SIMPEX + 4º MOBICIT
CONEXÕES QUE MOVEM o FUTURO
Energia e Inteligência para Cidades Vivas
Realização: UniSENAI, Instituto SENAI de Inovação, Instituto SENAI de Tecnologia, fapesc
Apoio: Even3

FROM ABSTRACT MATHEMATICS TO DIGITAL SECURITY: ELLIPTIC CURVES AS A TOOL FOR INTEGRATING THEORY AND PRACTICE

Matheus Luan Krueger*
SENAI Santa Catarina University Center - UniSENAI

1. Introduction

Bridging abstract mathematical concepts and real-world applications remains a central challenge in higher education, particularly in domains such as cryptography [1], where advanced mathematical structures underpin modern technological systems. In this context, elliptic curves (ECs) stand out as a compelling example of how such structures power widely deployed technological systems, especially in digital security and cryptographic protocols. Their relevance becomes even more pronounced as digital infrastructures scale to support smart cities and interconnected environments with large-scale data generation and exchange, where the demand for lightweight, efficient, and provably secure cryptographic primitives places ECs at the forefront of modern security design [2]. This duality between mathematical abstraction and practical application makes their study particularly relevant from a pedagogical perspective. This work proposes a progressive pedagogical approach that starts from the general formulation of cubic curves, evolves to the characterization of ECs and their normalized forms, and culminates in the analysis of their use in cryptographic systems (*e.g.*, elliptic curve cryptography - ECC), highlighting how abstract mathematics finds direct relevance in present-day technological demands, fostering student motivation by demonstrating that rigorous mathematical theory is embedded in real-world practice.

2. Theoretical background

A general planar cubic curve defined over a field K can be described by a polynomial equation of degree 3 in two variables: $F(x,y) = c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3 + c_4x^2 + c_5xy + c_6y^2 + c_7x + c_8y + c_9$ (Eq. 1), where $F \in K[x,y]$ is a cubic polynomial in x and y with its coefficients $c_i \in K$ [3]. In its most general form, such an equation involves multiple coefficients and reflects the broad diversity of cubic curves, most of which do not satisfy the conditions required for cryptographic use. A fundamental requirement is non-singularity, that is, the absence of points where the partial derivatives vanish simultaneously. Geometrically, singular points correspond to cusps or self-intersections, which prevent the development of a well-defined algebraic structure. In addition, it is necessary that the curve admits at least one rational point over the base field K. The choice of such a point as the identity element, usually denoted by O and corresponding in projective coordinates to the point at infinity, endows the curve with a group structure that constitutes the algebraic foundation for all cryptographic applications of ECs. Under these conditions, such curves are known as ECs, that is, smooth projective curves of genus 1 equipped with a distinguished rational point [1].

Mathematically, any EC can be defined by the Long Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (Eq. 2), where $a_i \in K$ [1]. In cryptographic contexts, K is typically a finite prime field F_p [2]. Through suitable coordinate transformations, this equation can be normalized into simpler forms while preserving its essential algebraic structure [4], a process that is fundamental for both theoretical analysis and computational implementation. When char(K) ≠ 2,3, this representation can be reduced to the Short Weierstrass form: $y^2 = x^3 + ax + b$ (Eq. 3) [2], which is widely adopted in cryptographic protocols such as NIST P-256 and secp256k1 (Bitcoin). While the Weierstrass models are the most traditional, modern industrial standards frequently employ alternative representations to optimize performance and security. In particular, Montgomery curves, defined by $By^2 = x^3 + Ax^2 + x$ (Eq. 4), are preferred for high-speed key exchanges (*e.g.*, X25519) due to their efficient scalar multiplication. Additionally, Edwards curves, expressed as $x^2 + y^2 = 1 + dx^2y^2$ (Eq. 5), are widely used in digital signature schemes (*e.g.*, Ed25519) because their complete addition formulas eliminate exceptional cases, thereby increasing resistance against certain attacks [2, 4]. Together, these four representations provide the algebraic foundation for most modern ECC implementations, and their systematic

* matheus.krueger@edu.sc.senai.br

progression from general to specialized forms constitutes the theoretical backbone of the pedagogical approach proposed in this work.

