

Arithmetic of Points on Elliptic Curve $E(\mathbb{Q}_p)$ over p -adic Field \mathbb{Q}_p modulo p^2 in Projective Coordinates

T. Sai Tejaswini, P. Anuradha Kameswari*

Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India

Received October 8, 2025; Revised January 8, 2026; Accepted January 20, 2026

Cite This Paper in the Following Citation Styles

(a): [1] T. Sai Tejaswini, P. Anuradha Kameswari, "Arithmetic of Points on Elliptic Curve $E(\mathbb{Q}_p)$ over p -adic Field \mathbb{Q}_p modulo p^2 in Projective Coordinates," *Mathematics and Statistics*, Vol.14, No.1, pp. 73-90, 2026. DOI: 10.13189/ms.2026.140107.

(b): T. Sai Tejaswini, P. Anuradha Kameswari (2026). Arithmetic of Points on Elliptic Curve $E(\mathbb{Q}_p)$ over p -adic Field \mathbb{Q}_p modulo p^2 in Projective Coordinates. *Mathematics and Statistics*, 14(1), 73-90. DOI: 10.13189/ms.2026.140107.

Copyright ©2026 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract Elliptic Curve Cryptosystems (ECC) have emerged as a powerful alternative to traditional public-key cryptosystems, offering equivalent security with significantly smaller key sizes. The efficiency of ECC, in terms of minimizing encryption time and enhancing computational performance, is strongly influenced by the number of point addition and doubling computations required in elliptic curve arithmetic. In this context, the study of arithmetic of points in elliptic curves plays a crucial role. This study emphasizes computations in projective coordinates of points on elliptic curves defined over the p -adic field \mathbb{Q}_p . A comparative study shows that arithmetic in projective coordinates reduces the number of operations required, thereby enhancing the efficiency relative to the affine coordinate system. The coordinate-level p -adic expansions of the arithmetic may be obtained by employing p -adic expansion techniques to the arithmetic of points on the elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^n)$ in projective coordinates for $n = 2, 3, \dots$. In this paper, coordinate-level p -adic expansions of the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ in projective coordinates are formulated, an algorithm for the computations is given illustrating the step-by-step process for computing point addition and doubling in $E(\mathbb{Q}_p)(\text{mod } p^2)$ and its efficiency over the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ in affine coordinates is described. This provides a systematic framework for performing elliptic curve arithmetic efficiently.

Keywords Elliptic Curve in Projective Coordinates, Arithmetic of Points in Projective Coordinates

1 Introduction

The origins of Elliptic Curve Cryptography (ECC) are deeply rooted in the development of elliptic curve theory. The general form of an elliptic curve over a field \mathbb{K} is given as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (*)$$

These curves in the case of the characteristic $\neq 2, 3$ are represented by the Weierstrass equation given as $y^2 = x^3 + Ax + B$. These curves on the real number field \mathbb{R} exhibit a rich algebraic structure, allowing a group law. This group property is purely theoretical initially, but later becomes the key to cryptographic applications.

In 1985, Victor S. Miller at IBM and Neal Koblitz at the University of Washington proposed the use of elliptic curves for cryptographic purposes [1], using the group of points on an elliptic curve over a finite field that provides comparable security with significantly smaller key sizes. Based on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), it is computationally more difficult than the traditional discrete logarithm problem used in earlier schemes. Researchers began exploring the computational aspects of elliptic curves in finite fields, leading to algorithms for point addition, scalar multiplication, and discrete logarithms in these structures. These discoveries revealed that elliptic curves could form the foundation for Elliptic curve cryptosystems (ECC).

In theory, elliptic curve cryptography is secure. In practice, ECC security depends on parameters such as the size of the underlying elliptic curve and the length of the ECC key. ECC requires a shorter key length to achieve the same level of security as in RSA cryptosystems. A 256-bit elliptic curve cryptography key with elliptic curve $E(\mathbb{F}_p)$ over finite field \mathbb{F}_p [2] is equivalent to a 3072-bit RSA key over \mathbb{F}_p in terms of security strength. In other words, using a smaller key in ECC can provide the same level of security as using a larger key in RSA. Since the key size is smaller, ECC also consumes less computational power.

In the context of improving the efficiency of cryptosystems with elliptic curves, the study of elliptic curves $E(\mathbb{Q}_p)$ over p -adic number field \mathbb{Q}_p was consequential. The elliptic curve $E(\mathbb{Q}_p)$ over p -adic field \mathbb{Q}_p provides a large key space for cryptosystems. This study emphasizes computations with projective coordinates of points on elliptic curves defined over the p -adic field \mathbb{Q}_p . A comparative study of computations with projective coordinates and affine coordinates is demonstrated which shows that arithmetic in projective coordinates outperforms significantly by reducing the number of operations required, thereby enhancing the efficiency relative to the affine coordinate system. In section V, a comparative study on the efficiency of arithmetic of points on $E(\mathbb{F}_p)$ in affine and projective coordinates is given. In section VI, the arithmetic of points on an elliptic curve over p -adic field \mathbb{Q}_p in projective coordinates is studied. In section VII, a comparative study on the efficiency of arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ in affine and projective coordinates is described. In section VIII, the conclusions of the paper are described.

2 Theoretical Background

The efficiency of ECC mainly depends on the addition and doubling of points on an elliptic curve, and the improvement in the sense to reduce time for encryption and increase the time for decryption will be achieved by reducing the number of point additions and doublings, which deeply depends on the use of an appropriate coordinate system. Further, it is observed that the arithmetic of points on elliptic curve $E(\mathbb{F}_p)$ over a finite field \mathbb{F}_p [3] in projective coordinates is more efficient than with respect to the affine coordinate system [4],[5],[6]. Contemplating this for the elliptic curve $E(\mathbb{Q}_p)$ over p -adic field \mathbb{Q}_p [7], the study of the arithmetic of points in $E(\mathbb{Q}_p)$ in projective coordinates is important. In the arithmetic of points on $E(\mathbb{Q}_p)$ in affine coordinates, the coordinate-level p -adic expansion of points [8],[9],[10],[11] is obtained in stepwise: first by implementing arithmetic of points on elliptic curve $E(\mathbb{F}_p)$, then implementing arithmetic of points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$, and subsequently on the arithmetic of points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^3)$ over p -adic field \mathbb{Q}_p , and so on. In this context, the study of the arithmetic of points on elliptic curve $E(\mathbb{Q}_p)$ over the p -adic field \mathbb{Q}_p modulo p^n is therefore of critical significance.

In the study of arithmetic of points on $E(\mathbb{Q}_p)$ with projective coordinates, the coordinate-level p -adic expansions of the arithmetic can be obtained by employing p -adic expansion techniques to the arithmetic of points on the elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^n)$ in projective coordinates for $n = 2, 3, \dots$

Now, to study the arithmetic of points on the elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^n)$ in projective coordinates, we obtain the points on the elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^n)$ in projective coordinates by a process of lifting points of $E(\mathbb{Q}_p)(\text{mod } p^{n-1})$ in affine coordinates and then obtain the corresponding projective points. In particular note, the set of all points on the elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^n)$ is precisely the elliptic curve $E(\mathbb{F}_p)$ over finite field \mathbb{F}_p ; for $n = 1$, the points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic field \mathbb{Q}_p are obtained by lifting the points on elliptic curve $E(\mathbb{F}_p)$ and the points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^3)$ are obtained by lifting the points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$, and so on. In paper [4], the study of the lifts of points on $E(\mathbb{Q}_p)(\text{mod } p^n)$ in affine coordinates to points on $E(\mathbb{Q}_p)(\text{mod } p^{n+1})$ for all n is described with illustrations on the points on the elliptic curve $y^2 = x^3 + x + 1$ on $E(\mathbb{Q}_5)(\text{mod } 5^2)$.

A graph representing the lifts of the points from $E(\mathbb{F}_5)$ in affine coordinates to $E(\mathbb{Q}_5)(\text{mod } 5^2)$ for points in affine coordinates for the elliptic curve $y^2 = x^3 + x + 1$ is given in Figure 1.

3 Objectives

The objective of this study is to develop an efficient computation technique for point addition and doubling on elliptic curves defined over the p -adic field \mathbb{Q}_p in projective coordinates, specifically under modulo p^2 , using coordinate-level arithmetic for cryptographic applications and to compare the efficiency of arithmetic of points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic number field \mathbb{Q}_p in both affine and projective coordinate systems to identify computational efficiency for cryptographic applications.

4 Contribution of the Study

The study of the efficiency of arithmetic of points on elliptic curve $E(\mathbb{F}_p)$ over finite field \mathbb{F}_p is extended to analyze the efficiency of arithmetic of points on elliptic curve $E(\mathbb{Q}_p)$ over p -adic number field \mathbb{Q}_p defined over \mathbb{Z}_p with projective coordinates. The paper [7] contributes to the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic number field \mathbb{Q}_p defined over \mathbb{Z}_p in affine coordinates and also in finding the lifts of points in $E(\mathbb{F}_p)$ to points in $E(\mathbb{Q}_p)(\text{mod } p^2)$ in affine coordinates. In this paper, we proceed to describe arithmetic of points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic number field \mathbb{Q}_p defined over

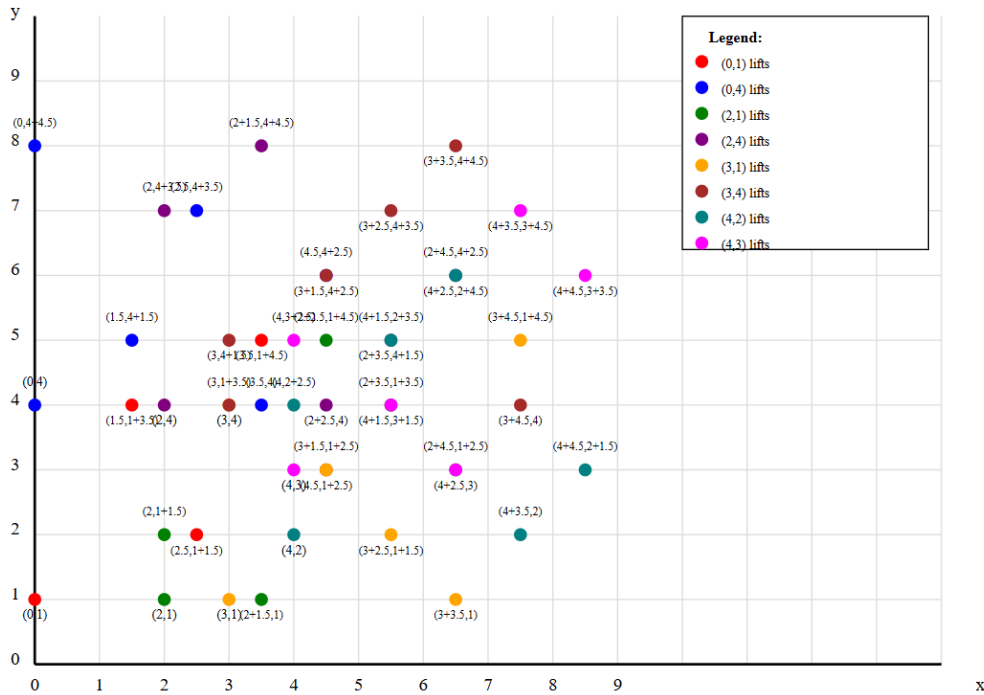


Figure 1. Points on the curve $E(\mathbb{Q}_5) : y^2 = x^3 + x + 1 \pmod{5^2}$ defined over \mathbb{Z}_5

\mathbb{Z}_p in projective coordinates by implementing the arithmetic of points on $E(\mathbb{Q}_p)$ and making a comparative study to ensure its efficiency.

