Topics in Discrete Mathematics - Cryptography
Problem Sheet 3

Daniel P. Martin

University of Bristol 2018-2019

1 Part A

For this part of the question let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_{11}$.

Question 1. Show that $\mathcal{E}$ is non-singular.

Question 2. Compute x^2 for all $x \in \mathbb{F}_{11}$.

Question 3. Compute x^3 for all $x \in \mathbb{F}_{11}$.

Question 4. Compute $x^3 + 2x + 1$ for all $x \in \mathbb{F}_{11}$.

Question 5. Hence give all the points on $\mathcal{E}$.

Question 6. The list of points should include $(0, 1)$. Find the tangent to $\mathcal{E}$ at $(0, 1)$ and identify another point on $\mathcal{E}$ which also lies on the tanget. Hence, or otherwise, compute $(0, 1) + (0, 1)$

Question 7. The list of points should include $(8, 1)$. Find the tangent to $\mathcal{E}$ at $(8, 1)$ and identify another point on $\mathcal{E}$ which also lies on the tanget. Hence, or otherwise, compute $(8, 1) + (8, 1)$

Question 8. The list of points should include $(10, 3)$ and $(5, 9)$ which are on the line $y = x + 4$. Find a third point on $\mathcal{E}$ which is also on the line. Hence, or otherwise calculate $(10, 3) + (5, 9)$.

2 Part B

For this part of the question let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_{13}$.

Question 9. Show that $\mathcal{E}$ is non-singular.

Question 10. Compute x^2 for all $x \in \mathbb{F}_{13}$.

Question 11. Compute x^3 for all $x \in \mathbb{F}_{13}$.

Question 12. Compute $x^3 + x + 1$ for all $x \in \mathbb{F}_{13}$.

Question 13. Hence give all the points on $\mathcal{E}$.

Question 14. The list of points should include $(12, 8)$, compute the point $2(12, 8)$ on $\mathcal{E}$.

3 Part C

This part of the exercise sheet will go through and show that the elliptic curve group is indeed a group.

Question 15. Prove the elliptic curve group satisfies the following group axioms:

- Identity
- Inverse
- Closure

The harder one to prove is associativity. We give a few examples before proving it for arbitrary groups.

Question 16. Consider the elliptic curve from Part A of this worksheet. Choose five examples and show that the group operation is associative.

To prove associativity you may assume the following theorem.

Theorem 1 (Cayley-Bacharach Theorem). *Let $X_1, X_2 \subset \mathbb{P}^2$ be cubic plane curves meeting in nine points $p_1, \ldots, p_9$. If $X \subset \mathbb{P}^2$ is any cubic containing $p_1, \ldots, p_8$, then X contains p_9 as well.*

Question 17. Using the Cayley-Bacharach Theorem, or otherwise, prove that the elliptic curve group is associative.