P-adic numbers applied on an elliptic curve cryptography

Maherindrainibelahasa[1] Ratsimamitaka Edouard
Ph D Student
University of Antananarivo in STII Madagasikara

Ravaliminoarimalalason[2] Toky Basilide
Doctor
University of Antananarivo in ESPA Madagasikara

Randimbindrainibe[3] Falimanana
Professor
University of Antananarivo in ESPA Madagasikara

Abstract

This paper use the group of K -rational points of elliptic curve over p-adic numbers field in cryptography. Since this group is an abelian group and can be made cyclic, « addition » on this group have also important geometrical interpretation

We introduice some notations in section 1 and review some properties of a p-adic numbers.

In section 2, we review group structure of elliptic curves over the field $\mathbb{Q}_p$ of p-adic numbers.In section 3 we show one possibility to apply the group of $\mathbb{Q}_p$ -rational points on an elliptic curve in cryptography.In sectio 4, we give an example of cryptosystem based on the key exchange of Diffie-HellmanThe section 5 is reserved for the conclusion.

Key words : *p-adic integers- p-adic numbers- p-adic valuation- p-adic absolute values- elliptic curve- rational point of elliptic curve- trace of elliptic curve- recductuin modulo p- cryptosystem- public key.*

Notation :

$\mathbb{Z}_p$: Set of p-adic integers , $\mathbb{Q}_p$: Set of p-adic numbers

$v_p(x)$: p-adic valuation,

$|x|_p$: p-adic absolute value,

$E(\mathbb{Q}_p)$: Set of an ellipti curve $\mathbb{Q}_p$ -rationnels points.

$\#E(\mathbb{Q}_p) : E(\mathbb{Q}_p)$ cardinal

Introduction :

Victor Miller and Neal Koblitz were, independently, the first to propose elliptic curve in cryptography. Since some cryptograph worked on this because of its security, it can use short key size to gain the same level of security for example.

Elliptic curve cryptography was applied in a public key cryptosystem like RSA, based on the difficulty to factor a big number into product of prime numbers or the key exchange of Diffie-Hellman based on the difficulty to resolve the logarithm discret problem.

In this paper we propose a cryptosystem upon elliptic curve over the p-adic numbers, where p is a prime number (praticaly large).

We have considered an ellipptic curve of prime order to focus on the faiseability of such crytosystem so that apply this in a publc key cryptosystem. we will explain, for example, how we can find the group of p-adic points on an elliptic curve.

1. p-adic numbers

A p-adic numbers can be presented of the formal power serie :

$$a_{-n}p^{-n}+\cdots+a_0+a_1p+\cdots+a_mp^m+\cdots \quad a_i\in\{0,1,\ldots,p-1\} \tag{1}$$

$\mathbb{Q}_p$ is the set of a p-adic numbers.

$\mathbb{Z}_p$ is the set of p-adic integers (i.e., all powers of p are non-negative.)

1.1.P-adic numbers propeties :

Definition 1: p-adic valuation of a rational number :

Let p be a prime, and $a\in\mathbb{Q}^*$ a rational number. Write $a=p^{\rho}\cdot\frac{x}{y}$ with $x,y,\rho\in\mathbb{Z}$ and p divides neither x nor y. The p-adic valuation of a, denoted by $v_p(a)$,is defined as $v_p(a)=\rho$, with $v_p(0)=\infty$.

Definition 2: p-adic absolute value

Let p be a prime and $a\in\mathbb{Q}^*$. The p-adic absolute value of a, denoted by $|.|_p$, is defined as

$$|.|_p:\mathbb{Q}\to\mathbb{Q}_+:$$

$$|a|_p=\begin{cases}p^{-v_p(a)} & a\neq 0\\ 0 & a=0\end{cases}$$

Remark :

A p-adic number is called p-adic integer if $v_p(a)\geq 0$.

$\mathbb{Z}_p=\{a_0+a_1p+\ldots,a_i\in\ 0,\ldots,p-1\}$

$p^n\mathbb{Z}_p=\{a_0p^n+a_1p^{n+1}+\ldots,a_i\in\ 0,\ldots,p-1\}$

$v_p(x)\geq n$, for all $x\in p^n\mathbb{Z}_p$.

1.2. Characteristic of the p-adics

the **characteristic** of a field k, denoted $char(\mathrm{k})$ is the order of the smallest prime subfield of k, or 0 if k has no smallest prime subfield (for example, $\mathbb{Q}$ or $\mathbb{R}$).

The field of p-adics $\mathbb{Q}_p$ has characteristic 0, not p. This is due to the fact that Q, which has characteristic 0, is a subfield of $\mathbb{Q}_p$.

Property 1:

Since, for all prime p, $char\left(\mathrm{F}_p\right) = p$.

