Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 31
Sage LAB!—Primitive Roots

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".

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 **c31**, 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 c31 worksheet attached**).

Primitive Roots

Consider $\mathbb{Z}/n\mathbb{Z}$. There are $\phi(n)$ units. We proved that each of these units has a *multiplicative order* (often just *order*). Recall the order of a unit a is the smallest exponent x such that $a^x \equiv 1 \pmod{n}$. We will prove that there is a unit a with order $\phi(n)$ (and explore the implications). Such a unit is called a *primitive root*.

Polynomial Rings

1. We can use Sage to define the polynomial ring $R[x]$ corresponding to a ring R. Sage a little bit blurs R and $R[x]$: Defines a ring of polynomials named R over the ring of integers mod 12 by running: `R.<x>= PolynomialRing()`.

2. Run: `f=x^6-1`. We just defined x to be the x in a polynomial ring—so this polynomial is actually in R. Check.

3. Now let's check our theorem on the number of roots of this polynomial. Run: `f.roots()`.

$(\mathbb{Z}/p\mathbb{Z})^*$ is a Cycle

4. In class we showed that 2 is a primitive root in $\mathbb{Z}/13\mathbb{Z}$. Find all the powers of 2 (mod 13). Check that indeed they are all different.

Quadratic Residues

d is a *quadratic residue* in $\mathbb{Z}/p\mathbb{Z}$ if there is an $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv d \pmod{p}$.

5. Find all the quadratic residues in $\mathbb{Z}/13\mathbb{Z}$.

   The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 if a (co-prime to p) is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$, and -1 otherwise.

6. Run: `legendre_symbol(a,13)` to check all the quadratic residues a we found in $\mathbb{Z}/13\mathbb{Z}$.

7. Now find all the quadratic residues in $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, and $\mathbb{Z}/47\mathbb{Z}$.

8. Do you see any pattern? Can you make a conjecture? Can you prove it?

Extras

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