Math 116 Spring 2022
Homework 6

Due Friday, May 20th

See https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/ell_finite_field.html for instructions on Elliptic curves over finite fields in Sage.

Problem 1. (by hand) Let $E : Y^2 = X^3 + X + 2$.

(a) Find list of points of $E(\mathbb{F}_5)$.

(b) Compute the addition table for $E(\mathbb{F}_5)$.

Problem 2. (with Sage) Let $E\colon Y^2 = X^3 + 2X + 5$.

(a) Find list of points of $E(\mathbb{F}_1 1)$.

(b) Compute the addition table for $E(\mathbb{F}_{11})$.

Problem 3. (6.8, with Sage) Let E be the elliptic curve $E\colon Y^2 = x^3 + x + 1$. Let $P = (4, 2)$ and $Q = (0, 1)$ be points on $E(\mathbb{F}_5)$. Find a positive integer n such that $Q = nP$.

Problem 4. (6.9) Let E be an elliptic curve over $\mathbb{F}_p$ and let P and Q be points in $E(\mathbb{F}_p)$. Assume that Q is a multiple of P and let $n_0 > 0$ be the smallest solution to $Q = nP$. Also let $s > 0$ be the smallest solution to $SP = \mathcal{O}$. Prove that every solution fo $Q = nP$ is of the form $n_0 + is$ for some $i \in \mathbb{Z}$.