2.Elliptic curve over $\mathbb{Q}_p$:

2.1. Introduction :

The rational point of an elliptic curve, which is an algebraic variety, i.e set of solutions points of an equation of the type : $y^2 = x^3 + ax + b$, with x, y belong to a finit field.

Solutions of these equations form, together with the « infinit point » O an abelian group. O is the neutral element of the group.

The operation of this group have a geometrical interpretation, so we can compute additional points on the curve.

Si le groupe est d'ordre premier, il est cyclique, c'est-à-dire qu'il existe un point qui engendre le groupe par additions successives.

If the group has a prime order, it is cyclic group, then it has a generator point. Thus , we can compute all of the points of the curve.

Since all theory lie on an abelian group can be applied on an elliptic curve. So, key exchange of Diffie-Hellman can be computed on the group of rational point on an elliptic curve.

Since $char\left(\mathbb{Q}_p\right) = 0$, we can define an elliptic curve on $\mathbb{Q}_p$.

Definition 1: Elliptic curve :

An elliptic curve is a vurve defined over a field K by an equation of the form :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathrm{k} \quad (1)$$

Definition 2: field, the **K-rational points**

For K a field, the K **-rational points** on a Weierstrass equation E over K are the pairs $\left(x, y\right) \in K \times K$ that satisfy E, together with O, the point at infinity

The set of K-rational points and is denoted $E\left(K\right)$, and describes an elliptic curve.

$$E\left(\mathrm{k}\right) = \left\{ \begin{matrix} \left(x, y\right) \in \mathrm{k}^2 \left| y^2 + a_1xy + \right. \\ a_3y = x^3 + a_2x^2 + a_4x + a_6 \end{matrix} \right\} \cup O$$

If $char\left(K\right) > 3$, the equation can be reduced of the form :

$$y^2 = x^3 + Ax + B$$

Since ,

$$E(\mathrm{k}) = \left\{ \begin{matrix} (x,y) \in \mathrm{k}^2 \\ y^2 = x^3 + Ax + B \end{matrix} \right\} \cup O$$

Définition 3: Courbe non-singulière :

The simplified equation will suffice for our purposes. E is non-singular if the discriminant, $\Delta = -16\left(4a^3 + 27b^2\right)$, is not zero.

Définition 4: Trace of an elliptic curve E

Let E be an elliptic curve over a finite field Fp. The **trace** t is defined by:

$$\#E\left(\mathrm{F}_p\right) = p + 1 - t \tag{2}$$

where $E\left(\mathrm{F}_p\right)$ is the number of elements in $E\left(\mathrm{F}_p\right)$

2.2. Counting rational point on elliptic curve:

Generlity :

Let E/F_q a curve over a finit field F_q. Find approximat value or exact value of the solutions number of the equation :

$$E : y^2 + a_1xy + a_3y = x^3 + x^2 + a_4x + a_6 \quad (x,y) \in \mathrm{F}_q \tag{3}$$

For x there is at most two y ,then $\#E\left(\mathrm{F}_q\right)$ verify :

$$\#E\left(\mathrm{F}_q\right) \le 2q + 1 \text{(whith the O)}$$

Let $x \in \mathrm{F}_q$, $f(x) = x^3 + Ax + B$ is a square in the probability $0{,}5$, thus the approximation of $\#E\left(\mathrm{F}_q\right)$ is :

$$\#E\left(\mathrm{F}_q\right) \approx \frac{1}{2} \times 2p + 1 \text{points.} \tag{4}$$

Theorem 1 : (Hasse) :

Let E/F_q an elliptic curve over F_q :

$$\left|\#E\left(\mathrm{F}_q\right) - q - 1\right| \le 2\sqrt{q} \tag{5}$$

$$\Leftrightarrow q + 1 - 2\sqrt{q} \le \#E\left(\mathrm{F}_q\right) \le q + 1 + 2\sqrt{q}$$

Proposition 1 : Legendre formula:

Let :

$$\begin{aligned} \chi : \mathrm{F}_p &\to \{-1,01\} \\ x &\to \left(\frac{x}{p}\right) \end{aligned} \tag{6}$$

Then :

$$\chi(0) = 0 \text{ et } \chi(x) = \begin{cases} 1 \text{ if } x \text{ is square} \neq 0 \text{ in } \mathrm{F}_p \\ -1 \text{ not} \end{cases} \tag{7}$$

Proposition 2:

$$\#E(\mathrm{F}_q) = p + 1 + \sum_{x \in \mathrm{F}_p} \chi\left(x^3 + Ax + B\right) \tag{8}$$

Proof :

♣

Let $x \in \mathrm{F}_p$:

- There are two points x-coordinate in $E(\mathrm{F}_p)$ if $\chi\left(x^3 + Ax + B\right) = 1$,
- no point x- coordinate if $\chi\left(x^3 + Ax + B\right) = -1$
- exactly one point x -coordinate if $\chi\left(x^3 + Ax + B\right) = 0$

♦

Remark :

Legendre formula is valid for « little » prime number, approximately 10^6 *or* 10^7.

