**Homework 10**

**Instructions:** Do as many of the problems as you like, but make sure to complete at least **three**. Then I will create a solution from your work.

1. Solve the following quadratic congruences, if possible. If not possible, justify why.

For each of these we can use the quadratic formula (the slightly modified form of )

a.

* Using the above equation and and simplifying we obtain .
* By Euler's criterion we know that 2 has a square root modulo 17 because .
* Through guess-and-check we can determine that 6 is one of the square roots of 2 modulo 17.
* Additionally, so . This tells us that .
* Putting this all together and simplifying we obtain

b.

* With the quadratic equation we obtain .
* Using WolframAlpha we can find that . Thus, by Euler's Criterion, 11 does not have a square root modulo 17.
* So no solution exists for the given congruence.

c.

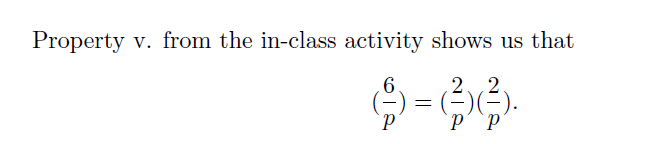
* With the quadratic equation we obtain .
* Modulo 17, the square root of 9 is 3 because and the inverse of 6 is 3 because .
* With these substitutions we obtain

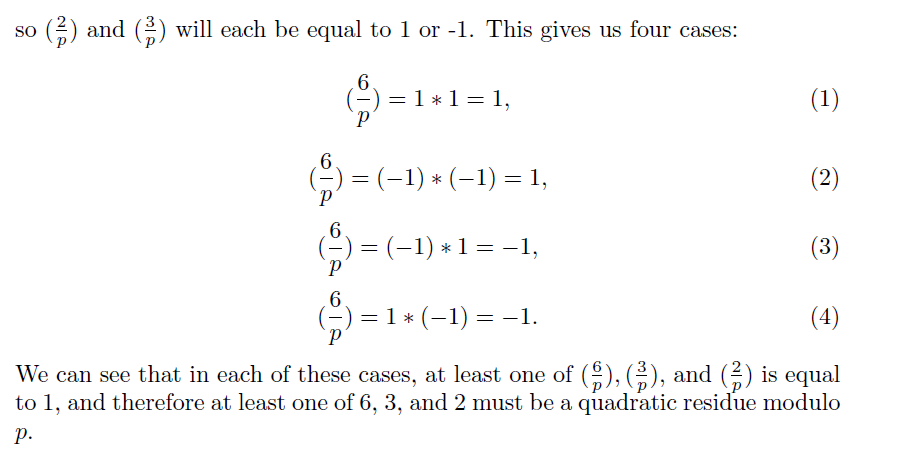
1. Calculate  
   a. The second term is 1 because 144 is a square and the first term is 1 because 601=1 (mod 4). So the final result is 1.

b. This is equal to -1 because 607=3 (mod 4).  
  
c. This is also equal to 1, using a similar process as in a.

* Since , we can rewrite this as .
* We know so and so .
* Using quadratic reciprocity we know .
* We can easily see that .
* Additionally, since then by Theorem 2 of the in class activity, .
* Thus, so and .

1. Let be a prime number. Show that at least one of 2, 3, or 6 must be a quadratic residue modulo *p.*

**

**

1. Let *p* be an odd prime and suppose that *a* is an element modulo *p* with odd order. Show that *a* is a quadratic residue. (Hint: Euler’s criterion)

* Let *g* be the order of *a*. By assumption *g* is odd. We know meaning . Since *p* is odd, *p-1* is even. Since *g* is odd, this also means that .
* Thus, since by definition, we also know .
* Finally, by Euler's criterion this means and is a quadratic residue modulo *p*.

1. Compute by hand (Hint: 8831 is prime and )

Using QR:

Note that the second term on the left hand side reduces to (9/11)=1 (9 is clearly a square), so the first term must be -1.

as well.

The second term on the left reduces to (15/19), which is -1 because 15 is not a square mod 19 (trial-error, or 15^9=-1 (mod 19)). Therefore, the first term must be 1.

The second term reduces to (16/41)=1, therefore the first term is 1 too.

This gives us

1. Let *p* be an odd prime not equal to 5. Show that if and only if

First, note that Then by QR, if

Therefore, is equal to and the latter is equal to 1 if and only if This is the same condition as given in the problem statement.