Elliptic Curve Exercises:

1. Let $\boldsymbol{E}(a, b)$ be the Weierstrass elliptic curve

$$y^2 - (x^3 + ax + b) = 0.$$

Given two distinct points $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$ on $\boldsymbol{E}$ work out the equation for the coordinates of $p_1 \oplus p_2$. Here $\oplus$ denotes the group law. Hint: Let the equation for the line through p_1 and p_2 be $y = mx + b$. Plug this into the equation for $\boldsymbol{E}$ and observe that the coefficient of x^2 is simultaneously mx and also one of the symmetric polynomials in x_1, x_2, x_3.

2. With the same notation as in Problem 1, find the formula for $p \oplus p$ where $p = (x, y)$. Hint: Use $y = mx + b$ again.

3. Consider the elliptic curve $\boldsymbol{E}(1, 1)$ over $\boldsymbol{Z}/5$. Is this a nonsingular curve? How many points does it have?

4. Say that a point p on an elliptic curve $\boldsymbol{E}$ is an *inflection point* if the line L_p tangent to $\boldsymbol{E}$ at p does not intersect $\boldsymbol{E}$ in any other point besides p. Prove that this definition is equivalent to the one given in the notes. That is, there is a projective transformation T such that

- $T(p) = [0 : 1 : 0]$
- $T(L_p)$ is the line $Z = 0$.
- The Equation for $T(\boldsymbol{E})$ has a term of the form Ax^3 where $A \neq 0$.
- The equation for $T(\boldsymbol{E})$ has no terms of the form Cx^2y or Cxy^2 or Cy^3.

Hint: you don't need to know the formula for T. You just have to know that T maps tangent lines of $\boldsymbol{E}$ to tangent lines of $T(\boldsymbol{E})$.

5. Let P_1 and P_2 be two distinct conic sections in $\boldsymbol{P}^2(\boldsymbol{R})$. Prove that there is some line L such that L intersects P_1 in two points and L intersects P_2 in 2 points. Hint: if you move the picture around by projective transformations you don't change the conclusion of the problem, and you might be able so simplify things.