Math 5020 - Elliptic Curves
Homework 3 (the exercise below)

Problem 1 The elliptic curve $y^2 = x^3 + 2x^2 - 3x$ satisfies $E(\mathbb{Q})[4] = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, i.e., the full 2-torsion is defined over $\mathbb{Q}$ and there is also a point of order 4 defined over $\mathbb{Q}$. The goal of this exercise is to uniquely determine $\mathbb{Q}(E[4])$ and $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$:

1. Find the coordinates of generators of $E(\mathbb{Q})[4]$, i.e., find $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, with $x_i, y_i \in \mathbb{Q}$ such that P has exact order 4 and Q has exact order 2, but $2P \neq Q$. (You may use SageMath or Magma here).
2. Find $2P$ (**do not** use a computer for the rest of the problem. Instead, use directly the formulae in p. 54. Note: there is a typo in the formula for b_2 in p. 42 (in the first edition). The correct formula is $b_2 = a_1^2 + 4a_2$).
3. Find the coordinates of a point $R = (x_3, y_3) \in E(\overline{\mathbb{Q}})$ such that $2R = Q$ (once again, simply use p. 54).
4. Show that $\mathbb{Q}(E[4]) = \mathbb{Q}(x_3, y_3)$ and determine this field. Use this to calculate the group structure of $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$.
5. Identify $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$ with a subgroup of $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$, where the $\mathbb{Z}/4\mathbb{Z}$-basis for $E[4]$ is $\{P, R\}$.
6. What is the Galois orbit of R? That is, find:
$$\{T \in E[4] : T = \sigma(R) \text{ for some } \sigma \in \mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})\}.$$
You should write each T as a linear combination of P and R.
7. Can you find the coordinates of a point on $E(\overline{\mathbb{Q}})$ of order 8?