EXTRA HINTS FOR EXERCISE SHEET 9

Exercise 9.1. For part (1), follow Example 8.22. For part (2), first of all you need to realise that O is such a point. For any point $P \in C_2$ satisfying $P + P = O$, you can rewrite the condition as $P = -P$ and use the simplified group law 9.4 (or rather, Remark 9.5). For part (3), $-A$ and $-B$ can be easily obtained using the simplified group law 9.4 (or rather, Remark 9.5). The sum $A + B$ can be computed following Example 9.6.

Exercise 9.2. For part (1), follow the proof of Theorem 8.8. For part (2), you need to find the order of the P in the group law. In other words, what is the minimal positive integer n, such that the sum of n copies of P is the identity element O. So you can try to compute $R = P + P$, then $R + R$. You will find $R \neq O$ but $R + R = O$. So what is the answer to the question? For part (3), you just need to use Exercise 9.1 (2).

Exercise 9.3. The key observation here is that the polynomial defining the given curve does not meet the requirement of the simplified group law 9.4. Therefore we can only use the original group law 9.1. For part (1), given a point $P \in C$, how to find its inverse? It is not immediately clear from the group law 9.1, but the third paragraph in the proof of Proposition 9.8 explains how to do that. For part (2), you cannot be wrong by following the group law 9.1. But at a certain point, you will find that the result in part (1) can be used to avoid doing the same computation again.

Exercise 9.4. This is Pascal's mystic hexagon – a very interesting result in projective geometry, which can be proved in a similar way to the proof of the associativity in the group law on an elliptic curve. For part (1), you can draw an ellipse for the conic, then follow the description in the question. Part (2) should be clear from the picture. Part (3) is a direct application of Lemma 9.12.

Date: November 27, 2015.