

College of Staten Island
Department of Mathematics
Course Outline: Math 347
Number Theory

Spring 2006
Pribitkin

Text: Elementary Number Theory and its Applications, Kenneth H. Rosen, 5th edition, Addison-Wesley, 2005

LESSON	SECTION	TOPIC	HOMEWORK
1		Overview: What is Number Theory?, Primes, Historical Figures	Read “What is Number Theory?”
2	1.1 1.2 1.3 1.4	Numbers and Sequences Sums and Products Mathematical Induction The Fibonacci Numbers	1.1/1,7,9,13,15,21,42 1.2/8,15,16,18 1.3/7,10,11,14,31,32 1.4/8,9,18,19,28
3	1.5 2.1	Divisibility Representations of Integers	1.5/3,5,6,13,21,22,34,35 2.1/1,5,6,14,28,30,31
4	3.1	Prime Numbers	3.1/1,3,5,6,13,24,25
5	3.2	The Distribution of Primes	3.2/1,2,3,10,12,21,22
6	3.3 3.4	Greatest Common Divisors The Euclidean Algorithm	3.3/1,3,4,5,8,9,15,22 3.4/1,3,5,7,19,20
7	3.5	The Fundamental Theorem of Arithmetic	3.5/1,5,7,8,11,15,16,31,33,41,43, 47,53,55,60,68,74
8	3.6	Factorization Methods and the Fermat Numbers	3.6/1,3,5,7,14,15,16,17
9	3.7	Linear Diophantine Equations	3.7/1,7,11,17,19,20,21,22,24
10	4.1 4.2	Introduction to Congruences Linear Congruences	4.1/1,5,6,10,16,23,27,28 4.2/1,5,9,13,14,15,16,18
11		TEST #1 (Lessons 1-9)	
12	4.3	The Chinese Remainder Theorem	4.3/3,4,7,12,13,15,16,18,19,20, 27,30,32,35
13	4.5	Systems of Linear Congruences	4.5/1,2,3
14	5.1 5.2	Divisibility Tests The Perpetual Calendar	5.1/2,3,4,11,13,17,19,22 5.2/1,2,3,6,7,10,13
15	6.1	Wilson’s Theorem and Fermat’s Little Theorem	6.1/3,7,11,16,19,22,25,33,36,37, 40,42,49
16	6.2 6.3	Pseudoprimes Euler’s Theorem	6.2/1,3,7,9,16,17,20 6.3/1,3,7,8,9,15,18,20
17	7.1	The Euler Phi-function	7.1/1,2,4,6,15,23,27,43,44,48
18	7.2 7.3	The Sum and Number of Divisors Perfect Numbers and Mersenne Primes	7.2/1,2,7,9,20,23 7.3/1,3,5,10,11,15,25,26,27,29, 30,35
19	7.4	Möbius Inversion	7.4/1,5,7,9,10,17,21,22,25,30,31
20		TEST #2 (Lessons 10,12-19)	
LESSON	SECTION	TOPIC	HOMEWORK

21	8.1	Character Ciphers	8.1/1,3,6,7,9,13
	8.2	Block and Stream Ciphers	8.2/1,2,7,13,16,17,18
22	8.3	Exponentiation Ciphers	8.3/1,2,4,6
	8.4	Public Key Cryptography	8.4/1,3,4,5,6,8,12
23	9.1	The Order of an Integer and Primitive Roots	9.1/1,4,5,7,15,16
	9.2	Primitive Roots for Primes	9.2/1,3,7,8,10
24	9.3	The Existence of Primitive Roots	9.3/2,3,7,11,13
	9.4	Index Arithmetic	9.4/1,2,3,5,6,7,9,10,12,13,16,17
25	9.5	Primality Tests Using Orders of Integers and Primitive Roots	9.5/1,2,5,9,11,13,14
	9.6	Universal Exponents	9.6/1,2,3,4,5,6,8,9,11,12,15
26	11.1	Quadratic Residues and Nonresidues	11.1/1,3,7,13,19,21,25,27,28,35
	11.2	The Law of Quadratic Reciprocity TEST #3 (Take-Home on Lessons 21-25)	11.2/1,3,6,7,14,15,16
27	11.3	The Jacobi Symbol	11.3/1,2,4,5,9,10,12,13,14,16
	11.4	Euler Pseudoprimes TEST #3 Due	11.4/1,3,8,9
28	13.1	Pythagorean Triples	13.1/1,3,5,8,10,11,12,14,15,16
	13.2	Fermat's Last Theorem	13.2/1,4,5,6,11,13,14,16,24,26
	13.3	Sums of Squares	13.3/1,2,4,5,6,7,9,11,12,13,22

Always read the pertinent sections from the book prior to doing homework!