Computation of the discrete logarithm on elliptic curves of trace one [*]

Tutorial

Jean Monnerat

Security and Cryptography Laboratory,
Swiss Federal Institute of Technology, CH-1015 Lausanne, Switzerland
Jean.Monnerat@epfl.ch

Abstract. The security of several elliptic curve cryptosystems is based on the difficulty to compute the discrete logarithm problem. The motivation of using elliptic curves in cryptography is that there is no known sub-exponential algorithm which solves the Elliptic Curve Discrete Logarithm Problem (ECDLP) in general. However, it has been shown that some special curves do not possess a difficult ECDLP. In 1999, an article of Nigel Smart provides a very efficient method for solving the ECDLP when the underlying elliptic curve is of trace one. In this note, we describe this method in more details and recall the mathematical background in order to understand it.

1   The elliptic curves

We recall here the definition of an elliptic curve and its group law. In order to do this, we introduce the projective space.

Definition 1. *Let K be a field. The projective n-space $\mathbb{P}^n(K)$ over K is the set of equivalence classes*

$$\left(K^{n+1}\backslash\{(0,\dots,0)\}\right)/\sim,$$

where

$$(x_0,\dots,x_n) \sim (y_0,\dots,y_n)$$

if and only if there exists a $\lambda \in K^*$ such that $y_i = \lambda x_i$ for all $0 \leq i \leq n$.

---

[*] This is the report of a Graduate School project supervised by Prof. Serge Vaudenay.
 Technical report EPFL/IC/2002/49

Notation An equivalence class containing $(x_0, x_1 \ldots, x_n)$ is denoted by $(x_0 : x_1 : \ldots : x_n)$.

Definition 2. *Let $\overline{K}$ be the algebraic closure of the field K. A Weierstrass equation is a homogeneous equation of degree 3 of the form*

$$Y^2 Z + a_1 XYZ + a_2 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3,$$

where a_1, a_2, a_3, a_4, a_6 are elements of $\overline{K}$. Moreover, the Weierstrass equation is said to be non-singular if for all projective points $P = (X : Y : Z) \in \mathbb{P}^2(\overline{K})$ satisfying

$$F(X,Y,Z) := Y^2 Z + a_1 XYZ + a_2 YZ^2 - X^3 - a_2 X^2 Z - a_4 XZ^2 - a_6 Z^3 = 0,$$

at least one of the three partial derivatives $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$, $\frac{\partial F}{\partial Z}$ is non-zero at P. If it is not the case for a point P, the Weierstrass equation is said to be singular and P is called a singular point.

Definition 3. *An elliptic curve E is the set of all solutions in $\mathbb{P}^2(\bar{K})$ of a Weierstrass equation.*

We see that, there is exactly one point in E whose Z-coordinate is equal to 0, namely $(0 : 1 : 0)$. This point is called the point at infinity and is denoted by $\mathcal{O}$.

Definition 4. *Let $\widehat{K}$ be a field satisfying $K \subset \widehat{K} \subset \overline{K}$. A point (X, Y, Z) is $\widehat{K}$-rational if there exist $\lambda \in \overline{K}$ and $(\widehat{X}, \widehat{Y}, \widehat{Z}) \in \widehat{K}^3$ such that*

$$(X, Y, Z) = \lambda(\widehat{X}, \widehat{Y}, \widehat{Z}).$$

The set of the $\widehat{K}$-rational points of an elliptic curve E is denoted by $E(\widehat{K})$.

By using the non homogeneous coordinates $x = X/Z, y = Y/Z$, the Weierstrass equation has the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{1}$$

We notice that an elliptic curve E is then the set of all solutions of the equation (1) in the affine plane $\overline{K} \times \overline{K}$ together with $\mathcal{O}$. If the coefficients a_1, a_2, a_3, a_4, a_6 lie in K, we say that E is defined over K and we write E/K. We remark too that the set $E(\widehat{K})$ is composed of the solutions of (1) in $\widehat{K}^2$ and the infinity point $\mathcal{O}$.

