**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 an inverse 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.

* Seeing that 601, 607, and 461 are each prime, for each of these we could use the fact that .
* We may also use quadratic reciprocity which states that for distinct odd primes *p, q* then . This can be used along with the fact that .

a.

* This can be rewritten as .
* Sicne , .
* Since we know by property (iv) of the in class activity.
* Thus .

b.

* Since we know by property (iv) of the in class activity.
* Alternatively we could use . These explanations both stem from the same place mathematically.

c.

* 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.*
2. 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 Eulers criterion this means and is a quadratic residue modulo *p*.

1. Compute by hand (Hint: 8831 is prime and )
2. Let *p* be an odd prime not equal to 5. Show that if and only if