Journal homepage http://revistas.unitru.edu.pe/index.php/SSMM

SELECCIONES MATEMÁTICAS
Universidad Nacional de Trujillo
ISSN: 2411-1783 (Online)
2023; Vol. 10(2): 333-338.

The Frobenius endomorphism to Elliptic Curves and same properties

O Endomorfismo de Frobenius para Curvas Elípticas e algumas propriedades

Jaime Edmundo Apaza Rodriguez

Received, Set. 22, 2023; *Accepted, Oct. 30, 2023;* *Published, Dec. 27, 2023*

How to cite this article:
Apaza Rodriguez J.E. *The Frobenius endomorphism to Elliptic Curves and same properties*. Selecciones Matemáticas. 2023;10(2):333–338. http://dx.doi.org/10.17268/sel.mat.2023.02.09

Abstract

In this work we present the Frobenius endomorphism for Elliptical Curves defined over finite fields and some of their properties relative to their kernel and the condition of separability.

Keywords . Frobenius endomorphism; elliptic curve; finite field.

Resumo

Neste trabalho apresentamos o endomorfismo de Frobenius para Curvas Elípticas definidas sobre corpos finitos e algumas de suas propriedades relativas a seu núcleo e à condição de separabilidade.

Palavras-chave. Endomorfismo de Frobenius; Curva Elíptica; Corpo Finito.

1. Introdução. Seja $\mathbb{K}$ um corpo finito e E uma curva elíptica definida sobre $\mathbb{K}$. Dado que existem apenas finitos pares (x, y) com $x, y \in \mathbb{K}$, o grupo $E(\mathbb{K})$ é finito. Várias propriedades desse grupo, por exemplo, sua ordem, acabam sendo importantes em muitos contextos. Os resultados não são apenas interessantes por si só, mas também são pontos de partida para as aplicações criptográficas. Por outro lado, certos automorfismos do grupo $E(\mathbb{K})$ são peculiares e fornecem informações importantes quando agem sobre as coordenadas de pontos em $E(\mathbb{K})$. Em particular temos o endomorfismo de Frobenius, o qual será apresentado neste trabalho assim como algumas de suas propriedades relativas ao núcleo e a separabilidade.

2. Endomorfismos de curvas elípticas. Seja E uma curva elíptica definida sobre um corpo $\mathbb{K}$ arbitrário. Um endomorfismo de E é um homomorfismo $\alpha : E(\overline{\mathbb{K}}) \longrightarrow E(\overline{\mathbb{K}})$ que está dado por funções racionais. Em outras palavras, $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, onde P_1, P_2 são pontos em $E(\overline{\mathbb{K}})$, e existem funções racionais (quocientes de polinômios) $R_1(x, y), R_2(x, y)$, com coeficientes em $\overline{\mathbb{K}}$ tais que

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

para todo $(x, y) \in E(\overline{\mathbb{K}})$. Dado que α é homomorfismo, temos que $\alpha(\infty) = \infty$. Também iremos assumir que α não é trivial, ou seja, existe algum ponto (x, y) tal que $\alpha(x, y) \neq \infty$ [1].

Example 2.1. *Sejam, a curva* $E : y^2 = x^3 + Ax + B$ *e a aplicação* $\alpha(P) = 2P$. *Então* α *é um homomorfismo e* $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, *onde*

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x,$$

*Departamento de Matemática, UNESP, Ilha Solteira, São Paulo, Brasil. (jaime.rodriguez@unesp.br).

$$R_2(x,y) = \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y.$$

Estas contas provém das fórmulas adição para ponto duplo numa curva elíptica pois $\alpha(P) = 2P$. Dado que α é um homomorfismo dado por funções racionais, temos que α é um endomorfismo de E.

