Due Wednesday, November 3 at the beginning of class. All chapter and exercise numbers refer to Silverman's *A Friendly Introduction to Number Theory*, 4th edition.

(1) Ex. 19.4. For part (b), you only need to find the first three values of k.

(2) One of the following five integers is prime and the other four are composite:

$$56052361, 72498253, 118901521, 218472931, 295688467.$$

- (a) Apply the Fermat test to each of these integers. (Stop after you find the integer is composite, or after 3 tests.)
- (b) Of the numbers for which part (a) was inconclusive, apply the Rabin-Miller test to deduce which number is prime. (To be clear, the Rabin-Miller test does **not** prove the remaining number is prime, but since you are given that one number is prime, you can make the deduction.)

(3) Ex 20.3

(4) Ex. 21.1

(5) Ex. 21.3

(6) Ex. 20.2 (b)–(d) & Ex. 21.5

(7)
- (a) Let p be a prime such that $p \not\equiv 5 \bmod 8$. Use Legendre symbols to show $x^8 \equiv 16 \bmod p$ has a solution.
- (b) Suppose $y \in \mathbb{Z}$ such that $y^2 \equiv -1 \bmod p$. Show that $\{\pm 1 \pm y\}$ (signs independent) are solutions of $x^4 \equiv -4 \bmod p$.
- (c) Deduce that $x^8 \equiv 16 \bmod p$ has a solution even if $p \equiv 5 \bmod 8$.

(8) Suppose n is the product of distinct primes. Fix $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Show that a is a quadratic residue modulo n (i.e. $x^2 \equiv a \bmod n$ has a solution) if and only if a is a quadratic residue modulo p for all primes $p \mid n$.