Elliptic curves

Homework n°4

Exercise 1

Let E_1 and E_2 be two elliptic curves over the finite field $\mathbf{F}_q$. Assume that there exists a non-zero isogeny $\psi : E_1 \to E_2$ defined over $\mathbf{F}_q$.

(a) Show that card $E_1(\mathbf{F}_q) = $ card $E_2(\mathbf{F}_q)$. *Hint :* use the description of the $\mathbf{F}_q$-points in terms of the Frobenius morphism.

(b) Is the result true if we only assume that E_1 and E_2 are isogenous over $\overline{\mathbf{F}_q}$? *Hint :* find two elliptic curves which are isomorphic over $\overline{\mathbf{F}_q}$ but not over $\mathbf{F}_q$.

Exercise 2

Determine the structure of the torsion subgroup of $E(\mathbf{Q})$ for the following elliptic curves :

(a) $E : y^2 = x^3 + 1$;

(b) $E : y^2 = x(x-1)(x+2)$;

(c) $E : y^2 = x^3 - 43x + 166$.