Edoardo Persichetti Lecture 8: Pairings 09/04/2014

Exercise 1 Let $E : y^2 = x^3 + 4x$ over $\mathbb{F}_{11}$ and $P = (0, 0)$, $Q = (2, 4)$, $R = (4, 5)$, $S = (6, 3)$. Consider the divisor $D := [P] + [Q] + [R] + [S] - 4[\infty]$.

- Is this a principal divisor?
- If yes, find a function f such that $div(f) = D$. If not, explain why.

Exercise 2 .

- Let $f(x)$ and $g(x)$ be rational functions. Prove that $div(f(x)g(x)) = div(f(x)) + div(g(x))$ (equivalently, $div(f(x)/g(x)) = div(f(x)) - div(g(x))$).
- Let E be a nonsingular elliptic curve. Find a divisor for the rational function $f(x, y) = y$.
- Compute, using the definition, $e_2(P_1, P_2)$ for any two points P_1, P_2.

Exercise 3 Prove that the Weil pairing is alternating.

Hint: use the fact that $e_n(P, P) = 1$ for all points P.

Exercise 4 Let P_1, P_2 be a basis of $E[n]$. Show that $e_n(P_1, P_2)$ is a *primitive* n-th root of unity.

Exercise 5 Let E be an elliptic curve defined over $\mathbb{K}$, $n \in \mathbb{Z}^+$. Then $E[n] \subset E(\mathbb{K}) \Rightarrow \mu_n \subset \mathbb{K}$.