M E T U
Department of Mathematics

Group	**Elliptic Curves in Cryptography** **Midterm I**	List No.

Code : *IAM 505* Acad. Year : *2013* Semester : *Fall* Instructor : *Küçüksakallı* Date : *07/11/2013* Time : *10:40* Duration : *110 minutes*	Name : Last Name : Signature : 6 QUESTIONS ON 4 PAGES 30 TOTAL POINTS

1	2	3	4	5	6		

1. (6pts) Consider the projective elliptic curve $E : y^2z = x^3 + 8z^3$. For each of the following projective lines l_i, find the points in the intersection $E \cap l_i$ with multiplicities.

- $l_1 : x - y + 2z = 0.$

- $l_2 : x + 2z = 0$

- $l_3 : y = 0$

2. (8pts) Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ defined over a field K of characteristic not equal to 2 or 3. Let P and Q be points on E different than the point at infinity. Give explicitly the coordinates of $P + Q$ (according to the group law on E) if

- P and Q are different,

- P and Q are the same.

3. (5pts) Let $\{T_1, T_2\}$ be a basis of $E[n]$. Show that the Weil pairing $e_n(T_1, T_2)$ is a primitive n-th root of unity.

4. (3pts) Let E be the elliptic curve $y^2 = x^3 - x$ defined over the field $\mathbb{F}_{11}$. Find a point

$$P \in E(\mathbb{F}_{11}) \cap E[3]$$

different than the point at infinity. (Hint $\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$.)

5. (3pts) You are given that the map $\alpha : (x, y) \mapsto (-x, iy)$ is an endomorphism of

$$E : y^2 = x^3 - x.$$

What is the degree of α? Is it true that $\alpha = [n]$ for some integer $n \in \mathbb{Z}$.

6. (5pts) Let E be the elliptic curve $y^2 = x^3 - x$ defined over $\mathbb{F}_7$. List all elements of $E(\mathbb{F}_7)$ and determine its group structure. Find $E(\mathbb{F}_7) \cap E[p]$ for each prime number p.