2B, 12.3) Due today: • Read Crypto: 12.4-5, RQ • D 12.3 • W 10.8	Quadratic Reciprocity (Crypto, 12.4-5) Due today: • Read Crypto: 13.3-4, RQ • D 12.5 • W 12.3
Apr 3, 2023	Apr 5, 2023	Apr 7, 2023
Euler Pseudoprimes (Crypto, 13.3-4) Due today: • Read Crypto: 9.6, 10.3, RQ • D 13.3-4 • W 12.5	Square roots mod p and mod n (Crypto, 9.6, 10.3) Quiz 7: Quadratic Symbols Due today: • Read Crypto: 14.3A, RQ • D 9.6, 10.3 • W 13.4	Easter Break
Apr 10, 2023	Apr 12, 2023	Apr 14, 2023
Oblivious Transfer (Simple Version) (Crypto, 14.3A) Due today: • Read ??, RQ • D 14.3A • W 10.3	Prerequisite Material from Ch 5-7: Units, Associates, "Primes" Due today: • Read 8.1, RQ • D Prereq • W 14.3	8.1 Arithmetic in Gaussian and Eisenstein Integers Due today: • Read 8.2-I, RQ • D 8.1 • W Prereq
Apr 17, 2023	Apr 19, 2023	Apr 21, 2023
8.2-I Primes in the Gaussian Integers Due today: • Read 8.2-II, RQ • D 8.2-I • W 8.1	8.2-II Primes in the Eisenstein Integers Due today: • Read 8.3, RQ • D 8.2-II • W 8.2-I	8.3 FLT for Exponent 3 Quiz 8: History Due today: • D 8.3 • W 8.2-II

Assigned Homework Problems

Topic	Discussion	Written
C 12.3	1*, 2*, 3*	4*
C 12.5	1, 2, 3, 4, 5, 6	7
C 13.3	1*, 2*, 3*, 4*	
C 13.4	2*	3*
C 9.6	2*, 3*	
C 10.3	3, 6, 7	4
C 14.3A	1*, 2*, 3*, 4*	7*
Prereq	4.45*, 6.10*	4.45*
8.1	1*, 2, 7	5
8.2-I	8*, 10, 11, (12), (13), 15	9
8.2-II	18, 21, 26 i - iv	20
8.3	31, 32, 33	

*An asterisk indicates that a modification or hint has been provided.

EE stands for "Extra Exercise."