Research Article GU J Sci 39(3): 1336-1350 (2026) DOI: 10.35378/gujs.1863003

Gazi University

Journal of Science

http://dergipark.org.tr/gujs

# On the Point at Infinity of Elliptic Curves and a New Group Structure on the Quadratic Curve $x^2$

Israfil OKUMUS[1], Ercan CELIK[2,3,*]

[1] Erzincan Binali Yıldırım University, Faculty of Science and Art, Department of Mathematics, Erzincan/ Türkiye
[2] Kyrgyz-Turkish Manas University, Department of Applied Mathematics and Informatics, Bishkek/ Kyrgyzstan
[3] Ataturk University, Faculty of Science, Department of Mathematics, Erzurum/ Türkiye

## Highlights

- New geometric view: identity linked to the line at infinity.
- Abelian group constructed on the curve $y = x^2$.
- Non-elliptic curves enable new crypto structures beyond elliptic curve cryptography.

**Article Info**

*Received: 13 Jan 2026*
*Accepted: 11 May 2026*

**Keywords**

*Elliptic curves*
*Point at infinity*
*Quadratic curves*
*Group law*
*Geometric interpretation*

## Abstract

Elliptic curves play a fundamental role in contemporary cryptography due to their deep algebraic properties and their ability to provide high levels of security with relatively small parameter sizes. The theoretical and practical foundations of elliptic curve cryptography (ECC) were established through independent contributions by Koblitz and Miller, whose pioneering work demonstrated that the group structure induced by elliptic curves could be effectively employed in public-key cryptographic schemes. Since then, ECC has become a cornerstone of modern cryptographic protocols, including widely deployed mechanisms such as the Elliptic Curve Digital Signature Algorithm (ECDSA). In this study, we re-examine the algebraic and geometric significance of the point at infinity. Rather than treating this element as an abstract artifact, we introduce an alternative geometric interpretation by associating the identity with the line at infinity. This perspective preserves the classical group law while offering a more intuitive and geometrically transparent understanding of the identity element within the elliptic curve framework. Motivated by the chord-and-tangent addition law on elliptic curves, we further extend these ideas to a non-elliptic setting by defining a new binary operation on the quadratic curve $y = x^2$. Consequently, the resulting algebraic system forms an abelian group. The proposed approach not only enhances the conceptual clarity of the group law underlying elliptic curves but also illustrates how similar algebraic constructions can arise in alternative geometric contexts. These findings provide a theoretical framework that may inspire future explorations of cryptographic primitives beyond classical elliptic curve models.

## 1. INTRODUCTION

Elliptic Curves (ECs) have long attracted sustained attention in algebraic geometry and number theory due to their highly structured arithmetic behaviour and deep connections with fundamental theoretical problems. The development of the Weierstrass normal form has played a central role in formalizing the study of elliptic curves by providing a unified representation that bridges algebraic definitions with analytic interpretations, thereby shaping much of the modern theory of these objects [1].

Beyond their intrinsic mathematical interest, elliptic curves have demonstrated remarkable relevance in addressing long-standing problems in number theory. A particularly influential example is Fermat's Last Theorem, whose proof by Andrew Wiles relies crucially on elliptic curves, highlighting the profound and nontrivial interplay between arithmetic geometry and Diophantine equations.

*Corresponding author, e-mail: ercan.celik@mans.edu.kg

Modern public-key cryptography originated with the introduction of key exchange by Whitfield Diffie and Martin Hellman in 1976 [2], followed by the RSA cryptosystem proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 [3]. Subsequently, Taher ElGamal introduced an encryption and signature scheme based on the discrete logarithm problem [4]. Around the same period, Claus-Peter Schnorr proposed an efficient digital signature scheme grounded in the discrete logarithm problem, known as the Schnorr signature, which is notable for its simplicity, provable security properties, and efficiency [5].

Recent studies have also explored optimization techniques for classical public-key systems such as RSA, particularly focusing on improving the balance between encryption and decryption costs through modified key generation algorithms [6,7].

The relevance of elliptic curves to cryptographic applications became evident in the mid-1980s, when Victor S. Miller and Neal Koblitz independently proposed utilizing the algebraic structure of elliptic curves to construct secure public-key cryptosystems [8,9]. These developments can be viewed as natural extensions of earlier breakthroughs in public-key cryptography.

In contrast to classical number-theoretic systems based on integer factorization or discrete logarithms in multiplicative groups, Elliptic Curve Cryptography exploits the hardness of the elliptic curve discrete logarithm problem. This enables ECC to achieve comparable, and often stronger, levels of security than RSA while using significantly smaller key sizes. Consequently, ECC has become particularly attractive for deployment in resource-constrained environments such as mobile devices, embedded systems, smart cards, and modern blockchain infrastructures [10].

A prominent instantiation of ECC is the Elliptic Curve Digital Signature Algorithm (ECDSA), which was introduced by Johnson, Menezes, and Vanstone [11] and subsequently standardized by the National Institute of Standards and Technology (NIST) in FIPS 186, 186-2 [12,13]. ECDSA has since been widely adopted in secure communication protocols and digital asset systems due to its efficiency and strong security properties. Continued research in elliptic curve representations and implementations has led to further refinements, including the introduction of Edwards curves [14] and twisted Edwards curves [15], which offer more efficient and symmetric addition formulas. These advances culminated in the standardization of the Edwards-curve Digital Signature Algorithm (EdDSA) in FIPS 186-5 [16], contributing to improved performance, resistance to implementation errors, and enhanced overall security.