Para as funções racionais que descrevem um endomorfismo de E, será de utilidade ter uma forma padrão. Por simplicidade assumiremos que a curva elíptica E está dada na forma de Weierstrass. Seja $R(x,y)$ qualquer função racional. Como $y^2 = x^3 + Ax + B$, para todo $(x,y) \in E(\overline{\mathbb{K}})$, podemos substituir qualquer potência par de y por um polinômio em x e substituir qualquer potência ímpar de y por y vezes um polinômio em x e obter uma função racional que é a mesma função $R(x,y)$ inicial agindo sobre pontos de $E(\overline{\mathbb{K}})$. Por isso podemos assumir que

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Multiplicando numerador e denominador por $p_3 - p_4 y$ e substituindo y^2 por $x^3 + Ax + B$ obtemos

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}.$$

Consideremos um endomorfismo dado por $\alpha(x,y) = (R_1(x,y), R_2(x,y))$, como antes. Dado que α é um homomorfismo, temos $\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y)$. Isto significa que

$$R_1(x,-y) = R_1(x,y) \quad e \quad R_2(x,-y) = -R_2(x,y).$$

Por causa disto, se R_1 é da forma $R(x,y) = \frac{q_1(x)+q_2(x)y}{q_3(x)}$, então $q_2(x) = 0$ e se R_2 é também dessa forma, então $q_1(x) = 0$. Portanto, podemos assumir que

$$\alpha(x,y) = (r_1(x), r_2(x)y),$$

onde r_1, r_2 são funções racionais [2].

Veja-se agora o que acontece quando uma das funções racionais não está definida num ponto. Escrevemos $r_1(x) = p(x)/q(x)$, onde os polinômios p e q não tem fator comum. Se $q(x) = 0$ para algum ponto (x,y), então assumimos que $\alpha(x,y) = \infty$. Se $q(x) \neq 0$, temos que $r_2(x)$ está definida e portanto α está definida.

Definimos o grau de α por

$$grau(\alpha) = max\{grau(p(x)), grau(q(x))\},$$

se α é não trivial. Quando $\alpha = 0$, temos $grau(0) = 0$.

Seja $\alpha \neq 0$. Dizemos que $\alpha = (r_1(x,y), r_2(x,y)y)$ é um endomorfismo separável se $r_1'(x)$ não é identicamente zero. Isto equivale a afirmar que $p'(x)$ ou $q'(x)$ não são identicamente zeros (em característica 0, um polinômio não constante terá derivada não nula. Em característica $p > 0$, os polinômios com derivada zero são exatamente aqueles da forma $g(x^p)$).

Example 2.2. *Do exemplo 2.1, sejam a curva $E : y^2 = x^3 + Ax + B$ e a aplicação $\alpha(P) = 2P$. Então tinhamos que $\alpha(x,y) = (R_1(x,y), R_2(x,y))$, onde*

$$R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x.$$

O fato de $y^2 = x^3 + Ax + B$ e algumas pequenas contas, permitem obter

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

Assim temos que $grau(\alpha) = 4$. O polinômio $q'(x) = 4(3x^2 + A)$ é não nulo (incluindo o caso de característica 3, pois se $A = 0$ então $x^3 + B$ teria raízes múltiplas, que contraria a hipótese). Portanto α é separável.

3. O Endomorfismo de Frobenius. Uma importante aplicação entre curvas elípticas definidas sobre corpos finitos do tipo $\mathbb{F}_q$, onde $q = p^n$, para algum n número natural e p primo, é o famoso endomorfismo de Frobenius. Em geral, uma aplicação do tipo $x \longmapsto x^p$ pertence ao grupo de Galois $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ e quando se considera a curva sobre $\overline{\mathbb{F}}_p$ induz um endomorfismo, chamado de Frobenius. Em termos gerais, o interesse pelo endomorfismo de Frobenius é que seus pontos fixos, quando age sobre uma curva algebrica cualquer, correspondem à soluções módulo p [2].

Para E curva elíptica sobre $\mathbb{F}_q$ temos

$$\phi_q(x, y) = (x^q, y^q).$$

Esta aplicação desempenha um papel importante na teoria das Curvas Elípticas.

Definição 3.1. *Considere o corpo $\mathbb{F}_q$ e $\overline{\mathbb{F}}_q$ seu fecho algebrico. A aplicação $\phi_q : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$, dada por $\phi_q(x) = x^q$, é o endomorfismo de Frobenius.*

Este endomorfismo, agindo sobre as coordenadas dos pontos do grupo $E(\overline{\mathbb{F}}_q)$, é tal que

$$\phi_q(x, y) = (x^q, y^q) \quad e \quad \phi_q(\infty) = \infty.$$

O endomorfismo de Frobenius ϕ_q desempenha um papel fundamental na teoria das curvas elípticas definidas sobre $\mathbb{F}_q$.

