Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 7s (2025)

Elliptic Curves over p-adic field Q_p and its p-adic point addition

P. Anuradha Kameswari[1] and T. Sai Tejaswini[2]

[1,2]Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India., panuradhakameswari@yahoo.in, tejutanniru89@gmail.com.

Article History:

Received: *28-10-2024*

Revised:*12-11-2024*

Accepted:*19-12-2024*

Abstract: Public-key cryptosystems with the Elliptic curve $E(F_p)$ over finite field F_p are an alternative to RSA with finite fields. In the context of improving the efficiency of cryptosystems with elliptic curves, the study of elliptic curves $E(Q_p)$ over p-adic number field Q_p was consequential. In this paper we first obtain all the points in the elliptic curve $E(Q_p)$ over p-adic number field Q_p as lifts of the points in $E(F_p)$ to $E(Q_p)(mod\ p^2)$ and then $E(Q_p)(mod\ p^2)$ to $E(Q_p)(mod\ p^3)$ and so on and then to evaluate the arithmetic on $E(Q_p)$, we first proceed to describe the implementation of the arithmetic of points on $E(Q_p)$ to points on $E(Q_p)(mod\ p^2)$ and then give the algorithms for the computations.

Keywords: Elliptic curves, p-adic field, Arithmetic of p-adic numbers, Elliptic curve over a field κ.

1. Introduction

Elliptic curve cryptography is one of majorly using cryptosystems in the current century which provides higher security and greater efficiency. It provides considerable security with smaller key size compared to any other public key cryptosystems. In the context of improving the efficiency of cryptosystems with elliptic curves, the study of cryptosystems with elliptic curves $E(Q_p)$ over p-adic field Q_p was consequential and the arithmetic of points in $E(Q_p)$ is implemented to points on $E(Q_p)(mod\ p^2)$ over p - adic number field Q_p . In this paper, we obtain all the points in the elliptic curve $E(Q_p)(mod\ p^2)$ over p-adic number field Q_p as lifts of the points in $E(F_p)$ then describe the implementation of the arithmetic of points on $E(Q_p)$ to points on $E(Q_p)(mod\ p^2)$ and then give the algorithms for the computations. For this, In section 2, we describe the p-adic field Q_p and arithmetic operations on p-adic numbers and In section 3, we describe elliptic curve over p-adic field Q_p and obtain the points in elliptic curve $E(Q_p)(mod\ p^2)$ over Q_p by considering the lift of points in $E(F_p)$ to $E(Q_p)(mod\ p^2)$. In section 4, we implement the arithmetic of points on $E(Q_p)$ to points on elliptic curve $E(Q_p)(mod\ p^2)$ over p-adic field Q_p .

1.1 Elliptic Curves over a field κ

Definition 1.1 (Elliptic curve equation over field κ with $Char\ \kappa \neq 2,3$). *For any field κ with characteristic $\kappa \neq 2,3$ the elliptic curve E over κ is denoted by $E(\kappa)$ and is given as*

$$E(\kappa) = \{(\alpha, \beta) \in \kappa \times \kappa / \beta^2 = \alpha^3 + A\alpha + B\} \cup \{\mathcal{O}\}$$

Where $\{\mathcal{O}\}$ is the point at infinity and $A, B \in \kappa$ such that the discriminant $\Delta = -(4A^3 + 27B^2) \neq 0$.

The equation $\beta^2 = \alpha^3 + A\alpha + B$ is called Weierstrass equation.

Definition 1.2 (Elliptic curve equation over field κ with $Char\ \kappa = 3$). *For any field κ with characteristic $\kappa = 3$ the elliptic curve E over κ is denoted by $E(\kappa)$ and is given as*

$$E(\kappa) = \{(\alpha, \beta) \in \kappa \times \kappa / \beta^2 = \alpha^3 + A\alpha^2 + B\alpha + C\} \cup \{\mathcal{O}\}$$

Where $\{\mathcal{O}\}$ is the point at infinity and $A, B, C \in \kappa$ such that the discriminant $\Delta = -4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2 \neq 0$.

Definition 1.3 (Elliptic curve equation over field κ with $Char\ \kappa = 2$). *For any field κ with characteristic $\kappa = 2$ the elliptic curve E over κ is denoted by $E(\kappa)$ and is given as*

$$E(\kappa) = \{(\alpha, \beta) \in \kappa \times \kappa / \beta^2 + \alpha\beta = \alpha^3 + a_2{}'\alpha^2 + a_6{}'\} \cup \{\mathcal{O}\}$$

or

$$E(\kappa) = \{(\alpha, \beta) \in \kappa \times \kappa / \beta^2 + a_3{}'\beta = \alpha^3 + a_2{}'\alpha^2 + a_6{}'\} \cup \{\mathcal{O}\}$$

Where $\{\mathcal{O}\}$ is the point at infinity and $a_2{}', a_3{}', a_4{}', a_6{}' \in \kappa$ such that $a_3{}' \neq 0$ and $a_6{}' \neq 0$.

Remark 1. The discriminant $\Delta \neq 0$ assures that the roots of the cubic equation

$$\beta^2 = \alpha^3 + A\alpha + B$$

are distinct as $\Delta = \big((e_1 - e_2)(e_2 - e_3)(e_3 - e_1)\big)^2$ for e_1, e_2, e_3 are the cube roots and basing on this point the arithmetic on elliptic curve $E(\kappa)$ is established.

Example 1.1. *Find the points on an elliptic curve $E: y^2 = x^3 + x + 1$ over F_5. In finding points on E, we first consider all the possible values of x which are $0,1,2,3,4$ and then find y which is a square of $x^3 + x + 1 (mod 5)$ and the following table represents the points in $E(F_5)$.*

x	$x^3 + x^2 + 1$	y	**Points on $E(F_5)$**
0	1	1,4	$(0,4), (0,1)$
1	3	-	-
2	1	1,4	$(2,1), (2,4)$
3	1	1,4	$(3,1), (3,4)$
$\mathcal{O}$	$\mathcal{O}$	$\mathcal{O}$	$\mathcal{O}$

The points in $E(F_5)$ are $\{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4)(4,2), (4,3)\} \cup \{\mathcal{O}\}$.

1.2 Arithmetic on elliptic curve over a field κ

The hidden beauty of ECC lies in adding two points on elliptic curve in such a way that it is completely different from any other point additions that are generally used. The addition law on elliptic curves is explained geometrically below. Let us suppose an elliptic curve over a field of characteristic $\kappa \neq 2,3$ then the curve equation over the field κ is given as

$$E(\kappa): \beta^2 = \alpha^3 + A\alpha + B$$

Let $P_1 = (\alpha_1, \beta_1)$ and $P_2 = (\alpha_2, \beta_2)$ be two points on the given elliptic curve E. Draw a line L through P_1 and P_2, then L intersects E in a third point P_3' as $\Delta \neq 0$. Reflect P_3' across X-axis to obtain P_3 . Now we define the sum of P_1 and P_2 as P_3 and is denoted as $P_1 + P_2 = P_3$ given as $P_3 = (\alpha_3, \beta_3)$ as shown in fig. 1.

The set of points on an elliptic curve over a field κ forms a group which is also abelian with respect to point addition defined above.

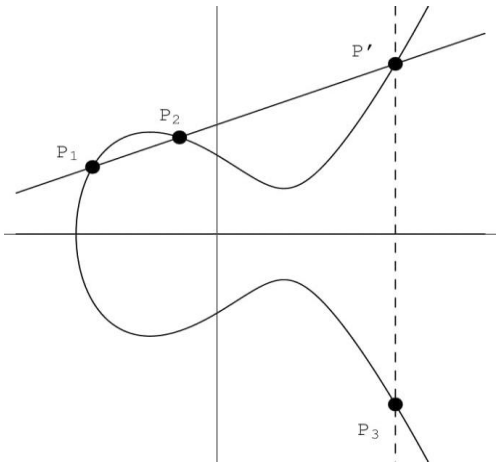

Figure 1: Geometric Interpretation of Point Addition on curve of the form $\beta^2 = \alpha^3 + A\alpha + B$

The point addition and doubling formula for points on an elliptic curve on a field κ with $Char\kappa = 2$ and $Char\kappa = 3$ and $Char\kappa \neq 2,3$ under different conditions at points P_1 and P_2 is given in the table below.

Field κ	**Elliptic curve**	**Slope m**		**$P_1 + P_2 = P_3$**		
		$P_1 \neq P_2$	$P_1 = P_2$	$P_1 \neq P_2$ $\alpha_1 \neq \alpha_2$	$P_1 \neq P_2$ $\alpha_1 = \alpha_2$	$P_1 = P_2$
Char $\kappa \neq 2,3$	$\beta^2 = \alpha^3 + A\alpha + B$	$\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}$	$\frac{3\alpha_1^2 + A}{2\beta_1}$	$\alpha_3 = m^2 - \alpha_1 - \alpha_2$ $\beta_3 = m(\alpha_1 - \alpha_3) - \beta_1$	$\mathcal{O}$	$\alpha_3 = m^2 - 2\alpha_1$ $\beta_3 = m(\alpha_1 - \alpha_3) - \beta_1$
Char $\kappa = 3$	$\beta^2 = \alpha^3 + A\alpha^2 + B\alpha + C$	$\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}$	$\frac{3\alpha_1^2 + 2A\alpha + B}{2\beta_1}$	$\alpha_3 = m^2 - A - \alpha_1 - \alpha_2$ $\beta_3 = m(\alpha_1 - \alpha_3) - \beta_1$	$\mathcal{O}$	$\alpha_3 = m^2 - A - 2\alpha_1$ $\beta_3 = m(\alpha_1 - \alpha_3) - \beta_1$
Char $\kappa = 2$	$\beta^2 + \alpha\beta = \alpha^3 + a_2\alpha^2 + a_6$ or $\beta^2 + a'_3\beta = \alpha^3 + a'_2\alpha^2 + a'_6$	$\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}$ $\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}$	$\frac{\alpha_1^2 + \beta_1}{\alpha_1}$ $\frac{\alpha_1^2 + a_4}{a_3}$	$\alpha_3 = m^2 + m + \alpha_1 + \alpha_2 + a_2$ $\beta_3 = m(\alpha_1 + \alpha_3) + \alpha_3 + \beta_1$	$\mathcal{O}$ $\mathcal{O}$	$\alpha_3 = \frac{\alpha_1^4 + a_6}{\alpha_1^2}$ $\beta_3 = \alpha + \beta$ $\alpha_3 = \frac{\alpha_1^4 + a_4^2}{a_3^2}$ $y_3 = a_3 + \beta$