Definition 5. *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. The trace of Frobenius t at q is defined by*

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

where the symbol $\#$ denotes the cardinality of a set.

Remark A trace equal to one corresponds to the case where the number of rational points is the order of the finite field.

We consider now an elliptic curve E defined over a field K with $\mathrm{char}(K) \neq 2, 3$ and given by the Weierstrass equation (1). Since $\mathrm{char}(K) \neq 2$, the change of variables

$$(x, y) \longrightarrow \left(x, y - \frac{a_1}{2} - \frac{a_3}{2} \right)$$

is allowed and transforms E/K to the curve

$$E'/K : y^2 = x^3 + a_2' x^2 + a_4' x + a_6'.$$

Since $\mathrm{char}(K) \neq 3$, the admissible change of variables

$$(x, y) \longrightarrow \left(\frac{x - 3a_2'}{36}, \frac{y}{216} \right)$$

transforms E' to the curve

$$E''/K : y^2 = x^3 + ax + b,$$

where $a, b \in K$.
Hence, we can always assume that E/K has the above form, if $\mathrm{char}(K) \neq 2, 3$.

2   The goup law

In this section, we introduce a certain addition law under which the points on an elliptic curve E form an abelian group. We present here a formula which holds on every elliptic curve given by the Weierstrass equation (1).
We define this addition law as following:

1. $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E$.
2. If $P = (x_1, y_1)$, then its inverse element is defined by $-P := (x_1, -y_1 - a_1 x_1 - a_3)$, i.e. $P + (-P) := P - P := \mathcal{O}$. (We remark that P and $-P$ are the only points on E with x-coordinate equal to x_1.)
3. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ such that $P_1 \neq \mathcal{O}, P_2 \neq \mathcal{O}$, $P_1 \neq -P_2$. Define

$$\lambda := \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu := \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

when $x_1 \neq x_2$, and set

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \mu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$$

when $x_1 = x_2$. If we set $P_3 = (x_3, y_3) = P_1 + P_2$, then P_3 is given by

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3.$$

Remark If E is defined on a field K, the set $E(K)$ with this addition law form a subgroup of $(E, +)$.

If we consider an elliptic curve E/K with $\mathrm{char}(K) \neq 2, 3$ given by

$$y^2 = x^3 + a_4 x + a_6, \tag{2}$$

we obtain an addition law that is easier to compute. Namely, if $P = (x, y)$, then $-P = (x, -y)$ and $P_1 + P_2 = P_3 = (x_3, y_3)$ is given by the following computations

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \\ \frac{3x_1^2 + a_4}{2y_1}, & \text{if } x_1 = x_2. \end{cases}$$

4

Notation For a positive integer n, we let $[n]$ denote the multiplication by n map

$$[n]\, P := P + P + P + \cdots \quad (n \text{ times}),$$

for any $P \in E$.

3 Introduction to the p-adic numbers

We introduce here the p-adic numbers and their basic properties.

Definition 6. *Let p be a prime number and a a rational number. a can be expressed as*

$$a = p^r \frac{m}{n}$$

where $r \in \mathbb{N}$ and m, $n \in \mathbb{Z}$ are not divisible by p. We then define

$$\operatorname{ord}_p(a) := r \quad and \quad |a|_p := \begin{cases} p^{-r} & if\ a \neq 0 \\ 0 & if\ a = 0. \end{cases}$$

Proposition 7. *The function $|.|_p : \mathbb{Q} \to [0,\infty)$ is a norm on $\mathbb{Q}$, i.e.*
(i) $\quad |a|_p = 0 \iff a = 0$
(ii) $\quad |ab|_p = |a|_p |b|_p$
(iii) $\quad |a + b|_p \leq |a|_p + |b|_p.$

Remark
i) $|.|_p$ satisfies a still stronger condition than (iii), namely $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.
ii) This norm induces a metric $d_p(.,.)$ on $\mathbb{Q}$ defined by

$$d_p(a, b) = |a - b|_p$$

.