Example 3.1. *Seja $\mathbb{K}$ um corpo de característica $p > 0$, com $q = p^r$ e E uma curva elíptica dada pela equação de Weierestrass. A curva $E^{(q)}/\mathbb{K}$ definida sobre $\mathbb{K}$ é obtida elevando os coeficientes da equação de E à potência q e o endomorfismo de Frobenius ϕ_q é dado por $\phi_q(x, y) = (x^q, y^q)$.*

Dado que $E^{(q)}$ é o lugar geométrico dos zeros da equação de Weierstrass, então é uma curva elíptica desde que sua equação seja não-singular.

Se $\mathbb{K} = \mathbb{F}_q$ então a aplicação q-ésima potência de $\mathbb{K}$ em $\mathbb{K}$ é a identidade, tem-se que $E^{(q)} = E$ e portanto ϕ_q é o endomorfismo de Frobenius. Assim, o conjunto de pontos fixos por ϕ_q é exatamente $E(\mathbb{F}_q)$, ou seja, $\phi_q(E(\mathbb{F}_q)) = E(\mathbb{F}_q)$.

4. Propriedades fundamentais. [3], [2]

Lema 4.1. *Seja E uma curva elíptica definida sobre $\mathbb{F}_q$ e $(x, y) \in E(\overline{\mathbb{F}}_q)$. Então*

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$,
2. $(x, y) \in E(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y)$.

Demonstração: Sabemos que

$$(a + b)^q = a^q + b^q \quad e \quad a^q = a,$$

se q é uma potência da característica do corpo e para todo $a \in \mathbb{F}_q$.

1) Vamos considerar a forma generalizada da equação de Weierstrass para a curva E. Assim temos

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

onde $a_i \in \mathbb{F}_q$, para todo i.

Logo

$$(y^q)^2 + a_1(x^qy^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6.$$

Isto significa que $(x^q, y^q) \in E$.

2) Sabemos que $x \in \mathbb{F}_q \iff \phi_q(x) = x$ e $y \in \mathbb{F}_q \iff \phi_q(y) = y$. Logo

$$(x, y) \in E(\mathbb{F}_q) \iff x, y \in \mathbb{F}_q \iff \phi_q(x) = x \ e \ \phi_q(y) = y \iff \phi_q(x, y) = (x, y).$$

Example 4.1. *Consideremos a curva elìptica $E : y^2 + xy = x^3 + 1$ definida sobre $\mathbb{F}_2$. Temos que $E(\mathbb{F}_2) = \{\infty, (0, 1), (1, 0), (1, 1)\}$. Este é um grupo cíclico de ordem 4. Os pontos $(1, 0)$ e $(1, 1)$ são de ordem 4 e o ponto $(0, 1)$ tem ordem 2.*

Agora vamos obter o grupo $E(\mathbb{F}_4)$. Sabemos que $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, onde ω satisfaz a relação $\omega^2 + \omega + 1 = 0$ (que implica $\omega^3 = 1$, após multiplicar por $\omega + 1$). Obtemos os elementos de $E(\mathbb{F}_4)$:

$$\begin{aligned}
x &= 0 \implies y^2 = 1 \implies y = 1;\\
x &= 1 \implies y^2 + y = 0 \implies y = 0, 1;\\
x &= \omega \implies y^2 + wy = 0 \implies y = 0, \omega;\\
x &= \omega^2 \implies y^2 + \omega^2 y = 0 \implies y = 0, \omega^2;\\
x &= \infty \implies y = \infty.
\end{aligned}$$

Assim temos

$$E(\mathbb{F}_4) = \{\infty, (0,1), (1,0), (1,1), (\omega,0), (\omega,\omega), (\omega^2,0), (\omega^2,\omega^2)\}.$$