5 Efficiency of Arithmetic of Points on $E(\mathbb{F}_p)$ in Affine and Projective Coordinates

The study of the efficiency of arithmetic of points on elliptic curve $E(\mathbb{F}_p)$ over finite field \mathbb{F}_p is based on the evaluation of point addition and point doubling with the formulas in [6]. The point addition in affine coordinates involves 3 multiplications, 6 subtractions, 1 squaring, and 1 field inversion. From [7], point addition in projective coordinates involves 20 multiplications, 3 additions, 7 subtractions, 4 squaring, and 0 field inversions. Hence, the arithmetic of points in projective coordinates is more efficient as inversion is quite costly with 1 inversion approximately equal to 266 multiplications. The corresponding comparative study is described in Table 1 and Figure 2 provides a clear depiction of the number of operations for point addition in affine and projective coordinates on an elliptic curve $E(\mathbb{F}_p)$ over a finite field \mathbb{F}_p in terms of the number of multiplications, the number of additions or subtractions, and the number of squaring.

Table 1. Number of operations for point addition in Affine coordinate system in $E(\mathbb{F}_p)$

Description	No. of Multiplications	No. of Additions	No. of Subtractions	No. of Squarings	No. of Inversions
Point Addition	3	0	6	1	1
Point Doubling	3	5	3	2	1

The point doubling in affine coordinates involves 3 multiplications, 5 additions, 3 subtractions, 2 squarings, and 1 field inversion. From [7], point doubling in projective coordinates involves 12 multiplications, 36 additions, 3 subtractions, 7 squarings, and 0 field inversions. The corresponding comparative study is described in Table 2 and Figure 3 provides a clear depiction of the number of operations for point doubling in affine and projective coordinates on an elliptic curve $E(\mathbb{F}_p)$ over a finite field \mathbb{F}_p in terms of number of multiplications and number of additions or subtractions and number of squaring and the time taken for these operations are in the order:

$$Time (Multiplication) > Time (Squaring) > Time (Addition/ Subtraction)$$

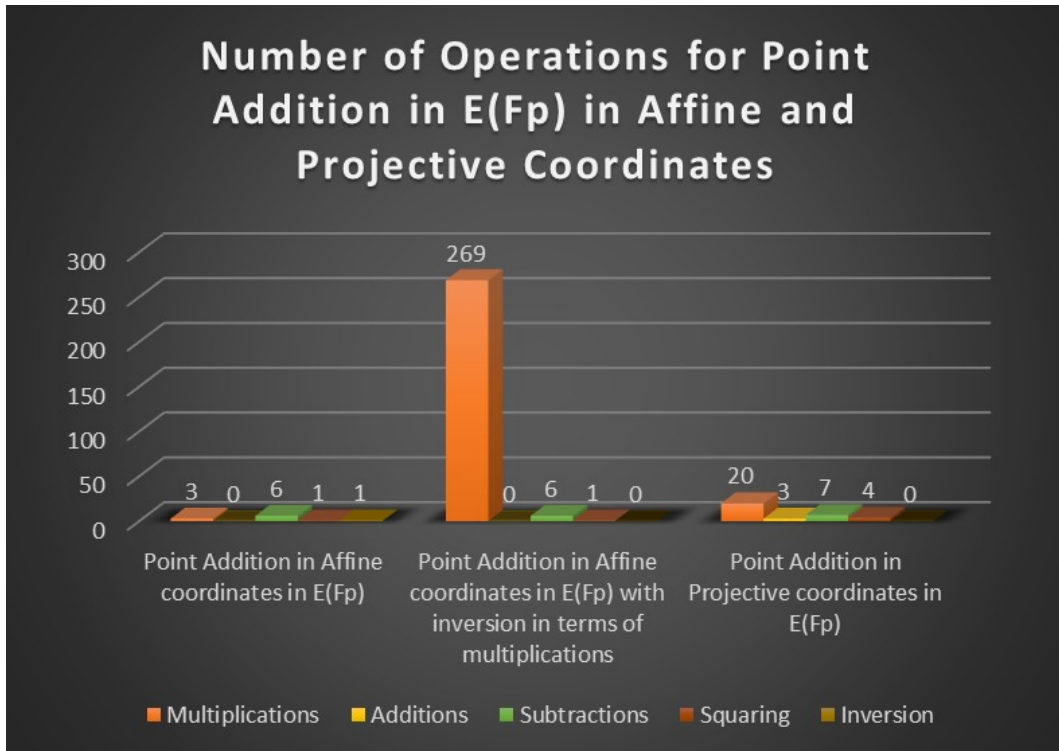


Figure 2. Number of operations of Point Addition in Affine and Projective coordinates in $E(\mathbb{F}_p)$

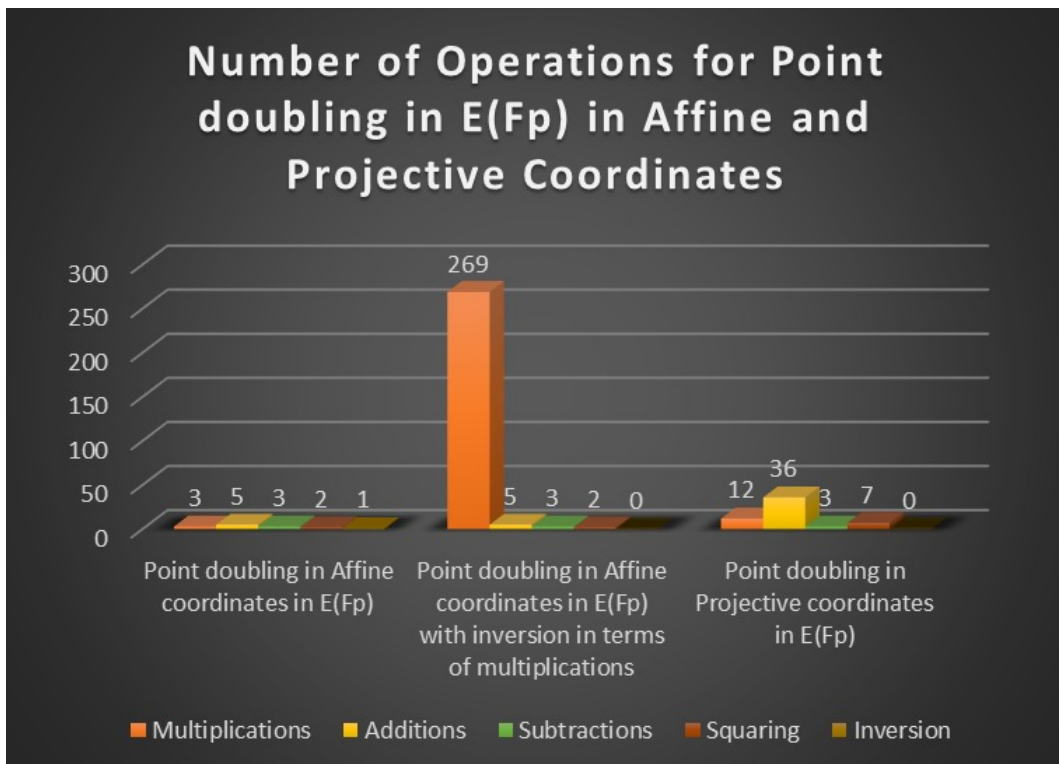


Figure 3. Number of operations of Point doubling in Affine and Projective coordinates in $E(\mathbb{F}_p)$

Table 2. Number of operations for Point doubling in Affine coordinate system in $E(\mathbb{F}_p)$

Description	No. of Multiplications	No. of Additions	No. of Subtractions	No. of Squarings	No. of Inversions
Point Addition	20	3	7	4	0
Point Doubling	12	36	3	7	0

This study of the efficiency of arithmetic of points on elliptic curve $E(\mathbb{F}_p)$ over a finite field \mathbb{F}_p from [13],[14] suggests an improvement in arithmetic of points on elliptic curve over p -adic number field \mathbb{Q}_p defined over \mathbb{Z}_p with projective coordinates. In [7], the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic number field \mathbb{Q}_p defined over \mathbb{Z}_p in affine coordinates is described. In this paper, we proceed to describe arithmetic of points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic number field \mathbb{Q}_p defined over \mathbb{Z}_p in projective coordinates. In the following section, we implement the arithmetic of points on $E(\mathbb{Q}_p)$ to points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic field \mathbb{Q}_p defined over \mathbb{Z}_p in projective coordinates.

6 Arithmetic of Points on Elliptic Curve $E(\mathbb{Q}_p)$ over p -adic Field \mathbb{Q}_p in Projective Coordinates

Contemplating the efficiency of arithmetic of points on $E(\mathbb{Q}_p)$ and comparing it with the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ in projective coordinates, this section analyzes the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ and presents the corresponding coordinate formulas. To study the arithmetic of points on an elliptic curve $E(\mathbb{Q}_p)$ over the p -adic field \mathbb{Q}_p in projective coordinates, we first consider the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ by reducing the arithmetic of points on $E(\mathbb{Q}_p)$ modulo p^2 . Likewise, the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^3)$ in projective coordinates is obtained by reducing the arithmetic of points on $E(\mathbb{Q}_p)$ modulo p^3 , and so on. The addition of points on the elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ in the affine coordinate system is analyzed in [7].

In [12],[15], the arithmetic of two points $P_1 = [X_1 : Y_1 : Z_1]$ and $P_2 = [X_2 : Y_2 : Z_2]$ on an elliptic curve $Y^2Z = X^3 + AXZ^2 + BZ^3$ over a field K denoted by $P_3 = P_1 + P_2 = [X_3 : Y_3 : Z_3]$ and is given as

For $P_1 \neq \pm P_2$,

$$\begin{cases} X_3 = (X_2Z_1 - X_1Z_2) \cdot (Y_2Z_1 - Y_1Z_2)^2 Z_1Z_2 - (X_2Z_1 - X_1Z_2)^4 - 2(X_2Z_1 - X_1Z_2)^3 X_1Z_2 \\ Y_3 = (Y_2Z_1 - Y_1Z_2) \cdot \left\{ (X_2Z_1 - X_1Z_2)^2 X_1Z_2 - (Y_2Z_1 - Y_1Z_2)^2 Z_1Z_2 + (X_2Z_1 - X_1Z_2)^3 + 2(X_2Z_1 - X_1Z_2)^2 X_1Z_2 \right\} \\ \quad - (X_2Z_1 - X_1Z_2)^3 Y_1Z_2 \\ Z_3 = (X_2Z_1 - X_1Z_2)^3 Z_1Z_2 \end{cases} \tag{1}$$

For $P_1 = P_2$,

$$\begin{cases} X_3 = 2Y_1Z_1 \left\{ (AZ_1^2 + 3X_1^2)^2 - 8X_1Y_1^2Z_1 \right\} \\ Y_3 = (AZ_1^2 + 3X_1^2) \left\{ 4X_1Y_1^2Z_1 - (AZ_1^2 + 3X_1^2)^2 + 8X_1Y_1^2Z_1 \right\} - 8Y_1^4Z_1^2 \\ Z_3 = 8Y_1^3Z_1^3 \end{cases} \tag{2}$$

