

This is the third set of exercises, based on the material in Chapter III, sections 1 and 2 in Silverman's book.

- (1) Prove the *duplication formula*; If  $P = (x, y)$  is a point on the elliptic curve  $E$ , prove that

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}.$$

(This is also (d) on page 54 in Chapter III.)

- (2) Exercise 3.1  
(3) Exercise 3.8 (a)