Definition 8. *The field $\mathbb{Q}_p$ of p-adic numbers is the completion of $\mathbb{Q}$ for the metric d_p, i.e. $a \in \mathbb{Q}_p$ if and only if there exists a sequence $(a_n)_{n \in \mathbb{N}}$ such that*

$$|a_n - a|_p \longrightarrow 0 \ as\ n \to \infty.$$

We provided above an abstract definition of the p-adic numbers, but we have not still showed how such numbers may look like. We give here their natural representation. As the real numbers can be represented by decimals, p-adic numbers can be represented by infinite series of the form

$$c_{-n}p^{-n} + \ldots + c_0 + c_1 p + \ldots + c_m p^m + \ldots,$$

where the c_i's are integers such that $0 \leq c_i \leq p - 1$. By definition of d_p, we easily remark that this serie converges with respect to this metric.

Definition 9. *An element $a \in \mathbb{Q}_p$ is called a p-adic integer, if $\operatorname{ord}_p(a) \geq 0$. The set of the p-adic integers is denoted as $\mathbb{Z}_p$.*

Remark Do not confound $\mathbb{Z}_p$ with the field of the residue classes of the integers modulo p, i.e, $\mathbb{Z}/p\mathbb{Z}$!

Computing with p-adic numbers works similar as with rational numbers. Instead to use the decimal expansion, we work with the coefficients of the powers of p. The difference is that the elementar operations (addition, multiplication, ...) go from left to right rather than right to left.

Example

$$\begin{aligned} & 4 + 3 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \ldots \\ & \underline{- (3 + 4 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^3 + \ldots)} \\ & = 1 + 4 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + \ldots \end{aligned}$$

An other possibility to calculate with p-adic numbers is to consider the partial sums of the p-adic expansion until the nth power and compute modulo p^n. For example, the first terms of the 5-adic expansion of $3/2$ are obtained by computing $3/2 \bmod 5^4 = 314 = 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3$.
For more details on p-adic numbers, see [2].

6

4 Expansion around $\mathcal{O}$ of an elliptic curve

We consider an elliptic curve E/K given by a Weierstrass equation like in (1). We would like to represent the rational points of E with one parameter in K. In order to do this, we make the change of variables

$$z = -\frac{x}{y} \quad \text{and} \quad w = -\frac{1}{y}.$$

We notice that this coordinate z has no connection with the projective coordinate Z. The point $\mathcal{O}$ is now represented as the pair $(0,0)$ in the (z,w)-plane. The Weierstrass equation (1) for E takes the form

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 zw^2 + a_6 w^3 \quad (:= f(z,w)) \quad (3)$$

We substitute the equation into itself recursively and obtain w as a power series in z. Hence,

$$
\begin{aligned}
w &= z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 \\
&= z^3 + (a_1 z + a_2 z^2)\Big(z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3\Big) \\
&\quad + (a_3 + a_4 z)\Big(z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3\Big) \\
&\quad + a_6\Big(z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3\Big) + \cdots \\
&= z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1 a_2 + a_3)z^6 \\
&\quad + (a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4)z^7 + \cdots
\end{aligned}
$$

In fact, we should still show that a such recursion converges to a power series. For a proof of this, we refer to the chapter IV of [4]. Using the power series $w(z)$, we find the Laurent series for x and y,

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3)z^2 - \cdots \quad (4)$$

$$y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3)z + \cdots \quad (5)$$

Thus, we see that the pair $(x(z), y(z))$ yields a solution in the sense of formal power series, i.e., if we substitute the formal power series

$x(z)$, $y(z)$ in the two sides of equality (1), we get the same formal power series on each side. Then, if we want to produce some points of $E(K)$ using z-coordinate, we have to verify that the series $x(z), y(z)$ converge in the field K. In the field $\mathbb{Q}_p$, it is the case if $\operatorname{ord}_p(z) \geq 1$ (i.e. $z \in p\mathbb{Z}_p$) and if the coefficients a_1, a_2, a_3, a_4, a_6 lie in $\mathbb{Z}_p$. This gives an injection $p\mathbb{Z}_p \longrightarrow E(\mathbb{Q}_p)$ whose the inverse is given by $z = -x(z)/y(z)$.

