Cryptographic Engineering
Spring Term 2018

Homework Assignment 02:
Let the elliptic curve equation $y^2 = x^3 + 3x + 4$ defined over the finite field $GF(37)$ be given. Do the following:

1. What is Δ? Is this curve nonsingular?
2. Apply Hasse's theorem and find the range of the order of the group.
3. Compute all elements of the elliptic curve group by enumeration.
4. Find the exact order of the group.
5. Find a primitive element of the group. Call that P.
6. Compute $Q = [31]P$ using the binary method:

$$\begin{aligned} P \oplus P &\rightarrow [2]P \\ [2]P \oplus P &\rightarrow [3]P \\ [3]P \oplus [3]P &\rightarrow [6]P \\ [6]P \oplus P &\rightarrow [7]P \\ [7]P \oplus [7]P &\rightarrow [14]P \\ [14]P \oplus P &\rightarrow [15]P \\ [15]P \oplus [15]P &\rightarrow [30]P \\ [30]P \oplus P &\rightarrow [31]P \end{aligned}$$

7. Compute $Q = [31]P$ using the NAF method:

$$\begin{aligned} P \oplus P &\rightarrow [2]P \\ [2]P \oplus [2]P &\rightarrow [4]P \\ [4]P \oplus [4]P &\rightarrow [8]P \\ [8]P \oplus [8]P &\rightarrow [16]P \\ [16]P \oplus [16]P &\rightarrow [32]P \\ [32]P \oplus (-P) &\rightarrow [31]P \end{aligned}$$