

MATH 332 - ALGEBRA AND NUMBER THEORY : HOMEWORK 7

DUE FRIDAY, OCTOBER 12TH (NO LATER THAN 12PM)

CHAPTER 5: QUADRATIC CONGRUENCES

Solve the following exercises from Adler & Coury:

Exercises (pages 153, 154):

1, 3, 8, 9, 11, 13, 18, 23, 32.

Also:

Problem 1. Show that if p is prime and $p \geq 7$ then there are always two consecutive quadratic residues modulo p , i.e. there is an integer a such that a and $a + 1$ are quadratic residues.

Problem 2. In the first prelim (Theory Question 2), you can find a sketch of a proof of the fact that there are infinitely many primes congruent to 3 modulo 4 (i.e. of the form $4k + 3$). Prove that there exist infinitely many primes congruent to 1 modulo 4, as follows:

Assume that there are only finitely many primes congruent to 1 modulo 4, which are p_1, \dots, p_n . Let $N = 4(p_1 \cdot p_2 \cdots p_n)^2 + 1$ and show that N has a prime factor congruent to 1 modulo 4 which is different from p_1, \dots, p_n .