				$\propto_3 = m^2 + \propto_1 + \propto_2$ $\beta_3 = m(\propto_1 + \propto_3)$ $+ \propto_3 + a_3$		

Table 1: Table for Arithmetic of Points in $E(\kappa)$

2. p-adic numbers

Definition 2.1 (p-adic valuation). *The p-adic valuation $v_p(\alpha)$ is given as for any $\alpha \in Q^*$ and $x = p^{\rho}.\frac{m}{n}$ with $m, n, \rho \in Z$, p is a prime, and $p \nmid mn$. Also, $v_p(0) = \infty$.*

Remark 2. The p-adic valuation satisfies the following properties:

For any $a, b \in Q$

1. $v_p(ab) = v_p(a) + v_p(b)$

2. $v_p(a + b) \geq min\{v_p(a), v_p(b)\}$ with $v_p(a) \neq v_p(b)$

3. $v_p(a) = \infty$ if and only if $x = 0$

Definition 2.2 (p-adic norm). *Let p be a prime and $\alpha \in Q$ then p-adic norm is given as*

$$|\alpha|_p = \begin{cases} p^{-v_p(\alpha)} & \text{if } \alpha \neq 0 \\ 0 & \text{if } \alpha = 0 \end{cases}$$ *p-adic norm $|x|_p$ is non-archimedean norm of x on Q.*

Definition 2.3 (p-adic numbers). *For any fixed prime p. The completion of Q with respect to p-adic norm $|\ |_p$ is denoted as Q_p which is called the field of p-adic numbers. we have Q_p as a field of characteristic 0.*

Proposition 1. *If $\alpha \in Q_p$ then there exists a unique sequence of integers α_i's with $0 \leq x_i \leq p - 1$ and $x_i = 0$ for i sufficiently negative such that $\alpha = \sum_{i=-\infty}^{\infty} \alpha_i\, p^i$*

Note 1. The partial sums of the series $\alpha = \sum_{i=-\infty}^{\infty} \alpha_i\, p^i$ form a Cauchy sequence and x is the limit of this sequence.

Remark 3. Every $x \in Q_p$ has unique representation depending on its p-adic valuation $|x|_p$ i.e., either $|x|_p \geq 1$ or $|x|_p \leq 1$.

If $x \in Q_p$ with $|x|_p \leq 1$, we can represent x as a sequence given as

$$x = x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1} = \sum_{n=0}^{\infty} x_n\, p^n$$

where $x_i \in 0,1,2,\ldots p - 1$.

If $x \in Q_p$ with $|x|_p \geq 1$, we can represent x as a sequence given as

$$x = \ldots + x_{-2} p^{-2} + x_{-1} p^{-1} + x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1} = \sum_{n=-\infty}^{\infty} x_n\, p^n$$

where $x_i \in 0,1,2,\ldots p - 1$.

Remark 4. For every $x \in Q_p$ with $x = \sum_{n=-m}^{\infty} x_n p^n$, the canonical expression of a is given as

$$x = \ldots x_n \ldots x_2 x_1 x_0 . x_{-1} x_{-2} x_{-3} \ldots x_{-m}$$

Definition 2.4 (p-adic integers Z_p). *A p-adic number $x \in Q_p$ is said to be p-adic integer if its canonical expression contains only non-negative powers of p. Set of p-adic integers is denoted by Z_p which is a sub-ring of Q_p.*

$$Z_p = \{x \in Q_p \; with \; |x| \leq 1\}$$
$$= \{x \in Q_p \; with \; v_p(x) \geq 0\}$$

One can also perform arithmetic operations like addition, subtraction, multiplication and division of any two p-adic numbers.

2.1 Arithmetic operations on p-adic numbers.

Every number $\alpha \in Q_p$ for p being a prime has its p-adic expansion given as

$$\alpha = \ldots + \alpha_{-2} p^{-2} + \alpha_{-1} p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 + \ldots$$

while some are finite expansions including only positive powers of p in its expansion.

Example 2.1.1. *1.* $320 = 5 + 3 \times 7 + 6 \times 7^2 = 635$ *in* Q_7
2. $108 = 3 + 1 \times 7 + 2 \times 7^2 = 213$ *in* Q_7
3. $\frac{1}{2} = 3 + 2 \times 5 + 2 \times 5^2 + \ldots = \ldots 2223$ *in* Q_5
Also, negative of $x \in Q_p$ is given as $-x = x \times (-1)$ with its p-adic expansion given as

$$-1 = (p-1) + (p-1) \times p + (p-1) \times p^2 + \ldots$$

i.e., $-1 = 4 + 4.5 + 4.5^2 + \ldots$ in Q_5

Arithmetical operations in Q_p extend ordinary arithmetic operations on Natural numbers N. p-adic addition and multiplication are performed from right to left with a carry. Also, p-adic division will be performed from right to left but different from long division as in N.

Example 2.1.2. *Addition, Multiplication and Division in 7-adic field Q_7 are given below for* 320 *and* 108 *expanded in Q_7 in above examples.*

$320 + 108 = 1151$ *given as*

$$\begin{array}{c} 5 + 3 \times 7 + 6 \times 7^2 \\ + \\ 3 + 1 \times 7 + 2 \times 7^2 \\ \hline 1 + 5 \times 7 + 1 \times 7^2 + 1 \times 7^3 \\ \hline \end{array}$$

$320 - 108 = 422$ *given as*

$$\begin{array}{c} 5 + 3 \times 7 + 6 \times 7^2 \\ - \\ 3 + 1 \times 7 + 2 \times 7^2 \\ \hline \end{array}$$

$$2 + 2 \times 7 + 4 \times 7^2$$

$$- - - - - - - - - - - - - - - - - - -$$

Also, $320 \times 108 = 202521$ *given as*

$$\begin{array}{r} 5 + 3 \times 7 + 6 \times 7^2 \\ \times \quad 3 + 1 \times 7 + 2 \times 7^2 \\ \hline - \\ 1 + 4 \times 7 + 5 \times 7^2 + 2 \times 7^3 \\ 5 \times 7 + 3 \times 7^2 + 6 \times 7^3 \\ 3 \times 7^2 + 0 \times 7^3 + 6 \times 7^4 + 1 \times 7^5 \\ \hline - \\ 1 + 2 \times 7 + 5 \times 7^2 + 2 \times 7^3 + 0 \times 7^4 + 2 \times 7^5 \\ \hline - \end{array}$$

Also,

$$\begin{array}{r} \frac{302}{108} = \ldots.244 \\ 3 + 1 \times 7 + 2 \times 7^2 \;)\; 5 + 3 \times 7 + 6 \times 7^2 \;(\; 4 + 4 \times 7 + 2 \times 7^2 \\ 5 + 5 \times 7 + 1 \times 7^2 + 1 \times 7^3 \\ \hline - \\ 5 \times 7 + 4 \times 7^2 + 6 \times 7^3 + 6 \times 7^4 + \cdots \\ 5 \times 7 + 5 \times 7^2 + 1 \times 7^3 + 1 \times 7^4 \\ \hline - \\ 6 \times 7^2 + 4 \times 7^3 + 6 \times 7^4 + \cdots \\ 6 \times 7^2 + 2 \times 7^3 + 4 \times 7^4 \\ \hline - \\ 2 \times 7^3 + 0 \times 7^4 + 6 \times 7^5 + \cdots \\ \hline - \end{array}$$

3. Elliptic curves $E(Q_p)$ over p-adic field Q_p and points in $E(Q_p)(mod\ p^n)$ for $n > 1$

In the context of studying point addition on $E(Q_p)$, we have to study the relation between the points in $E(Q_p)$ and the points in $E(F_p)$. We first proceed to study the reduction of points on $E(Q_p)$ to $modp$. for any element $\tilde{x} \in Z_p$, there is a natural reduction $\tilde{x} \to x$ from $Z_p \to F_p$. But, such reduction cannot be extended from Q_p to F_p as reduction is not injection whereas any ring homomorphism from Q_p would always be an injection. Therefore, an elliptic curve over Q_p in general cannot be reduced to F_p . But, note as for any $x \in Z_p$, as x can be reduced to an element in F_p naturally, to reduce an elliptic curve over Q_p, we need to consider $E(Q_p)$ to be defined over Z_p

For an elliptic curve defined over Z_p, the point $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in E(Q_p)$ defined over Z_p is such that either $(\tilde{\alpha}, \tilde{\beta}) \in Z_p \times Z_p$ or $(\tilde{\alpha}, \tilde{\beta}) \notin Z_p \times Z_p$ i.e., $(\tilde{\alpha}, \tilde{\beta}) \in Z_p \times Q_p$ or $(\tilde{\alpha}, \tilde{\beta}) \in Q_p \times Z_p$ or $(\tilde{\alpha}, \tilde{\alpha}) \in Q_p \times Q_p$. Note for $(\tilde{\alpha}, \tilde{\beta}) \in Z_p \times Z_p$, we have $\tilde{\alpha} = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots$ and $\tilde{\beta} = \beta_0 + \beta_1 p + \beta_2 p^2 + \ldots$, Note there is a natural reduction to $F_p(modp)$ i.e., $(\tilde{\alpha}, \tilde{\beta}) \to (\alpha_0, \beta_0)$ from $E(Q_p) \to E(F_p)$.

Note for $(\tilde{\alpha}, \tilde{\beta}) \notin Z_p \times Z_p$, we consider the corresponding projective co-ordinates of

$$\tilde{P} = [A : B : \Gamma] \ni A, B, \Gamma \in Z_p$$

and obtain natural reduction $\tilde{P} \to P$ from $E(Q_p) \to E(F_p)$.

Hence, for an elliptic curve $E(Q_p)$ defined over Z_p, its points can always be reduced to points in $E(F_p)$, the elliptic curve over a finite field F_p. However if our elliptic curve $E(Q_p)$ is not defined over Z_p, there is an elliptic curve $E'(Q_p)$ such that $E' \cong E$ where E' is the elliptic curve defined over Z_p i.e., the coefficients of curve $E(Q_p)$ are in Z_p under the mapping $(\alpha, \beta) \to (v^{-2}\alpha, v^{-3}\beta)$.

Hence for further study, without loss of generality, we consider $E(Q_p)$ is always defined over Z_p.

