Math 314 - Fall 2016 **Name:**

Mission 5 Due October 4, 2016

What affected me most profoundly was the realization that the sciences of cryptography and mathematics are very elegant, pure sciences. I found that the ends for which these pure sciences are used are less elegant.

— James Sanborn

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 (or use the same folder as the latex code on SMC).
- Either print out this assignment and write your answers on it, or edit the latex source on SMC and type your answers in the document. 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 $g(x) = x^5 + x^3 + x^2 + 1$ and $h(x) = x^2 + x + 1$ 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. Compute $\varphi(60)$ and $\varphi(91)$.

3. Let $p \equiv 3 \pmod 4$ be prime, and write $p = 4k + 3$. Show the equation $x^2 \equiv -1 \pmod p$ has no solutions. (Hint: Suppose x exists. Raise both sides to the power (p-1)/2 and use Fermat's theorem.)

2. Recommended Exercises

These will not be graded.

- Section 3.13: # 14, 15