Math 314 - Spring 2019 **Name:**
Mission 5 Due March 12, 2019

It used to be expensive to make things public and cheap to make them private. Now its expensive to make things private and cheap to make them public.

— Clay Shirky

Guidelines

- All work must be shown for full credit.
- You can choose to use SageMath code to help you solve the problems. If you do, print out your code.
- Either print out this assignment and write your answers on it, or edit the latex source. Make sure you still show your work! There is one point of extra credit available on this assignment if you use LaTeX
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
  □ I worked with the following classmate(s): ____________________
  □ I did not receive any help on this assignment.

1. Graded Problems

1. Let $f(x) = x^5 + x^3 + x^2 + 1$ and $g(x) = x^3 + x + 1$ be polynomials with coefficients in $\mathbb{F}_2$, the ring (field) of integers modulo 2. Compute $f(x) + g(x)$ and $f(x) \times g(x)$.

2. Write down all of the 8 elements of field $\mathbb{F}_8$ using the irreducible polynomial $x^3 + x + 1$. Multiply each element by $x^2 + x$. What is the inverse of $x^2 + x$ in this field?

3. Use the fermat primality test to test whether 33 is prime using first the base $a = 10$ and then the base $a = 2$.

4. Use the rules for Legendre symbols (not Jacobi symbols) to determine whether 83 is a square modulo 149. (Note 149 is prime)

5. Repeat question 1 using the rules for Jacobi Symbols instead to determine whether 83 is a square modulo 149. (Don't factor odd composite numbers)

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 3.13: # 29, 33