Lemme 1:

Let $P \in E(\mathrm{F}_q)$, Such that ord $P = d$. Assume :

$$d > 4\sqrt{p} \tag{9}$$

Let m such that $mP = O$ *and* $m \in \mathrm{F}_p$, Thus $\#E(\mathrm{F}_p) = m$.

More m is the one multiple of d in F_p.

2.3. Groupe des points rationnels d'une courbe elliptique :

Addition of points on elliptic curve is defined by :

Let $P, Q \in E(\mathrm{k})$, then $R = P + Q$ is:

- If $P = O$, then $R = Q$; if $Q = 0$, then $R = P$,
- if $x_P = x_Q$, and $y_P = -y_Q$, then $R = O$,
- Let,

$$\lambda = \begin{cases} \dfrac{3x_P^2 + A}{2y_P}, & if\ P = Q \\ \dfrac{y_P - y_Q}{x_P - y_Q}, & \text{if not} \end{cases} \quad (10)$$

$$R = \left(\lambda^2 - x_P - x_Q, \lambda\left(-\lambda^2 + 2x_P + x_Q\right) - y_P\right)$$

Property 1:

$\left(E\left(\mathrm{F}_p\right), +\right)$ is an abelian group.

Example :

Cryptography on elliptic cyrves.

$$E : y^2 = x^3 + x + 6 \text{ on } \mathrm{F}_{11} \quad (11)$$

Square :

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	4	3	7	9	4	1

Rational points :

x	**0**	**1**	**2**	**3**
$x^3 + x + 6$	**6**	**8**	**5**	**3**
$x^3 + x + 6$ QR	**non**	**non**	**oui**	**Oui**
y	**_**	**_**	**4 ; 7**	**5 ; 6**

4	**5**	**6**	**7**	**8**	**9**	**10**
8	**4**	**8**	**4**	**9**	**7**	**4**
non	**oui**	**non**	**oui**	**oui**	**non**	**oui**
_	**2 ; 9**	**_**	**2 ; 9**	**3 ; 8**	**_**	**2 ; 9**

$$E(\mathrm{F}_{11}) = \left\{ \begin{matrix} (2;4),(2;7),(3;5),(3;6),(5;2) \\ ,(5;9),(7;2),(7;9),(8;3),(8;8) \\ ,(10;2),(10;9),O \end{matrix} \right\}$$

$$\#E(\mathrm{F}_{11}) = ord_{11}E(\mathrm{F}_{11}) = 13. \quad (12)$$

$\#E(\mathrm{F}_{11}) = ord_{11}E(\mathrm{F}_{11}) = 13$ is prime, this group is cyclic, every point $\neq O$ (point at infini) is a generator .

Take $P(2,7)$.

2.4. Elliptic Curves over the p-adics :

2.4.1.Généralités :

Since $\mathbb{Q}_p$ is a field of characteric 0, we can define an elliptic curve on $\mathbb{Q}_p$.

All of the theories on elliptic curve down in the precedent chapter are applicable there.

Particularly, since the field charcteristc is different from 2 and 3, the simplified equation on Weierstrass is applied .

Let $\tilde{E}(\mathrm{F}_p)$ the group of points satisfaying Weiersrass equation on F_p, and $E(\mathbb{Q}_p)$ the group of points satisfaying Weiersrass equation on $\mathbb{Q}_p$

2.4.2. Lifting from $\tilde{E}(\mathrm{F}_p)$ to $E(\mathbb{Q}_p)$

The first map is from $E(\mathbb{Q}_p)$ to $\tilde{E}(\mathrm{F}_p)$.

A point $P \in E(\mathbb{Q}_p)$ is called a lift of a point $\tilde{P} \in \tilde{E}(\mathrm{F}_p)$ if it reduces mod p to $\tilde{P}$

Définition 1: Reducing modulo p **from** $E(\mathbb{Q}_p)$ **to** $\tilde{E}(\mathrm{F}_p)$**:**

This reduction is a map :

$$E(\mathbb{Q}_p) \to \tilde{E}(\mathrm{F}_p) . \quad (13)$$

Because we are allowed to take out non-zero multiples in projective coordinates any point $P \in E(\mathbb{Q}_p)$ can be written in as (X,Y,Z), where X,Y,Z are p-adic integers and at least one is not divisble by p.
We define a map:

$$\begin{aligned} r_p : \ \mathbb{Q}_p &\to \mathbb{Z}/p\mathbb{Z} \\ \sum_{n\geq 0} a_n p^n &\to a_0 \end{aligned} \quad (14)$$