If $P_1 = -P_2$, then $P_1 + P_2 = \mathcal{O}$

Now, for $K = \mathbb{Q}_p$, the p -adic field, we have for an elliptic curve E over \mathbb{Q}_p defined over \mathbb{Z}_p , the points \tilde{P}_1 and \tilde{P}_2 in projective coordinates are given as $\tilde{P}_1 = [\tilde{X}_1 : \tilde{Y}_1 : \tilde{Z}_1]$ and $\tilde{P}_2 = [\tilde{X}_2 : \tilde{Y}_2 : \tilde{Z}_2]$ where

$$\tilde{X}_1 = X_{10} + X_{11}p + X_{12}p^2 + \dots$$

$$\tilde{Y}_1 = Y_{10} + Y_{11}p + Y_{12}p^2 + \dots$$

$$\tilde{Z}_1 = Z_{10} + Z_{11}p + Z_{12}p^2 + \dots$$

and

$$\tilde{X}_2 = X_{20} + X_{21}p + X_{22}p^2 + \dots$$

$$\tilde{Y}_2 = Y_{20} + Y_{21}p + Y_{22}p^2 + \dots$$

$$\tilde{Z}_2 = Z_{20} + Z_{21}p + Z_{22}p^2 + \dots$$

with each coordinate in its p -adic expansion and by the point addition in $E(\mathbb{Q}_p)$ in projective coordinates, we have $\tilde{P}_1 + \tilde{P}_2 = \tilde{P}_3$ say with $\tilde{P}_3 = [\tilde{X}_3 : \tilde{Y}_3 : \tilde{Z}_3]$ with each coordinate given as

$$\tilde{X}_3 = X_{30} + X_{31}p + X_{32}p^2 + \dots$$

$$\tilde{Y}_3 = Y_{30} + Y_{31}p + Y_{32}p^2 + \dots$$

$$\tilde{Z}_3 = Z_{30} + Z_{31}p + Z_{32}p^2 + \dots$$

The point \tilde{P}_3 could be known with the evaluation of X_{3n} 's, Y_{3n} 's and Z_{3n} 's for all $n = 0, 1, 2, \dots$ by implementing the arithmetic of points \tilde{P}_1 and \tilde{P}_2 in $E(\mathbb{Q}_p)$ to the points \tilde{P}_{1n} and \tilde{P}_{2n} in $E(\mathbb{Q}_p)(\text{mod } p^{n+1})$ for all $n = 1, 2, \dots$, where the points \tilde{P}_{1n} and \tilde{P}_{2n} are the points obtained by considering \tilde{P}_1 and \tilde{P}_2 modulo p^{n+1} . Now note for any point \tilde{P}_1 in $E(\mathbb{Q}_p)$ in projective coordinates with the coordinate level p -adic expansion is given as

$$\tilde{P}_1 = [\tilde{X}_1 : \tilde{Y}_1 : \tilde{Z}_1] = [X_{10} + X_{11}p + X_{12}p^2 + \dots : Y_{10} + Y_{11}p + Y_{12}p^2 + \dots : Z_{10} + Z_{11}p + Z_{12}p^2 + \dots]$$

we denote the point \tilde{P}_1 modulo p^{n+1} as \tilde{P}_{1n} for all $n = 1, 2, \dots$. In particular, the coordinate level p -adic expansion of \tilde{P}_{1n} for $n = 2$ in projective coordinates is given as

$$\tilde{P}_{11} = [\tilde{X}_{11} : \tilde{Y}_{11} : \tilde{Z}_{11}] = [X_{10} + X_{11}p : Y_{10} + Y_{11}p : Z_{10} + Z_{11}p]$$

In the following theorem we formulate the coordinate level p -adic expansion of the arithmetic of points on $E(\mathbb{Q}_p)(\text{mod } p^2)$.

Theorem 1. *Let $E(\mathbb{Q}_p)$ be an elliptic curve over p -adic number field \mathbb{Q}_p defined on \mathbb{Z}_p given as*

$$E(\mathbb{Q}_p) : Y^2Z = X^3 + AXZ^2 + BZ^3$$

then for any points \tilde{P}_1 and \tilde{P}_2 on an elliptic curve $E(\mathbb{Q}_p)$ in projective coordinates, the arithmetic of the points \tilde{P}_{11} and \tilde{P}_{21} in $E(\mathbb{Q}_p)(\text{mod } p^2)$ where $\tilde{P}_{11} = [\tilde{X}_{11} : \tilde{Y}_{11} : \tilde{Z}_{11}] = [X_{10} + X_{11}p : Y_{10} + Y_{11}p : Z_{10} + Z_{11}p]$ and $\tilde{P}_{21} = [\tilde{X}_{21} : \tilde{Y}_{21} : \tilde{Z}_{21}] = [X_{20} + X_{21}p : Y_{20} + Y_{21}p : Z_{20} + Z_{21}p]$ is obtained by implementing the arithmetic of points \tilde{P}_1 and \tilde{P}_2 on elliptic curve $E(\mathbb{Q}_p)$ to the points \tilde{P}_{11} and \tilde{P}_{21} on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ and $\tilde{P}_{11} + \tilde{P}_{21} = \tilde{P}_{31}$ is given as

$$\tilde{P}_{31} = [\tilde{X}_{31} : \tilde{Y}_{31} : \tilde{Z}_{31}] = [X_{30} + X_{31}p : Y_{30} + Y_{31}p : Z_{30} + Z_{31}p]$$

and the p -adic expansions $X_{30} + X_{31}p$, $Y_{30} + Y_{31}p$, $Z_{30} + Z_{31}p$ are expressed in terms of $X_{10}, X_{11}, Y_{10}, Y_{11}, Z_{10}, Z_{11}, X_{20}, X_{21}, Y_{20}, Y_{21}, Z_{20}, Z_{21}$.

Proof. Consider

$$\tilde{P}_{11} = [\tilde{X}_{11} : \tilde{Y}_{11} : \tilde{Z}_{11}] = [X_{10} + X_{11}p : Y_{10} + Y_{11}p : Z_{10} + Z_{11}p]$$

and

$$\tilde{P}_{21} = [\tilde{X}_{21} : \tilde{Y}_{21} : \tilde{Z}_{21}] = [X_{20} + X_{21}p : Y_{20} + Y_{21}p : Z_{20} + Z_{21}p]$$

By the implementation of the arithmetic of points \tilde{P}_1, \tilde{P}_2 in $E(\mathbb{Q}_p)$ in projective coordinates as in (1) to points $\tilde{P}_{11}, \tilde{P}_{21}$ in $E(\mathbb{Q}_p)(\text{mod } p^2)$, we have

$$\tilde{X}_{31} \equiv \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right) \cdot \left(\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21} \right)^2 \tilde{Z}_{11}\tilde{Z}_{21} - \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^4 - 2 \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^3 \tilde{X}_{11}\tilde{Z}_{21} \pmod{p^2}$$

$$\tilde{Y}_{31} \equiv \left(\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21} \right) \cdot \left\{ \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^2 \tilde{X}_{11}\tilde{Z}_{21} - \left(\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21} \right)^2 \tilde{Z}_{11}\tilde{Z}_{21} \right.$$

$$\left. + \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^3 + 2 \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^2 \tilde{X}_{11}\tilde{Z}_{21} \right\} - \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^3 \tilde{Y}_{11}\tilde{Z}_{21} \pmod{p^2}$$

$$\tilde{Z}_{31} \equiv \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^3 \cdot \tilde{Z}_{11}\tilde{Z}_{21} \pmod{p^2}$$

First, note the following expansions that are required to evaluate $\tilde{X}_{31}, \tilde{Y}_{31}, \tilde{Z}_{31}$

Upon reducing each expansion to modulo p^2 , we have

$$\begin{aligned} \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right) &\equiv \left(X_{20} + X_{21}p \right) \cdot \left(Z_{10} + Z_{11}p \right) + \left((p-1) + (p-1)p \right) \cdot \left(X_{10} + X_{11}p \right) \cdot \left(Z_{20} + Z_{21}p \right) \\ &\equiv \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) + \left\{ X_{20}Z_{11} + X_{21}Z_{10} + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right\} p \pmod{p^2} \quad (3) \end{aligned}$$

$$\Rightarrow (\tilde{X}_{21}\tilde{Z}_{11}-\tilde{X}_{11}\tilde{Z}_{21})^2 \equiv (X_{20}Z_{10}+(p-1)X_{10}Z_{20})^2 + 2(X_{20}Z_{10}+(p-1)X_{10}Z_{20}) \cdot \left\{ X_{20}Z_{11} + X_{21}Z_{10} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}) \right\} p \pmod{p^2} \tag{4}$$

$$\Rightarrow (\tilde{X}_{21}\tilde{Z}_{11}-\tilde{X}_{11}\tilde{Z}_{21})^3 = \left(X_{20}Z_{10}+(p-1)X_{10}Z_{20} + \left[X_{20}Z_{11} + X_{21}Z_{10} + (p-1)\{X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}\} \right] p \right)^3 \\ \equiv (X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 + 3(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^2 \cdot (X_{20}Z_{11} + X_{21}Z_{10} + (p-1)\{X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}\}) p \pmod{p^2} \tag{5}$$

$$\Rightarrow (\tilde{X}_{21}\tilde{Z}_{11}-\tilde{X}_{11}\tilde{Z}_{21})^4 = \left(X_{20}Z_{10}+(p-1)X_{10}Z_{20} + \left\{ X_{20}Z_{11} + X_{21}Z_{10} + (p-1)\{X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}\} \right\} p \right)^4 \\ \equiv (X_{20}Z_{10} + (p-1)X_{10}Z_{20})^4 + 4(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 \cdot (X_{20}Z_{11} + X_{21}Z_{10} + (p-1)\{X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}\}) p \pmod{p^2} \tag{6}$$

Similarly, we have

$$\Rightarrow (\tilde{Y}_{21}\tilde{Z}_{11}-\tilde{Y}_{11}\tilde{Z}_{21}) \equiv (Y_{20}Z_{10}+(p-1)Y_{10}Z_{20}) + (Y_{20}Z_{11}+Y_{21}Z_{10}+(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}) p \pmod{p^2} \tag{7}$$

$$\Rightarrow (\tilde{Y}_{21}\tilde{Z}_{11}-\tilde{Y}_{11}\tilde{Z}_{21})^2 \equiv (Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^2 + 2(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20}) \cdot \left(Y_{20}Z_{11} + Y_{21}Z_{10} + (p-1)\{Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20}\} \right) p \pmod{p^2} \tag{8}$$

$$\Rightarrow (\tilde{Y}_{21}\tilde{Z}_{11}-\tilde{Y}_{11}\tilde{Z}_{21})^3 \equiv (Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^3 + 3(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^2 \cdot (Y_{20}Z_{11} + Y_{21}Z_{10} + (p-1)\{Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20}\}) p \pmod{p^2} \tag{9}$$

$$\Rightarrow (\tilde{Y}_{21}\tilde{Z}_{11}-2\tilde{Y}_{11}\tilde{Z}_{21}) \equiv (Y_{20}Z_{10}+2(p-1)Y_{10}Z_{20}) + (Y_{20}Z_{11}+Y_{21}Z_{10}+2(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}) p \pmod{p^2} \tag{10}$$

