Mathematics 3159A **Bradley Assaly-Nesrallah**
Introduction to Cryptography
Assignment 5, Problem 1 Due Date: December 1, 2020

Solution

We fix a prime p and a positive integer k. Define $\mathbb{F}_{p^k}$ as the field with p^k elements, given by polynomials of degree less than k over $\mathbb{F}_p$. Let $\varphi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be a map given by $\varphi(a) = a^p$.

1. We want to show that φ is a homomorphism by checking the additive and multiplicative homomorphism properties:

Proof. We want to show that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a) \cdot \varphi(b) \forall a, b \in \mathbb{F}_{p^k}$ as follows:
Let $a, b \in \mathbb{F}_{p^k}$, so $\varphi(a+b) = (a+b)^p = \sum_{i=0}^{p} \frac{p!}{i!(p-1)!} a^{p-i} b^i$ by the binomial theorem which holds in $\mathbb{F}_{p^k}$,
Since $p | \frac{p!}{i!(p-1)!}, 1 \leq i \leq p-1 \implies \frac{p!}{i!(p-1)!} \equiv 0 \mod p$ so $\sum_{i=0}^{p} \frac{p!}{i!(p-1)!} a^{p-i} b^i = a^p + b^p$ thus $\varphi(a+b) = \varphi(a) + \varphi(b)$ so the additive property holds,
Let $a, b \in \mathbb{F}_{p^k}$, so $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a) \cdot \varphi(b)$ so the multiplicative property holds
Thus φ is a homomorphism as required, so we are done.

□

2. We want to show that φ behaves like the identity function on constant polynomials:

Proof. We want to show that $\varphi(a) = a \forall a \in \mathbb{F}_p$ as follows: Let $a \in \mathbb{F}_p$, $\varphi(a) = a^p \equiv a \mod p$ by Fermat's Little Theorem,
Thus $\varphi(a) = a \forall a \in \mathbb{F}_p$, as required so we are done.

□

3. Let $f(X, Y) \in \mathbb{F}_p[X, Y]$ and suppose that $(a, b) \in \mathbb{F}_{p^k}^2$ is a root of f.
We want to show that $(\varphi(a), \varphi(b))$ is also a root of f.

Proof. We want to show that $f((\varphi(a), \varphi(b))) = 0$ as follows:
We know $f(a, b) = 0 = 0^p = f(a, b)^p = f(a^p, b^p) = f((\varphi(a), \varphi(b)))$,
thus $f((\varphi(a), \varphi(b)) = 0$ and $(\varphi(a), \varphi(b))$ is a root of f as required.

□

We now deduce that for any elliptic curve E defined over $\mathbb{F}_p$, the map $\bar{\varphi} : E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$ given by $\bar{\varphi}(a, b) = (\varphi(a), \varphi(b))$ is well-defined:

Proof. To deduce that $\bar{\varphi}$ is well defined it is sufficient to show that $(a, b) \in E \implies \varphi(a, b) \in E$:

Let $E : y^2 = x^3 + ax + b$ and let $(x, y) \in E$,
So $\bar{\varphi}(x, y) = (\varphi(x), \varphi(y)) = (x^p, y^p)$ and,
$(y^p)^2 - (x^p)^3 - a(x^p) - b = (y^2)^p - (x^3)^p - a^p(x^p) - b^p = (y^2 - x^3 - ax - b)^p = 0^p = 0$
Thus $\bar{\varphi}(x, y) \in E$ as required so $\bar{\varphi}$ is well-defined so we are done.

$\square$

4. Let E be an elliptic curved defined over $\mathbb{F}_p$, the map $\bar{\varphi} : E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$ given by $\bar{\varphi}(a, b) = (\varphi(a), \varphi(b))$. We want to show that $\bar{\varphi}$ is a group homomorphism from E to itself:

Proof. We want to show that $\bar{\varphi}(P \oplus Q) = \bar{\varphi}(P) \oplus \bar{\varphi}(Q) \forall P, Q \in E(\mathbb{F}_p)$ as follows:
Let $P, Q \in E(\mathbb{F}_p)$, so $P = (x, y) \in E$ and $Q = (v, w) \in E$,
Observe, $\bar{\varphi}(P \oplus Q) = \bar{\varphi}((x \oplus v, y \oplus w) = (\varphi(x \oplus v), \varphi(y \oplus w)) = (\varphi(x) \oplus \varphi(v)), (\varphi(y) \oplus \varphi(w)) = (x^p \oplus v^p, y^p \oplus w^p)$ by φ a homomorphism and,
and $\bar{\varphi}(P) \oplus \bar{\varphi}(Q) = \bar{\varphi}((x, y) \oplus \bar{\varphi}(v, w) = (\varphi(x), \varphi(y)) \oplus (\varphi(v), \varphi(w)) = (x^p, y^p) \oplus (v^p, w^p) = (x^p \oplus v^p, y^p \oplus w^p)$ by φ a homomorphism ,
We know that $y^2 - x^3 - ax - b = 0$,
So, $(y^p \oplus w^p)^2 - (x^p \oplus v^p)^3 - a(x^p \oplus v^p) - b = 0$
$((y \oplus w)^p)^2 - ((x \oplus v)^p)^3 - a(x \oplus v)^p - b = 0$,
$((y \oplus w)^p)^2 - ((x \oplus v)^p)^3 - a(x \oplus v)^p - b = 0$, as required
Thus $\bar{\varphi}(P \oplus Q) = \bar{\varphi}(P) \oplus \bar{\varphi}(Q) \forall P, Q \in E(\mathbb{F}_p)$, so $\bar{\varphi}$ is a group homomorphism as required and we are done.

$\square$