Math 314 - Fall 2018 **Name:**

Mission 11 Due December 10th, 2018

It is possible to write endlessly on elliptic curves. (This is not a threat.)

— Serge Lang

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. Suppose Alice uses a hash function that produces 40 bit digests. She uses this hash along with RSA to sign contracts. Eve wants to use a birthday attack to trick her into signing a bad contract. She drafts a contract and finds 10 places that she could make a change to the contract without changing its meaning. Is this likely to be enough to make the attack work? What if she finds 15 places? 25 places?

2. List all of the points on the elliptic curve $y^2 \equiv x^3 + x + 4 \pmod 7$. (Hint: Start by computing all the values of $y^2 \pmod 7$.)

3. Let $P = (4, 3)$ and $Q = (5, 1)$ be points on the elliptic curve $y^2 \equiv x^3 + x + 4 \pmod 7$. Compute $P + Q$ and $P + P$.

4. Suppose E is an elliptic curve mod p. Show that there cannot be more than $2p + 1$ points on this curve. (Hint: use the fact that for a fixed value of c, $y^2 \equiv c \pmod{p}$ can never have more than two solutions.)