

Homework No.2 for Math 6170

Deadline: March 22.

Just write down your answer, **no reasons needed**.

Problem 1. Let (E, O) be the elliptic curve over K given by the equation

$$Y^2Z = (X - a_1Z)(X - a_2Z)(X - a_3Z)$$

with $O = [0, 1, 0]$ and $a_1, a_2, a_3 \in K$ are distinct. It is easy to see that $P_1 = [a_1, 0, 1], P_2 = [a_2, 0, 1], P_3 = [a_3, 0, 1]$ are in E . Compute $P_i + P_j$ for $1 \leq i, j \leq 3$. What can you say about the set $\{O, P_1, P_2, P_3\}$.