For

$$\tilde{X}_{31} \equiv (\tilde{X}_{21}\tilde{Z}_{11}-\tilde{X}_{11}\tilde{Z}_{21}) \cdot (\tilde{Y}_{21}\tilde{Z}_{11}-\tilde{Y}_{11}\tilde{Z}_{21})^2 \tilde{Z}_{11}\tilde{Z}_{21} - (\tilde{X}_{21}\tilde{Z}_{11}-\tilde{X}_{11}\tilde{Z}_{21})^4 - 2(\tilde{X}_{21}\tilde{Z}_{11}-\tilde{X}_{11}\tilde{Z}_{21})^3 \tilde{X}_{11}\tilde{Z}_{21} \pmod{p^2}$$

On substituting (2),(5),(6) and (7) expansions modulo p^2 in the formula of \tilde{X}_{31} , we have

$$\Rightarrow \tilde{X}_{31} \equiv \left((Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^2 + 2(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20}) \cdot [Y_{20}Z_{11}+Y_{21}Z_{10}+(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}] p \right) \cdot \left(X_{20}Z_{10}+(p-1)X_{10}Z_{20} + [X_{20}Z_{11} + X_{21}Z_{10} + (p-1)\{X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}\}] p \right) \cdot (Z_{10}Z_{20} + \{Z_{11}Z_{20} + Z_{10}Z_{21}\} p) + ((p-1)+(p-1)p) \cdot \left((X_{20}Z_{10}+(p-1)X_{10}Z_{20})^4 + 4(X_{20}Z_{10}+(p-1)X_{10}Z_{20})^3 \cdot [X_{20}Z_{11}+X_{21}Z_{10}+(p-1)\{X_{10}Z_{20}+X_{10}Z_{21}+X_{11}Z_{20}\}] p + 2((p-1)+(p-1)p) \cdot \left((X_{20}Z_{10}+(p-1)X_{10}Z_{20})^3 + 3(X_{20}Z_{10}+(p-1)X_{10}Z_{20})^2 \cdot \right. \right.$$

$$\left[X_{20}Z_{11} + X_{21}Z_{10} + (p-1)\{X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20}\} \right] p \cdot \left(X_{10}Z_{20} + \{X_{11}Z_{20} + X_{10}Z_{21}\} p \right) \pmod{p^2}$$

Then the p -adic expansion of \tilde{X}_{31} is given as

$$\begin{aligned} \tilde{X}_{31} &\equiv Z_{10}Z_{20}(X_{20}Z_{10} + (p-1)X_{10}Z_{20}) \cdot (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20})^2 + (p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^4 + 2(p-1) \\ &\quad (X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 X_{10}Z_{20} + \left[2(X_{20}Z_{10} + (p-1)X_{10}Z_{20}) \cdot (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20}) \cdot \{Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1) \right. \\ &\quad \left. (Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20})\} Z_{10}Z_{20} + (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20})^2 \cdot \{X_{21}Z_{10} + X_{20}Z_{11} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20})\} \right. \\ &\quad \left. Z_{10}Z_{20} + (Z_{11}Z_{20} + Z_{10}Z_{21}) \cdot (X_{20}Z_{10} + (p-1)X_{10}Z_{20}) \cdot (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20})^2 + 4(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 \cdot \right. \\ &\quad \left. \{X_{21}Z_{10} + X_{20}Z_{11} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20})\} + (p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^4 + 6(p-1)(X_{20}Z_{10} \right. \\ &\quad \left. + (p-1)X_{10}Z_{20})^2 \cdot \{X_{21}Z_{10} + X_{20}Z_{11} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20})\} X_{10}Z_{20} + 2(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 \cdot \right. \\ &\quad \left. (X_{11}Z_{20} + X_{10}Z_{21}) + 2(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 X_{10}Z_{20} \right] p \pmod{p^2} \end{aligned}$$

$$\therefore \tilde{X}_{31} \equiv X'_{30} + X'_{31}p \pmod{p^2}$$

where

$$\left\{ \begin{aligned} X'_{30} &\equiv Z_{10}Z_{20}(X_{20}Z_{10} + (p-1)X_{10}Z_{20}) \cdot (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20})^2 + (p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^4 \\ &\quad + 2(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 X_{10}Z_{20} \pmod{p^2} \\ X'_{31} &\equiv 2(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20}) \cdot (X_{20}Z_{10} + (p-1)X_{10}Z_{20}) \cdot \{Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1)(Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20})\} \\ &\quad \cdot Z_{10}Z_{20} + (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20})^2 \cdot \{X_{21}Z_{10} + X_{20}Z_{11} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20})\} Z_{10}Z_{20} \\ &\quad + (Z_{11}Z_{20} + Z_{10}Z_{21}) \cdot (X_{20}Z_{10} + (p-1)X_{10}Z_{20}) \cdot (Y_{20}Z_{10} + (p-1)Y_{10}Z_{20})^2 + 4(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 \\ &\quad \cdot \{X_{21}Z_{10} + X_{20}Z_{11} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20})\} + (p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^4 \\ &\quad + 6(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^2 \cdot \{X_{21}Z_{10} + X_{20}Z_{11} + (p-1)(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20})\} X_{10}Z_{20} \\ &\quad + 2(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 \cdot (X_{11}Z_{20} + X_{10}Z_{21}) + 2(p-1)(X_{20}Z_{10} + (p-1)X_{10}Z_{20})^3 X_{10}Z_{20} \pmod{p^2} \end{aligned} \right. \quad (11)$$

For

$$\begin{aligned} \tilde{Y}_{31} &\equiv (\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21}) \left\{ (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^2 \tilde{X}_{11}\tilde{Z}_{21} - (\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21})^2 \tilde{Z}_{11}\tilde{Z}_{21} + (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^3 \right. \\ &\quad \left. + 2(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^2 \tilde{X}_{11}\tilde{Z}_{21} \right\} - (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^3 \tilde{Y}_{11}\tilde{Z}_{21} \pmod{p^2} \\ \Rightarrow \tilde{Y}_{31} &\equiv (\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21}) (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^2 \tilde{X}_{11}\tilde{Z}_{21} - (\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21})^3 \tilde{Z}_{11}\tilde{Z}_{21} + (\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21}) (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^3 \\ &\quad + 2(\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21}) (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^2 \tilde{X}_{11}\tilde{Z}_{21} - (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^3 \tilde{Y}_{11}\tilde{Z}_{21} \pmod{p^2} \\ \Rightarrow \tilde{Y}_{31} &\equiv (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21})^2 \left\{ 3(\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21}) \tilde{X}_{11}\tilde{Z}_{21} + (\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21}) (\tilde{Y}_{21}\tilde{Z}_{11} - 2\tilde{Y}_{11}\tilde{Z}_{21}) \right\} \\ &\quad - (\tilde{Y}_{21}\tilde{Z}_{11} - \tilde{Y}_{11}\tilde{Z}_{21})^3 \tilde{Z}_{11}\tilde{Z}_{21} \pmod{p^2} \end{aligned}$$

Now, substituting (3),(4),(7),(9) and (10) expansions modulo p^2 in the formula of \tilde{Y}_{31} , we have

$$\begin{aligned} \Rightarrow \tilde{Y}_{31} \equiv & \left((X_{20}Z_{10}+(p-1)X_{10}Z_{20})^2 + 2(X_{20}Z_{10}+(p-1)X_{10}Z_{20}) \cdot [X_{20}Z_{11}+X_{21}Z_{10}+(p-1)\{X_{10}Z_{20}+X_{10}Z_{21}+X_{11}Z_{20}\}]p \right) \\ & \left\{ 3(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20} + [Y_{20}Z_{11}+Y_{21}Z_{10}+(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}]p) (X_{10}Z_{20}+(X_{10}Z_{21}+X_{11}Z_{20})p) \right. \\ & + (X_{20}Z_{10}+(p-1)X_{10}Z_{20} + \{X_{20}Z_{11}+X_{21}Z_{10}+(p-1)(X_{10}Z_{20}+X_{10}Z_{21}+X_{11}Z_{20})\}p) (Y_{20}Z_{10}+2(p-1)Y_{10}Z_{20} \\ & \left. + (Y_{20}Z_{11}+Y_{21}Z_{10}+2(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\})p) \right\} + ((p-1)+p(p-1)) \left((Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^3 \right. \\ & \left. + 3(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^2 [Y_{20}Z_{11}+Y_{21}Z_{10}+(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}]p \right) \\ & (Z_{10}Z_{20}+(Z_{10}Z_{21}+Z_{11}Z_{20})p) \pmod{p^2} \end{aligned}$$

Then the p -adic expansion of \tilde{Y}_{31} is given as

$$\begin{aligned} \tilde{Y}_{31} \equiv & (X_{20}Z_{10}+(p-1)X_{10}Z_{20})^2 \left\{ 3X_{10}Z_{20}(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20}) + (X_{20}Z_{10}+(p-1)X_{10}Z_{20}) [Y_{20}Z_{10}+2(p-1)Y_{10}Z_{20}] \right\} \\ & + (p-1)(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^3 Z_{10}Z_{20} + \left\{ (X_{20}Z_{10}+(p-1)X_{10}Z_{20})^2 \left(3(X_{10}Z_{21}+X_{11}Z_{20}) \cdot (Y_{20}Z_{10}+(p-1)Y_{10}Z_{20}) \right. \right. \\ & \left. \left. + 3X_{10}Z_{20}(Y_{21}Z_{10}+Y_{20}Z_{11}+(p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}) \right) + (X_{20}Z_{10}+(p-1)X_{10}Z_{20}) [Y_{20}Z_{11}+Y_{21}Z_{10} \right. \\ & \left. + 2(p-1)(Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20})] + (X_{20}Z_{11}+X_{21}Z_{10}+(p-1)\{X_{10}Z_{20}+X_{10}Z_{21}+X_{11}Z_{20}\}) \cdot [Y_{20}Z_{10}+2(p-1)Y_{10}Z_{20}] \right\} \\ & + (p-1)(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^3 [Z_{11}Z_{20}+Z_{10}Z_{21}] + 3(p-1)Z_{10}Z_{20}(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^2 (Y_{21}Z_{10}+Y_{20}Z_{11} \\ & + (p-1)\{Y_{10}Z_{20}+Y_{10}Z_{21}+Y_{11}Z_{20}\}) + 2(X_{20}Z_{10}+(p-1)X_{10}Z_{20}) \cdot (X_{21}Z_{10}+X_{20}Z_{11}+(p-1)\{X_{10}Z_{20}+X_{10}Z_{21}+X_{11}Z_{20}\}) \cdot \\ & [3X_{10}Z_{20}(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20}) + (X_{20}Z_{10}+(p-1)X_{10}Z_{20}) \cdot (Y_{20}Z_{10}+2(p-1)Y_{10}Z_{20})] \\ & \left. + (p-1)Z_{10}Z_{20}(Y_{20}Z_{10}+(p-1)Y_{10}Z_{20})^3 \right\} p \pmod{p^2} \end{aligned}$$

$$\therefore \tilde{Y}_{31} \equiv Y'_{30} + Y'_{31}p \pmod{p^2}$$

where

$$\left\{ \begin{array}{l} Y'_{30} \equiv \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left\{ 3X_{10}Z_{20} \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) + \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \right. \\ \left. \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right) \right\} + (p-1) \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^3 Z_{10}Z_{20} \pmod{p^2} \\ Y'_{31} \equiv \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left\{ 3 \left(X_{10}Z_{21} + X_{11}Z_{20} \right) \cdot \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) \right. \\ + 3X_{10}Z_{20} \left(Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1) \left\{ Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right\} \right) + \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \\ \left\{ Y_{20}Z_{11} + Y_{21}Z_{10} + 2(p-1) \left[Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right] \right\} + \left(X_{20}Z_{11} + X_{21}Z_{10} + (p-1) \left\{ X_{10}Z_{20} + X_{10}Z_{21} \right. \right. \\ \left. \left. + X_{11}Z_{20} \right\} \right) \cdot \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right) \left. \right\} + (p-1) \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right)^3 \left(Z_{11}Z_{20} + Z_{10}Z_{21} \right) \\ + 3Z_{10}Z_{20} \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right)^2 \cdot \left(Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1) \left\{ Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right\} \right) \\ + 2 \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left(X_{21}Z_{10} + X_{20}Z_{11} + (p-1) \left\{ X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right\} \right) \cdot \\ \left\{ 3X_{10}Z_{20} \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) + \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left[Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right] \right\} \\ + (p-1)Z_{10}Z_{20} \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^3 \pmod{p^2} \end{array} \right. \quad (12)$$

