

## Number Theory: Study Guide for Test 2

### Wilson's Theorem

5.4 Use Wilson's Theorem

Solve  $x^2 + 1 \equiv 0 \pmod{p}$ , for  $p \equiv 1 \pmod{4}$

### Euler's Generalization of Fermat's Little Theorem

7.2 Compute  $\varphi(n)$  from the prime factorization of  $n$

7.3 Use Euler's Generalization of Fermat's Little Theorem

7.3 Know how the RSA Public Key Cryptosystem works, i.e., roles of  $n$ ,  $j$ ,  $k$ , etc.

Use the Euclidean Algorithm to find  $j$ , given  $n$  and  $k$

### Order, Primitive Roots, and Indices

8.1 Find the order of an element  $(\text{mod } n)$  using the definition

Show that an element is a primitive root of  $n$

Be familiar with Theorem 8.1 and its corollaries

Use Theorem 8.1 to shorten order calculations

8.4 Find the index of  $a$  relative to  $r \pmod{p}$

Use the Laws of Indices

### Quadratic Congruences and Quadratic Residues

9.1 Find QRs and QNRs of  $p$  by definition, i.e., find squares  $(\text{mod } p)$

Use quadratic residues to solve  $ax^2 + bx + c \equiv 0 \pmod{p}$

9.2 Find QRs and QNRs of  $p$  using Legendre symbols

Calculate Legendre symbols by:

Theorem 9.2, Euler's Criterion, Gauss' Lemma, Index Criterion,  
Quadratic Nature of 2, Quadratic Reciprocity Law

Use quadratic residues to solve quadratic congruences

### Know How To

1. State by name:

Wilson's Theorem, Euler's Generalization of Fermat's Little Theorem,  
Primitive Root Theorem, Laws of Indices, Euler's Criterion, Gauss' Lemma,  
Index Criterion, Quadratic Nature of 2, Quadratic Reciprocity Law

2. Prove: Theorem 7.1, Theorem 8.1, Laws of Indices

### Study Class Notes, collected homework, and other homework

#### The other homework was:

**p101** #1, 3, 4, 11, 15, 18; **p133** #1, 4ab, 9; **p138** #2, 5, 7, 8, 10; **p156** #10, 11;

**p161** #1ab, 6a, 10, 12a; **p177** #1, 2, 3, 4, 6a; **p183** #1ab, 2, 4, 7, 10, 11a;

**p194** #1, 5; **p200** #1abc, 3