EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 10 **Professor Dunham**
7 April 2020 **Due: 14 April 2020**

Review Text: Chapter 9.

1. For each of the following elliptic curves, determine if they are singular or non-singular.
   (a) $E:\ y^2 = x^3 + x + 1 \pmod{\mathbb{Z}_3}$.
   (b) $E:\ y^2 = x^3 + x + 2 \pmod{\mathbb{Z}_7}$.
   (c) $E:\ y^2 = x^3 + x + 3 \pmod{\mathbb{Z}_{23}}$.

2. Consider the elliptic curve $E:\ y^2 = x^3 + x + 6 \pmod{\mathbb{Z}_7}$.
   (a) Compute all points on E over $\mathbb{Z}_7$.
   (b) What is the order of the group? *Hint:* Do not miss the point at infinity.
   (c) Perform the addition $(2,3) + (6,2)$.
   (d) Perform the addition $(2,3) + (2,3)$.
   (e) Perform the addition $(2,3) + (2,4)$.
   (f) Given the element $\alpha = (2,3)$, determine the order of α. Is α a primitive element?
   (g) Will all points on E be primitive with the exception of the point at infinity?
   (h) What is the group structure of the elliptic curve?

3. Consider the elliptic curve $E:\ y^2 = x^3 + 3x \pmod{\mathbb{Z}_7}$.
   (a) Compute all points on E over $\mathbb{Z}_7$.
   (b) What is the order of the group? *Hint:* Do not miss the point at infinity.
   (c) Perform the addition $(1,2) + (5,0)$.
   (d) Perform the addition $(1,2) + (1,2)$.
   (e) Perform the addition $(1,2) + (3,6)$.
   (f) Given the element $\alpha = (1,2)$, determine the order of α. Is α a primitive element?
   (g) Find the order of the other elements in E.
   (h) What is the group structure of the elliptic curve?