At the algebraic core of elliptic curve cryptography lies a group structure defined through a geometrically motivated point addition law on the set of curve points. This operation endows the curve with an abelian group structure, which serves as the mathematical foundation for cryptographic constructions. The identity element of this group is represented by a distinguished non-affine point, commonly referred to as the point at infinity, which arises naturally when the affine elliptic curve is completed in the projective plane [17]. While this construction is well established within algebraic geometry, its abstract nature can pose conceptual challenges for students and practitioners whose primary focus lies in applied cryptography. This observation has motivated ongoing efforts to seek alternative geometric viewpoints that retain algebraic rigor while offering greater intuitive accessibility.

In this study, we revisit the role of the point at infinity and propose an alternative viewpoint by interpreting it in terms of the line at infinity. This reformulation preserves the fundamental properties of the group law but provides a more accessible geometric representation of the identity element in elliptic curve arithmetic.

Building on this perspective, we further extend the classical group-law framework by introducing a novel point addition operation on the quadratic curve $y = x^2$. Inspired by the geometric construction of elliptic curve addition, this operation is rigorously shown to satisfy the axioms of an abelian group—closure, associativity, commutativity, and the existence of identity and inverse elements. By exploring such alternative algebraic structures, we aim to broaden the theoretical landscape of elliptic curve mathematics and offer insights that may inform the design of future cryptographic protocols.

The organization of this paper is designed to present the necessary theoretical background before introducing the main contributions of the study in a structured and coherent manner.

Section 2 reviews the classical group law on elliptic curves, focusing on both its algebraic formulation and its geometric interpretation. This section establishes the fundamental framework required for understanding the role of the identity element and the chord-and-tangent construction underlying elliptic curve arithmetic.

In section 3, we revisit the notion of the point at infinity and propose an alternative geometric interpretation based on the concept of the line at infinity. This perspective provides a more intuitive understanding of the identity element while remaining consistent with the classical group law.

Section 4 introduces the main contribution of this study. In this section, we define a novel binary operation on the quadratic curve ($y = x^2$), inspired by the geometric principles of elliptic curve addition. We rigorously prove that this operation satisfies the axioms of an abelian group, including closure, associativity, commutativity, and the existence of identity and inverse elements.

Finally, section 5 summarizes the main results of the study and outlines several directions for future research. These include the investigation of the proposed structure over finite fields, its algebraic properties, and its potential implications for generalized curve-based cryptographic frameworks. Related studies on modified elliptic curve constructions further illustrate the flexibility of curve-based algebraic systems [17].

Unlike classical approaches that treat the point at infinity as a purely projective artifact, our approach provides a limit-based geometric interpretation that enhances intuitive understanding. Furthermore, while previous studies have focused primarily on cubic curves, the present work extends the group-law concept to a quadratic curve, thereby demonstrating that such algebraic structures are not restricted to elliptic curves. To the best of our knowledge, this type of construction on the curve $y = x^2$ has not been explicitly formulated in the literature.

## 2. GROUP LAW ON AN ELLIPTIC CURVE AND GEOMETRIC INTERPRETATION

This section presents a concise overview of the algebraic group structure associated with elliptic curves, which forms the mathematical foundation of elliptic-curve-based cryptographic constructions. In particular, the group law defined on elliptic curves underlies both the security assumptions and the practical efficiency of modern cryptographic protocols. The fundamental properties of elliptic curve groups enable the design of public-key cryptosystems that provide strong security guarantees while maintaining computational efficiency. As a result, elliptic curve groups have become a preferred choice in applications where performance, scalability, and resource constraints are critical [18-20].

Assume that the base field $K$ satisfies $\mathrm{char}(K) \neq 2,3$. Under this assumption, an elliptic curve defined over $K$ can be expressed in short Weierstrass form.

Let $E$ denote an elliptic curve defined over a field $K$, given by

$$E: y^2 = x^3 + ax + b, a, b \in K, \tag{1}$$

where the non-vanishing of the discriminant

$$\Delta(E) = -16(4a^3 + 27b^2) \neq 0$$

ensures that the curve is non-singular. The set of $K$-rational points on $E$, denoted by $E(K)$, consists of all pairs $(x, y) \in K^2$ satisfying Equation (1), together with an additional distinguished element $\mathcal{O}$, called the point at infinity, which serves as the identity element in the abelian group structure.

Let $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ be two points in $E(K)$. The binary operation that equips $E(K)$ with a group structure is defined algebraically in a manner that reflects an underlying geometric construction.

Central to this structure is the inclusion of the distinguished element $\mathcal{O}$, which arises naturally when the curve is considered in its projective closure. This element acts as the neutral element of the group, satisfying

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

An essential feature of the group law is the existence of inverse elements. For each point $P \in E(K)$, there exists a unique point $-P \in E(K)$ such that

$$P + (-P) = \mathcal{O}.$$

Geometrically, the inverse of a point is obtained by reflecting it across the $x$-axis, yielding

$$-P := (x_1, -y_1).$$

This corresponds to two points sharing the same $x$-coordinate while having opposite $y$-coordinates. The vertical line passing through these points intersects the curve in exactly these two affine points together with the point at infinity. Consequently, the sum of a point and its inverse yield the identity element.