Definition 3.1. (Lift of a point). *The set of all lifts of points from F_p to Z_p is denoted as $L(F_p)$. For any $(x_0, y_0) \in F_p \times F_p$, the point $(\alpha, \beta) = (\tilde{x}, \tilde{y}) \in Z_p \times Z_p$ is called a lift of a point (x_0, y_0) from F_p to Z_p and is defined as*

$L(F_p) = \{(\tilde{x}, \tilde{y}) \in Z_p \times Z_p / \tilde{x} = x_0 + x_1 p + x_2 p^2 + \ldots and \tilde{y} = y_0 + y_1 p + y_2 p^2 + \ldots \text{ with } (x_0, y_0) \in F_p \times F_p\}$

Definition 3.2. *The set of all lifts of points on elliptic curve over finite field F_p is given as for any $(\alpha, \beta) = (x_0, y_0) \in E(F_p)$ the point $(\tilde{x}, \tilde{y}) \in E(Q_p)$ is called a lift of a point (x_0, y_0) from $E(F_p)$ to $E(Q_p)$ and is defined as*

$L\left(E(F_p)\right) = \{(\tilde{x}, \tilde{y}) \in Z_p \times Z_p / \tilde{x} = x_0 + x_1 p + x_2 p^2 + \cdots \quad and \quad \tilde{y} = y_0 + y_1 p + y_2 p^2 + \cdots \quad with \ (x_0, y_0) \in E(F_p) \ and \ \tilde{y}^2 = \tilde{x}^3 + A\tilde{x} + B\}$

Now in the following theorems, we describe the points in $E(Q_p)$ defined over Z_p as as lift of each point $(x_0, y_0) \in E(F_p)$.

Theorem 3.1. Let E be an elliptic curve over Q_p defined over Z_p then each point in $E(F_p)$ is a reduction of a point in $E(Q_p)$.

Proof. By definition,

$$E(Q_p) = \{(\alpha, \beta) \in Q_p \times Q_p / \beta^2 = \alpha^3 + A\alpha + B\} \cup \{\tilde{\mathcal{O}}\}$$

$$and$$

$$E(F_p) = \{(\alpha, \beta) \in F_p \times F_p / \beta^2 = \alpha^3 + A\alpha + B\} \cup \{\tilde{\mathcal{O}}\}$$

Let $P = (x_0, y_0)$ be a point in $E(F_p)$ such that $P \neq \mathcal{O}$, then for $P = (x_0, y_0)$ we have $y_0^2 = x_0^3 + Ax_0 + B$.
Now to find $\tilde{P}$ lift of P such that $\tilde{P} \in E(Q_p)$.

Let $\tilde{P} = (\tilde{x}, \tilde{y}) \in Z_p \times Z_p$ be a lift of $P = (x_0, y_0)$, then we have $\tilde{x}, \tilde{y}$ are p-adic integers having the form

$$\tilde{x} = x_0 + x_1 p + x_2 p^2 + \ldots$$

$$\tilde{y} = y_0 + y_1 p + y_2 p^2 + \ldots$$

with $x_0, y_0, x_1, y_1, x_2, y_2, \ldots \in F_p$. Now if $\tilde{P} = (\tilde{x}, \tilde{y}) \in E(Q_p)$ then $\tilde{y}^2 = \tilde{x}^3 + A\tilde{x} + B$, i.e., for $\tilde{P} = (x_0 + px_1 + p^2x_2 + \ldots, y_0 + py_1 + p^2y_2 + \ldots)$ we have

$(y_0 + y_1p + y_2p^2 + \ldots)^2 = (x_0 + x_1p + x_2p^2 + \ldots)^3 + A(x_0 + x_1p + x_2p^2 + \ldots) + B$

$y_0^2 + y_1^2p^2 + 2y_0y_1p + p^2t = x_0^3 + 3x_0^2x_1p + 3x_0x_1^2p^2 + p^3x_1^3 + Ax_0 + Apx_1 + B + p^2k$

let $\widetilde{P_1}$ be the lift of P modulo p^2 given as $\widetilde{P_1} = (\tilde{x}_1, \tilde{y}_1)$ with

$$\tilde{x}_1 = x_0 + x_1p$$

$$\tilde{y}_1 = y_0 + y_1p$$

note $\tilde{P}_1 \in E(Q_p)(mod\ p^2)$

$$y_0^2 + y_1^2p^2 + 2y_0y_1p = x_0^3 + 3x_0^2x_1p + 3x_0x_1^2p^2 + p^3x_1^3 + Ax_0 + Apx_1 + B$$

$$y_0^2 + 2py_0y_1 \equiv x_0^3 + 3x_0^2x_1p + Ax_0 + Apx_1 + B(mod\ p^2)$$

Now as $(x_0, y_0) \in E(F_p)$ note $y_0^2 = x_0^3 + Ax_0 + B$, substituting in above equation, we have

$$2py_0y_1 \equiv 3x_0^2x_1p + Apx_1(mod\ p^2)$$

As x_0, y_0 are known, we can obtain y_1 in terms of x_1 by assigning values for x_1 in F_p , Therefore

$$y_1 \equiv (2py_0)^{-1}(3x_0^2x_1p + Apx_1)(mod\ p^2)$$

$$\widetilde{P_1} = (\tilde{x}_1, \tilde{y}_1) = (x_0 + x_1p, y_0 + y_1p) = \left(x_0 + px_1, y_0 + p(2py_0)^{-1}(3x_0^2x_1p + Apx_1)\right)(mod\ p^2)$$

Note $\tilde{y}_1^2 = \tilde{x}_1^3 + A\tilde{x}_1 + B(mod\ p^2)$

Consider $(\tilde{y}_1)^2 = \left(y_0 + p(2py_0)^{-1}(3x_0^2x_1p + Apx_1)\right)^2 \equiv (\tilde{y})^2(mod\ p^2)$

But note we have

$$\begin{aligned}
\tilde{x}_1^3 + A\tilde{x}_1 + B &= (x_0 + x_1p)^3 + A(x_0 + x_1p) + B \\
&= x_0^3 + x_1^3p^3 + 3p^2x_0x_1^2 + 3px_0^2x_1 + Ax_0 + Apx_1 + B \\
&\equiv x_0^3 + Ax_0 + B(mod\ p^2) \\
&\equiv y_0^2(mod\ p^2) \\
&\equiv (\tilde{y})^2(mod\ p^2)
\end{aligned}$$

Therefore, $\tilde{y}_1^2 = \tilde{x}_1^3 + A\tilde{x}_1 + B(mod\ p^2)$.

Hence, $(\tilde{x}_1, \tilde{y}_1)$ satisfies the given curve $\beta^2 = \alpha^3 + A\alpha + B(mod\ p^2)$, Now repeating the above argument for $mod\ p^3$ and using $(\tilde{x}_1, \tilde{y}_1) \in E(Q_p)(mod\ p^2)$. let $\widetilde{P_2}$ be the lift of P modulo p^3 given as $\widetilde{P_2} = (\tilde{x}_2, \tilde{y}_2)$ with

$$\tilde{x}_2 = x_0 + x_1p + x_2p^2$$

$$\tilde{y}_2 = y_0 + y_1p + y_2p^2$$

note $\tilde{P}_2 \in E(Q_p)(mod\ p^3)$

As x_0, x_1, y_0, y_1 are known, we can obtain y_2 in terms of x_2 by assigning values for x_2 in F_p . Also

we can see that $(\tilde{x}_2, \tilde{y}_2)$ satisfies the given curve $\beta^2 = \alpha^3 + A\alpha + B$ modulo p^3. Proceeding so on, let $\tilde{P}_i$ be the lift of P modulo p^{i+1} given as $\tilde{P}_i = (\tilde{x}_i, \tilde{y}_i)$ with

$$\tilde{x}_i = x_0 + x_1 p + x_2 p^2 + \ldots + x_i p^i$$

$$\tilde{y}_i = y_0 + y_1 p + y_2 p^2 + \ldots + y_i p^i$$

note $\tilde{P}_2 \in E(Q_p)(mod\ p^{i+1})$

As $x_0, x_1, \ldots x_{i-1}, y_0, y_1, \ldots y_{i-1}$ are known, we can obtain y_i in terms of x_i by assigning values for x_i in F_p . Also we can see that $(\tilde{x}_i, \tilde{y}_i)$ satisfies the given curve $\beta^2 = \alpha^3 + A\alpha + B$ modulo p^{i+1}.

Hence, $(\tilde{x}, \tilde{y}) = (x_0 + px_1 + p^2 x_2 + \ldots, y_0 + py_1 + p^2 y_2 + \ldots)$ satisfies the curve $\beta^2 = \alpha^3 + A\alpha + B$. i.e., the lift $\tilde{P}$ of P is in $E(Q_p)$.

Therefore, for $P \neq \mathcal{O} \in E(F_p)$ there lies a lift $\tilde{P}$ in $Z_p \times Z_p$ such that $\tilde{P} \in E(Q_p)$, with reduction of $\tilde{P}$ is P itself.

Hence, for all $P \in E(F_p)$ such that $P \neq \mathcal{O}$, P is the reduction of some $\tilde{P} \in E(Q_p)$ with $\tilde{P}$ in $Z_p \times Z_p$.

