(1) Let $d$ be a nonzero rational number. We have seen in class that the curve
$$E : X^3 + Y^3 = dZ^3$$
is an elliptic curve over $\mathbb{Q}$. We define the group law on $E$ so that the point $O = [1, -1, 0]$ becomes the identity for the group operations. In this exercise we will develop explicit equations for the group law on $E$.

(a) Show that three points of $E$ add to $O$ if and only if they are colinear.

(b) Find an explicit formula for the inverse of a point $P = [X, Y, Z]$ on $E$.

(c) If $P = [X, Y, Z]$ is a point on $E$, show that
$$2P = [−Y(X^3 + dZ^3), X(Y^3 + dZ^3), X^3Z − Y^3Z].$$

(d) Develop an analogous formula for the sum of two distinct points.

(2) Let $E$ be an elliptic curve over $\mathbb{Q}$, given by a homogeneous Weierstrass equation
$$F(X_0, X_1, X_2) = X_0^3X_2 - X_1^3 - aX_1^2X_2 - bX_1X_2^2 - cX_2^3 = 0.$$Let $P$ be a point on $E$.

(a) Show that $3P = O$ if and only if the tangent line to $E$ at $P$ intersects $E$ only at $P$.

(b) Show that $3P = O$ if and only if the Hessian matrix
$$(\frac{\partial^2 F}{\partial X_i \partial X_j})(P))_{0 \leq i, j \leq 2}$$has determinant 0.

(c) What are the possibilities for the number of rational points $P$ on $E$ such that $3P = O$?

(3) Suppose that $E : y^2 = x^3 + ax^2 + bx + c$ is an elliptic curve over $\mathbb{Q}$ and that $P = (x, y)$ is a point on $E$.

(a) Find a formula for the $y$-coordinate of the point $2P$ in terms of $x$ and $y$. (The formula for the $x$-coordinate of $2P$ is given on page 31 of Silverman/Tate.)

(b) Find a polynomial in $x$ whose roots are the $x$-coordinates of the points $P = (x, y)$ satisfying $3P = O$. (Hint: Rewrite $3P = O$ as $2P = −P$.)

(4) Find a necessary and sufficient condition that a line $y = ℓx + m$ should be an inflectional tangent to the elliptic curve
$$E : y^2 = x^3 + ax + b.$$ (I.e., the line should be a tangent line to the curve at a point $P$ such that $P$ is an inflection point.)

Use this to find a general formula for elliptic curves of the form $y^2 = x^3 + ax + b$ that have a rational point of order 3.