The addition of two distinct points that are neither equal nor inverses of one another is determined by the line passing through them. In this case, the slope $\lambda$ of the line joining $P$ and $Q$ is given by

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{2}$$

When $P = Q$, the line becomes the tangent to the curve at $P$, and the slope is given by

$$\lambda = \frac{3x_1^2 + a}{2y_1}. \tag{3}$$

These expressions reflect the local geometric behaviour of the curve and ensure consistency between the algebraic definition of the operation and its geometric interpretation.

Once the slope $\lambda$ is determined using Equation (2) or Equation (3), the coordinates of the resulting point $R := P + Q$ are obtained from (4) and (5), where the $x$-coordinate is given by

$$x_3 = \lambda^2 - x_1 - x_2, \tag{4}$$

and the corresponding $y$-coordinate is given by

$$y_3 = \lambda(x_1 - x_3) - y_1. \tag{5}$$

Geometrically, as described by Equation (4) and Equation (5), the point $R$ is obtained by first identifying the third intersection point of the line with the curve and then reflecting this point across the $x$-axis, ensuring closure of the operation.

Equipped with this addition law, the set $E(K)$ satisfies all axioms of an Abelian group. The operation is closed and associative, the point at infinity $\mathcal{O}$ serves as the identity element, and each point admits a unique inverse. Moreover, the symmetry inherent in the construction guarantees commutativity. This algebraic structure forms the mathematical foundation of elliptic-curve-based cryptographic systems, linking geometric intuition with rigorous algebraic formalism.

### 2.1. Geometric Interpretation

The point addition operation on an elliptic curve can be interpreted through a classical geometric construction. Consider two distinct points $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ on the curve, with $x_1 \neq x_2$. The

straight line determined by these two points intersects the elliptic curve at exactly one additional point, which we denote by $R \coloneqq (x_3, y_3)$. This third intersection point arises from Bézout's theorem and reflects the cubic nature of the defining equation of the curve.

To obtain the sum of $P$ and $Q$ under the group law, the point $R$ is then reflected across the $x$-axis. The resulting point, denoted by $-R := (x_3, -y_3)$ , is defined to be the group sum $P + Q$. This construction ensures that the algebraic formulas defining the addition operation are consistent with a clear geometric picture and that the resulting point remains on the curve. A visual representation of this process, illustrating the chord connecting $P$ and $Q$, its third intersection with the curve, and the subsequent reflection step, is shown in Figure 1.

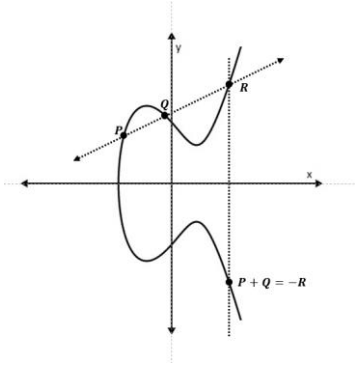


***Figure 1.*** *Geometric visualization of the point addition process for two distinct points on an elliptic curve*

The geometric interpretation of the group operation in the special case where the two points coincide, namely $P = Q$, is obtained through a tangent-based construction. In this situation, the tangent line to the elliptic curve at the point $P$ is considered instead of a secant line. This tangent intersects the curve at a second point, denoted by $R$, which accounts for the multiplicity of the intersection at $P$.

The group-theoretic doubling of the point $P$ is then defined by reflecting the point $R$ across the $x$-axis, yielding the point $-R$. This reflected point represents the sum $2P$ under the elliptic curve group law. A schematic depiction of this tangent-based construction, illustrating the intersection and reflection steps, is shown in Figure 2.

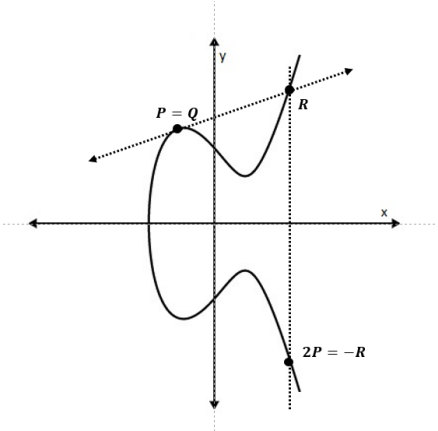


***Figure 2.*** *Visualization of the elliptic curve group law in the special case of coincident points, illustrating the tangent intersection and reflection process*

The geometric meaning of the relation between a point and its inverse under the elliptic curve group law can be visualized through a simple yet fundamental construction. Given a point $P$ on the curve, its inverse $-P$ lies on the same vertical line and is obtained by reflecting $P$ across the $x$-axis. The vertical line passing through both $P$ and $-P$ intersects the elliptic curve only at these two affine points. When the curve is viewed

in its projective closure, this vertical line meets the curve at an additional point located at infinity, which is identified with the identity element $\mathcal{O}$ of the group.

From this geometric perspective, the sum of a point and its inverse is naturally associated with the point at infinity, thereby justifying the group-theoretic relation $P + (-P) = \mathcal{O}$. This interpretation highlights the essential role of the point at infinity in ensuring closure and consistency of the group law. A graphical representation of this construction, emphasizing the vertical alignment of $P$ and $-P$ and their relation to the identity element, is shown in Figures 3 and 4.