Now for $P = \mathcal{O}$, the lift of point at infinity $\mathcal{O}$ can be obtained by considering the corresponding elliptic curve involving Z-coordinate is as $Y^2 Z = X^3 + AXZ^2 + BZ^3$. Now considering the point at infinity $\mathcal{O} = [0:1:0]$ which is an equivalence class of points $(0, k, 0)$. We have for $\mathcal{O}$ as $(0, k, 0)$, the lift of $P = \mathcal{O} = (0, k, 0)$ is given as

$$\tilde{P} = [\tilde{X}, \tilde{Y}, \tilde{Z}] = (0 + X_1 p + X_2 p^2 + \ldots, k + Y_1 p + Y_2 p^2 + \ldots, 0 + Z_1 p + Z_2 p^2 + \ldots)$$

such that $\tilde{P}$ satisfies the curve $Y^2 Z = X^3 + AXZ^2 + BZ^3$. Hence, we have

$$(k + Y_1 p + Y_2 p^2 + \ldots)^2 (0 + Z_1 p + Z_2 p^2 + \ldots) =$$
$$(0 + X_1 p + X_2 p^2 + \ldots)^3 + A(0 + X_1 p + X_2 p^2 + \ldots)(0 + Z_1 p + Z_2 p^2 + \ldots)^2 + B(0 + Z_1 p + Z_2 p^2 + \ldots)^3$$

On reducing $mod p^2$, we have

$$(k + Y_1 p)^2 (0 + Z_1 p) = (0 + X_1 p)^3 + A(0 + X_1 p)(0 + Z_1 p)^2 + B(0 + Z_1 p)^3 (mod\ p^2)$$

$$(k^2 + Y_1^2 p^2 + 2kY_1 p) Z_1 p \equiv X_1^3 + AX_1 Z_1 p^2 + BZ_1 p^3 (mod\ p^2)$$

$$k^2 Z_1 p \equiv 0 (mod\ p^2)$$

$$Z_1 p \equiv 0 (mod\ p^2)$$

$$Z_1 \equiv 0 (mod\ p)$$

Also, note $Z_1 \equiv 0 (mod\ p) \Rightarrow X_1 \equiv 0 (mod\ p)$

Therefore, substituting in $\tilde{P}$ we have for $\tilde{P}(mod\ p^2) = \tilde{P}_1$ say $\Rightarrow \tilde{P}_1 = (0, k + pY_1, 0)(mod\ p^2)$

Proceeding as above for $mod\ p^3$, we have

$$\tilde{P}_2 = (0, k + Y_1 p + Y_2 p^2, 0)(mod\ p^3)$$

On continuing so on, we have $Z_n \equiv 0 (mod\ p)$ for $n = 0,1,2,\ldots$ Hence,

$$\tilde{P} = (0, k + Y_1 p + Y_2 p^2 + \ldots, 0)$$

$$= (0, 1 + Y_1 p + Y_2 p^2 + \ldots, 0)$$

Therefore,

$$\tilde{P} = [\tilde{X}, \tilde{Y}, \tilde{Z}] = (0,1 + Y_1 p + Y_2 p^2 + \ldots, 0)$$

for all $Y_i \in F_p$ are the lifts of point at infinity $\mathcal{O} \in E(F_p)$ and is denoted as $\tilde{\mathcal{O}}$. Therefore, for $P = \mathcal{O} \in E(F_p)$, there exists the lift $\tilde{\mathcal{O}} \in E(Q_p)$ such that $\mathcal{O}$ is the reduction of a point $\tilde{\mathcal{O}} \in E(Q_p)$.
Therefore, each point in $E(F_p)$ is a reduction of a point in $E(Q_p)$.

Theorem 3.2. Let E be an elliptic curve over Q_p defined over Z_p then each point in $E(Q_p)$ defined over Z_p is a lift of a point in $E(F_p)$.

Proof. By definition

$$E(Q_p) = \{(\alpha, \beta) \in Q_p \times Q_p / \beta^2 = \alpha^3 + A\alpha + B\} \cup \{\tilde{\mathcal{O}}\}$$

$$and$$

$$E(F_p) = \{(\alpha, \beta) \in F_p \times F_p / \beta^2 = \alpha^3 + A\alpha + B\} \cup \{\tilde{\mathcal{O}}\}$$

Now, note for any point $\tilde{P} = (\tilde{x}, \tilde{y}) \in E(Q_p)$ then we have two cases.
(i) $\tilde{P} \in Z_p \times Z_p$ (ii) $\tilde{P} \notin Z_p \times Z_p$.
case (i): for $\tilde{P} \in Z_p \times Z_p$, we have

$$\tilde{P} = (x_0 + px_1 + p^2 x_2 + \ldots, y_0 + py_1 + p^2 y_2 + \ldots)$$

Reduction of $\tilde{P}$ is $\tilde{P}(mod\ p) = (x_0, y_0) \in E(F_p)$ Hence, $\tilde{P}$ is a lift of $(x_0, y_0) \in E(F_p)$.
case(ii): if $\tilde{P} \notin Z_p \times Z_p$ then we have either both $\tilde{x}, \tilde{y} \notin Z_p$ or exactly one of $\tilde{x}, \tilde{y}$ is in Z_p.
Now for $\tilde{P} = (\tilde{x}, \tilde{y})$ with both $\tilde{x}, \tilde{y} \notin Z_p$, $\tilde{P}$ is the lift of point at infinity $\mathcal{O} \in E(F_p)$, follows from [8].
Now for $\tilde{P} \notin Z_p \times Z_p$ with exactly one of $\tilde{x}, \tilde{y}$ is in Z_p then we have$(\tilde{x}, \tilde{y})$ such that either $\tilde{x} \in Z_p, \tilde{y} \notin Z_p$ or $\tilde{x} \notin Z_p, \tilde{y} \in Z_p$.
then, if $\tilde{P}$ is not reduction of point at infinity $\mathcal{O} \in E(F_p)$ then $\tilde{P}$ reduction is of the form $[X, Y, Z]$ with $Z \neq 0 \Rightarrow (X, Y, Z) = (x, y, 1)$
$\Rightarrow \tilde{P}$ is the lift of $(\alpha, \beta) \in E(F_p)$, then note $(\tilde{x}, \tilde{y})$ is a lift of $(\alpha, \beta) \in E(F_p)$. But any lift of $(\alpha, \beta) \in E(F_p)$ are in $Z_p \times Z_p$, which is a contradiction.
Hence, there are no $\tilde{P} \in E(Q_p)$ such that $\tilde{P} = (\tilde{x}, \tilde{y}) \notin Z_p \times Z_p$ such that exactly one of $\tilde{x}, \tilde{y} \notin Z_p$.
Hence, for all $\tilde{P} \in E(Q_p)$, $\tilde{P}$ is a lift of a point P in $E(F_p)$.

Remark 5. We can obtain all the points in $E(Q_p)$ by starting with points in $E(F_p)$ and lifting each point in $E(F_p)$ to $E(Q_p)(mod\ p^2)$ as described in theorem 3.1 and lifting of each point in $E(Q_p)(mod\ p^2)$ to $E(Q_p)(mod\ p^3)$ and so on. The lifting of points from $E(F_p)$ to obtain points in $E(Q_p)$ is depicted in the following figure 2.

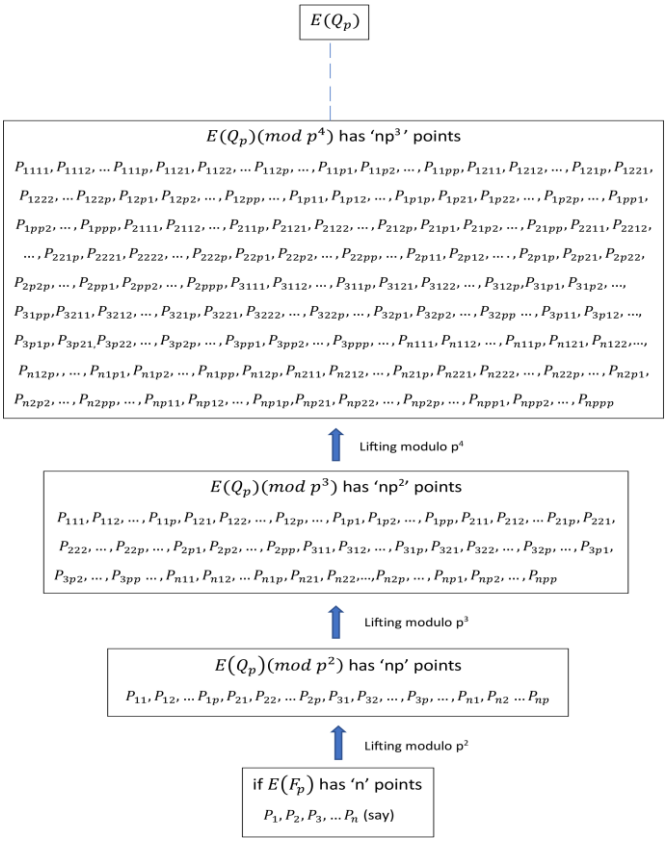

Figure 2: Flowchart for points in $E(Q_p)$

The points in $E(Q_p)(mod\ p^2)$ which are obtained by lifting of points in $E(F_p)$ are given in the following example for $p = 5$.

Example 3.1. *Consider the elliptic curve* $y^2 = x^3 + x + 1$ *, then we have*

$$E(F_5) = \{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4)(4,2), (4,3)\} \cup \{\mathcal{O}\}$$

A lift of any point in $E(F_5)$ *to a point in* $Z_5 \times Z_5(mod 5^2)$ *is given as in the following process:*

Let $P = (2,1) \in E(F_5)$. *Lift* $P(2,1)$ *to* $\tilde{P} = (2 + px_1, 1 + py_1)(mod 5^2)$, $0 \leq x_1, y_1 < 5$

then $\tilde{P} \in E(Q_5)(mod 5^2)$ *then as P satisfies* $y^2 = x^3 + x + 1$ *, note*

$$(1 + py_1)^2 = (2 + px_1)^3 + 2 + px_1 + 1(mod 5^2)$$

Now expressing y_1 *in terms of* x_1*, we have*

$$y_1 \equiv x_1 + 4(mod 5)$$

Substituting for y_1 *in* $\tilde{P} = (2 + px_1, 1 + py_1)(mod 5^2)$*, we have*

$$\tilde{P} = (2 + 5x_1, 21 + 5x_1)(mod 5^2)$$

Each point in $E(F_5)$ *may be lifted in a similar manner to obtain points in* $E(Q_5)(mod 5^2)$ *as given in the table below.*

Points in $\boldsymbol{E(F_5)}$	***Lifting point in*** $\boldsymbol{E(Q_5)(mod5^2)}$
$P_1 = (0,1)$	$(5x_1, 1 + 3x_1.5)(mod5^2)$
$P_2 = (0,4)$	$(5x_1, 4 + (2x_1 + 4).5)(mod5^2)$
$P_3 = (2,1)$	$(2 + 5x_1, 1 + (4x_1 + 1).5)(mod5^2)$
$P_4 = (2,4)$	$(2 + 5x_1, 4 + (x_1 + 3).5)(mod5^2)$
$P_5 = (3,1)$	$(3 + 5x_1, 1 + (3 + 4x_1).5)(mod5^2)$
$P_6 = (3,4)$	$(3 + 5x_1, 4 + (x_1 + 1).5)(mod5^2)$
$P_7 = (4,2)$	$\big(4 + 5x_1, 2 + 5(2 + x_1)\big)(mod5^2)$
$P_8 = (4,3)$	$(4 + 5x_1, 3 + (2 + 4x_1).5)(mod5^2)$
$\mathcal{O}$	$\tilde{\mathcal{O}}$

