Math 366 - Quiz 2

Name and Student ID:

Question (5 + 2 pts.): Let C be the elliptic curve given by the equation $y^2 = x^3 - 3x^2 + 5x + 1$ and let $P = (1, 2)$ and $R = (3, 4)$ be two given points on C.
a) Find $P + R$ and $2P = P + P$ where $+$ denotes the group operation on the elliptic curve C.
b) Why are there infinitely many solutions $(x, y) \in \mathbb{Q}^2$ of the given cubic equation of C?

$C: y^2 = f(x) = x^3 + ax^2 + bx + c = x^3 - 3x^2 + 5x + 1$.

a) For $P+R$, let $P*R = (x_3, y_3)$, then $P+R = (x_3, -y_3)$

$\lambda = \frac{4-2}{3-1} = 1$ · slope of the line through P and R

L: $y = \lambda x + v$: line through P and R

$2 = 1 \cdot 1 + v \Rightarrow v = 1$

$P*R$ is the 3rd intersection of L and C

$x_3 = \lambda^2 - a - x_1 - x_2 = 1^2 - (-3) - 1 - 3 = 0$

$y_3 = \lambda x_3 + v \Rightarrow y_3 = 1 \cdot 0 + 1 = 1$

$P + R = (0, -1)$

For $2P = P + P$

Let L: Tangent line to C at P, $L: y = \lambda x + v$

$C: y^2 = f(x) = x^3 - 3x^2 + 5x + 1 \Rightarrow \lambda = \left.\frac{dy}{dx}\right|_{P=(1,2)} = \left.\frac{f'(x)}{2y}\right|_{(1,2)} = \left.\frac{3x^2 - 6x + 5}{2y}\right|_{(1,2)}$

$L: y = \lambda x + v$

$2 = \frac{1}{2} \cdot 1 + v \Rightarrow v = \frac{3}{2}$

$\lambda = \frac{1}{2}$

$P * P = (x_3, y_3) \Rightarrow x_3 = \lambda^2 - a - x_1 - x_2 = \left(\frac{1}{2}\right)^2 - (-3) - 1 - 1 = \frac{5}{4}$

$y_3 = \lambda x_3 + v = \frac{1}{2} \cdot \frac{5}{4} + \frac{3}{2} = \frac{17}{8} \Rightarrow 2P = P + P = (x_3, -y_3) = \left(\frac{5}{4}, -\frac{17}{8}\right)$

$2P = \left(\frac{5}{4}, -\frac{17}{8}\right)$

b) $P = (1, 2)$ is a rational point and $2P = \left(\frac{5}{4}, -\frac{17}{8}\right)$ is a rational pt on C. $C: y^2 = x^3 - 3x^2 + 5x + 1$ (integer coefficients, $a, b, c \in \mathbb{Z}$), then by Nagell-Lutz Theorem $2P$ has infinite order since its coordinates are not integers. Then P also has infinite order in the group C. Then all $kP, k \in \mathbb{Z}$ are distinct points on C and kP are rational since P is rational!