Explicit Arithmetic for Modular Curves

Exercises II

(A) Let
$$E\ :\ Y^2 = X^3 + 2.$$
Let $P = (0, \sqrt{2}) \in E[3]$. Show that $[(E, P)] \in Y_1(3)(\mathbb{Q})$.

(B) Let
$$E\ :\ Y^2 = X^3 + 1.$$
Let $P = (\sqrt[3]{-4}, \sqrt{-3}) \in E[3]$. Show that $[(E, P)] \in Y_1(3)(\mathbb{Q})$.

(C) Let C be a curve of genus $g \geq 1$ over K. Let P, $Q \in C(K)$. Suppose P, Q are linearly equivalent. Prove that $P = Q$.

(D) Let d be a positive integer, and write $B_d = (3^{d/2} + 1)^2$. Let $p > B_d$ be prime. Show that if K is a number field of degree d and E/K is an elliptic curve with a K-point of order p then E has potentially multiplicative reduction at all primes $\mathfrak{q}$ of K above 3.
Remark: Merel's uniform boundedness theorem says that if E is an elliptic curve defined over a number field of degree d and p is a prime $> B_d$ then E has no p-torsion. This exercise is one small step in Merel's proof.