Representation of lifting of points $P_1, P_2, \dots P_8$ in $E(F_5)$ to $E(Q_5)(mod\ 5^2)$

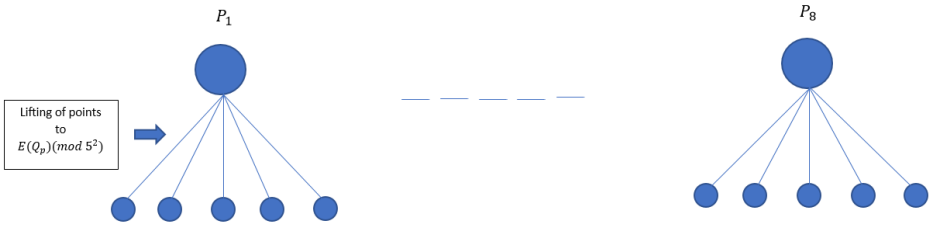

Figure 3: Lifting of Points in $E(F_5)$ to $E(Q_5)(mod\ 5^2)$

Assigning $x_1 = 0,1,2,3,4$ *in the above table, we have all lifting points in* $E(Q_5)(mod5^2)$ *in the following table.*

Lifting point in $\boldsymbol{E(Q_5)(mod5^2)}$	$\boldsymbol{x_1 = 0}$	$\boldsymbol{x_1 = 1}$	$\boldsymbol{x_1 = 2}$	$\boldsymbol{x_1 = 3}$	$\boldsymbol{x_1 = 4}$
$(5x_1, 1 + 3x_1.5)(mod5^2)$	$(0,1)$	$(1.5,1 + 3.5)$	$(2.5,1 + 1.5)$	$(3.5,1 + 4.5)$	$(4.5,1 + 2.5)$
$(5x_1, 4 + (2x_1 + 4).5)(mod5^2)$	$(0,4 + 4.5)$	$(1.5,4 + 1.5)$	$(2.5,4 + 3.5)$	$(3.5,4)$	$(4.5,4 + 2.5)$
$(2 + 5x_1, 1 + (4x_1 + 1).5)(mod5^2)$	$(2,1 + 1.5)$	$(2 + 1.5,1)$	$(2 + 2.5,1 + 4.5)$	$(2 + 3.5,1 + 3.5)$	$(2 + 4.5,1 + 2.5)$
$(2 + 5x_1, 4 + (x_1 + 3).5)(mod5^2)$	$(2,4 + 3.5)$	$(2 + 1.5,4 + 4.5)$	$(2 + 2.5,4)$	$(2 + 3.5,4 + 1.5)$	$(2 + 4.5,4 + 2.5)$

Lifting point in $E(Q_5)(mod5^2)$	$x_1 = 0$	$x_1 = 1$	$x_1 = 2$	$x_1 = 3$	$x_1 = 4$
$(3 + 5x_1, 1 + (3 + 4x_1).5)(mod5^2)$	$(3,1 + 3.5)$	$(3 + 1.5,1 + 2.5)$	$(3 + 2.5,1 + 1.5)$	$(3 + 3.5,1)$	$(3 + 4.5,1 + 4.5)$
$(3 + 5x_1, 4 + (x_1 + 1).5)(mod5^2)$	$(3,4 + 1.5)$	$(3 + 1.5,4 + 2.5)$	$(3 + 2.5,4 + 3.5)$	$(3 + 3.5,4 + 4.5)$	$(3 + 4.5,4)$
$(4 + 5x_1, 2 + 5(2 + x_1))(mod5^2)$	$(4,2 + 2.5)$	$(4 + 1.5,2 + 3.5)$	$(4 + 2.5,2 + 4.5)$	$(4 + 3.5,2)$	$(4 + 4.5,2 + 1.5)$
$(4 + 5x_1, 3 + (2 + 4x_1).5)(mod5^2)$	$(4,3 + 2.5)$	$(4 + 1.5,3 + 1.5)$	$(4 + 2.5,3)$	$(4 + 3.5,3 + 4.5)$	$(4 + 4.5,3 + 3.5)$
$\tilde{O}$	$\tilde{O}$	$\tilde{O}$	$\tilde{O}$	$\tilde{O}$	$\tilde{O}$

In order to obtain the lift points $E(Q_5)(mod5^3)$, we repeat the above process for considered point in $E(Q_5)(mod5^2)$ and obtain all lifts in $E(Q_5)(mod5^3)$. On repeating in such a manner, we can obtain lift points in $E(Q_5)(mod5^n)$ for any positive integer n. The lifting of points from $E(F_5)$ to $E(Q_5)(mod5^3)$ are represented pictorially in fig 4.

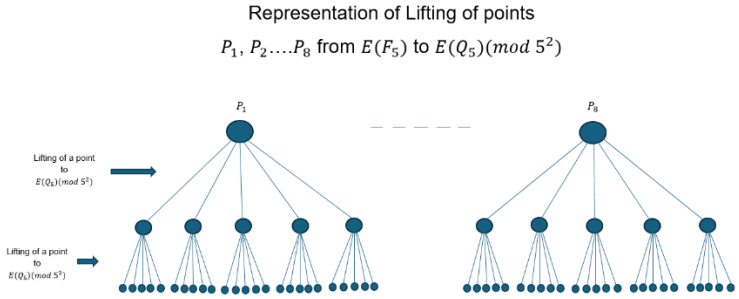

Figure 4: Lifting of Points in $E(F_5)$ to $E(Q_5)(mod\ 5^2)$

The table below shows the difference in number of points from $E(F_5)$ to $E(Q_5)(mod\ 5^2)$ which provides large key space for cryptographic purpose.

Points in $E(F_5)$	*Points in* $E(Q_5)(mod\ 5^2)$				
$(0,1)$	$(0,1)$	$(1.5,1 + 3.5)$	$(2.5,1 + 1.5)$	$(3.5,1 + 4.5)$	$(4.5,1 + 2.5)$
$(0,4)$	$(0,4 + 4.5)$	$(1.5,4 + 1.5)$	$(2.5,4 + 3.5)$	$(3.5,4)$	$(4.5,4 + 2.5)$
$(2,1)$	$(2,1 + 1.5)$	$(2 + 1.5,1)$	$(2 + 2.5, 1 + 4.5)$	$(2 + 3.5,1 + 3.5)$	$(2 + 4.5,1 + 2.5)$

Points in $E(F_5)$	*Points in* $E(Q_5)(\text{mod } 5^2)$				
$(2,4)$	$(2,4 + 3.5)$	$(2 + 1.5,4 + 4.5)$	$(2 + 2.5,4)$	$(2 + 3.5,4 + 1.5)$	$(2 + 4.5,4 + 2.5)$
$(3,1)$	$(3,1 + 3.5)$	$(3 + 1.5,1 + 2.5)$	$(3 + 2.5,1 + 1.5)$	$(3 + 3.5,1)$	$(3 + 4.5,1 + 4.5)$
$(3,4)$	$(3,4 + 1.5)$	$(3 + 1.5,4 + 2.5)$	$(3 + 2.5,4 + 3.5)$	$(3 + 3.5,4 + 4.5)$	$(3 + 4.5,4)$
$(4,2)$	$(4,2 + 2.5)$	$(4 + 1.5,2 + 3.5)$	$(4 + 2.5,2 + 4.5)$	$(4 + 3.5,2)$	$(4 + 4.5,2 + 1.5)$
$(4,3)$	$(4,3 + 2.5)$	$(4 + 1.5,3 + 1.5)$	$(4 + 2.5,3)$	$(4 + 3.5,3 + 4.5)$	$(4 + 4.5,3 + 3.5)$
$\mathcal{O}$	$\tilde{\mathcal{O}}$	$\tilde{\mathcal{O}}$	$\tilde{\mathcal{O}}$	$\tilde{\mathcal{O}}$	$\tilde{\mathcal{O}}$

4. Implementing Arithmetic of points on elliptic curve $E(Q_p)$ over p-adic field Q_p to $E(Q_p)(mod\ p^2)$

In the context of improvising the efficiency of cryptosystems with elliptic curves, the purpose of studying arithmetic of points in elliptic curves $E(Q_p)$ over p-adic field Q_p is necessary. To study arithmetic of points in $E(Q_p)$, we first study arithmetic of points in $E(Q_p)\ (mod\ p^2)$ by extending arithmetic of points in $E(F_p)$ and then the arithmetic of points in $E(Q_p)\ (mod\ p^3)$ by extending arithmetic of points in $E(Q_p)\ (mod\ p^2)$ and so on. In this section, we have derived formula for arithmetic of points in $E(Q_p)(mod\ p^2)$ and had given an algorithm along with code in Python language.

Now, to implement the arithmetic of points on elliptic curve $E(Q_p)$ over Q_p to $E(Q_p)\ (mod\ p^2)$, if$E(\kappa)$ is an elliptic curve defined over a field κ with $Char\kappa \neq 2,3$, given as

$$E:\ \beta^2 = \alpha^3 + A\alpha + B$$

then for $P_1 = (\alpha_1, \beta_1)$ and $P_2 = (\alpha_2, \beta_2)$ in $E(\kappa)$, the point addition of P_1 and P_2 denoted as $P_1 + P_2$ and is given as

$$P_1 + P_2 = \begin{cases} (m^2 - \alpha_1 - \alpha_2, m(\alpha_1 - \alpha_3) - \beta_1) \quad \text{with} \quad m = \frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1} \quad \text{if} \quad P_1 \neq P_2 \\ (m^2 - 2\alpha_1,\ m(\alpha_1 - \alpha_3) - \beta_1) \quad \text{with} \quad m = \frac{3\alpha_1^2 + A}{2\beta_1} \quad \text{if} \quad P_1 = P_2 \end{cases} \text{---------- (1)}$$

Now, In particular for $K = Q_p$, the p-adic field For an elliptic curve E over Q_p defined over Z_p, the points $\tilde{P}_1$ and $\tilde{P}_2$ are given as

$$\tilde{P}_1 = (\tilde{x}_1, \tilde{y}_1) = (x_{10} + x_{11}p + x_{12}p^2 + \ldots, y_{10} + y_{11}p + y_{12}p^2 + \ldots)$$

$$and$$

$$\tilde{P}_2 = (\tilde{x}_2, \tilde{y}_2) = (x_{20} + x_{21}p + x_{22}p^2 + \ldots, y_{20} + y_{21}p + y_{22}p^2 + \ldots)$$

with each coordinate in its p-adic expansion and by the point addition in $E(Q_p)$, we have $\tilde{P}_1 + \tilde{P}_2 = \tilde{P}_3$ say with $\tilde{P}_3 = (\tilde{x}_3, \tilde{y}_3)$ given as

$$\tilde{P}_3 = (\tilde{x}_3, \tilde{y}_3) = (x_{30} + x_{31}p + x_{32}p^2 + \ldots, y_{30} + y_{31}p + y_{32}p^2 + \ldots)$$

The point $\tilde{P}_3$ could be known with the evaluation of x_{3i}'s and y_{3i}'s for all $i = 0,1,2, \ldots$. Now to obtain x_{3i}'s and y_{3i}'s for all $i = 0,1,2, \ldots$, we implement the arithmetic of points $\tilde{P}_1$ and $\tilde{P}_2$ in $E(Q_p)$ to the points $\tilde{P}_{1n}$ and $\tilde{P}_{2n}$ in $E(Q_p)(mod\ p^{n+1})$ and obtain x_{3i}'s and y_{3i}'s for all $i = 0,1,2, \ldots n$, 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}.

