18.781, Fall 2007 Problem Set 5
Due: FRIDAY, October 12

1. Complete the following problems from Niven-Zuckerman-Montgomery (henceforth NZM):

   Read section 2.11 and complete the following problems:

   NZM 2.11: 1, 6, 11

   NZM 3.1: 5, 7, 10, 12, 14, 17, 18, 20

2. PARI PROGRAM OF THE WEEK:

   We know that quadratic residues mod p are always easy to find (e.g. 1 mod p), but what about non-residues? First, write a PARI program to investigate what proportion of residues mod p are quadratic residues vs. non-residues. Can you explain or prove your answer?

   What about the smallest quadratic non-residue? How big is it, in terms of p? Write a PARI program to test how large the smallest quadratic NON-residue is. Given any N, do you think you can find a prime p with the smallest quadratic NON-residue $> N$?