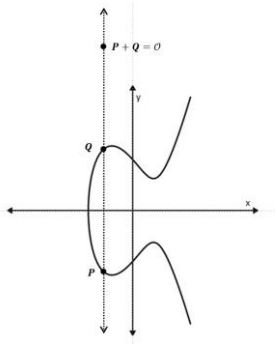


***Figure 3.*** *Addition of a point and its inverse on an elliptic curve*

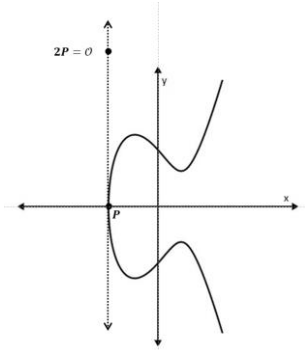


***Figure 4.*** *Special geometric configuration arising when two coincident points satisfy* $y = 0$*, highlighting the behavior of the group law*

This geometric construction is consistent with the algebraic definition of the group law on elliptic curves and provides intuitive insight into the role of the point at infinity.

When elliptic curves are considered within the framework of the projective plane $\mathbb{P}_K^2$, certain geometric properties become more transparent. Any two vertical lines of the form $x = c_1$ and $x = c_2$, although parallel in the affine plane, intersect at a common point in the projective setting. This intersection occurs at the homogeneous coordinate

$$(0:1:0) \tag{6}$$

which is interpreted as the point at infinity. Within this framework, an elliptic curve possesses exactly one such point at infinity, uniquely represented by Equation (6). The geometric significance of this point is further emphasized by the fact that its tangent line coincides with the line at infinity, which intersects the curve only at this distinguished point.

Beyond the geometric interpretation, the algebraic structure of elliptic curves allows for repeated application of the group operation. Adding a point $P \in E$ to itself yields the point $2P$, and this process can be iterated to define scalar multiplication by any positive integer $k$. Scalar multiplication is defined as

$$Q = kP = \sum_{i=1}^{k} P\,. \tag{7}$$

This operation is fundamental to elliptic curve arithmetic and forms the computational core of elliptic curve cryptography.

In cryptographic applications over finite fields $\mathbb{F}_q$, scalar multiplication acquires a concrete interpretation. The integer $k$ is typically chosen as a secret parameter (private key), while the resulting point

$$Q := kP \tag{8}$$

is made public and serves as the corresponding public key.

This asymmetric relationship between $k$ and $Q$, as defined in Equation (8), is central to a wide range of cryptographic protocols, including the Elliptic Curve Digital Signature Algorithm (ECDSA). In such schemes, the private key is used to generate digital signatures, whereas the public key enables efficient and reliable verification.

Owing to these properties, elliptic curve–based cryptography has become a foundational component of secure communication systems, digital identity frameworks, and modern cryptocurrency platforms. One of the key advantages of elliptic curve cryptography lies in its ability to achieve high levels of security with significantly smaller key sizes compared to classical systems such as RSA, making it particularly well suited for blockchain technologies and resource-constrained environments.

An important theoretical result supporting elliptic curves over finite fields is Hasse's theorem [21] which was originally conjectured by Emil Artin [22] in the context of his work on quadratic fields and higher congruences. Let $\#E(\mathbb{F}_q)$denote the number of $\mathbb{F}_q$-rational points on the curve. Then

$$\left|\#E(\mathbb{F}_q) - (q+1)\right| \leq 2\sqrt{q}\,. \tag{9}$$

This bound shows that the number of points is tightly concentrated around $q+1$. The significance of Equation (9) extends beyond theory, as it directly impacts the security and efficiency of elliptic curve cryptosystems. In practice, accurate estimates of $\#E(\mathbb{F}_q)$are essential for selecting secure curve parameters and ensuring resistance against discrete logarithm attacks.

Although the point at infinity is an indispensable component of the elliptic curve group law, its traditional treatment as an abstract projective artifact often obscures its geometric meaning. From a geometric perspective, the point at infinity arises as the common intersection of all vertical lines, as expressed in (6). This observation suggests that the identity element is not merely an isolated point, but rather a manifestation of the behaviour of the curve at infinity.

Motivated by this insight, one may reinterpret the identity element as a limiting geometric object associated with the line at infinity. This perspective suggests that the essential features of the group law arise from the interaction between lines and curves, rather than from the specific cubic form.

If this is the case, then similar algebraic structures may emerge in alternative geometric settings. In particular, the mechanism underlying scalar multiplication in Equation (7) and its cryptographic realization in Equation (8) suggests that group operations can be generalized beyond classical elliptic curves.

In the following section, we build on this idea by introducing a novel group structure on the quadratic curve $y = x^2$, inspired by elliptic curve addition, while preserving key algebraic properties such as closure, inverses, and associativity.

## 3. A NEW DEFINITION OF THE INFINITY ELEMENT ON ELLIPTIC CURVES

Given the inherently abstract role played by the point at infinity in the classical elliptic curve group law, we propose an alternative formulation aimed at providing a more transparent geometric and algebraic interpretation of this element. Rather than viewing the point at infinity solely as a formal object introduced through projective completion, we reinterpret it through a limiting geometric construction that we refer to as the line at infinity. This perspective highlights the geometric origin of the identity element and offers a more intuitive understanding of its function within the group law on elliptic curves.

More specifically, instead of introducing the identity element as an isolated point, we consider a family of horizontal lines of the form $y = k$, where $k \in \mathbb{Q}^+$ and $k \to \infty$. By replacing the abstract point at infinity with this limiting process, we define an extended set

$$E'(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{y = k \mid k \to \infty\} \tag{10}$$

which augments the affine points of the elliptic curve $E'$ over the field $K$ with a geometric representative of infinity. In this formulation, the infinite element is not treated as a single point a priori, but rather as the limit of a family of lines whose behaviour captures the same algebraic role.