Como a característica do corpo é 2*, então existe ao menos um ponto de ordem* 2*. De fato,* $(0,1)$ *tem ordem* 2*. Portanto,* $E(\mathbb{F}_4)$ *é um grupo cíclico de ordem* 8*, onde qualquer dos pontos contendo* ω *ou* ω^2 *é um gerador, o que pode ser verificado diretamente ou observando que esses elementos não pertencem ao subgrupo* $E(\mathbb{F}_2)$ *de ordem* 4*. Dado que* $\phi_2(x,y) = (x^2, y^2)$ *é o endomorfismo de Frobenius, verifica-se que* ϕ_2 *permuta os elementos de* $E(\mathbb{F}_4)$ *e*

$$E(\mathbb{F}_2) = \{(x,y) \in E(\mathbb{F}_4) : \phi_2(x,y) = (x,y)\}.$$

Obsdervação 4.1. *Em geral, para qualquer curva elíptica* E *definida sobre* $\mathbb{F}_q$ *e qualquer extensão* $\mathbb{F}$ *de* $\mathbb{F}_q$*, o endomorfismo de Frobenius* ϕ_q *permuta os elementos de* $E(\mathbb{F})$ *e fixa os elementos do subgrupo* $E(\mathbb{F}_q)$*.*

Lema 4.2. *Seja* E *uma curva elíptica definida sobre* $\mathbb{F}_q$*. Então* ϕ_q *é um endomorfismo de* E*, de grau* q *e não separável.*

Demonstração: Dado que $\phi_q(x,y) = (x^q, y^q)$, esta aplicação está dada por funções racionais e seu grau é q.

Vamos mostrar que $\phi_q : E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q)$ é um homomorfismo. De fato, sejam $(x_1,y_1),\ (x_2,y_2) \in E(\overline{\mathbb{F}}_q)$, com $x_1 \neq x_2$. Sabemos que a soma é (x_3,y_3), onde

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{com } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Observar que estamos operando com a forma de Weierstrass. O caso da forma generalizada de Weierstrass é essencialemente a mesma.

Elevando à potência q cada expressão acima obtemos

$$x_3^q = m'^2 - x_1^q - x_2^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{com } m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

Isto implica que $\phi_q(x_3,y_3) = \phi_q(x_1,y_1) + \phi_q(x_2,y_2)$.

Os casos onde $x_1 = x_2$ ou um dos pontos é ∞ são similares. No entanto, existe uma sutileza no caso de somar um ponto consigo mesmo. A fórmula do ponto duplo afirma que $2(x_1,y_1) = (x_3,y_3)$, onde

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{com } m = \frac{3x_1^2 + A}{2y_1}.$$

Quando elevamos à potência q obtemos

$$x_3^q = m'^2 - 2^q x_1^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{com } m' = \frac{3^q (x_1^2)^q + A^q}{2^q y_1^q}.$$

Dado que $2, 3\ e\ A \in \mathbb{F}_q$, temos que $2^q = 2, 3^q = 3, A^q = A$. Isto significa que temos obtido o duplo do ponto (x^q, y^q) sobre E.

Em vista de que ϕ_q é um homomorfismo dado por funções racionais, então é um endomorfismo de E. Como $q = 0$ em $\mathbb{F}_q$, a derivada de x^q é identicamente zero. Portanto, ϕ_q não é separável.

□

O resultado a seguir fornece uma condição suficiente para a não separabilidade de um endomorfismo de uma curva elíptica E definida sobre um corpo qualquer $\mathbb{K}$. Neste caso o endomorfismo mencionado é geral, não necessariamente de Frobenius.

proposição 4.1. *Seja* $\alpha \neq 0$ *um endomorfismo separável na curva elíptica* E*. Então* $grau(\alpha) = card(Ker(\alpha))$*, onde* $Ker(\alpha)$ *é o núcleo de* $\alpha : E(\overline{\mathbb{K}}) \longrightarrow E(\overline{\mathbb{K}})$*. Se* $\alpha \neq 0$ *é não separável, então* $grau(\alpha) > card(ker(\alpha))$*.*

Demonstração: Escrevamos $\alpha(x,y) = (r_1(x), r_2(x)y)$ onde $r_1(x) = p(x)/q(x)$, como antes. Então $r_1' \neq 0$, de modo que $p'q - pq'$ não é o polinômio zero.

