CPSC/PMAT 629 — Elliptic Curves and Cryptography
ASSIGNMENT 2

Problem 1. *Projective coordinates*

Let $\mathbb{K}$ be a field of characteristic different from 2, 3. In such fields, inversion of elements is very expensive compared to multiplication and squaring — one inversion takes approximately as much time as 50-80 multiplications, depending on your hardware and software — so we want to do elliptic curve arithmetic without inversions. Therefore, one uses projective coordinates.

(1) Construct doubling formulas for standard projective coordinates for an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{K}$ that require no inversions. Hint: convert projective points to affine first, then back to projective.
(2) Derive formulas for addition of two points in mixed coordinates, i.e. one point is assumed to be given in affine representation, the other in projective, and their sum is a projective point, requiring no inversions. Don't forget the case where the two points are equal or inverse to each other.
(3) Determine the minimum number of multiplications and squarings required to use your formulas from (1) and (2), along with the number of intermediate values that must be stored.
(4) Determine the minimum number of multiplications and squaring required to use your formulas from (1) and (2) if you are not allowed to store intermediate values for reuse.

Problem 2. *3-torsion in characteristic 2*

Let E be an elliptic curve in characteristic 2. Show that

$$E[3] \equiv \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \ .$$

Hint: Use the formulas for point doubling in characteristic 2 for the two different models of an elliptic curve.

Problem 3. *Weil pairing on basis elements*

Prove that $e_n(T_1, T_2)$ is a primitive nth root of unity if $\{T_1, T_2\}$ is a basis of $E[n]$.

Problem 4. *Elliptic curve discrete logarithm problem*

Recall that the *discrete logarithm problem* in a field $\mathbb{K}$ is, given elements $a, b \in \mathbb{K}$, determine an integer k such that $a^k = b$, if such an integer exists.

The *elliptic curve discrete logarithm problem* is, given points P and Q, on an elliptic curve, determine an integer k such that $[k]P = Q$ if such an integer exists.

(1) Consider an elliptic curve E defined over a field $\mathbb{K}$, and let P be a point of order n on E where n is not divisible by the characteristic of the field. Let $Q \in E[n]$. Show that $Q \in \langle P \rangle$ (i.e. there exists an integer k such that $Q = [k]P$) if and only if $e_n(P, Q) = 1$.
(2) Let P be as in part (1) and $Q = [k]P$. Use the Weil Pairing to show that the elliptic curve discrete logarithm problem (with respect to Q and P) can be solved by solving a discrete logarithm problem in $\mu_n \subseteq \mathbb{K}(\zeta_n)$, i.e. in the smallest field containing $\mathbb{K}$ and ζ_n.

(3) Consider the case of $\mathbb{K} = \mathbb{F}_q$. Determine a criterion for the smallest integer k such that $\mu_n \subseteq \mathbb{F}_{q^k}$ (again, assuming $\gcd(n, q) = 1$). What does this say about the complexity of the discrete logarithm problem on an elliptic curve versus a finite field?

Problem 5. *An elliptic curve group structure computation*

Let E be the elliptic curve defined by

$$y^2 = x^3 + x + 1 \quad \text{over } \mathbb{F}_5 \ .$$

(1) Show that the point $(0, 1)$ on E does not have order 3.
(2) Show that the point $[3](0, 1)$ on E does have order 3.
(3) Determine the order of the group $E(\mathbb{F}_5)$ (with proof). Argue why this group must be cyclic and find and a generator. Note: no credit will be given for brute force solutions!