To illustrate how this construction reproduces the identity behaviour of the classical group law, consider the points $P := (x_1, y_1)$, $Q := (x_1, -y_1)$, $R := (x_2, y_2)$, and $S := (x_2, -y_2)$ belonging to Equation (10), with $x_1 \neq x_2$. Under the standard elliptic curve addition, each pair of points sharing the same $x$-coordinate but opposite $y$-coordinates corresponds to inverse elements. In the proposed framework, the sum $P + Q$ is associated with a point $\mathcal{O}(x_1, k)$ lying on the line $y = k$, while the sum $R + S$ similarly yields a point $\mathcal{O}'(x_2, k)$ on the same family of horizontal lines.

As $k \to \infty$, the slopes of the lines connecting $\mathcal{O}$ to $R$ and $\mathcal{O}$ to $S$, denoted by $M_{OR}$ and $M_{OS}$, respectively, converge to the slope $M_{RS}$. In this limiting regime, the distinction between the points $\mathcal{O}$ and $\mathcal{O}'$ disappears, and they merge into a single geometric object representing infinity. Consequently, the addition of inverse pairs such as $R + S$ naturally yields the identity element in this extended sense. This limiting behaviour reproduces the defining property of the identity in the elliptic curve group law without requiring the introduction of an abstract point from the outset. The corresponding geometric configurations are depicted in Figure 5.

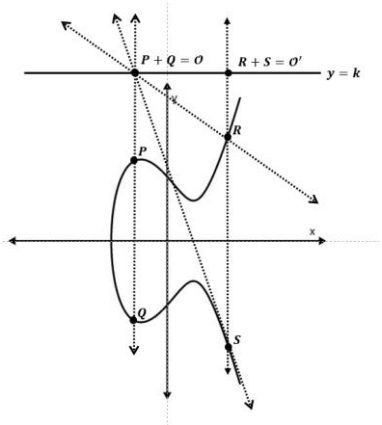


***Figure 5.*** *Geometric representation of the identity element obtained through a limiting construction associated with a horizontal line approaching infinity. The projective completion of the elliptic curve introduces the line at infinity*

From the perspective of projective geometry, this construction is consistent with the projective completion of elliptic curves, in which the line at infinity plays a fundamental role. In the projective plane, all vertical lines intersect at a common point on the line at infinity, which is precisely the classical point at infinity used in elliptic curve theory. The present approach makes this connection explicit by interpreting the identity element as a geometric limit associated with the line at infinity, rather than as an isolated projective artifact. In doing so, it preserves the algebraic properties required for the group law while offering a conceptually clearer geometric foundation.

## 4. A NOVEL GROUP STRUCTURE ON THE QUADRATIC CURVE $y = x^2$

To ensure mathematical rigor, we explicitly verify that the proposed binary operation satisfies all group axioms, namely closure, associativity, the existence of an identity element, and the existence of inverse

elements. Attention is devoted to the limiting process used in the definition of the identity element, ensuring that the construction is well-defined and consistent within the underlying algebraic framework.

In this section, we introduce a group structure on the quadratic curve $y = x^2$ by defining a geometric operation inspired by the classical chord-and-tangent addition law on elliptic curves. Through this construction, we systematically analyze both the algebraic properties and the geometric interpretation of the resulting operation. We rigorously establish that the structure is closed under the operation, compatible with repeated compositions, and admits a well-defined neutral element together with inverse elements for each point. Consequently, the curve satisfies all axioms required to form an abelian group.

This construction highlights that the emergence of group structures is not inherently restricted to cubic curves. Rather, it demonstrates that fundamental ideas from elliptic curve theory and group theory can be meaningfully adapted to simpler polynomial curves. In this sense, the proposed framework provides a conceptual bridge between classical elliptic curve groups and alternative algebraic structures with potential theoretical and cryptographic significance.

**Definition 4.1.** Let $k \in \mathbb{Q}^-$ be a fixed constant. Define the set $E' \subset \mathbb{Q}^2$ by

$$E' := \{ (x, y) \in \mathbb{Q}^2 \mid y = x^2 \} \cup \{ (x, y) \in \mathbb{Q}^2 \mid y = k \}.$$

That is, $E'$ consists of all rational points on the parabola $y = x^2$ together with all rational points on the horizontal line $y = k$.

To construct a group structure on $E'$, we define the sum of two distinct points $P$ and $Q$ on the curve through a geometric procedure analogous to the elliptic curve addition law.

**Definition 4.2.** Let $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ be two distinct points on the curve $E'$, chosen such that $x_1 \neq x_2$, ensuring that the points do not form a symmetric pair with respect to the vertical axis.

To define the binary operation between $P$ and $Q$, consider the unique straight line determined by these two points in the affine plane. This line intersects the horizontal line $y = k$, at a unique point denoted by

$R' := (x_3, k)$ .

The $x$-coordinate $x_3$ uniquely determines a corresponding point

$R := (x_3, x_3^2)$

on the curve $E$.

The sum of $P$ and $Q$ is then defined as

$P + Q := R$ .

This construction mirrors the geometric spirit of the classical chord-and-tangent method used in elliptic curve theory, adapted here to a quadratic setting via an auxiliary horizontal line. A geometric illustration of this construction, including the intersection with the auxiliary horizontal line and the resulting point, is provided in Figure 6.

