Math 480A2, Homework 6

Due October 6, 2022

Homework is graded out of a total of 10 points. Collaboration is permitted, but you must list all coauthors on a problem's solution at the top of the page, and your writing must be your own.

Problem 1. (3 points) Consider an elliptic curve group E over the finite field $K = \mathbb{Z}/5\mathbb{Z}$. What are the possible sizes of E according to Hasse's inequality? For each of these possible sizes, list the groups E might be, presented as a cyclic group or sum of two cyclic groups, as in the structure theorem discussed in class.

Problem 2. (3 points) Describe an elliptic curve group E over $K = \mathbb{Z}/5\mathbb{Z}$ by giving a short Weierstrass equation for E, listing the points of E, and giving an addition table for the elliptic curve group operation $+$ on E. How can $(E, +)$ be written as a cyclic group or sum of cyclic groups? (*Hint:* for the prime field $\mathbb{Z}/p\mathbb{Z}$, elliptic curve groups exist having any size in the range given by Hasse's inequality.)

Problem 3. (2 points) Prove that a) the function $f(x) = \log(x)$ is $O(x)$, and b) the function $g(x) = 5,000x^2 + 10,000x$ is $O(x^2)$.

Challenge. (1 bonus point) Prove that the function $f(x) = e^{\sqrt{x}}$, defined on the nonnegative real numbers $\mathbb{R}_+$, is super-polynomial, but sub-exponential.

Problem 4. (2 points) Compute the discrete logarithm $\log_{12}(91)$ in the group $G = (\mathbb{Z}/101\mathbb{Z}, +)$ of integers modulo 101 under addition.