

## EXERCISES IN THE THEORY OF ELLIPTIC CURVES

Again the problems are chosen from the following canonical source. In fact, the exercise section has many other interesting problems which I didn't include simply because I wouldn't cover that much in my single lecture.

J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM 106, 1986

Chapter 3: Ex 3.3, 3.20, 3.22

Comment/Hint

3.3 This problem may be tedious but will give a little sense of how explicit computation can be done about group law.

3.20 As is explained in the text, the point of this exercise is to show that the  $j$ -invariant does not depend on the choice of base point  $O$ . Knowing that an elliptic curve has a group structure, one can easily see that the group-theoretic translation map can move around the base point  $O$ . Note that the translation map is certainly not an endomorphism of elliptic curves in our sense unless it is identity, but an isomorphism of algebraic curves. Also note that the Legendre equation presupposes that the base point  $O$  (or  $O'$ ) is chosen to be  $[0 : 1 : 0]$  in the projective coordinates.

3.22 Hint: Prop III.1.4. (b) and (c)

Chapter 6: Ex 6.6, 6.8, 6.9

Comment/Hint

6.8 This is one of the first steps in developing the theory of CM elliptic curves. A slight generalization of the first statement can be found with proof in Serre's article *Complex Multiplication* (see the very first theorem). There  $\mathcal{R}$  is not necessarily the ring of integers in  $\mathcal{K}$  but any order in  $\mathcal{K}$ . You can also see the appendix C §11 of Silverman or chapter 2 of Silverman's *Advanced Topics in the Arithmetic of Elliptic Curves*.