Then, to reduce a point mod p, we simply reduce each of its coordinates mod p:

$$\tilde{P} = (r_p(X), r_p(Y), r_p(Z)) \quad (15)$$

Definition 2 : Lifting from $\tilde{E}(\mathrm{F}_p)$ to $E(\mathbb{Q}_p)$:

Let $\tilde{P}$ be a point satisfying

$$\tilde{E}: y^2 = x^3 + ax + b, \tag{16}$$

where $a, b \in \mathrm{F}_p$, and $p \neq 2, 3.$

In affine coordinates, we may write $\tilde{P}(\tilde{x}, \tilde{y})$ where $\tilde{x}, \tilde{y} \in \mathrm{F}_p$.

We wish to find p-adic integers x and y such that $P = (x, y) \in E(\mathbb{Q}_p)$ where E is $\tilde{E}$ viewed over the p-adics. $\mathbb{Q}_p$

Let :

$$f(x, y) = y^2 - x^3 - ax - b,\ a, b \in \mathbb{Q}_p \tag{17}$$

x, y satisfy E if, and only if $f(x, y) = 0$.

let $x = \tilde{x}$, y is a p-adic integer such that : $P = (x, y) \in E(\mathbb{Q}_p)$.

Since y is a p-adic integer y :

$$y = h_0 + h_1 p + h_2 p^2 + O(p^3) \text{ où } h_i \in \{0, 1, \ldots, p-1\} \tag{18}$$

Because we require $f(x, y) = 0$, on it must also be that $f(x, y) = 0 \bmod p^i$ for any $i > 0$ (and indeed any modulus)tout $i > 0$: $f(x, y) \equiv 0 \pmod{p^i}$
we have that:

$$\begin{gathered}\left(h_0 + h_1 p + h_2 p^2 + O(p^3)\right)^2 - \\ \left(\tilde{x}^3 + a\tilde{x} + b\right) \equiv 0 \pmod{p}\end{gathered} \tag{19}$$

Reducing gives:

$$h_0^2 - \tilde{x}^3 - a\tilde{x} - b \equiv 0 \pmod{p},$$

Thus :

$$h_0 = \tilde{y} \tag{20}$$

Now by the same token (and replacing h_0 with $\tilde{y}$:

$$\left(\tilde{y}+h_1p+h_2p^2+O\left(p^3\right)\right)^2- \left(\tilde{x}^3+a\tilde{x}+b\right)\equiv 0\left(\mathrm{mod}\ p^2\right) \quad (21)$$

which reduces to:

$$\left(\tilde{y}+h_1p\right)^2-\tilde{x}^3-a\tilde{x}-b\equiv 0\left(\mathrm{mod}\ p^2\right)$$

$$\tilde{y}^2+2\tilde{y}h_1p-\tilde{x}^3-a\tilde{x}-b\equiv 0\left(\mathrm{mod}\ p^2\right)$$

$$\left(\tilde{y}-\tilde{x}^3-a\tilde{x}-b\right)+2\tilde{y}h_1p\equiv 0\left(\mathrm{mod}\ p^2\right)$$

$$f\left(\tilde{x},\tilde{y}\right)+2\tilde{y}h_1p\equiv 0\left(\mathrm{mod}\ p^2\right)$$

$$p\left[\frac{f\left(\tilde{x},\tilde{y}\right)}{p}+2\tilde{y}h_1\right]\equiv 0\left(\mathrm{mod}\ p^2\right)$$

$$\frac{f\left(\tilde{x},\tilde{y}\right)}{p}+2\tilde{y}h_1\equiv 0\left(\mathrm{mod}\ p\right)$$

$$h_1=-\frac{f\left(\tilde{x},\tilde{y}\right)}{2p\tilde{y}}\left(\mathrm{mod}\ p\right). \quad (22)$$

the formula for h2:

$$\left(\tilde{y}+h_1p+h_2p^2\right)^2-\tilde{x}^3-a\tilde{x}-b\equiv 0 \left(\mathrm{mod}\ p^3\right)$$

$$\left(\tilde{y}+h_1p+h_2p^2\right)^2-\tilde{x}^3-a\tilde{x}-b\equiv 0 \left(\mathrm{mod}\ p^3\right)$$

$$\left(\tilde{y}+h_1p\right)^2+2\left(\tilde{y}+h_1p\right)h_2p^2-\tilde{x}^3-a\tilde{x}-b\equiv 0 \left(\mathrm{mod}\ p^3\right)$$