Now, we can look for an addition law on the formal power series that corresponds to the addition law on $E(K)$. This is given by a formal power series. Let (z_1, w_1), (z_2, w_2) two points of E in the (z, w)-plane, then the z-coordinate of the sum of these points z_3 is obtained by

$$
\begin{aligned}
z_3 = F(z_1, z_2) = z_1 + z_2 &- a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) \\
&- (2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3)z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \cdots
\end{aligned}
\tag{6}
$$

The used development to find this function F is explained in [4] chapter IV.

Definition 10. *Let E be an elliptic curve defined over $\mathbb{Q}_p$. The group $\widehat{E}(p\mathbb{Z}_p)$ is the set $p\mathbb{Z}_p$ with the addition law*

$$
x \oplus y := F(x, y) \text{ for all } x, y \in p\mathbb{Z}_p,
$$

where F is the formal power series defined in (6).

5   The reduction modulo p

In this section, we shall introduce the reduction of an elliptic curve $E/\mathbb{Q}_p$ modulo p and provide some results about this.

Definition 11. *Let π the function that reduces p-adic integers modulo p, i.e.*

$$
\begin{aligned}
\pi : \quad \mathbb{Z}_p &\longrightarrow \mathbb{F}_p \\
a_0 + a_1 p + \cdots &\longmapsto a_0,
\end{aligned}
$$

E an elliptic curve defined over $\mathbb{Q}_p$ given by a Weierstrass equation (1) and P be a point of $E(\mathbb{Q}_p)$. The reduction of E modulo p is

the elliptic curve $\widetilde{E}/\mathbb{F}_p$ obtained after reducing the coefficients of E modulo p, namely

$$\widetilde{E} : y^2 + \widetilde{a}_1 xy + \widetilde{a}_3 y = x^3 + \widetilde{a}_2 x^2 + \widetilde{a}_4 x + \widetilde{a}_6,$$

where $\widetilde{a}_i := \pi(a_i)$. The point P can be represented as $(x_1 : y_1 : z_1)$ with $x_1, y_1, z_1 \in \mathbb{Z}_p$ and at least one of x_1, y_1, z_1 in $\mathbb{Z}_p \backslash p\mathbb{Z}_p$. The reduced point $\widetilde{P}$ of P is obtained by reducing every projective coordinate of P modulo p, namely

$$\widetilde{P} = (\pi(x_1) : \pi(y_1) : \pi(z_1)) := (\widetilde{x}_1 : \widetilde{y}_1 : \widetilde{z}_1).$$

We finally get a reduction map

$$E(\mathbb{Q}_p) \longrightarrow \widetilde{E}(\mathbb{F}_p)$$
$$P \longmapsto \widetilde{P}.$$

Remark From now, we will always suppose that the reduce curve $\widetilde{E}/\mathbb{F}_p$ is non-singular.

Definition 12. *The set $E_1(\mathbb{Q}_p)$ is defined as follows*

$$E_1(\mathbb{Q}_p) = \left\{ P \in E(\mathbb{Q}_p) \,\middle|\, \widetilde{P} = \mathcal{O} \right\}$$

Example We give here an example of reduction. Let

$$E : y^2 = x^3 + 39x^2 + x + 39$$

be an elliptic curve defined over $\mathbb{Q}_{43}$ and $P = (10 \cdot 43^{-2} + 10 \cdot 43^{-1} + \cdots, 21 \cdot 43^{-3} + 40 \cdot 43^{-2} + \cdots)$ a point on this curve. We see that its reduced curve modulo 43 has the same Weierstrass equation, because every coefficients lie already in $\mathbb{F}_{43}$. Since $(x : y : 1) = (\frac{X}{Z} : \frac{Y}{Z} : 1)$ holds for any point on an elliptic curve, we have

$$P = (10 \cdot 43^{-2} + \cdots : 21 \cdot 43^{-3} + \cdots : 1) = (10 \cdot 43 + \cdots : 21 + \cdots : 43^3).$$

Hence, we have $\widetilde{P} = \mathcal{O}$, because

$$\widetilde{P} = (0 : 21 : 0) = (0 : 1 : 0).$$

Proposition 13. *Let E be an elliptic curve defined over $\mathbb{Q}_p$ and $\widehat{E}(p\mathbb{Z}_p)$ like above. Then the map*

$$\vartheta_p : \widehat{E}(p\mathbb{Z}_p) \longrightarrow E_1(\mathbb{Q}_p)$$

$$z \longmapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)} \right)$$

is a group isomorphism.

