Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 37
Sage LAB—Quadratic Reciprocity!

Organizational Notes

1. A Zoom recording link and class notes will be sent out after each Zoom class.

2. Remember to send your answers to the classroom worksheets, and pdfs of your Lab work. Title your email with enough to help me record your "participation".

3. Homework #6 is due Mon., Nov. 16.

Logging into Sage/CoCalc

1. Start the Chrome browser.
2. Go to `http://cocalc.com` and sign in.
3. You should see an existing Project for our class. Click on that.
4. Click "New", call it **c37**, then click "Sage Worksheet".
5. For each problem number, label it in the Sage cell where the work is. So for Problem 1, the first line of the cell should be `#Problem 1`.
6. When you are finished with the worksheet, click "make pdf", email me the pdf (at `clarson@vcu.edu`, with a header that says **Math 305 c37 worksheet attached**).

Our ultimate goal is to prove:

(Gauss' Quadratic Reciprocity Law) For distinct odd primes p and q,

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Next we'll need Euler's Criterion and Gauss' Lemma. We'll investigate these computationally before we prove them. That is, we'll try better to understand what they say by computing examples.

1. (Euler's Criteria). $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, for prime p. Check for $p = 47$, and every $a \in 1..(p-1)$.

2. **(Gauss' Lemma)**. Let p be an odd prime and let a be a non-multiple of p. Form the integers:

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

and reduce them $\pmod{p}$ to lie in the interval $(-\frac{p}{2}, \frac{p}{2})$. Let ν be the number of negative integers in this collection. Then:

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

Check for $p = 7$ and a few values of a (a non-multiple of p); and $p = 47$, a few values of a.

3. **(Legendre Symbol of 2)**. What is $\left(\frac{2}{p}\right)$? Find this for prime p for $p = 3..47$. Is there a pattern?

4. (Lemma 4.3.3). Let $a, b \in \mathbb{Q}$. Claim: For any integer n:

$$\#((a,b) \cap \mathbb{Z}) \equiv \#((a, b+2n) \cap \mathbb{Z}) \pmod{2},$$

provided that each interval in the congruence is non-empty.

How can we test this?

Extras

5. If p and $p+2$ are both prime, they are called *twin primes*. Find the first several pairs of twin primes.