$$f\left(\tilde{x},\tilde{y}+h_1p\right)+2\left(\tilde{y}+h_1p\right)h_2p^2\equiv 0 \left(\mathrm{mod}\ p^3\right)$$

$$p^2\left[\frac{f\left(\tilde{x},\tilde{y}+h_1p\right)}{p^2}+2\left(\tilde{y}+h_1p\right)h_2\right].. \equiv 0\left(\mathrm{mod}\ p^3\right)$$

$$\frac{f\left(\tilde{x},\tilde{y}+h_1 p\right)}{p^2}+2\left(\tilde{y}+h_1 p\right)h_2 \equiv 0 \pmod{p}$$

$$h_2 \equiv -\frac{f\left(\tilde{x},\tilde{y}+h_1 p\right)}{2\left(\tilde{y}+h_1 p\right)p^2}\pmod{p} \quad (23)$$

2.5. The groups $E_n\left(\mathbb{Q}_p\right)$

These are subgroup of $E\left(\mathbb{Q}_p\right)$

Definition 1:

Let $E\left(\mathbb{Q}_p\right)$ an elliptic curve. The group $E_1\left(\mathbb{Q}_p\right)$ is defined by :

$$E_1\left(\mathbb{Q}_p\right)=\left\{P\in E\left(\mathbb{Q}_p\right)\middle|\tilde{P}=O\right\} \quad (24)$$

In over words, E_1 is the set of points on E that reduce modulo p to O.

Proposition 1:

$$E\left(\mathbb{Q}_p\right)\Big/E_1\left(\mathbb{Q}_p\right)\cong E\left(\mathrm{F}_p\right) \quad (25)$$

Démonstration :

♣

Let :

$$r: E\left(\mathbb{Q}_p\right)\to E\left(\mathrm{F}_p\right)$$
$$P \to \tilde{P}$$

Then :

$$Ker\left(r\right)=\left\{P\in E\left(\mathbb{Q}_p\right)\middle|r\left(P\right)=\tilde{P}=O\right\}$$
$$=E_1\left(\mathbb{Q}_p\right)$$

The result follows from the First Isomorphism Theorem.

♦

Definition 2:

The subgroup $E_n\left(\mathbb{Q}_p\right)\left(n\in\mathbb{N}\right)$ of $E\left(\mathbb{Q}_p\right)$ is defined by :

$$E_n\left(\mathbb{Q}_p\right)=\left\{P\in E\left(\mathbb{Q}_p\right)\middle|v_p\left(x_P\right)\le -2n\right\}\cup\left\{O\right\} \quad (27)$$

where x_P is the x-coordinate of P.

In particular :

$$E_1(\mathbb{Q}_p) = \left\{ P \in E(\mathbb{Q}_p) \middle| v_p(x_P) \le -2 \right\} \cup \{O\} \quad (28)$$

Remark :

1. $E_n(\mathbb{Q}_p)$ is a subgroup of $E_k(\mathbb{Q}_p)$ for all $k < n$.

Since a, b are p-adic integers : $v_p(a) \ge 0$ et $v_p(b) \ge 0$. x and y must satisfy

$$y^2 = x^3 + ax + b$$

$$2v_p(y) \ge \min \begin{Bmatrix} 3v_p(x), v_p(a) + v_p(x), \\ v_p(b) \end{Bmatrix}$$

$$v_p(x) < 0 \text{ and } v_p(a) \ge 0 \ , \ v_p(b) \ge 0$$

Then :

$$2v_p(y) = 3v_p(x)$$

Since $v_p(x)$ are integer :

$v_p(x) = -2n$ et $v_p(y) = -3n$ for all integers n.

1.

$$\#\left(E(\mathbb{Q}_p) \Big/ E_1(\mathbb{Q}_p) \right) = p \quad (30)$$

Propriété 1 :Property of finit groupe(Generator of cyclic group)

If G is a finite group who's number of element is prime, then G is cyclic and any element, not neutral, of G is generator.

Démonstration :

♣

Let p the number of elements of G and $a \in G$ such that $a \ne e$, by Lagrange theorem, the number of elements of the subgroup $\langle a \rangle$ de G generated by a divides p, thus :

$$\#\langle a \rangle = 1 \text{ or } \#\langle a \rangle = p.$$

Since $a \in \langle a \rangle$, the subgroup $\langle a \rangle$ is not reduce to $\{e\}$, then $\#\langle a \rangle = p$.

Since $\langle a \rangle \subset G$ and $\#G = p$, then $\langle a \rangle = G$, for all $a \in G$.

♦

Example :

Let E an elliptic curve over F_{19} defined as:

$$E:\ y^2 = x^3 + x + 4 \text{ sur } \mathrm{F}_{19}$$

In $K = \mathrm{F}_{19}$, $s(5,1) \in E(\mathrm{F}_{19})$.