In particular, on considering $\tilde{P}_1$, $\tilde{P}_2$ to $mod\ p^2$, we have

$$\tilde{P}_{11} = (\tilde{x}_{11}, \tilde{y}_{11}) = (x_{10} + x_{11}p, y_{10} + y_{11}p) and \tilde{P}_{21} = (\tilde{x}_{21}, \tilde{y}_{21}) = (x_{20} + x_{21}p, y_{20} + y_{21}p)$$

Now we obtain the arithmetic of points $\tilde{P}_{11}$ and $\tilde{P}_{21}$ in $E(Q_p)(mod\ p^2)$ by implementing the point addition in $E(Q_p)$ and obtain $x_{30}, x_{31}, y_{30}, y_{31}$.

In the following theorem we describe the implementation of the arithmetic of points on elliptic curve $E(Q_p)$ defined over Z_p to $E(Q_p)$ $(mod\ p^2)$.

Theorem 4.1. Consider an elliptic curve $E(Q_p)$ defined over Z_p given as

$$E(Q_p): y^2 = x^3 + Ax + B$$

over Q_p defined over Z_p. For any points $\tilde{P}_1, \tilde{P}_2$ in $E(Q_p)$, the arithmetic of points $\tilde{P}_{11} = (\tilde{x}_{11}, \tilde{y}_{11}) = (x_{10} + x_{11}p, y_{10} + y_{11}p)$ and $\tilde{P}_{21} = (\tilde{x}_{21}, \tilde{y}_{21}) = (x_{20} + x_{21}p, y_{20} + y_{21}p)$ in $E(Q_p)(mod\ p^2)$ may be obtained by implementing the point addition of points $\tilde{P}_1, \tilde{P}_2$ in $E(Q_p)$ to the points $\tilde{P}_{11}, \tilde{P}_{21}$ in $E(Q_p)(mod\ p^2)$ and $\tilde{P}_{31}$is given as

$$\tilde{P}_{31} = \tilde{P}_{11} + \tilde{P}_{21} = (\tilde{x}_{31}, \tilde{y}_{31}) = (x_{30} + x_{31}p, y_{30} + y_{31}p)$$

such that

$$\begin{cases} x_{30} + x_{31}p \text{ is the } p\text{-adic expansion of } {x_{30}}' + {x_{31}}'p \text{ modulo } p^2 \\ y_{30} + y_{31}p \text{ is the } p\text{-adic expansion of } {y_{30}}' + {y_{31}}'p \text{ modulo } p^2 \end{cases}$$

where ${x_{30}}', {x_{31}}', {y_{30}}', {y_{31}}'$ given as follows

for $\tilde{P}_{11} \neq \tilde{P}_{21}$

$$\begin{cases} {x_{30}}' = m_0^2 + (p-1)(x_{10} + x_{20}) \\ {x_{31}}' = 2m_0m_1 + (p-1)(x_{10} + x_{11} + x_{20} + x_{21}) \\ {y_{30}}' = m_0x_{10} + (p-1)(m_0x_{30} + y_{10}) \\ {y_{31}}' = m_1x_{10} + m_0x_{11} + (p-1)(m_1x_{30} + m_0x_{30} + m_0x_{31} + y_{10} + y_{11}) \end{cases}$$

where $\widetilde{m}_1 = \frac{\tilde{y}_{21}-\tilde{y}_{11}}{\tilde{x}_{21}-\tilde{x}_{11}} = m_0 + m_1 p.$

for $\tilde{P}_{11} = \tilde{P}_{21}$

$$\begin{cases} x_{30}{}' = m_0^2 + (p-1)2x_{10} \\ x_{31}{}' = 2\big(m_0 m_1 + (p-1)(x_{10}+x_{11})\big) \\ y_{30}{}' = m_0 x_{10} + (p-1)(m_0 x_{30} + y_{10}) \\ y_{31}{}' = m_1 x_{10} + m_0 x_{11} + (p-1)(m_1 x_{30} + m_0 x_{30} + m_0 x_{31} + y_{10} + y_{11}) \end{cases}$$

where $\widetilde{m}_1 = \frac{3\tilde{x}_{11}^2 + A}{2\tilde{y}_{11}} = m_0 + m_1 p.$

Proof. Consider $\tilde{P}_{11} = (\tilde{x}_{11}, \tilde{y}_{11}) = (x_{10} + x_{11}p, y_{10} + y_{11}p)$ and $\tilde{P}_{21} = (\tilde{x}_{21}, \tilde{y}_{21}) = (x_{20} + a_{21}p, y_{20} + y_{21}p)$

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

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

$$\tilde{P}_{31} = \tilde{P}_{11} + \tilde{P}_{21} = (\widetilde{m}_1^2 - \tilde{x}_{11}^2 - \tilde{x}_{21}^2, \widetilde{m}_1(\tilde{x}_{11} - \tilde{x}_{31}) - \tilde{y}_{11})$$

The x-coordinate of $\tilde{P}_{31}$ is given as

$$x(\tilde{P}_{31}) = \widetilde{m}_1^2 - \tilde{x}_{11}^2 - \tilde{x}_{21}^2$$

$$= (m_0^2 + 2m_0 m_1 p) + \big((p-1) + (p-1)p\big)(x_{10} + x_{11}p) + \big((p-1) + (p-1)p\big)(x_{20} + x_{21}p)$$

$$= m_0^2 + 2m_0 m_1 p + (p-1)x_{10} + \big((p-1)(x_{10}+x_{11})\big)p + (p-1)x_{20} + \big((p-1)(x_{20}+x_{21})\big)p$$

$$= m_0^2 + (p-1)x_{10} + (p-1)x_{20} + 2m_0 m_1 p + \big((p-1)(x_{10}+x_{11})\big)p + \big((p-1)(x_{20}+x_{21})\big)p$$

$$= m_0^2 + (p-1)(x_{10}+x_{20}) + \big(2m_0 m_1 + (p-1)(x_{10}+x_{11}) + (p-1)(x_{20}+x_{21})\big)p$$

Therefore,

$$x_{30}{}' = m_0^2 + (p-1)(x_{10}+x_{20})$$

$$x_{31}{}' = 2m_0 m_1 + (p-1)(x_{10}+x_{11}+x_{20}+x_{21})$$

Now, by considering p-adic expansion of $x_{30}{}' + x_{31}{}'p$ modulo p^2, we have

$$x(\tilde{P}_{31}) = x_{30} + x_{31}p$$

The y-coordinate of $\tilde{P}_{31}$ is given as

$$y(\tilde{P}_{31}) = \widetilde{m}_1(\tilde{x}_{11} - \tilde{x}_{31}) - \tilde{y}_{11}$$

$$= (m_0 + m_1 p)\Big(x_{10} + x_{11}p + \big((p-1) + (p-1)p\big)(x_{30} + x_{31}p)\Big) + \Big(\big((p-1) + (p-1)p\big)(y_{10} + y_{11}p)\Big)$$

$$= (m_0 + m_1 p)\big(x_{10} + (p-1)x_{30} + \big(x_{11} + (p-1)(x_{30} + x_{31})\big)p\big) + (p-1)y_{10} + (p-1)(y_{10} + y_{11}))p$$

$$= m_0 x_{10} + (p-1)m_0 x_{30} + (m_1 x_{10} + m_0 x_{11} + (p-1)(m_1 x_{30} + m_0 x_{30} + m_0 x_{31})p) + (p-1)y_{10} + (p-1)(y_{10} + y_{11})$$

$$= m_0 x_{10} + (p-1)(m_0 x_{30} + y_{10}) + \big(m_1 x_{10} + m_0 x_{11} + (p-1)(m_1 x_{30} + m_0 x_{30} + m_0 x_{31} + y_{10} + y_{11})\big)p$$

Therefore,

$$y_{30}{}' = m_0 x_{10} + (p-1)(m_0 x_{30} + y_{10})$$

$$y_{31}{}' = m_1 x_{10} + m_0 x_{11} + (p-1)(m_1 x_{30} + m_0 x_{30} + m_0 x_{31} + y_{10} + y_{11})$$

Now, by considering p-adic expansion of $y_{30}{}' + y_{31}{}'p$ modulo p^2, we have

$$y\big(\tilde{P}_{31}\big) = y_{30} + y_{31}p$$

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

By the implementation of arithmetic of points $\tilde{P}_1, \tilde{P}_2$ in $E\big(Q_p\big)$ as in (1) to the points $\tilde{P}_{11}, \tilde{P}_{21}$ in $E\big(Q_p\big)(mod\ p^2)$, we have

$$\tilde{P}_{31} = \tilde{P}_{11} + \tilde{P}_{21} = (\tilde{m}_1^2 - 2\tilde{x}_{11}^2 - \tilde{x}_{21}^2, \tilde{m}_1(\tilde{x}_{11} - \tilde{x}_{31}) - \tilde{y}_{11})$$