Remark Using the formulas (4) and (5) we see that $\mathrm{ord}_p(x(z)) = -2$ and $\mathrm{ord}_p(y(z)) = -3$ for $z \in p\mathbb{Z}_p$. Moreover, this point P takes the form

$$P = (a_{-2}p^{-2} + \cdots : b_{-3}p^{-3} + \cdots : 1) \sim (a_{-2}p + \cdots : b_{-3} + \cdots : p^3)$$

in projective coordinates. Thus, we deduce that P reduces to $\mathcal{O}$ modulo p i.e., $P \in E_1(\mathbb{Q}_p)$.

For an exhaustive proof of Proposition 13, we refer to [4] p.175.

Proposition 14. *Let E be an elliptic curve defined over $\mathbb{Q}_p$, $\widetilde{E}(\mathbb{F}_p)$ be its reduction curve modulo p and $E_1(\mathbb{Q}_p)$ defined like before. Then*

$$E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \simeq \widetilde{E}(\mathbb{F}_p). \tag{7}$$

Proof. It suffices to consider the reduction map modulo p

$$\pi : E(\mathbb{Q}_p) \longrightarrow \widetilde{E}(\mathbb{F}_p).$$

This function is an homomorphism. By definition, we see that

$$\ker(\pi) = E_1(\mathbb{Q}_p).$$

Applying the first isomorphism Theorem of the group theory on π shows that (7) holds. $\qquad\square$

6   The formal logarithm

In this section, we provide a group isomorphism

$$\log_{\mathcal{F}} : \widehat{E}(p\mathbb{Z}_p) \longrightarrow p\mathbb{Z}_p,$$

10

where $p\mathbb{Z}_p$ is equipped with the usual addition law. We notice that a such function have to satisfy the condition

$$\log_{\mathcal{F}} F(z_1, z_2) = \log_{\mathcal{F}}(z_1) + \log_{\mathcal{F}}(z_2) \quad z_1, z_2 \in p\mathbb{Z}_p, \qquad (8)$$

where F is the formal power series defined in (6). In order to produce this logarithm function, we first look for a power series P, such that

$$P(F(T, S))F_X(T, S) = P(T) \qquad (9)$$

holds, where F_X denotes the partial derivative of F with respect to the first variable. Since $F(0, S) = S$, we get

$$P(S)F_X(0, S) = P(0).$$

Hence, every P satisfying (9) has the form

$$P(T) = aF_X(0, T)^{-1}$$

for an $a \in \mathbb{Q}_p$. We choose here $a = 1$ and P has then the form

$$P(T) = 1 + d_1 T + d_2 T^2 + d_3 T^3 + \cdots . \qquad (10)$$

We are now in position to define the logarithm map. It is the power series

$$\log_{\mathcal{F}}(T) = \int P(T) dT = T + \frac{d_1}{2} T^2 + \frac{d_2}{3} T^3 + \cdots \qquad (11)$$

We verify that it is an homomorphism by integrating the equation (9) with respect to T. We have

$$\log_{\mathcal{F}} F(T, S) = \log_{\mathcal{F}}(T) + C(S),$$

where $C(S)$ is a constant depending on S. Choosing $T = 0$ shows that

$$C(S) = \log_{\mathcal{F}}(S).$$

To show that $\log_{\mathcal{F}}$ produces an isomorphism from $\widehat{E}(p\mathbb{Z}_p)$ to $p\mathbb{Z}_p$, it suffices to find an inverse power series that converges on $p\mathbb{Z}_p$. This inverse is provided by a classical result on the formal power series and the convergence is due to the definition of the p-adic metric d_p.

