Name and Surname:
Student Number:

Math 366 - Spring 2015 - METU

Quiz 2

Question 1: Fill in the following blanks:

Theorem (Nagell-Lutz): Let $E : y^2 = x^3+ax+b$ be an elliptic curve with $a, b \in \mathbb{Z}$. Let $P(x_0, y_0) \in E$ be a <u>rational point of finite order</u>. Then x_0 and y_0 are integers; and either <u>$y = 0$</u> or else <u>y divides $D = -4a^3 - 27b^2$</u>.

Question 2: Let $E : y^2 = x^3 + 8$. Consider $P = (-2, 0), Q = (1, 3), R = (2, 4)$ and $S = (46, 312)$ which are points on E. For each of these points, determine if it has finite order or not.

Solution: The point $P = (-2, 0)$ is a torsion point of order two since there is a vertical tangent at that point. The point $S = (46, 312)$ is not a torsion point by Nagell-Lutz theorem since 312 does not divide $D = -27 \cdot 8^2$. The remaining two points, namely Q and R, have integer y coordinates dividing D. **This agrees with the conclusion of Nagell-Lutz theorem but we can't make any conclusions yet!** Note that

$$Q + Q = (-7/4, -13/8) \qquad \text{and} \qquad R + R = (-7/4, 13/8).$$

Now it follows by Nagell-Lutz theorem that $2Q$ and $2R$ are points of infinite order because their coordinates are not integers. As a result Q and R have infinite order as well.