The x-coordinate of $\tilde{P}_{31}$ is given as

$$x\big(\tilde{P}_{31}\big) = \tilde{m}_1^2 - 2\tilde{x}_{11}^2$$

$$= (m_0^2 + 2m_1 p) + 2\big((p-1) + (p-1)p\big)(x_{10} + x_{11}p)$$

$$= m_0^2 + 2m_0 m_1 p + 2(p-1)x_{10} + 2\big((p-1)(x_{10} + x_{11})\big)p$$

$$= m_0^2 + 2(p-1)x_{10} + 2m_0 m_1 p + 2\big((p-1)(x_{10} + x_{11})\big)p$$

$$= m_0^2 + 2(p-1)x_{10} + \big(2m_0 m_1 + 2(p-1)(x_{10} + x_{11})\big)p$$

Therefore,

$$x_{30}{}' = m_0^2 + 2(p-1)x_{10}$$

$$x_{31}{}' = 2\big(m_0 m_1 + (p-1)(x_{10} + x_{11})\big)$$

Now, by considering p-adic expansion of $x_{30}{}' + x_{31}{}'p$ modulo p^2, we have

$$x\big(\tilde{P}_{31}\big) = x_{30} + x_{31}p$$

The y-coordinate of $\tilde{P}_{31}$ is given as

$$y\big(\tilde{P}_{31}\big) = \tilde{m}_1(\tilde{x}_{11} - \tilde{x}_{31}) - \tilde{y}_{11}$$

which on repeating above process, we have

$$y_{30} = m_0x_{10} + (p-1)(m_0x_{30} + y_{10})$$

$$y_{31} = m_1x_{10} + m_0x_{11} + (p-1)(m_1x_{30} + m_0x_{30} + m_0x_{31} + y_{10} + y_{11})$$

Now, by considering p-adic expansion of $y_{30}' + y_{31}'p$ modulo p^2, we have

$$y(\tilde{P}_{31}) = y_{30} + y_{31}p$$

Field κ	**Elliptic curve**	**Slope m**		$\boldsymbol{P_{11} + P_{21} = P_{31}}$		
		$P_{11} \neq P_{21}$	$P_{11} = P_{21}$	$P_{11} \neq P_{21}$ with $\tilde{x}_{11} = \tilde{x}_{21}$	$P_{11} \neq P_{21}$ with $\tilde{x}_{11} \tilde{x}_{21}$	$P_{11} = P_{21}$
Char $\kappa \neq 2, 3$	$\beta^2 = \propto^3 + A \propto + B$	$\frac{\tilde{y}_{21} - \tilde{y}_{11}}{\tilde{x}_{21} - \tilde{x}_{11}}$	$\frac{3\tilde{x}_{11}^2 + A}{2\tilde{y}_{11}}$	$\begin{cases} x_{30}' = m_0^2 + (p-1)(x_{10} + \\ x_{31}' = 2m_0m_1 + (p-1)(x \\ y_{30}' = m_0x_{10} + (p-1)(m \\ y_{31}' = m_1x_{10} + m_0x_{11} + (p \end{cases}$	$\mathcal{O}$	$\begin{cases} x_{30}' = m_0^2 + (p-1)2x_{10} \\ x_{31}' = 2(m_0m_1 + (p-1)(x_{10} + x_{11} \\ y_{30}' = m_0x_{10} + (p-1)(m_0x_{30} + y_{3} \\ y_{31}' = m_1x_{10} + m_0x_{11} + (p-1)(m \end{cases}$

Table 2: Arithmetic of Points in $E(Q_p)(mod\ p^2$

Example 4.1. *For* $\tilde{P}_{11} = (4 + 2.5, 2 + 4.5)$ *and* $\tilde{P}_{21} = (2 + 1.5, 4 + 4.5)$ *then by above formulas, we have*

$$\begin{aligned} \tilde{P}_{11} + \tilde{P}_{21} &= (3.5 + (2 + 2.5)5, 4 + 4.5 + (3.5 + 1.5^2)5) \\ &= (3.5 + 2.5 + 2.5^2, 4 + 4.5 + 3.5^2 + 1.5^3) \\ &= (3.5^3, 4 + 4.5 + 3.5^2 + 1.5^3) \\ &= (0, 4 + 4.5)(mod 5^2) \end{aligned}$$

The step-by-step procedure for point addition on elliptic curve $E(Q_p)mod\ p^2$ over p-adic field Q_p defined over Z_p using addition and multiplication process as in Q_p was discussed below. The code for arithmetic of points in $E(Q_p)mod\ p^2$ and arithmetic operations of numbers in Q_p are included below.

Algorithm: The step-by-step procedure is termed as Algorithm.

Algorithm for Point Addition in $(Q_p)(mod\ p^2)$: Consider an Elliptic curve$\beta^2 = \alpha^3 + A\alpha + B$ over Q_p. Let $\tilde{P}_1, \tilde{P}_2$ be two points in $E(Q_p)$ then for $\tilde{P}_1$ and $\tilde{P}_2$ considered in $E(Q_p)(mod\ p^2)$ given as $\tilde{P}_{11} = (\tilde{x}_{11}, \tilde{y}_{11}) = (x_{10} + x_{11}p, y_{10} + y_{11}p)$ and $\tilde{P}_{21} = (x_{20} + x_{21}p, y_{20} + y_{21}p)$ respectively. The point addition $\tilde{P}_{11} + \tilde{P}_{21} = \tilde{P}_{31} = (x_{30} + x_{31}p, y_{30} + y_{31}p)$ in $E(Q_p)(mod\ p^2)$ is obtained by the steps in the following algorithm.

Step-I: Compute the slope $\tilde{m}_1 = m_0 + m_1 p$ of $\tilde{P}_{11}$ and $\tilde{P}_{21}$ given as

$$\tilde{m}_1 = \begin{cases} \dfrac{\tilde{y}_{21} - \tilde{y}_{11}}{\tilde{x}_{21} - \tilde{x}_{11}} \text{ for } \tilde{P}_{11} \neq \tilde{P}_{21} \\ \dfrac{3\tilde{x}_{11}^2 + A}{2\tilde{y}_{11}} \text{ for } \tilde{P}_{11} = \tilde{P}_{21} \end{cases}$$

Step-II: Compute $x_{30}', x_{31}', y_{30}', y_{31}'$ using formulas
For $\tilde{P}_{11} \neq \tilde{P}_{21}$:

$$\begin{cases} x_{30}' = m_0^2 + (p-1)(x_{10} + x_{20}), \\ x_{31}' = 2m_0 m_1 + (p-1)(x_{10} + x_{11} + x_{20} + x_{21}), \\ y_{30}' = m_0 x_{10} + (p-1)(m_0 x_{30} + y_{10}), \\ y_{31}' = m_1 x_{10} + m_0 x_{11} + (p-1)(m_1 x_{30} + m_0 x_{30} + m_0 x_{31} + y_{10} + y_{11}) \end{cases}$$

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

$$\begin{cases} x_{30}' = m_0^2 + (p-1)2x_{10}, \\ x_{31}' = 2\big(m_0 m_1 + (p-1)(x_{10} + x_{11})\big), \\ y_{30}' = m_0 x_{10} + (p-1)(m_0 x_{30} + y_{10}), \\ y_{31}' = m_1 x_{10} + m_0 x_{11} + (p-1)(m_1 x_{30} + m_0 x_{30} + m_0 x_{31} + y_{10} + y_{11}) \end{cases}$$

Step-III: To evaluate x_{30} and x_{31}, consider the value $N = x_{30}' + x_{31}' p$ and write the p-adic expansion of N and consider $N(mod\ p^2)$ to obtain x_{30} and x_{31}.
Step-IV: To evaluate y_{30} and y_{31}, consider the value $M = y_{30}' + y_{31}' p$ and write the p-adic expansion of M and consider $M(mod\ p^2)$ to obtain y_{30} and y_{31}.
Step-V: From the values of x_{30} and x_{31} in Step-III and y_{30} and y_{31} in Step-IV, the point addition $\tilde{P}_{11} + \tilde{P}_{21}$ is given as:

$$\tilde{P}_{31} = (x_{30} + x_{31}p, y_{30} + y_{31}p)$$

For an Elliptic curve $y^2 = x^3 + x + 1$ over $Q_{999983}(mod\ 999983^2)$, Consider two points $\tilde{P}_{11} = (371181 + 9738 \times 999983\ ,\ 209555 + 151202 \times 999983)$ and $\tilde{P}_{21} = (540108 + 4976 \times 999983\ ,\ 254286 + 183355 \times 999983)$ with slope of P_1 and P_2 given as $\tilde{m}' = 383473 + 214267 \times 999983$ and $\tilde{P}_{11} + \tilde{P}_{21} = \tilde{P}_{31}$ is given as

$$\tilde{P}_{31} = (130341 + 144599 \times 999983\ ,\ 997817 + 451277 \times 999983)$$

