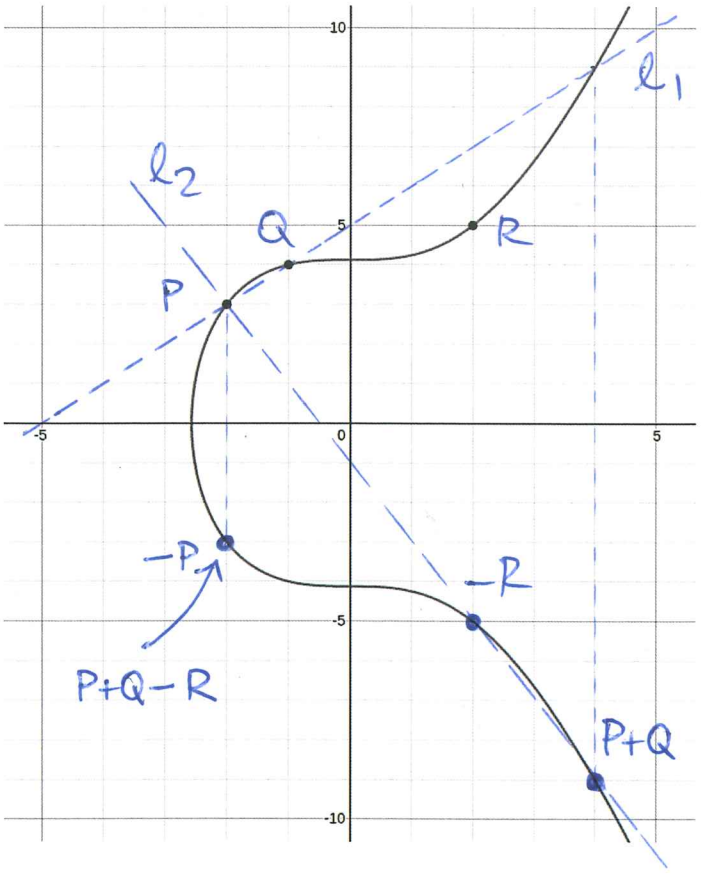
Name and Surname:

Math 366 - Spring 2020 - METU

Quiz 2

Question: The elliptic curve $E : y^2 = x^3 + 17$ has points $P = (-2, 3), Q = (-1, 4)$ and $R = (2, 5)$. Compute $P + Q - R$ by using the elliptic group law.



Recall that if $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ are points on E with $x_1 \neq x_2$ then $P_3(x_3, y_3) = P_1 + P_2$ is given by equations

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = -(\lambda x_3 + \nu)$$

where $\lambda = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}$

and $\nu = -\lambda x_1 + y_1$

One can use these formulas to obtain $P + Q = (4, -9)$ and $(4, -9) + (2, -5) = (-2, -3)$.

On the other hand, the coordinates of the points that appear in the computations are quite simple. One can use the equations of lines $\ell_1 : y = x + 5$ and $\ell_2 : y = -2x - 1$ to get to the same conclusion.

In summary, we have $P + Q - R = -P$