3. Pedagogical approach

The pedagogical approach proposed in this work follows a progressive and application-driven structure, organized into four stages mirroring the mathematical progression from general cubic curves to specialized EC representations. In the first stage, students are introduced to the general formulation of cubic curves (Eq. 1), grounded in geometric visualization over $\mathbb{R}$. This entry point leverages prior familiarity with continuous curves, reducing the cognitive barrier to more abstract algebraic content. In the second stage, coordinate transformations lead to the Long Weierstrass form (Eq. 2), allowing students to observe how algebraic manipulation preserves structural properties while simplifying the curve. In the third stage, depending on the target application, this representation is further reduced to the Short Weierstrass (Eq. 3), Montgomery (Eq. 4), or Edwards (Eq. 5) forms, each directly connected to a concrete cryptographic protocol such as secp256k1, X25519, or Ed25519 [5]. A fundamental conceptual shift occurs in the fourth stage, with the transition from continuous structures over $\mathbb{R}$ to discrete sets of points over finite fields F_p. As illustrated in Figs. 1 and 2, the same curve that appears as a smooth geometric object over $\mathbb{R}$ becomes a scattered set of points over F_p, intuitively motivating the concepts of modular arithmetic and field reduction that underlie real-world cryptographic implementations.

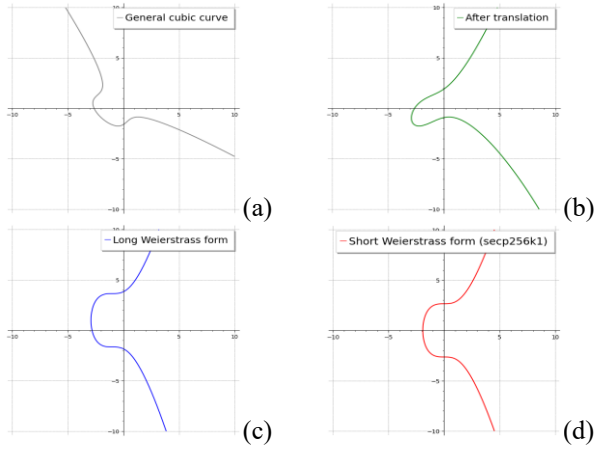

Fig. 1. *Progressive reduction of a general planar cubic curve to the Short Weierstrass form over $\mathbb{R}$: (a) general cubic curve, (b) after translation, (c) Long Weierstrass form, (d) Short Weierstrass form (secp256k1).*

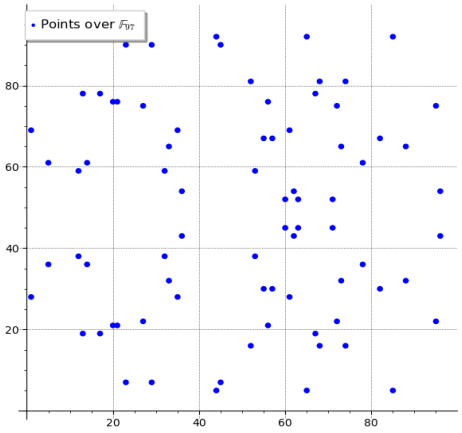

Fig. 2. *The same curve (secp256k1: $y^2 = x^3+7$) defined over the field F_{97}, illustrating the discrete set of points that characterizes ECs in cryptographic applications, where larger fields are employed in practice.*

4. Results and discussions

The proposed approach suggests strong potential for bridging abstract mathematics and practical applications in higher education. The geometric contrast between continuous curves over $\mathbb{R}$ and discrete points over F_p provides an intuitive anchor for modular arithmetic and field reduction. Connecting each algebraic representation to a concrete cryptographic protocol reinforces the perception that rigorous mathematical theory is deeply embedded in modern technological practice, fostering student motivation and engagement in mathematically demanding disciplines, particularly in fields such as digital security and smart cities.

5. References

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed. New York, NY, USA: Springer, 2009.
[2] J. M. Miret, R. Moreno, J. Pujolàs, and M. Valls, “Algorithms and cryptographic protocols using elliptic curves”, *Contrib. Sci.*, vol. 3, no. 4, pp. 481–491, 2007.
[3] I. Vainsencher, *Introdução às Curvas Algébricas Planas*, 1st ed. Rio de Janeiro, RJ, Brasil: IMPA, 2014.
[4] M. P. Seguí, “Elliptic curves: various models and their addition laws - a study in computer algebra", Master’s thesis, Faculty of Science, Radboud Univ. Nijmegen, Nijmegen, Netherlands, 2022.
* matheus.krueger@edu.sc.senai.br

[5] L. Chen, D. Moody, A. Regenscheid, A. Robinson, and K. Randall, “Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters”, NIST Special Publication 800-186, 2023.

* matheus.krueger@edu.sc.senai.br