Now, substituting expansion (5) modulo p^2 in the formula of \tilde{Z}_{31} , we have

$$\begin{aligned} \tilde{Z}_{31} &\equiv \left(\tilde{X}_{21}\tilde{Z}_{11} - \tilde{X}_{11}\tilde{Z}_{21} \right)^3 \tilde{Z}_{11}\tilde{Z}_{21} \pmod{p^2} \\ &\Rightarrow \tilde{Z}_{31} \equiv \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} + \left[X_{20}Z_{11} + X_{21}Z_{10} + (p-1) \left\{ X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right\} \right] p \right)^3 \cdot \\ &\quad \left(Z_{10}Z_{20} + \left\{ Z_{10}Z_{21} + Z_{11}Z_{20} \right\} p \right) \pmod{p^2} \end{aligned}$$

Then the p -adic expansion of \tilde{Z}_{31} is given as

$$\begin{aligned} \tilde{Z}_{31} &\equiv Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 + \left(3Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left\{ X_{20}Z_{11} + X_{21}Z_{10} \right. \right. \\ &\quad \left. \left. + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right\} + \left(Z_{11}Z_{20} + Z_{10}Z_{21} \right) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \right) p \pmod{p^2} \end{aligned}$$

$$\therefore \tilde{Z}_{31} \equiv Z'_{30} + Z'_{31}p \pmod{p^2}$$

where

$$\left\{ \begin{array}{l} Z'_{30} \equiv Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \pmod{p^2} \\ Z'_{31} \equiv 3Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \left(X_{20}Z_{11} + X_{21}Z_{10} + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right) \\ \quad + \left(Z_{11}Z_{20} + Z_{10}Z_{21} \right) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \pmod{p^2} \end{array} \right. \quad (13)$$

For $\tilde{P}_{11} = \tilde{P}_{21}$:

By the implementation of the arithmetic of points \tilde{P}_1, \tilde{P}_2 in $E(\mathbb{Q}_p)$ as in projective coordinates in (2) to points $\tilde{P}_{11}, \tilde{P}_{21}$ in $E(\mathbb{Q}_p) \pmod{p^2}$, we have

$$\tilde{X}_{31} \equiv 2\tilde{Y}_{11}\tilde{Z}_{11} \left\{ \left(A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2 \right)^2 - 8\tilde{X}_{11}\tilde{Y}_{11}^2\tilde{Z}_{11} \right\} \pmod{p^2}$$

$$\tilde{Y}_{31} \equiv \left(A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2 \right) \left\{ 12\tilde{X}_{11}\tilde{Y}_{11}^2\tilde{Z}_{11} - \left(A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2 \right)^2 \right\} - 8\tilde{Y}_{11}^4\tilde{Z}_{11}^2 \pmod{p^2}$$

$$\tilde{Z}_{31} \equiv 8\tilde{Y}_{11}^3\tilde{Z}_{11}^3 \pmod{p^2}$$

First, note the following expansions that are required to evaluate $\tilde{X}_{31}, \tilde{Y}_{31}, \tilde{Z}_{31}$
 Upon reducing each expansion to modulo p^2 , we have

$$\begin{aligned} (A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2) &\equiv 3(X_{10}^2 + 2X_{10}X_{11}p) + A(Z_{10}^2 + 2Z_{10}Z_{11}p) \pmod{p^2} \\ &\equiv 3X_{10}^2 + AZ_{10}^2 + (6X_{10}X_{11} + 2AZ_{10}Z_{11})p \pmod{p^2} \end{aligned} \tag{14}$$

$$\Rightarrow (A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2)^2 \equiv (3X_{10}^2 + AZ_{10}^2)^2 + 2(3X_{10}^2 + AZ_{10}^2)(6X_{10}X_{11} + 2AZ_{10}Z_{11})p \pmod{p^2} \tag{15}$$

$$\Rightarrow \tilde{X}_{11}\tilde{Y}_{11}^2\tilde{Z}_{11} \equiv X_{10}Y_{10}^2Z_{10} + (X_{10}Y_{10}^2Z_{11} + 2X_{10}Y_{10}Y_{11}Z_{10} + X_{11}Y_{10}^2Z_{10})p \pmod{p^2} \tag{16}$$

$$\Rightarrow \tilde{Y}_{11}^4\tilde{Z}_{11}^2 \equiv Y_{10}^4Z_{10}^2 + (4Y_{10}^3Y_{11}Z_{10}^2 + 2Y_{10}^4Z_{10}Z_{11})p \pmod{p^2} \tag{17}$$

$$\Rightarrow \tilde{Y}_{11}^3\tilde{Z}_{11}^3 \equiv Y_{10}^3Z_{10}^3 + 3(Y_{10}^2Y_{11}Z_{10}^3 + Y_{10}^3Z_{10}^2Z_{11})p \pmod{p^2} \tag{18}$$

For

$$\tilde{X}_{31} \equiv 2\tilde{Y}_{11}\tilde{Z}_{11} \left\{ (A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2)^2 - 8\tilde{X}_{11}\tilde{Y}_{11}^2\tilde{Z}_{11} \right\} \pmod{p^2}$$

On substituting (15),(16) expansions modulo p^2 in the formula of \tilde{X}_{31} , we have

$$\begin{aligned} \tilde{X}_{31} &\equiv (2Y_{10}Z_{10} + 2(Y_{10}Z_{11} + Y_{11}Z_{10})p) \cdot \left\{ (3X_{10}^2 + AZ_{10}^2)^2 + 2(3X_{10}^2 + AZ_{10}^2) \cdot (6X_{10}X_{11} + 2AZ_{10}Z_{11})p + 8((p-1) + (p-1)p) \right. \\ &\quad \left. (X_{10}Y_{10}^2Z_{10} + [X_{10}Y_{10}^2Z_{11} + 2X_{10}Y_{10}Y_{11}Z_{10} + X_{11}Y_{10}^2Z_{10}]p) \right\} \pmod{p^2} \end{aligned}$$

Then the p -adic expansion of \tilde{X}_{31} is given as

$$\begin{aligned} \tilde{X}_{31} &\equiv \left(2Y_{10}Z_{10}(3X_{10}^2 + AZ_{10}^2)^2 + 16(p-1)X_{10}Y_{10}^3Z_{10}^2 \right) + \left\{ 4Y_{10}Z_{10}(3X_{10}^2 + AZ_{10}^2)(6X_{10}X_{11} + 2AZ_{10}Z_{11}) \right. \\ &\quad \left. + 16(p-1)(X_{10}Y_{10}^2Z_{10} + X_{10}Y_{10}^2Z_{11} + 2X_{10}Y_{10}Y_{11}Z_{10} + X_{11}Y_{10}^2Z_{10})Y_{10}Z_{10} + 2(Y_{10}Z_{11} + Y_{11}Z_{10}) \cdot \right. \\ &\quad \left. [(3X_{10}^2 + AZ_{10}^2)^2 + 8(p-1)X_{10}Y_{10}^2Z_{10}] \right\} p \pmod{p^2} \end{aligned}$$

$$\therefore \tilde{X}_{31} \equiv X'_{30} + X'_{31}p \pmod{p^2}$$

where

$$\begin{cases} X'_{30} \equiv 2Y_{10}Z_{10}(3X_{10}^2 + AZ_{10}^2)^2 + 16(p-1)X_{10}Y_{10}^3Z_{10}^2 \pmod{p^2} \\ X'_{31} \equiv 4Y_{10}Z_{10}(3X_{10}^2 + AZ_{10}^2) \cdot (6X_{10}X_{11} + 2AZ_{10}Z_{11}) \\ \quad + 16(p-1)(X_{10}Y_{10}^2Z_{10} + X_{10}Y_{10}^2Z_{11} + 2X_{10}Y_{10}Y_{11}Z_{10} + X_{11}Y_{10}^2Z_{10})Y_{10}Z_{10} \\ \quad + 2(Y_{10}Z_{11} + Y_{11}Z_{10}) \cdot \left\{ (3X_{10}^2 + AZ_{10}^2)^2 + 8(p-1)X_{10}Y_{10}^2Z_{10} \right\} \pmod{p^2} \end{cases} \tag{19}$$

For

$$\tilde{Y}_{31} \equiv (A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2) \left\{ 12\tilde{X}_{11}\tilde{Y}_{11}^2\tilde{Z}_{11} - (A\tilde{Z}_{11}^2 + 3\tilde{X}_{11}^2)^2 \right\} - 8\tilde{Y}_{11}^4\tilde{Z}_{11}^2 \pmod{p^2}$$

Now, substituting (14),(15),(16) and (17) expansions modulo p^2 in the formula of \tilde{Y}_{31} , we have

$$\begin{aligned} \Rightarrow \tilde{Y}_{31} &\equiv (3X_{10}^2 + AZ_{10}^2 + \{6X_{10}X_{11} + 2AZ_{10}Z_{11}\}p) \cdot \left\{ 12(X_{10}Y_{10}^2Z_{10} + (X_{10}Y_{10}^2Z_{11} + 2X_{10}Y_{10}Y_{11}Z_{10} + X_{11}Y_{10}^2Z_{10})p) \right. \\ &\quad \left. + ((p-1) + (p-1)p) \left\{ (3X_{10}^2 + AZ_{10}^2)^2 + 2(3X_{10}^2 + AZ_{10}^2) \cdot (6X_{10}X_{11} + 2AZ_{10}Z_{11})p \right\} + 8((p-1) + (p-1)p) \cdot \right. \end{aligned}$$

$$\left[Y_{10}^4 Z_{10}^2 + \left(4Y_{10}^3 Y_{11} Z_{10}^2 + 2Y_{10}^4 Z_{10} Z_{11} \right) p \right] \pmod{p^2}$$