Since, $5^3 + 5 + 4 = 134 \equiv 1 (\mathrm{mod} 19)$

Then $y^2 = 1(\mathrm{mod}19)$, *thus* $y = 1(\mathrm{mod}19)$ $(or\ -1)$.

Lift E/F_{19} on to $E/\mathbb{Q}_{19}$ where $a = 1$ and $b = 4$ as elements of $\mathbb{Q}_{19}$.

lift $s(5,1)$ on $S(5 + pu, 1 + pv)(\mathrm{mod}19^2)$.

$S \in E(\mathbb{Q}_{19})(\mathrm{mod}19^2)$, then :

$$(1+pv)^2 \equiv (5+pu)^3 + (5+pu) + 4 \quad (\mathrm{mod}19^2)$$

$$\equiv 125 + 3\cdot 5^2 \cdot pu + 5 + pu + 4 \ (\mathrm{mod}19^2)$$

$$\equiv 134 + 76\,pu \ (\mathrm{mod}19^2)$$

$$2pv \equiv 133 + 76\,pu \ (\mathrm{mod}19^2)$$

$$2pv \equiv 7\cdot 19 + 4\cdot 19\,pu \ (\mathrm{mod}19^2)$$

$$2v \equiv 7 + 4\,pu \ (\mathrm{mod}19)$$

$$2v \equiv 2\cdot 13 + 4\,pu \ (\mathrm{mod}19)$$

$$v \equiv 13 + 2\,pu \ (\mathrm{mod}19)$$

S is in the form :

$$S(5 + pu, 1 + p(13 + 2\,pu))(\mathrm{mod}19^2)$$

$$S(5 + pu, 1 + 13p)(\mathrm{mod}19^2)$$

$$S(5 + 19u, 1 + 13\cdot 19)(\mathrm{mod}19^2)$$

It turns out that $S\ (\mathrm{mod}19^3)$:

$$S = \begin{pmatrix} 5 + O(19^3), 1 + 13\cdot 19 + 10\cdot 19^2 + \\ O(19^3) \end{pmatrix}$$

point of $E(\mathbb{Q}_{19})$.

Compute $[2]P$.

If $S = (x, y)$, then $[2]S = (x_2, y_2)$ with :

$$x_2 = N^3 - 2x, \tag{31}$$

$$y_2 = N(x - x_2) - y \tag{32}$$

Where

$$N = \frac{3x^2 + a}{2y} \tag{33}$$

Compute N :
The numerator is

$$N_{num} = 3\left(5 + O\left(19^3\right)\right) + 1 = 16 + O\left(19^3\right) \tag{34}$$

the denominator is:

$$\begin{aligned} N_{dénom} &= 2\left(1 + 13 \cdot 19 + 10 \cdot 19^2 + O\left(19^3\right)\right) \\ &= 2 + 7 \cdot 19 + 2 \cdot 19^2 + O\left(19^3\right) \end{aligned} \tag{35)-(36}$$

$$N = \frac{N_{num}}{N_{dénom}} = 8 + 10 \cdot 19 + 12 \cdot 19^2 + O\left(19^3\right)$$

Now we may compute the coordinates:

$$\begin{aligned} x_2 = N^3 - 2x &= 8 + 10 \cdot 19 + 12 \cdot 19^2 + \\ &\quad O\left(19^3\right) \text{(37)-(38)} \\ &= 8 + 8 \cdot 19 + 18 \cdot 19^2 + O\left(19^3\right) \end{aligned}$$

$$\begin{aligned} y_2 &= N\left(x - x_2\right) - y \\ &= 13 + 5 \cdot 19 + 9 \cdot 19^2 + O\left(19^3\right) \end{aligned}$$

$$2S = \begin{pmatrix} 8 + 8 \cdot 19 + 18 \cdot 19^2 + O\left(19^3\right), \\ 13 + 5 \cdot 19 + 9 \cdot 19^2 + O\left(19^3\right) \end{pmatrix} . \tag{39}$$

3.Cryptography on elliptic curve:

3.1.Key exchange :

Alice wants to send a message, often called the plaintext, to Bob. In order to keep the eavesdropper Eve from reading the message, she encrypts it to obtain the ciphertext. When Bob receives the ciphertext, he decrypts it and reads the message. In order to encrypt the message :

- Alice uses an encryption key.
- Bob uses a decryption key to decrypt the ciphertext.

Clearly, the decryption key must be kept secret from Eve.

In this paper, we will use public key encryption, or asymmetric encryption.
In this case, Alice and Bob do not need to have prior contact.

Bob publishes a public encryption key $D_b = bP$, which all user uses (particularly Alice).