Seja $S = \{x \in \overline{\mathbb{K}} : (pq' - p'q)(x)q(x) = 0\}$. Seja $(a,b) \in E(\overline{K})$ tal que

1. $a \neq 0,\ b \neq 0, (a,b) \neq \infty$,
2. $grau(p(x) - aq(x)) = max\{grau(p), grau(q)\} = grau(\alpha)$,
3. $a \notin r_1(S)$,
4. $(a,b) \in \alpha(E(\overline{K}))$.

Dado que $pq' - p'q$ não é o polinômio zero, então S é finito e portanto sua imagem por α é finita. Vemos que a função $r_1(x)$ assume infinitos valores distintos quando x percorre $\overline{\mathbb{K}}$. Dado que para cada x,

existe um ponto $(x, y) \in E(\overline{\mathbb{K}})$, vemos que $\alpha(E(\overline{\mathbb{K}}))$ é um conjunto infinito. Por isso um tal ponto (a, b) existe.

Afirmamos que existem exatamente $grau(\alpha)$ pontos $(x_1, y_1) \in E(\overline{\mathbb{K}})$ tais que $\alpha(x_1, y_1) = (a, b)$. Para tais pontos temos que

$$\frac{p(x_1)}{q(x_1)} = a, \quad y_1 r_2(x_1) = b.$$

Dado que $(a, b) \neq \infty$, temos que $q(x_1) \neq 0$. Sendo que $r_2(x_1)$ é definida, $b \neq 0$ e $y_1 r_2(x_1) = b$, temos que $y_1 = b/r_2(x_1)$. Portanto, neste caso, como x_1 determina y_1, só precisamos contar os valores de x_1.

Por 2. temos que a equação $p(x) - aq(x) = 0$ tem $grau(\alpha)$ raízes , contando multiplicidades. Portanto devemos mostrar que $p - aq$ não tem raízes múltiplas. Suponha que x_0 seja uma raiz múltipla. Então

$$p(x_0) - aq(x_0) = 0 \quad e \quad p'(x_0) - aq'(x_0) = 0.$$

Agora, $apq' = a^2qq' \ \ e \ \ ap'q = a^2qq'$, de onde obtemos

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Como $a \neq 0$, isto implica que x_0 é uma raiz de $pq' - p'q = 0$ e assim $x_0 \in S$. Portanto $a = r_1(x_0) \in r_1(S)$, o que contraria a afirmação 3. Disto segue que $p - aq$ não tem raízes múltiplas e portanto tem $grau(\alpha)$ raízes distintas.

Dado que existem exatamente $grau(\alpha)$ pontos (x_1, y_1) com $\alpha(x_1, y_1) = (a, b)$, o núcleo de α tem $grau(\alpha)$ elementos. De fato, como α é um homomorfismo, para cada $(a, b) \in \alpha(E(\overline{K}))$, existem exatamente $grau(\alpha)$ pontos (x_1, y_1) com $\alpha(x_1, y_1) = (a, b)$.

Se α não for separável, então os passos da prova acima valem, exceto que $p' - aq'$ será sempre o polinômio zero, ou seja, o polinômio $p(x) - aq(x)$ sempre tem raízes múltiplas e portanto terá menos de $grau(\alpha)$ soluções.

□

Obsdervação 4.2. *Para aplicações posteriores, é necessário um critério adequado de separabilidade. Se (x, y) é um ponto sobre a curva elíptica $y^2 = x^3 + Ax + B$, então derivando y em relação a x obtemos $2yy' = 3x^2 + A$. Analogamente, podemos derivar uma função racional $f(x, y)$ em relação a x:*

$$\frac{d}{dx} f(x, y) = f_x(x, y) + f_y(x, y)y',$$

onde f_x e f_y denotam as derivadas parciais.

Neste sentido temos o seguinte resultado.