Then the p -adic expansion of \tilde{Y}_{31} is given as

$$\begin{aligned} \tilde{Y}_{31} \equiv & \left(3X_{10}^2 + AZ_{10}^2 \right) \cdot \left(12X_{10}Y_{10}^2Z_{10} + (p-1)(3X_{10}^2 + AZ_{10}^2)^2 \right) + (p-1)8Y_{10}^4Z_{10}^2 + \left[\left(3X_{10}^2 + AZ_{10}^2 \right) \cdot \left(12X_{10}Y_{10}^2Z_{11} \right. \right. \\ & + 24X_{10}Y_{10}Y_{11}Z_{10} + 12X_{11}Y_{10}^2Z_{10} \left. \left. + (p-1)(3X_{10}^2 + AZ_{10}^2)^2 \cdot \left(12X_{10}X_{11} + 4AZ_{10}Z_{11} \right) + (p-1)(3X_{10}^2 + AZ_{10}^2)^3 \right. \right. \\ & + 8(p-1)(Y_{10}^4Z_{10}^2 + 4Y_{10}^3Y_{11}Z_{10}^2 + 2Y_{10}^4Z_{10}Z_{11}) + \left. \left. \left(6X_{10}X_{11} + 2AZ_{10}Z_{11} \right) \left\{ \left(12X_{10}Y_{10}^2Z_{10} \right. \right. \right. \\ & \left. \left. \left. + (p-1)(3X_{10}^2 + AZ_{10}^2)^2 \right) + (p-1)8Y_{10}^4Z_{10}^2 \right\} \right] p \pmod{p^2} \end{aligned}$$

$$\therefore \tilde{Y}_{31} \equiv Y'_{30} + Y'_{31}p \pmod{p^2}$$

where

$$\begin{cases} Y'_{30} \equiv \left(3X_{10}^2 + AZ_{10}^2 \right)^2 \cdot \left\{ 12X_{10}Y_{10}^2Z_{10} + (p-1)(3X_{10}^2 + AZ_{10}^2)^2 \right\} + (p-1) \cdot 8Y_{10}^4 \pmod{p^2} \\ Y'_{31} \equiv \left(3X_{10}^2 + AZ_{10}^2 \right) \cdot \left(12X_{10}Y_{10}^2Z_{11} + 24X_{10}Y_{10}Y_{11}Z_{10} + 12X_{11}Y_{10}^2Z_{10} \right) + (p-1)(3X_{10}^2 + AZ_{10}^2)^2 \cdot \\ \left(12X_{10}X_{11} + 4AZ_{10}Z_{11} \right) + (p-1)(3X_{10}^2 + AZ_{10}^2)^3 + 8(p-1)(Y_{10}^4Z_{10}^2 + 4Y_{10}^3Y_{11}Z_{10}^2 + 2Y_{10}^4Z_{10}Z_{11}) \\ + \left(6X_{10}X_{11} + 2AZ_{10}Z_{11} \right) \cdot \left(12X_{10}Y_{10}^2Z_{10} + (p-1)(3X_{10}^2 + AZ_{10}^2)^2 \right) + (p-1) \cdot 8Y_{10}^4Z_{10}^2 \pmod{p^2} \end{cases} \quad (20)$$

For

$$\tilde{Z}_{31} \equiv 8\tilde{Y}_{11}^3\tilde{Z}_{11}^3 \pmod{p^2}$$

Now, substituting expansion (18) modulo p^2 in the formula of \tilde{Z}_{31} , the p -adic expansion of \tilde{X}_{31} is given as

$$\tilde{Z}_{31} \equiv 8Y_{10}^3Z_{10}^3 + 24\left\{ Y_{10}^2Y_{11}Z_{10}^3 + Y_{10}^3Z_{10}^2Z_{11} \right\} p \pmod{p^2}$$

$$\therefore \tilde{Z}_{31} \equiv Z'_{30} + Z'_{31}p \pmod{p^2}$$

where

$$\begin{cases} Z'_{30} \equiv 8Y_{10}^3Z_{10}^3 \pmod{p^2} \\ Z'_{31} \equiv 24\left(Y_{10}^2Y_{11}Z_{10}^3 + Z_{10}^2Z_{11}Y_{10}^3 \right) \pmod{p^2} \end{cases} \quad (21)$$

Hence, In both cases $\tilde{P}_{11} = \tilde{P}_{21}$ and $\tilde{P}_{11} \neq \tilde{P}_{21}$, the point

$$\tilde{P}_{31} = (\tilde{X}_{31} : \tilde{Y}_{31} : \tilde{Z}_{31}) = (X_{30} + X_{31}p : Y_{30} + Y_{31}p : Z_{30} + Z_{31}p)$$

is obtained by taking the p -adic expansion of $[X'_{30} + X'_{31}p : Y'_{30} + Y'_{31}p : Z'_{30} + Z'_{31}p]$ expressed in terms of $X_{10}, X_{11}, Y_{10}, Y_{11}, Z_{10}, Z_{11}, X_{20}, X_{21}, Y_{20}, Y_{21}, Z_{20}, Z_{21}$. ■

Example 1. For an elliptic curve $Y^2Z = X^3 + XZ^2 + Z^3$ over $\mathbb{Q}_5(\text{mod } 5^2)$, consider two points $\tilde{P}_{11} = [4 + 2.5 : 2 + 4.5 : 1]$ and $\tilde{P}_{21} = [2 + 1.5 : 4 + 4.5 : 1]$.

The addition of the points \tilde{P}_{11} and \tilde{P}_{21} can be evaluated by using the above formulas in the following manner.

$$\left\{ \begin{aligned} X'_{30} &\equiv Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^2 + (p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^4 \\ &\quad + 2(p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 X_{10}Z_{20} \pmod{p^2} \\ X'_{31} &\equiv 2 \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) \cdot \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left\{ Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1) \left(Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right) \right\} \cdot \\ &\quad Z_{10}Z_{20} + \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^2 \cdot \left\{ X_{21}Z_{10} + X_{20}Z_{11} + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right\} Z_{10}Z_{20} \\ &\quad + \left(Z_{11}Z_{20} + Z_{10}Z_{21} \right) \cdot \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^2 + 4(p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \cdot \\ &\quad \left\{ X_{21}Z_{10} + X_{20}Z_{11} + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right\} + (p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^4 \\ &\quad + 6(p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left\{ X_{21}Z_{10} + X_{20}Z_{11} + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right\} X_{10}Z_{20} \\ &\quad + 2(p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \cdot \left(X_{11}Z_{20} + X_{10}Z_{21} \right) + 2(p-1) \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 X_{10}Z_{20} \pmod{p^2} \end{aligned} \right.$$

$$\left\{ \begin{aligned} X'_{30} &= 1 \cdot 1(2 \cdot 1 + 4 \cdot 4 \cdot 1)(4 \cdot 1 + 4 \cdot 2 \cdot 1)^2 + 4 \cdot 18^4 + 2 \cdot 4 \cdot 18^3 \cdot 4 \cdot 1 \\ &= 2592 + 419904 + 186624 = 609120 \equiv 20 \pmod{5^2} \\ X'_{31} &= 2 \cdot 12 \cdot 18(4 \cdot 1 + 0 + 4(2 \cdot 1 + 0 + 4 \cdot 1)) \cdot 1 \cdot 1 + 12^2(1 \cdot 1 + 0 + 4(4 \cdot 1 + 0 + 2 \cdot 1)) \cdot 1 \cdot 1 \\ &\quad + 4 \cdot 4 \cdot 18^3(1 \cdot 1 + 0 + 4(4 \cdot 1 + 0 + 2 \cdot 1)) + 4 \cdot 18^4 + 6 \cdot 4 \cdot 18^2(1 \cdot 1 + 0 + 4(4 \cdot 1 + 0 + 2 \cdot 1)) \cdot 4 \cdot 1 \\ &\quad + 2 \cdot 4 \cdot 18^3(2 \cdot 1 + 0) + 2 \cdot 4 \cdot 18^3 \cdot 4 \cdot 1 \\ &= 12096 + 3600 + 2332800 + 419904 + 777600 + 93312 + 186624 \\ &= 3825936 \equiv 11 \pmod{5^2} \end{aligned} \right.$$

$$\therefore \tilde{X}_{31} \equiv 20 + 11.5 \equiv 4.5 + 1.5 \equiv 0 \pmod{5^2}$$

$$\left\{ \begin{aligned} Y'_{30} &\equiv \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left\{ 3X_{10}Z_{20} \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) + \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \right. \\ &\quad \left. \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right) \right\} + (p-1) \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^3 Z_{10}Z_{20} \pmod{p^2} \\ Y'_{31} &\equiv \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left\{ 3 \left(X_{10}Z_{21} + X_{11}Z_{20} \right) \cdot \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) \right. \\ &\quad + 3X_{10}Z_{20} \left(Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1) \left\{ Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right\} \right) + \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \\ &\quad \left\{ Y_{20}Z_{11} + Y_{21}Z_{10} + 2(p-1) \left[Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right] \right\} + \left(X_{20}Z_{11} + X_{21}Z_{10} + (p-1) \left\{ X_{10}Z_{20} + X_{10}Z_{21} \right. \right. \\ &\quad \left. \left. + X_{11}Z_{20} \right\} \right) \cdot \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right) \left. \right\} + (p-1) \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right)^3 \left(Z_{11}Z_{20} + Z_{10}Z_{21} \right) \\ &\quad + 3Z_{10}Z_{20} \left(Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right)^2 \cdot \left(Y_{21}Z_{10} + Y_{20}Z_{11} + (p-1) \left\{ Y_{10}Z_{20} + Y_{10}Z_{21} + Y_{11}Z_{20} \right\} \right) \\ &\quad + 2 \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left(X_{21}Z_{10} + X_{20}Z_{11} + (p-1) \left\{ X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right\} \right) \cdot \\ &\quad \left\{ 3X_{10}Z_{20} \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right) + \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right) \cdot \left[Y_{20}Z_{10} + 2(p-1)Y_{10}Z_{20} \right] \right\} \\ &\quad + (p-1)Z_{10}Z_{20} \left(Y_{20}Z_{10} + (p-1)Y_{10}Z_{20} \right)^3 \pmod{p^2} \end{aligned} \right.$$

$$\left\{ \begin{aligned} Y'_{30} &= 18^2(3.4.1(4.1 + 4.2.1) + 18.20) + 4.12^3.1.1 \\ &= 324(504) + 6912 = 170208 \equiv 8 \pmod{5^2} \\ Y'_{31} &= 18^2(3(0 + 2).12 + 3.4.1(4.1 + 0 + 4[2.1 + 0 + 4.1]) + 18(0 + 4.1 + 2.4[2.1 + 0 + 4.1]) \\ &\quad + (0 + 1.1 + 4[4.1 + 0 + 2.1]).(4.1 + 2.4.2.1)) + 0 + 3.1.1.20^2(4.1 + 0 + 4[2.1 + 0 + 4.1]) \\ &\quad + 2.18.(1.1 + 0 + 4[4.1 + 0 + 2.1]).(18^2(3.4.1(4.1 + 4.2.1) + 18.12) + 4.12^3.1.1) \\ &= 324(72 + 336 + 1880 + 500) + 0 + 33600 + 36.25.8 = 903312 + 33600 + 7200 = 944112 \equiv 12 \pmod{5^2} \end{aligned} \right.$$

$$\therefore \tilde{Y}_{31} \equiv 8 + 12.5 \equiv 3 + 1.5 + 2.5 \equiv 3 + 3.5 \pmod{5^2}$$

$$\begin{cases} Z'_{30} \equiv Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \pmod{p^2} \\ Z'_{31} \equiv 3Z_{10}Z_{20} \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^2 \cdot \left(X_{20}Z_{11} + X_{21}Z_{10} + (p-1) \left(X_{10}Z_{20} + X_{10}Z_{21} + X_{11}Z_{20} \right) \right) \\ \quad + \left(Z_{11}Z_{20} + Z_{10}Z_{21} \right) \cdot \left(X_{20}Z_{10} + (p-1)X_{10}Z_{20} \right)^3 \pmod{p^2} \end{cases}$$

$$\begin{cases} Z'_{30} = 1.1(2.1 + 4.4.1)^3 = 1.18^3 = 5832 \equiv 7 \pmod{5^2} \\ Z'_{31} = 3.1.1.18^2 \cdot (0 + 1.1 + 4(4.1 + 0 + 2.1)) + 0 \\ \quad = 972.25 = 24300 \equiv 0 \pmod{5^2} \end{cases}$$

$$\therefore \tilde{Z}_{31} \equiv 7 + 0.5 \equiv 2 + 1.5 \pmod{5^2}$$

Hence,

$$\tilde{P}_{11} + \tilde{P}_{21} = [0 : 3 + 3.5 : 2 + 1, 5]$$

Also, for $\tilde{P}_1 = [2 + 1.5 : 4 + 4.5 : 1]$, the doubling of the point \tilde{P}_1 represented as $2\tilde{P}_1$ can be evaluated by using the above formulas in the following manner.