He also has a private decryption key that allows him to decrypt
ciphertexts.
The most famous public key system is known as :

- RSA and is based on the difficulty of factoring integers into primes.
- Another wellknown system is due to ElGamal and is based on the difficulty of the discrete logarithm problem.

Alice and Bob agree on an elliptic curve *E* over a finite field F*q* : $y^2 = x^3 + Ax + B$ such
that the discrete logarithm problem is hard in *E*(F*q*). They also agree

on a point $P(x_P, y_P)$ *of* $E(\mathrm{F}_p)$ such that the subgroup generated by P has large order (usually, the curve and point are chosen so that the order is alarge prime).
One user chooses a secret integer u with $0 < u < q$ (his private key)computes $D_u = uP$ (his public key) and sends D_u to Bob.

1.2. Encryption and decryption :

Bob wants to send a message m to Alice. He transform the message to a ciphertext M .

Alice chooses a secret integer a , computes $D_A = ax_P$ where x_P is the x -coordonate of P , and sends D_A to Bob,
Bob chooses a secret integer b , computes $D_B = bx_P$, and sends D_B to Alice.

Alice computes *aPb* = *abP* .

Bob computes *bPa* = *baP* .

Bob compute $C = M + bD_A$
Bob send (D_B, C) to Alice ,
Alice receiv (D_B, C)
Alice compute $aD_B = abx_P$ and $C - aD_B = M + bD_A - abx_P = M$,

3.3.Verification :

$$bD_A = b(ax_P) = (ba)x_P = a(bx_P)aD_B$$

Remark :

Alice and Bob use some publicly agreed on method to extract a key from *abP* . For example, they could use the last 256 bits of the x -coordinate of $abP = (x, y) \in E(\mathrm{F}_p)$ as the key. Or they could evaluate a hash function at the x -coordinate.

4.Example :

lettre	**0**	**1**	**2**	**3**	**4**
entier	**0**	**1**	**2**	**3**	**4**

5	**6**	**7**	**8**	**9**	**A**	**B**	**C**
5	**6**	**7**	**8**	**9**	**10**	**11**	**12**

…	**.**	**,**	**:**	**;**	**!**	**?**	**esp**
…	**36**	**37**	**38**	**39**	**40**	**41**	**42**

The message « BONJOUR » is encrypt by the ciphertext.

$$=11+24\cdot 47+23\cdot 47^2+19\cdot 47^3+24\cdot 47^4+31\cdot 47^5+27\cdot 47^6 = 298232584907$$

$$27\ 31\ 24\ 19\ 23\ 24\ 11_{47}$$

Consider $E: y^2 = x^3 + 22x + 25$ *sur* F_{47}, we lift this curve onto a curve over $\mathbb{Q}_{47}$,

$$\tilde{E}: Y^2 = X^3 + 22X + 25.$$

x	0	1	2	3	4	5	6
x^2	0	1	4	9	16	25	36
y^2	**25**	**1**	30	**24**	36	**25**	44

7	8	9	10	11	12	13	14
2	17	34	27	3	28	8	37
5	**8**	**12**	23	0	43	**17**	22

15	16	17	18	19	20	21	22
37	21	7	42	32	24	18	14
17	**8**	1	2	**17**	5	19	**18**

23	24	25	26	27	28	29	30
12	12	14	21	7	32	42	7
8	**42**	32	31	45	33	**1**	**36**

31	32	33	34	35	36	37	38
21	37	8	28	3	27	6	34
42	33	**28**	33	7	**3**	**27**	38

39	40	41	42	43	44	45	46
17	2	36	25	16	9	4	1
42	45	**6**	**25**	**14**	26	20	**2**

Squares in F_{47} are writed fat.

From Legendre formula $< 10^6$, we have :

$$\left|E\left(\mathrm{F}_{47}\right)\right| = 47 + 1 + \sum_{x \in \mathrm{F}_{47}} \chi\left(x^3 + 22x + 25\right),$$

Where :

$$\chi(0) = 0 \text{ et } \chi(x) = \begin{cases} 1 \text{ if x is square } \neq 0 \text{ in } \mathrm{F}_{47} \\ -1 \text{ not} \end{cases}$$

$$\#E\left(\mathrm{F}_{47}\right) = 47 + 1 + 28 - 17 = 59$$

$\#E\left(\mathrm{F}_{47}\right)$ is a prime number, the group $E\left(\mathrm{F}_{47}\right)$ is cyclic and every points are generator of the group.

