

### Exercises elliptic curves, Fall 2009, week 5

Choose four of the exercises from either paragraphs 2,9,10 in Cassels' book, or from exercises 2.1, 2.4, 2.8, 2.9 in the book by Silverman and Tate, or 2.13 of the notes on elliptic curves by Peter Stevenhagen, or the two exercises below.

**C** Use methods from the first two weeks (isomorphism with  $\mathbb{C}/\Lambda$  where  $\Lambda$  is a lattice), to show that an elliptic curve over  $\mathbb{R}$  has at most three points of order 3.

**D** Let  $E$  be a smooth projective plane cubic curve over  $\mathbb{R}$  and  $\mathcal{O}$  an inflection point of  $E$ , so that  $E$  has the structure of an elliptic curve. Let  $E(\mathbb{R})[3]$  be the kernel of the map  $E(\mathbb{R}) \rightarrow E(\mathbb{R}), P \mapsto 3P$ . This exercise will also show that  $E(\mathbb{R})[3]$  has order at most 3. Suppose the contrary.

- (1) Show that there exists a subgroup  $G$  of  $E(\mathbb{R})[3]$  that is isomorphic to  $(\mathbb{Z}/3\mathbb{Z})^2$ .
- (2) Let  $G$  be such a subgroup. Let  $H$  be the set of lines in  $\mathbb{P}^2$  through (at least) two different points of  $G$ . Determine the size of  $H$ .
- (3) Show that every line in  $H$  contains exactly three points of  $G$ .
- (4) Show that each point in  $G$  lies on exactly four lines in  $H$ .
- (5) Show that  $\mathbb{P}^2$  does not contain 9 points such that the line through every two points contains exactly one more point. Conclude that  $E(\mathbb{R})[3]$  has order at most 3 (Hint: consider one of the lines as the line at infinity.)
- (6) A clever trick for the previous problem goes as follows (and is now an argument you are no longer allowed to use). Take an affine part of the cubic that contains all points of  $G$ . Consider all pairs  $(P, L)$  with  $P \in G$  and  $L \in H$  and  $P \notin L$  and choose one where the distance  $d$  from  $P$  to  $L$  is minimal. Let  $Q_1, Q_2, Q_3$  be the points on  $L$  and show that there are  $i, j \in \{1, 2, 3\}$  with  $i \neq j$  such that the distance from  $Q_i$  to the line through  $Q_j$  and  $P$  is less than  $d$ . Conclude that  $G$  has no more than three elements.
- (7) Why does the last argument not show that  $E(\mathbb{R})$  contains no finite subgroups of order at least 4?