$$\begin{cases} X'_{30} \equiv 2Y_{10}Z_{10} \left(3X_{10}^2 + AZ_{10}^2 \right)^2 + 16(p-1)X_{10}Y_{10}^3Z_{10}^2 \pmod{p^2} \\ X'_{31} \equiv 4Y_{10}Z_{10} \left(3X_{10}^2 + AZ_{10}^2 \right) \cdot \left(6X_{10}X_{11} + 2AZ_{10}Z_{11} \right) \\ \quad + 16(p-1) \left(X_{10}Y_{10}^2Z_{10} + X_{10}Y_{10}^2Z_{11} + 2X_{10}Y_{10}Y_{11}Z_{10} + X_{11}Y_{10}^2Z_{10} \right) Y_{10}Z_{10} \\ \quad + 2 \left(Y_{10}Z_{11} + Y_{11}Z_{10} \right) \cdot \left\{ \left(3X_{10}^2 + AZ_{10}^2 \right)^2 + 8(p-1)X_{10}Y_{10}^2Z_{10} \right\} \pmod{p^2} \end{cases}$$

$$\begin{cases} X'_{30} = 2.4.1.13^2 + 16.4.2.4^3.1^2 = 9544 \equiv 19 \pmod{5^2} \\ X'_{31} = 4.4.1.13(6.2.1 + 0) + 16.4(2.4^2.1 + 0 + 2.2.4.4.1 + 1.4^2.1).4.1 + 2(0 + 4.1)(13^2 + 8.4.2.4^2.1) \\ \quad = 2496 + 256(112) + 8(1193) = 40712 \equiv 12 \pmod{5^2} \end{cases}$$

$$\therefore \tilde{X}'_{31} \equiv 19 + 12.5 \equiv 4 + 3.5 + 2.5 \equiv 4 \pmod{5^2}$$

$$\begin{cases} Y'_{30} \equiv \left(3X_{10}^2 + AZ_{10}^2 \right)^2 \cdot \left\{ 12X_{10}Y_{10}^2Z_{10} + (p-1) \left(3X_{10}^2 + AZ_{10}^2 \right)^2 \right\} + (p-1) \cdot 8Y_{10}^4 \pmod{p^2} \\ Y'_{31} \equiv \left(3X_{10}^2 + AZ_{10}^2 \right) \cdot \left(12X_{10}Y_{10}^2Z_{11} + 24X_{10}Y_{10}Y_{11}Z_{10} + 12X_{11}Y_{10}^2Z_{10} \right) + (p-1) \left(3X_{10}^2 + AZ_{10}^2 \right)^2 \cdot \\ \quad \left(12X_{10}X_{11} + 4AZ_{10}Z_{11} \right) + (p-1) \left(3X_{10}^2 + AZ_{10}^2 \right)^3 + 8(p-1) \left(Y_{10}^4Z_{10}^2 + 4Y_{10}^3Y_{11}Z_{10}^2 + 2Y_{10}^4Z_{10}Z_{11} \right) \\ \quad + \left(6X_{10}X_{11} + 2AZ_{10}Z_{11} \right) \cdot \left(12X_{10}Y_{10}^2Z_{10} + (p-1) \left(3X_{10}^2 + AZ_{10}^2 \right)^2 \right) + (p-1) \cdot 8Y_{10}^4Z_{10}^2 \pmod{p^2} \end{cases}$$

$$\begin{cases} Y'_{30} = (3.2^2 + 1.1^2) \left(12.2.4^2.1 + 4(3.2^2 + 1.1^2)^2 \right) + 4.8.4^4 \\ \quad = 13^2(384 + 676) + 4(2048) = 179140 + 8192 = 187332 \equiv 7 \pmod{5^2} \\ Y'_{31} = 13(0 + 24.2.4.4 + 12.1.4^2.1) + 4.13^2(12.2 + 0) + 4.13^3 + 8.4(4^4.1^2 + 4.4^3.4.1^2 + 0) + (6.2.1 + 0)(12.1.4^2.1 + 4(13)^2) \\ \quad + 4.8.4^4.1^2 \\ \quad = 13(960) + 676(24) + 8788 + 32(1280) + 12(868) + 8192 = 97060 \equiv 10 \pmod{5^2} \end{cases}$$

$$\therefore Y_{31} \equiv 7 + 10.5 \equiv 2 + 1.5 \pmod{5^2}$$

$$\begin{cases} Z'_{30} \equiv 8Y_{10}^3Z_{10}^3 \pmod{p^2} \\ Z'_{31} \equiv 24 \left(Y_{10}^2Y_{11}Z_{10}^3 + Z_{10}^2Z_{11}Y_{10}^3 \right) \pmod{p^2} \end{cases}$$

$$\begin{cases} Z'_{30} = 8.(4)^3.(1)^3 = 512 \equiv 12 \pmod{5^2} \\ Z'_{31} = 24(4^2.4.1^3 + 0) = 24(64) = 1536 \equiv 11 \pmod{5^2} \end{cases}$$

$$\therefore \tilde{Z}_{30} \equiv 12 + 11.5 \equiv 2 + 2.5 + 1.5 \equiv 2 + 3.5 \pmod{5^2}$$

Hence,

$$2\tilde{P}_1 = [4 : 2 + 1.5 : 2 + 3.5]$$

The step by step procedure for point addition on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over the p -adic field \mathbb{Q}_p defined over \mathbb{Z}_p in projective coordinates using addition and multiplication operations performed as in \mathbb{Q}_p was discussed below.

Algorithm for Point Addition in $E(\mathbb{Q}_p)(\text{mod } p^2)$ in Projective coordinates : Consider an elliptic curve $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ over \mathbb{Q}_p . Let \tilde{P}_1, \tilde{P}_2 be two points on $E(\mathbb{Q}_p)$ defined over \mathbb{Z}_p in projective coordinates then by considering \tilde{P}_1 and \tilde{P}_2 modulo p^2 , the points $\tilde{P}_{11}, \tilde{P}_{21} \in E(\mathbb{Q}_p)(\text{mod } p^2)$ are given as $\tilde{P}_{11} = [\tilde{X}_{11} : \tilde{Y}_{11} : \tilde{Z}_{11}] = [X_{10} + X_{11}p : Y_{10} + Y_{11}p : Z_{10} + Z_{11}p]$ and $\tilde{P}_{21} = [\tilde{X}_{21} : \tilde{Y}_{21} : \tilde{Z}_{21}] = [X_{20} + X_{21}p : Y_{20} + Y_{21}p : Z_{20} + Z_{21}p]$ respectively. The addition of points \tilde{P}_{11} and \tilde{P}_{21} in $E(\mathbb{Q}_p)(\text{mod } p^2)$ is represented as $\tilde{P}_{11} + \tilde{P}_{21} = \tilde{P}_{31}$ and is given as

$$\tilde{P}_{31} = [\tilde{X}_{31} : \tilde{Y}_{31} : \tilde{Z}_{31}] = [X_{30} + X_{31}p : Y_{30} + Y_{31}p : Z_{30} + Z_{31}p]$$

is obtained by the steps in the following algorithm.

Step-I :- Check whether $\tilde{P}_{11} \neq \tilde{P}_{21}$ or $\tilde{P}_{11} = \tilde{P}_{21}$.

Step-II :- For $\tilde{P}_{11} \neq \tilde{P}_{21}$, evaluate $X'_{30}, X'_{31}, Y'_{30}, Y'_{31}, Z'_{30}, Z'_{31}$ using the formulas (11), (12), (13) in the above theorem.

Step-III :- For $\tilde{P}_{11} = \tilde{P}_{21}$, evaluate $X'_{30}, X'_{31}, Y'_{30}, Y'_{31}, Z'_{30}, Z'_{31}$ using the formulas (19), (20), (21) in the above theorem.

Step-IV :- From the values of $X'_{30}, X'_{31}, Y'_{30}, Y'_{31}, Z'_{30}, Z'_{31}$ in Step-II or Step-III, the arithmetic of points $\tilde{P}_{11}, \tilde{P}_{21}$ given as $\tilde{P}_{11} + \tilde{P}_{21} = \tilde{P}_{31}$ is obtained by taking the p -adic expansion of $[X'_{30} + X'_{31}p : Y'_{30} + Y'_{31}p : Z'_{30} + Z'_{31}p]$ and is given as

$$\tilde{P}_{31} = [\tilde{X}_{31} : \tilde{Y}_{31} : \tilde{Z}_{31}] = [X_{30} + X_{31}p : Y_{30} + Y_{31}p : Z_{30} + Z_{31}p]$$

The code for arithmetic of the points in $E(\mathbb{Q}_p)(\text{mod } p^2)$ in projective coordinates is given in the below GitHub link in python language.

<https://github.com/Tejusetty/elliptic-curve-point-additionprojectivecoordinates/blob/b8ecfa0157d9c19b0d164ba6f4e06ce4e9c884f9/projective%20addition%20on%20elliptic%20curve.py>

Example 2. For an elliptic curve $E : Y^2Z = X^3 + XZ^2 + Z^3$ over $\mathbb{Q}_{999983}(999983^2)$, consider two points $\tilde{P}_{11} = [3889+47892 \times 999983 : 890191+836190 \times 999983 : 1]$ and $\tilde{P}_{21} = [999041+79435 \times 999983 : 463676+771540 \times 999983 : 1]$ then with the help of above algorithm, \tilde{P}_{31} is given as

$$\tilde{P}_{31} = [213540 + 952346 \times 999983 : 182457 + 982335 \times 999983 : 495042 + 138205 \times 999983]$$

which is a lift of the point $[213540 : 182457 : 495042] \in E(\mathbb{F}_p)$.