The point $s(3,20)$ is in $E(\mathrm{F}_{47})$ lift into point on $E(\square_{47})$. Let :

$$S(3+pu,20+pv)\left(\mathrm{mod}\,47^2\right).$$

$$\begin{aligned} &S\in E(\square_{47})\Leftrightarrow \\ &(20+pv)^2=(3+pu)^3+22(3+pu) \\ &\qquad +25\left(\mathrm{mod}\,47^2\right) \end{aligned}$$

$$\Leftrightarrow 400+6pv=118+49pu\ \left(\mathrm{mod}\,47^2\right)$$

$$\Leftrightarrow 6pv=-282+49pu\ \left(\mathrm{mod}\,47^2\right)$$

$$\Leftrightarrow 6pv=1927+49pu\ \left(\mathrm{mod}\,47^2\right)$$

$$\Leftrightarrow 6pv=41p+49pu\ \left(\mathrm{mod}\,47^2\right)$$

$$\Leftrightarrow 6v=41+49u\ \left(\mathrm{mod}\,47\right)$$

$$\Leftrightarrow 6v=41+2u\ \left(\mathrm{mod}\,47\right)$$

$$\Leftrightarrow v=41\cdot 6^{-1}+2\cdot 6^{-1}u\ \left(\mathrm{mod}\,47\right)$$

Since $\mathrm{pgcd}(6,47)=1$, by Bézout theorem we have: $47\times(-1)+6\times 8=1$

Then : $6\times 8\equiv 1\left(\mathrm{mod}\,47\right)$ and $6^{-1}=8\ \left(\mathrm{mod}\,47\right)$

Thus $v=41\cdot 8+2\cdot 8u\ \left(\mathrm{mod}\,47\right)$

$$\Leftrightarrow v=46+16u\ \left(\mathrm{mod}\,47\right)$$

S is of the form $S(3+pu,20+pv)\left(\mathrm{mod}\,47^2\right)$

$$S\left(3+pu,20+p(46+16u)\right)\left(\mathrm{mod}\,47^2\right)$$

$$S\left(3+47u,20+46\times 47+16\times 47u\right)\left(\mathrm{mod}\,47^2\right)$$

$$S\left(3+47u,2182+16\times 47u\right)\ \left(\mathrm{mod}\,47^2\right)$$

Bob send to Alice :

$$D_B=3x_S=3(3+47u)$$

and

$$\begin{aligned} C &= M + 3D_A \\ &= \ldots 00\ 27\ 31\ 24\ 19\ 23\ 24\ 11_{47} \\ &\quad + 2\times 3\times(3+47u) \end{aligned}$$

$$\begin{aligned} &\ldots 27\ 31\ 24\ 19\ 23\ 30\ 29_{47} \\ &= 312.597.244.541\,(u=1) \end{aligned}$$

Alice compute :

$$2D_B = 2\times 3x_S = 2\times 3(3+47u)$$

et $C - 2D_B = M = 298.232.584.907$

She find the message by computing Elle retrouve le message par des divisions euclidiennes successives de M par 47.

5.Conclusion :

Actually many searcher work on elliptic curve cryptographic over finit field, for now on the point multiplication, reduction of the discret logarithm problem for specialcurves of Menezes. Okamoto and Vanstonen, the point couniting methode of Schoof etc…..

In this article, we worked on the K -rational group on elliptic curve over p-adic field In order to create a cryptosystem. We focused the work on elliptic curves whose orders are prime in order to focus on the cryptosystem's feasibility and apply it in a Public key encryption.
Few people work on elliptic over infinite field. The reason is that the points on these curves also form infinite field.
These case exceed the power of computers and are not within reach of cryptographyc research.
Other cases are treated in the search for generator which depend more on the structure of $E(\square_p)$.

Bibliography

[Ay] Yvette Amice. Les nombres p-adiques. Presses universitaires de France, 1975.
[BG] Introduction to p-adique numbers and valuation theory, George Bachman, Academic
[BS] Borevitsh_Shafarevitch. Théorie des nombres. Gauthier –Villars Paris 1967.
[CPi] Pierre Colmez. Les nombres p-adiques. Notes du cours de M2.
[Se] J.-P. Serre, Cohomologie galoisienne, Lectures Notes in Math. 5, Berlin- Heidelberg-New-york: Springer 1964.
[KN] Neal-Koblitz-p-adic-numbers p-adic-analysis and-zeta-functions-Springer-_1996
[KN] N. KoBLITZ: *Introduction to e//iptic curves and modular forms.* Graduate Texts in Math.97, Springer Verlag Berlin-Heidelberg-New-York 1984.
[KN] N. KOBLITZ: *Elliptic curve cryptosystems.* Math.Comp.(48): 203-209, 1987.
[KN] N. KoBLITZ : *CM curves with cryptographie properties.* Ad vance in Cryptology. . Crypto. 91; Lectures Notes in Computer Sciences, Vol 537. Springer Verlag. Berlin 1992
$[Sil]$ Joseph H. SILVERMAN . *The arithmétic of Elliptic Curves*. Springer, 1986.