Lema 4.3. *Sejam E a curva elíptica $y^2 = x^3 + Ax + B$ e (u, v) um ponto fixo sobre E. Escrevemos*

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

onde $f(x, y)$ e $g(x, y)$ são funções racionais de x, y (os coeficientes dependem de (u, v)) e y é vista como função de x satisfazendo a relação $dy/dx = (3x^2 + A)/(2y)$. Então

$$\frac{\frac{d}{dx} f(x, y)}{g(x, y)} = \frac{1}{y}.$$

Demonstração: As fórmulas de adição fornecem

$$f(x, y) = \left(\frac{y - v}{x - u}\right)^2 - x - u,$$

$$g(x, y) = \frac{-(y - v)^3 + x(y - v)(x - u)^2 + 2u(y - v)(x - u)^2 - v(x - u)^3}{(x - u)^3},$$

$$\frac{d}{dx} f(x, y) = \frac{2y'(y - v)(x - u) - 2(y - v)^2 - (x - u)^3}{(x - u)^3}.$$

Um cálculo simples, usando o fato de que $2yy' = 3x^2 + A$, produz

$$\begin{aligned}(x-u)^3(y\frac{d}{dx}f(x,y) &- g(x,y)) = \\ &= v(Au+u^3-v^2-Ax-x^3+y^2)+y(-Au-u^3+v^2+Ax+x^3-y^2).\end{aligned}$$

Dado que (u,v) e (x,y) estão sobre E, temos que $v^2 = u^3 + Au + B$ e $y^2 = x^3 + Ax + B$. Assim, da expressão acima obtemos $y\frac{d}{dx}f(x,y) = g(x,y)$, ou seja,

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}.$$

□

Obsdervação 4.3. *O lema acima diz que o diferencial dx/y é invariante por translação. De fato, é o único diferencial invariante por translação para a curva E, salvo múltiplo escalar.*

O resultado a seguir é fundamental na contagem dos pontos de curvas elípticas sobre corpos finitos usando o endomorfismo de Frobenius ϕ_q.

Assim, dado que ϕ_q é um endomorfismo sobre E, temos que $\phi_q^2 = \phi_q \circ \phi_q$ e $\phi_q^n = \phi_q \circ \cdots \circ \phi_q$, para $n \geq 1$, também são endomorfismos. Também, como a multiplicação por -1 é um endomorfismo, então a soma $\phi_q^n - 1$ é um endomorfismo de E.

proposição 4.2. *Seja uma curva E definida sobre $\mathbb{F}_q$ e $n \geq 1$. Então:*

1. $Ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.

2. $\phi_q^n - 1$ é um endomorfismo separável e assim $card(E(\mathbb{F}_{q^n})) = grau(\phi_q^n - 1)$.

Demonstração: Dado que ϕ_q^n é um endomorfismo de Frobenius sobre o corpo $\mathbb{F}_{q^n}$, então pelo lema 4.2 temos que $\phi_q^n(x,y) \in E(\overline{\mathbb{F}}_{q^n})$ e $(x,y) \in E(\mathbb{F}_{q^n}) \iff \phi_q^n(x,y) = (x,y)$. Isto implica 1., ou seja, $Ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$. A parte 2. segue do fato de que $grau(\phi_q^n - 1) = card(Ker(\phi_q^n - 1) = ord(E(\mathbb{F}_{q^n}))$.

□

5. Conclusões. Neste trabalho foram estudadas algumas propriedades do endomorfismo de Frobenius, relativas a seu núcleo e à condição de separabilidade. Num próximo trabalho pretende-se usar estas propriedades para mostrar um resultado, o Teorema de Hasse, o qual apresenta uma estimativa para o número de pontos racionais de uma curva elíptica definida sobre um corpo finito.

Contribuição do autor. O artigo foi desenvolvido na íntegra pelo autor JA.

Conflito de interesses. O autor declara não ter conflito de interesses.

ORCID and License
Jaime Edmundo Apaza Rodriguez https://orcid.org/0000-0002-1359-9898

Referências

[1] Meireles TAB. Curvas Elípticas e Criptografia[Dissertação de Mestrado]. Uberlandia: Universidade Federal de Uberlandia; 2020.

[2] Washington LC. Elliptic Curves, Number Theory and Criptography, Discrete Mathematics and its Applications. Second Edition. Maryland: Chapman and Hall/CRC, 2008.

[3] Silverman JH. The Arihmetic of Elliptic Curves. New York: Springer-Verlag, V 106, 2008.