which is a lift of a point $(130341, 997817) \in E(F_p)$.
The code for addition, subtraction, multiplication and division of p-adic numbers and finding slope points in $E(Q_p)(mod\ p^2)$ and Arithmetic of Points in $E(Q_p)(mod\ p^2)$ were given below in Python.

```
# to initialize run this cell
from sage.all import *
# make same length
def pad_with_zeros(expansion, length):
    return expansion + [0] * (length - len(expansion))
# function to add
def add_p_adic(expansion1, expansion2, p):
    #ensure both expansions are of same lengh
    max_length = max(len(expansion1), len(expansion2))
    expansion1 = pad_with_zeros(expansion1, max_length)
    expansion2 = pad_with_zeros(expansion2, max_length)
    result = []
    carry = 0
    for digit1, digit2 in zip(expansion1, expansion2):
        total = digit1 + digit2 + carry
        result.append(total % p)
        carry = total // p
    if carry > 0:
        result.append(carry)
    return result
# function to subtract
def subtract_p_adic(expansion1, expansion2, p):
    # Ensure both expansions are of same length
    max_length = max(len(expansion1), len(expansion2))
    expansion1 = pad_with_zeros(expansion1, max_length)
    expansion2 = pad_with_zeros(expansion2, max_length)
    result = []
    borrow = 0
    for digit1, digit2 in zip(expansion1, expansion2):
        total = digit1 - digit2 - borrow
        if total < 0:
            total += p
```

```
            borrow = 1
        else:
            borrow = 0
        result.append(total)
    # Remove trailing zeros
    while result and result[-1] == 0:
        result.pop()
    return result
# Function to multiply
def multiply_p_adic(expansion1, expansion2, p):
    #ensure both expansions are of same length
    max_length = max(len(expansion1), len(expansion2))
    expansion1 = pad_with_zeros(expansion1, max_length)
    expansion2 = pad_with_zeros(expansion2, max_length)
    result = [0] * (2 * max_length)
    for i in range(max_length):
        carry = 0
        for j in range(max_length):
            total = expansion1[i] * expansion2[j] + result[i+j] +
carry
            result[i + j] = total % p
            carry = total // p
        result[i + max_length] += carry

    # Removing trailing zeros
    while len(result) > 1 and result[-1] == 0:
        result.pop()
    return result
def divide_p_adic(expansion1, expansion2, p):
    #ensure both expansions are of same length
    max_length = max(len(expansion1), len(expansion2))
    expansion1 = pad_with_zeros(expansion1, max_length)
    expansion2 = pad_with_zeros(expansion2, max_length)
```

```
    K = pAdicField(p,max_length)
    padic_number_a = sum(c * K(p**i) for i, c in
enumerate(expansion1))
    padic_number_b = sum(c * K(p**i) for i, c in
enumerate(expansion2))
    result = padic_number_a/padic_number_b
    expansion = result.expansion()
    coefficients = [int(coef) for coef in expansion]
    return coefficients
def to_p_adic(n, p, precision):
    if p<=1:
        raise ValueError("Base p must be a prime number greater
then 1.")
    if n == 0:
        return [0]
    digits = []
    while n != 0:
        digits.append(n % p)
        n //= p
    return digits[0:precision]
def print_expansion(value, base, coefficients, precision):
    print(f"The {base}-adic expansion of {value} is: ", end=' ')
    for i in range(min(precision, len(coefficients))):
        print(f"{coefficients[i]}*{base}^{i}", end=' ')
        if (i < min(precision, len(coefficients)) - 1):
            print(f"+", end=' ')
        else:
            print(" ")
def calculate_p3(x1, x2, y1, y2, p, A, B):
    max_length = max(len(x1), len(x2), len(y1), len(y2))
    x1 = pad_with_zeros(x1, max_length)
    x2 = pad_with_zeros(x2, max_length)
    y1 = pad_with_zeros(y1, max_length)
```

```
    y2 = pad_with_zeros(y2, max_length)
    precision = max_length
    x10 = x1[0]
    y10 = y1[0]
    x11 = x1[1]
    y11 = y1[1]
    x20 = x2[0]
    y20 = y2[0]
    x21 = x2[1]
    y21 = y2[1]
    # Cheking P1=P2
pointEquality = x10 == x20 and x11 == x21 and y10 == y20 and y11 ==
y21
    if pointEquality:
        print("P1 == P2")
        Kx = pAdicField(p,max_length)
        x_for_solpe = sum(c * Kx(p**i) for i, c in enumerate(x1))
        y_for_solpe = sum(c * Kx(p**i) for i, c in
enumerate(y1))
        m_out = ((3 * x_for_solpe^2 ) + A) / (2 * y_for_solpe)
        m_exp = m_out.expansion()
        m = [int(coef) for coef in m_exp]
    else:
        print("P1 != P2")
    m = divide_p_adic(subtract_p_adic(y2, y1, p),
    subtract_p_adic(x2, x1, p), p)
    m0 = m[0]
    m1 = m[1]
    print(f"m0: {m0}")
    print(f"m1: {m1}")
    # P1 + P2 = P3
    if not pointEquality:
x3 = (m0 ** 2) + (p - 1) * (x10 + x20) + 2 * m0 * m1 *
```

```
    p + (p * (p - 1) * (x10 + x11 + x20 + x21))
        print(f"x3 = {x3}")
        try:
            p_adic_expansion_x = to_p_adic(x3, p, precision)
            print_expansion(x3, p, p_adic_expansion_x, precision)
        except ValueError as e:
            print(e)
y3 = m0 * x10 + (p - 1) * (m0 * p_adic_expansion_x[0] + y10) +
p * (m1 * x10 + m0 * x11) + p * (p - 1) * (m1 *
p_adic_expansion_x[0] +
m0 * p_adic_expansion_x[0] + m0 * p_adic_expansion_x[1] + y10 +
y11)
        print(f"y3 = {y3}")
        try:
            p_adic_expansion_y = to_p_adic(y3, p, precision)
            print_expansion(y3, p, p_adic_expansion_y, precision)
        except ValueError as e:
            print(e)
        return p_adic_expansion_x, p_adic_expansion_y

    else:
x3 = m0 ** 2 + (p - 1) * 2 * x10 + 2 * p * (m1 + (p - 1) * (x10 +
x11))
        print(f"x3 = {x3}")
        try:
            p_adic_expansion_x = to_p_adic(x3, p, precision)
            print_expansion(x3, p, p_adic_expansion_x, precision)
        except ValueError as e:
            print(e)
y3 = m0 * x10 + (p - 1) * (m0 * p_adic_expansion_x[0] + y10) +
p * (m1 * x10 + m0 * x11) + p * (p - 1) * ( m1 *
p_adic_expansion_x[0] +
m0 * p_adic_expansion_x[0] + m0 * p_adic_expansion_x[1] + y10 +
y11)
```

```
        print(f"y3 = {y3}")
        try:
            p_adic_expansion_y = to_p_adic(y3, p, precision)
            print_expansion(y3, p, p_adic_expansion_y, precision)
        except ValueError as e:
            print(e)
        return p_adic_expansion_x, p_adic_expansion_y
def take_input():
    expansion1 = [int(x) for x in input("Enter the first p-adic
expansion (comma-separated): ").split(',')]
    expansion2 = [int(x) for x in input("Enter the second p-adic
expansion (comma-separated): ").split(',')]
    p = int(input("Enter the base (prime number): "))
    return expansion1, expansion2, p
#%%# For addition run this cell
exp1, exp2, p = take_input()
result = add_p_adic(exp1, exp2, p)
print(f"The sum of the p-adic expansions is: {result}")
#%%# For subtraction run this cell
exp1, exp2, p = take_input()
result = subtract_p_adic(exp1, exp2, p)
print(f"The sum of the p-adic expansions is: {result}")
#%%# For multiplication run this cell
exp1, exp2, p = take_input()
result = multiply_p_adic(exp1, exp2, p)
print(f"The sum of the p-adic expansions is: {result}")
#%%# For division run this cell
exp1, exp2, p = take_input()
result = divide_p_adic(exp1, exp2, p)
print(f"The sum of the p-adic expansions is: {result}")
#%%# For calculation of slope run this cell
x1 = [int(x) for x in input("Enter the x1 p-adic expansion
(comma-separated): ").split(',')]
```

```
x2 = [int(x) for x in input("Enter the x2 p-adic expansion
(comma-separated): ").split(',')]
y1 = [int(x) for x in input("Enter the y1 p-adic expansion
(comma-separated): ").split(',')]
y2 = [int(x) for x in input("Enter the y2 p-adic expansion
(comma-separated): ").split(',')]
p = int(input("Enter the base (prime number): "))
max_length = max(len(x1), len(x2), len(y1), len(y2))
x1 = pad_with_zeros(x1, max_length)
x2 = pad_with_zeros(x2, max_length)
y1 = pad_with_zeros(y1, max_length)
y2 = pad_with_zeros(y2, max_length)
slope_result = divide_p_adic(subtract_p_adic(y2, y1,p),
subtract_p_adic(x2, x1, p), p)
print(slope_result)
#%%# To calculate P3 run this cell
print("Calculation of point on curve y^2=x^3 + Ax + B")
x1 = [int(x) for x in input("Enter the x1 p-adic expansion
(comma-separated): ").split(',')]
x2 = [int(x) for x in input("Enter the x2 p-adic expansion
(comma-separated): ").split(',')]
y1 = [int(x) for x in input("Enter the y1 p-adic expansion
(comma-separated): ").split(',')]
y2 = [int(x) for x in input("Enter the y2 p-adic expansion
(comma-separated): ").split(',')]
p = int(input("Enter the base (prime number): "))
A = int(input("Enter the value of A: "))
B = int(input("Enter the value of B: "))
p3_x, p3_y = calculate_p3(x1, x2, y1, y2, p, A, B)
print(f"P3: (x: {p3_x}, y:{p3_y}) ")
#%%
```

5. Conclusions

In this paper, the focus is on the points on elliptic curve $E(Q_p)$ over p-adic field Q_p and its arithmetic. All the points in elliptic curve $E(Q_p)$ are obtained by starting with points in $E(F_p)$ and lifting to $E(Q_p)(mod\ p^2)$ and then lifting each point in $E(Q_p)(mod\ p^2)$ to $E(Q_p)(mod\ p^3)$ and so on. The arithmetic of points on $E(Q_p)$ may be evaluated by implementing arithmetic of points in $E(Q_p)$ to $E(Q_p)(mod\ p^2)$. This study of arithmetic in $E(Q_p)(mod\ p^2)$ provides a key space for cryptosystems with $E(Q_p)(mod\ p^2)$ bigger than the key space of cryptosystems with $E(F_p)$ with an increase in level of security.

References

[1] J. H. Silverman and J. Tate. “Rational points on Elliptic Curves” Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[2] J. H. Silverman “The Arithmetic of Elliptic Curves” volume 106 of Graduate texts in Mathematics. Springer-Verlag, New York, 1996.

[3] Fernando Gouvea *p-adic Numbers: An Introduction* (Second Editon). Springer, NewYork, 1997.

[4] Neal Koblitz “*A course in number theory and cryptography*” ISBN 3-5780718 SPIN 10893308.

[5] J. Buchmann “*Introduction to cryptography*” , Springer-Verlag 2001.

[6] Lawrence C. Washington.“*Elliptic curves number theory and Cryptography”* CRC Press, Second Edition

[7] “*p-adic numbers applied on elliptic curve cryptography”* Maherindrainibelahasa, Ravaliminoarimalalason, Randimbindrainibe. Vol-5 Issue-2 2019, IJARIIE-ISSN(O)-2395-4396.

[8] Rosa Winter *“ Elliptic curves over Q_p ”*

[9] S. Katok. *"p-adic analysis compared with real"* volume 37 of *Student Mathematical Library.* American Mathematical Society, Providence, RI, 2007

[10] L. Praveen Kumar *"Arithmetic of Elliptic curves with Affine and Projective Coordinates and some cryptographic aspects"* 2015.

[11] N. Koblitz. *"p-adic numbers, p-adic analysis and zeta-functions"* volume 58 of *Graduate texts in Mathematics.* Springer-Verlag, New York, second edition, 1984.

[12] Alain M. Robert *"A Course in p-adic Analysis"* Volume 198 of *Graduate Texts in Mathematics* Springer-Verlag 2000.