

Unit 3 Plan

Mon	Wed	Fri
3.4 Gaussian and Eisenstein Integers (p 116-122 only) Due today: • Read 4.1-I, RQ • D 3.4 • W 3.3	Exam 2 (Ch 2-3)	4.1-I Congruence and Applications (through Example 4.7) Due today: • Read 4.1-II, RQ • D 4.1-I • W 3.4
Feb 27, 2023	Mar 1, 2023	Mar 3, 2023
Spring Break	Spring Break	Spring Break
Mar 6, 2023	Mar 8, 2023	Mar 10, 2023
4.1-II Fermat's Little Theorem and b-adic digits (p 136-140) Due today: • Read 4.1-III, RQ • D 4.1-II • W 4.1-I	4.1-III Linear Congruences and the CRT (through Example 4.26) Due today: • Read 4.1-IV, RQ • D 4.1-III • W 4.1-II	4.1-IV CRT Redux Due today: • Read Crypto: Intro, 1.1, 1.3, RQ • D 4.1-IV • W 4.1-III
Mar 13, 2023	Mar 15, 2023	Mar 17, 2023
Intro, Shift Cipher, OTP (Crypto, Intro, 1.1, 1.3) Quiz 5: Linear Cong. & CRT Due today: • Read Crypto: 1.6, 7.1, RQ • D 1.1, 1.3 • W 4.1-IV	Z/m, Trapdoors (Crypto, 1.6, 7.1) Due today: • Read Crypto: 7.2, RQ • D 1.6 • W 1.3	RSA (Crypto, 7.2) Due today: • Read Crypto: 9.5, RQ • D 7.2 • W 1.6
Mar 20, 2023	Mar 22, 2023	Mar 24, 2023
Fast Exponentiation Algorithm (Crypto, 9.5) Quiz 6: Z/m, Units Due today: • Read Crypto: 13.1-2, RQ • D 9.5 • W 7.2	Fermat Pseudoprimes (Crypto, 13.1-2) Due today: • Read Crypto: 10.8, 12.2A, RQ • D 13.1-2 • W 9.5	Euler's Criterion and the Legendre Symbol (Crypto, 10.8, 12.2A) Due today: • Read Crypto: 12.2B, 12.3, RQ • D 10.8 • W 13.2
Mar 27, 2023	Mar 29, 2023	Mar 31, 2023
Exam 3 (4.1, Crypto thru 9.5)	<i>Jacobi Symbol</i> (Crypto, 12.2B, 12.3)	<i>Quadratic Reciprocity</i> (Crypto, 12.4-5)

Assigned Homework Problems

Topic	Discussion	Written
4.1-I	1, 3, 12, (21)	2
4.1-II	4*, 6, 11, 14*	7
4.1-III	EE1*, EE2*, 16, EE3*	19*
4.1-IV	18*, 22*, 23	24
C 1.1	12	
C 1.3	1, 2, 7	3
C 1.6	3, 4, 22	5
C 7.2	1, 2, 4*, (10)	5*
C 9.5	1, 2, 5, 9*	12
C 13.1	1, 2, 7*, 8	
C 13.2	1, 2	3
C 10.8	10*, 11*, 12*	13*

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

EE stands for "Extra Exercise."