7 Efficiency of Arithmetic of Points on $E(\mathbb{Q}_p)(\text{mod } p^2)$ in Affine and Projective Coordinates

In [7], point addition on elliptic curve over p -adic field \mathbb{Q}_p modulo p^2 in affine coordinates is described, which involves 43 multiplications and 22 additions and 12 subtractions and 10 reductions and 2 field inversions and by above theorem, point addition on elliptic curve over p -adic field \mathbb{Q}_p modulo p^2 in projective coordinates involves 124 multiplications and 68 additions and 14 subtractions and 37 reductions and 0 field inversions. The corresponding comparative study is described in Table 3 and Figure 4 provides a clear depiction of the number of operations for point addition in affine and projective coordinates on an elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic field \mathbb{Q}_p modulo p^2 in terms of number of multiplications and number of additions/subtractions and number of reductions.

Table 3. Number of operations for Point addition in Affine coordinate system in $E(\mathbb{Q}_p)(\text{mod } p^2)$

Description	No. of Multiplications	No. of Additions	No. of Subtractions	No. of Reductions	No. of Inversions
Point Addition	43	22	12	10	2
Point Doubling	35	28	6	18	2

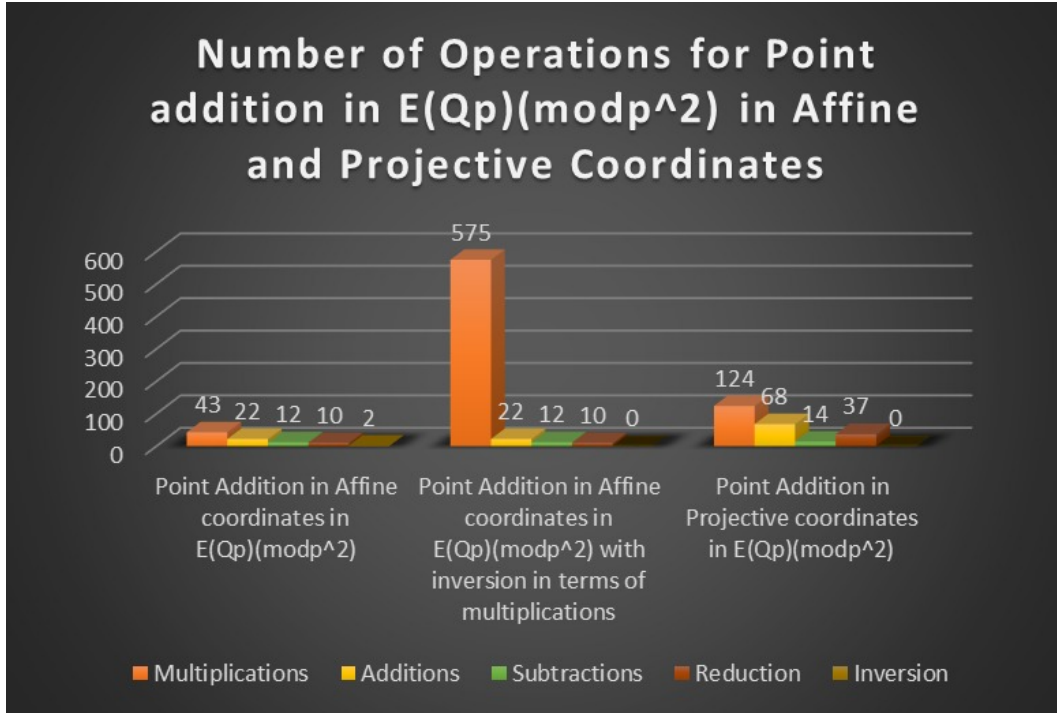


Figure 4. No. of operations in performing point addition in Affine and Projective coordinates in $E(\mathbb{Q}_p)(\text{mod } p^2)$

In [7], point doubling on elliptic curve over p -adic field \mathbb{Q}_p modulo p^2 in affine coordinates is described, which involves 35 multiplications, 28 additions, 6 subtractions, 18 reductions, and 2 field inversions, out of which the field inversion is expensive i.e., it takes more time which leads us to move to projective coordinates and by above theorem, point doubling on elliptic curve over p -adic field \mathbb{Q}_p modulo p^2 in projective coordinates involves 160 multiplications and 44 additions and 6 subtractions 94 reductions and 0 field inversions in projective coordinates over p -adic field \mathbb{Q}_p modulo p^2 . Hence, arithmetic of points in projective coordinates is more efficient as inversion is quite costly, since 1 inversion is approximately equal to 266 multiplications. The corresponding comparative study is described in Table 4 and Figure 5 provides a clear depiction of the number of operations for point doubling in affine and projective coordinates on an elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ over p -adic field \mathbb{Q}_p modulo p^2 in terms of the number of multiplications, the number of additions/subtractions, and the number of reductions, and the time taken for these operations are in the following order:

$$Time (Multiplication) > Time (p\text{-adic reduction}) > Time (Addition/ Subtraction)$$

Table 4. Number of operations for Point doubling in Affine coordinate system in $E(\mathbb{Q}_p)(\text{mod } p^2)$

Description	No. of Multiplications	No. of Additions	No. of Subtractions	No. of Reductions	No. of Inversions
Point Addition	124	68	14	37	0
Point Doubling	160	44	6	94	0

8 Conclusions

In this paper, the main focus is on the depiction of the efficiency in the arithmetic of points on an elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ in projective coordinates. In such process, the arithmetic of points on elliptic curve $E(\mathbb{Q}_p)$ in projective coordinates had been implemented to the arithmetic of points on elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ in projective coordinates and made a comparative study

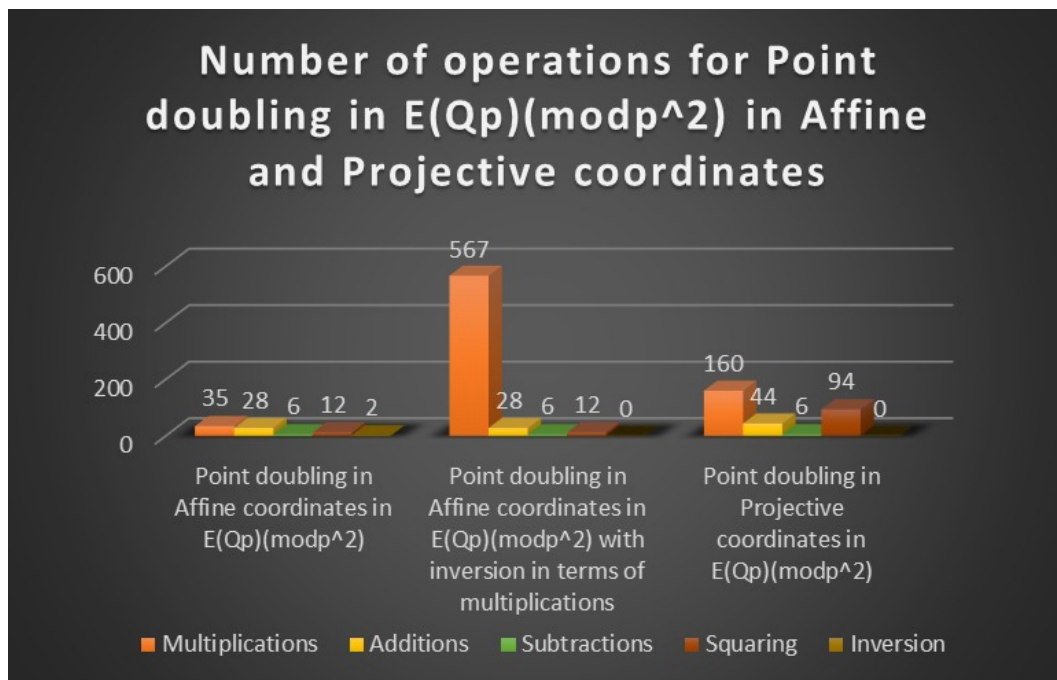


Figure 5. No. of operations in performing point doubling in Affine and Projective coordinates in $E(\mathbb{Q}_p)(\text{mod } p^2)$

for the number of operations to be performed in evaluating the arithmetic of points on an elliptic curve $E(\mathbb{F}_p)$ and the arithmetic of points on an elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ both in affine and projective coordinates. This study provides a clear view that arithmetic of points on an elliptic curve $E(\mathbb{Q}_p)(\text{mod } p^2)$ in projective coordinates is more efficient, that is, less expensive than affine coordinates. The presented approach not only improves computational speed but also maintains the mathematical robustness required for cryptographic applications. This work contributes to the broader effort of laying foundation for more efficient and secure ECC implementations with elliptic curve operations over p -adic fields.

Acknowledgments

This research was supported by the Department of Science and Technology (DST), Innovation in Science Pursuit for Inspired Research (INSPIRE) fellowship under the INSPIRE code *IF*200484. The authors thank DST-INSPIRE fellowship for their financial assistance which enabled us to conduct this study.

REFERENCES

- [1] Darrel Hankerson, Alfred J. Menezes and Scott Vanstone, "Guide to Elliptic Curve Cryptography," Springer-Verlag, 2004. ISBN 0-387-95273-X.
- [2] Neal Koblitz, "A course in number theory and cryptography," Graduate texts in Mathematics, Second Edition, Springer-Verlag., 1994. ISBN 3-540-78071-8.
- [3] J. H. Silverman, "The Arithmetic of Elliptic Curves," Graduate texts in Mathematics, Vol. 106, Springer-Verlag, New York, 1996.
- [4] Maherindrainibelahasa, Ravaliminoarimalalason, Randimbindrainibe, " p -adic numbers applied on elliptic curve cryptography," International Journal of Advance Research and Innovative Ideas in Education, Vol. 5, No. 2, pp. 213-229, 2019.
- [5] J. H. Silverman and J. Tate, "Rational points on Elliptic Curves," Undergraduate Texts in Mathematics, Springer-Verlag., New York, 1992.
- [6] Lawrence C. Washington, "Elliptic curves number theory and Cryptography," Second Edition, CRC Press, 2008. ISBN 978-1-4200-7146-7.
- [7] P. Anuradha Kameswari, T. Sai Tejaswini, "Elliptic curves over p -adic field \mathbb{Q}_p and its p -adic point addition," Communications on Applied Nonlinear Analysis, Vol. 32, No. 7s, pp. 856–882, 2024. DOI: <https://doi.org/10.52783/cana.v32.3491>

- [8] Fernando Gouvea, “ p -adic Numbers : An Introduction,” Universitext., Third Edition, Springer-Verlag., New York, 1997.
- [9] S. Katok, “ p -adic analysis compared with real,” Student Mathematical Library, Vol. 37, American Mathematical Society, Providence, RI, 2007.
- [10] N. Koblitz, “ p -adic numbers, p -adic analysis and zeta-functions,” Graduate texts in Mathematics, Second edition, Vol. 58, Springer-Verlag, New York, 1984.
- [11] Alain M. Robert, “A Course in p -adic Analysis,” Graduate Texts in Mathematics, Vol. 198, Springer-Verlag, New York, 2000.
- [12] L. Praveen Kumar, “Arithmetic of Elliptic curves with Affine and Projective Coordinates and some cryptographic aspects,” Ph.D. dissertation, Dept. Math., Andhra University, Vishakhapatnam, 2015.
- [13] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Updated Edition, Springer, 2020.
- [14] D. Bernstein, T. Lange, “A Survey of Elliptic Curve Cryptography (2023 Update),” *Journal of Cryptographic Engineering*, 2023.
- [15] J. H. Silverman, “The Arithmetic of Elliptic Curves,” 3rd Edition, Springer GTM 106, 2023.