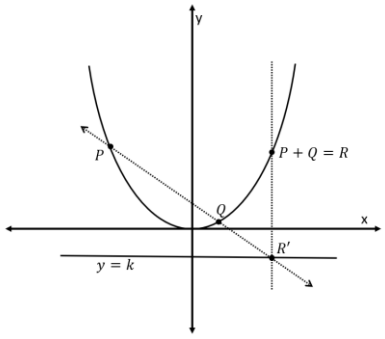


***Figure 6.*** *Point addition on the quadratic curve* $y = x^2$

From an algebraic perspective, the computation of the sum $P + Q$ can be carried out by explicitly analysing the linear relation determined by the two points. Consider two distinct points $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ lying on the quadratic curve under consideration.

Since the curve satisfies the relation

$$y = x^2 , \tag{11}$$

in Equation (11), the corresponding coordinates can be written as

$$y_1 = x_1^2, y_2 = x_2^2 . \tag{12}$$

Substituting these expressions into the standard difference quotient, we obtain the slope of the line passing through $P$ and $Q$:

$$m_d = \frac{y_2 - y_1}{x_2 - x_1}. \tag{13}$$

Using Equation (12) in Equation (13), this simplifies to

$$m_d = x_1 + x_2 . \tag{14}$$

Thus, the slope depends only on the sum of the $x$-coordinates. Using Equation (14), the equation of the line $d$ through $P$ can be written in point-slope form:

$$y - y_1 = m_d(x - x_1). \tag{15}$$

Substituting $m_d = x_1 + x_2$ and rearranging Equation (15), we obtain the explicit equation of $d$:

$$y = (x_1 + x_2)x - x_1x_2 . \tag{16}$$

To determine the outcome of the group operation, we examine the intersection of the line $d$ with the horizontal line

$$y = k, k \in \mathbb{Q},\ k \neq 0 . \tag{17}$$

Substituting Equation (16) into Equation (17), we obtain a linear equation in $x$:

$$(x_1 + x_2)x - x_1x_2 = k . \tag{18}$$

Solving (18) for $x$, we find the $x$-coordinate of the intersection point $R' = (x_3, k)$:

$$x_3 = \frac{k+x_1x_2}{x_1+x_2}. \tag{19}$$

This value of $x_3$ serves as the defining coordinate for the corresponding point on the curve and plays a central role in the construction of the group operation.

**Definition 4.3.** The identity element $\mathcal{O}$ is defined as a limiting object associated with the curve over $\mathbb{Q}$ given in Equation $(11)$. Consider the family of points

$$O' \coloneqq (a, a^2), a \in \mathbb{Q},$$

lying on the curve.

As $a \to \infty$, the points $O'$escape to infinity in the affine plane. We define the point at infinity, denoted by $\mathcal{O}$, as the formal limit of this family:

$$\mathcal{O} := \lim_{a\to\infty} (a, a^2). \tag{20}$$

This element is not an ordinary point of $\mathbb{Q}^2$, but a distinguished element adjoined to the set $E$. It serves as the identity element for the addition law defined on $E$.

**Theorem 4.4.** Let $E$ be the set defined above, equipped with the binary operation introduced in Definition 4.2 and let $\mathcal{O}$ denote the identity element defined in Definition 4.3. Then $(E, +)$ forms an abelian group.

For all $P, Q, R \in E$ such that $P := (x_1, y_1), Q \coloneqq (x_2, y_2), R := (x_3, y_3)$, the following properties hold

(i) $P + \mathcal{O} = \mathcal{O} + P = P$,

(ii) For every $P \in E$, there exists a unique $-P \in E$ such that $P + (-P) = \mathcal{O}$,

(iii) $(P + Q) + R = P + (Q + R)$,

(iv) $P + Q = Q + P$.

The proof follows by verifying each property individually using the algebraic form of the operation and its geometric interpretation.

**Proof.** We first verify the existence of an identity element.

(i) Let $O' := (a, a^2)$ be the auxiliary point representing $\mathcal{O}$. From Equation $(19)$, the $x$-coordinate of $P + O'$ is given by

$$x' = \frac{k+x_1a}{x_1+a}. \tag{21}$$

Dividing numerator and denominator of Equation $(21)$ by $a$, we obtain

$$x' = \frac{k/a+x_1}{x_1/a+1}. \tag{22}$$

Taking the limit in Equation $(22)$ as $a \to \infty$, we use the fact that $k/a \to 0$ and $x_1/a \to 0$, and hence

.

$$\lim_{a\to\infty} x' = x_1.$$

Therefore, by the definition of the point at infinity in Equation $(20)$, it follows that

$P + \mathcal{O} = P$ .

By symmetry of the construction, we also have $\mathcal{O} + P = P$. Hence, $\mathcal{O}$ is the identity element.

(ii) From Equation (19), the $x$-coordinate of $P + Q$ is

$$x' = \frac{k+x_1x_2}{x_1+x_2}. \tag{23}$$

To determine the inverse of a point $P$, we consider the limit $x_2 \to -x_1$. In this case, the denominator in Equation (23) satisfies

$x_2 \to -x_1$ ,

while the numerator $k + x_1x_2$ remains finite. Hence, the value of $x'$ becomes unbounded, so the resulting point escapes to infinity.

$x_1 + x_2 \to 0$,

while the numerator $k + x_1x_2$ remains finite. Hence, the value of $x'$ becomes unbounded, and the resulting point escapes to infinity.

