Math 112-40, Mr. Church, Homework 12 (last homework)

Due at the beginning of class on Wednesday, December 2.

Please staple your homework.

1. Exercise 7.10.

2. Exercise 7.11(a).

3. We saw last week that -1 has a square root modulo a prime p if and only if $p \equiv 1 \pmod 4$. Let's check this for a few examples:

   (a) Find a square root of -1 modulo 5 (that is, a number x so that $x^2 \equiv -1 \pmod 5$).

   (b) Find a square root of -1 modulo 11.

Now we'll investigate a related phenomenon.

   (c) Find a square root of 5 modulo 11.

   (d) Find a square root of 11 modulo 5 (this may be easier than you think).

This pattern follows from a beautiful theorem of Gauss, called quadratic reciprocity:

Theorem (Quadratic reciprocity): If p and q are primes and both $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$, then

$$p \text{ has a square root modulo } q \iff q \text{ has a square root modulo } p.$$