By Definition 4.3, this limiting position corresponds to the point at infinity $\mathcal{O}$. Therefore,

$P + (-P) = \mathcal{O}$

where $-P$ is defined by the condition $x_2 \to -x_1$. Thus, every point $P \in E$ admits an inverse element with respect to the defined operation. Moreover, this inverse is uniquely determined for each point on $E$.

Geometrically, this result is illustrated in Figure 7.

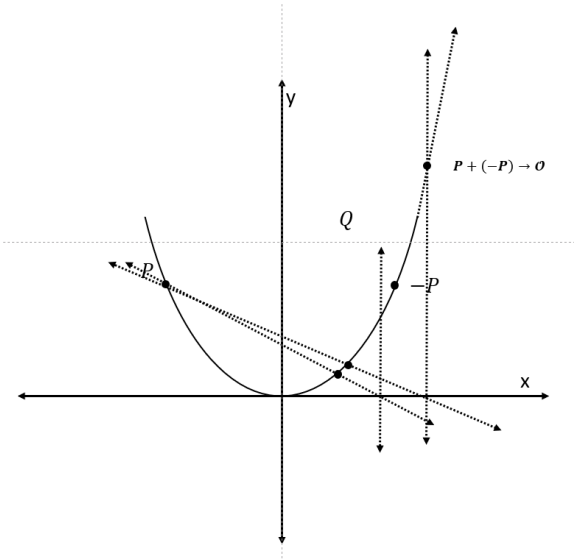


***Figure 7.*** *Geometric interpretation of the point at infinity on the quadratic curve $y = x^2$ obtained via the limiting process*

(iii) Let $P + Q = (x_4, y_4), (P + Q) + R = (x_5, y_5)$, From the addition formula Equation (19), we have

$x_4 = \frac{k+x_1x_2}{x_1+x_2}$.

Applying Equation $(19)$ again, we obtain

$$x_5 = \frac{k + x_4 x_3}{x_4 + x_3} = \frac{k(x_1 + x_2 + x_3) + x_1 x_2 x_3}{k + x_1 x_2 + x_2 x_3 + x_1 x_3}. \tag{24}$$

Similarly, define

$Q + R = (x_6, y_6), P + (Q + R) = (x_7, y_7)$.

Then

$x_6 = \frac{k + x_2 x_3}{x_2 + x_3}$.

And

$$x_7 = \frac{k + x_1 x_6}{x_1 + x_6} = \frac{k(x_1 + x_2 + x_3) + x_1 x_2 x_3}{k + x_1 x_2 + x_2 x_3 + x_1 x_3}. \tag{25}$$

Comparing Equation $(24)$ and Equation $(25)$, we obtain $x_5 = x_7$. Hence,

$(P + Q) + R = P + (Q + R)$.

Therefore, the addition operation on $E$ is associative.

(iv) From the explicit form of the addition formula, it is evident that interchanging $x_1$ and $x_2$ leaves the expression unchanged. Consequently, the order in which two points are added does not affect the result, and we have

$P + Q = Q + P$, for all $P, Q \in E$.

Furthermore, from Theorem 4.4, we have shown that all the group properties (identity, inverse, associativity, and commutativity) hold for the addition operation on $E$. Specifically, the commutative property and the existence of an identity element at infinity $\mathcal{O}$, along with inverses, confirm that the group structure defined in Definitions 4.2 and 4.3 forms an Abelian group on $E$.

Thus, we conclude that $E$ with the addition defined in Definition 4.1 and the point at infinity $\mathcal{O}$ defined in Definition 4.3 satisfies the conditions of an Abelian group.

## 5. RESULTS

Elliptic curve cryptography (ECC) derives its strength from the group law defined by point addition on elliptic curves over finite fields. The classical formulation of this law relies on the notion of the point at infinity as the identity element, which, although well established in algebraic geometry, may appear abstract from a geometric or applied perspective.

In this study, we revisited the algebraic and geometric role of the point at infinity and proposed an alternative interpretation in terms of the line at infinity. This formulation preserves the essential properties of the elliptic curve group law while providing a more intuitive and geometrically transparent representation of the identity element.

Building upon this reinterpretation, we introduced a novel point addition operation on the quadratic curve $y = x^2$. We rigorously established that this operation satisfies all axioms of an abelian group, including closure, associativity, commutativity, and the existence of identity and inverse elements. These results

demonstrate that the group-law framework is not inherently restricted to cubic curves and can be meaningfully extended to alternative algebraic settings.

The proposed approach contributes to the theoretical understanding of algebraic curve structures and highlights the potential for constructing group laws in non-elliptic contexts. This perspective may serve as a foundation for future investigations into generalized curve-based algebraic systems.

Although the introduced group structure is primarily theoretical, it raises important questions regarding its potential applicability in cryptographic settings, particularly in relation to the Discrete Logarithm Problem. Determining whether the corresponding problem on this structure exhibits sufficient computational hardness remains an open problem and constitutes a promising direction for future research. Moreover, exploring possible connections between such alternative group structures and emerging cryptographic paradigms may further expand the scope of curve-based cryptography beyond classical Elliptic Curve Cryptography.

## DECLARATION OF ARTIFICIAL INTELLIGENCE (AI) USE

When drafting the manuscript, neither generative AI agents nor large language models (LLMs) were used in any aspect of the study

## CONFLICT OF INTEREST

No conflict of interest was declared by the authors.

## REFERENCES

[1] Silverman, J.H., "The arithmetic of elliptic curves", Graduate Texts In Mathematics, Vol. 106, Springer, New York, (2009). DOI: https://doi.org/10.1007/978-0-387-09494-6

[2] Diffie, W., and Hellman, M.E., "New directions in cryptography", IEEE Transactions on Information Theory, 22(6): 644-654, (1976). DOI: https://doi.org/10.1109/TIT.1976.1055638

[3] Rivest, R.L., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2): 120-126, (1978). DOI: https://doi.org/10.1145/359340.359342

[4] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, 31(4): 469-472, (1985). DOI: https://doi.org/10.1109/TIT.1985.1057074

[5] Schnorr, C.-P., "Efficient identification and signatures for smart cards", Advances In Cryptology-CRYPTO '89, Lecture Notes in Computer Science, Vol. 435, Springer, Berlin, 239-252, (1990). DOI: https://doi.org/10.1007/0-387-34805-0_22

[6] Okumuş, İ., and Çelik, E., "A modified key generation algorithm to rebalanced-RSA and RPower-RSA", Manas Journal of Engineering, 12(2): 192-197, (2024). DOI: https://doi.org/10.51354/mjen.1524490

[7] Yerlikaya, T., and Aslanyürek, C., "RSA algoritmasının şifreleme hızını arttıran algoritmalar ve performansları", Düzce Üniversitesi Mühendislik Fakültesi Bilim ve Teknoloji Dergisi, 10(3): 853-862, (2019). DOI: https://doi.org/10.24012/dumf.559789

[8] Miller, V.S., "Use of elliptic curves in cryptography", Advances In Cryptology-CRYPTO '85, Lecture Notes In Computer Science, Vol. 218, Springer, Berlin, 417-426, (1986). DOI: https://doi.org/10.1007/3-540-39799-X_31

[9] Koblitz, N., "Elliptic curve cryptosystems", Mathematics of Computation, 48(177): 203-209, (1987). DOI: https://doi.org/10.1090/S0025-5718-1987-0866109-5

[10] Lahraoui, Y., Lazaar, S., Amal, Y., and Nitaj, A., "Securing data exchange with elliptic curve cryptography: a novel hash-based method for message mapping and integrity assurance", Cryptography, 8(2): 23, (2024). DOI: https://doi.org/10.3390/cryptography8020023

[11] Johnson, D., Menezes, A., and Vanstone, S., "The elliptic curve digital signature algorithm (ECDSA)", International Journal of Information Security, 1(1): 36-63, (2001). DOI: https://doi.org/10.1007/s102070100002

[12] National Institute of Standards and Technology (NIST), "Digital signature standard (DSS)", FIPS PUB 186, NIST, Gaithersburg, MD. https://csrc.nist.gov/pubs/fips/186/final

[13] National Institute of Standards and Technology (NIST), "Digital signature standard (DSS)", FIPS PUB 186-2, NIST, Gaithersburg, MD, (2000). https://csrc.nist.gov/files/pubs/fips/186-2/final/docs/fips186-2.pdf

[14] Edwards, H.M., "A normal form for elliptic curves", Bulletin of the American Mathematical Society, 44(3): 393-422, (2007). DOI: https://doi.org/10.1090/S0273-0979-07-01153-6

[15] Bernstein, D.J., Birkner, P., Lange, T., and Peters, C., "Twisted Edwards curves", Progress In Cryptology-AFRICACRYPT 2008, Lecture Notes in Computer Science, Vol. 5023, Springer, Berlin, 389-405, (2008). DOI: https://doi.org/10.1007/978-3-540-68164-9_26

[16] National Institute of Standards and Technology (NIST), "Digital signature standard (DSS)", FIPS PUB 186-5, NIST, Gaithersburg, MD, (2023). https://csrc.nist.gov/pubs/fips/186-5/final

[17] Sai Tejaswini, T., and Kameswari, P.A., "Arithmetic of points on elliptic curve over p-adic field in projective coordinates", Mathematics and Statistics, 14(1): 73-90, (2026). DOI: https://doi.org/10.13189/ms.2026.140107

[18] Kurt Pehlivanoğlu, M., and Yerlikaya, T., "A new modified cryptosystem based on Menezes–Vanstone elliptic curve cryptography algorithm that uses characters' hexadecimal values", Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on, IEEE, (2013). DOI: https://doi.org/10.1109/TAEECE.2013.6557316

[19] Yerlikaya, T., Buluş, E., and Buluş, N., "Arithmetic of elliptic curves and use in cryptography", IEEE SIU 2006, (2006). DOI: https://doi.org/10.1109/SIU.2006.1659692

[20] Karataş, İ., and Bayraklı, S., "Using elliptic curve cryptography for authentication and key exchange in constrained internet of things networks", İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 23(45): 114-132, (2024). DOI: https://doi.org/10.55071/ticaretfbd.1439890

[21] Hasse, H., "Zur Theorie der abstrakten elliptischen Funktionenkörper I", Journal Für Die Reine Und Angewandte Mathematik, 175: 55-62, (1936). DOI: https://doi.org/10.1515/crll.1936.175.55

[22] Artin, E., "Quadratische Körper im Gebiete der höheren Kongruenzen I", Mathematische Zeitschrift, 19(1): 153-206, (1924). DOI: https://doi.org/10.1007/BF01181073