Remark $\log_{\mathcal{F}}$ induces an isomorphism from $\widehat{E}(p^n\mathbb{Z}_p)$ to $p^n\mathbb{Z}_p$. (see [4] p.126)

For more details, we refer to the book of Silverman [4] chapter IV.

7 Some other results

We give here some results needed for the comprehension of the computation of the discrete logarithm on elliptic curve of trace one.

Definition 15. *Let E be an elliptic curve defined over $\mathbb{Q}_p$. For an integer $n > 0$, we define the subgroup*

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \,|\, \mathrm{ord}_p(x(P)) \leq -2n\} \cup \{\mathcal{O}\},$$

where $x(P)$ denotes the x-coordinate of the point P.

Remark According to Proposition 13, we remark that the set $E_1(\mathbb{Q}_p)$ defined before corresponds to the one defined here.
The group $E_n(\mathbb{Q}_p)$ is isomorph to $\widehat{E}(p^n\mathbb{Z}_p)$, indeed by Proposition 13, we see that

$$\vartheta_p\left(\widehat{E}(p^n\mathbb{Z}_p)\right) = E_n(\mathbb{Q}_p).$$

Hence, by the results of the section 6, we have then $E_n(\mathbb{Q}_p) \simeq p^n\mathbb{Z}_p$. Thus

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \simeq p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \simeq \mathbb{F}_p^+, \tag{12}$$

where $\mathbb{F}_p^+$ denotes the additive group of $\mathbb{F}_p$ i.e., $(\mathbb{Z}/p\mathbb{Z}, +)$.

Computation of a lift

We consider here a point $\widetilde{P}$ of a non-singular elliptic curve $\widetilde{E}$ defined over $\mathbb{F}_p$ and given by

$$\widetilde{E} : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$. E denotes the elliptic curve defined over $\mathbb{Q}_p$ given by the same Weierstrass equation as $\widetilde{E}$.

Definition 16. *Let $\widetilde{P}$ be a point of $\widetilde{E}(\mathbb{F}_p)$. A point $P \in E(\mathbb{Q}_p)$ is said to be the lift of $\widetilde{P}$ if it reduces to $\widetilde{P}$ modulo p.*

We provide here a method to compute a lift of $\widetilde{P} = (\widetilde{x}, \widetilde{y}) \in \mathbb{F}_p \times \mathbb{F}_p$, i.e. to find a pair $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $f(x, y) = 0$, where

$$f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6.$$

First, we choose $x = \widetilde{x}$. We compute then the p-adic expansion of $y = \widetilde{y} + h_1 p + h_2 p^2 + h_3 p^3 + \cdots$ as follows :

1. **Computation of h_1**

   We have to find $0 \leq h_1 \leq p-1$ such that $f(\widetilde{x}, \widetilde{y} + h_1 p) \equiv 0$ (mod p^2). In order to do that, we consider the following Taylor expansion of f:

   $$f(\widetilde{x}, \widetilde{y} + h_1 p) = f(\widetilde{x}, \widetilde{y}) + \frac{\partial f(\widetilde{x}, \widetilde{y})}{\partial y} h_1 p + \text{terms divisible by } p^2$$

   We have then

   $$f(\widetilde{x}, \widetilde{y}) + (2\widetilde{y} + a_1 \widetilde{x} + a_3) h_1 p \equiv 0 \quad (\text{mod } p^2)$$

   By definition of $\widetilde{x}$ and $\widetilde{y}$, we know that $f(\widetilde{x}, \widetilde{y})$ is divisible by p. Hence,

   $$\frac{f(\widetilde{x}, \widetilde{y})}{p} + h_1 (2\widetilde{y} + a_1 \widetilde{x} + a_3) \equiv 0 \quad (\text{mod } p)$$

   and thus

   $$h_1 = -\frac{f(\widetilde{x}, \widetilde{y})}{p(2\widetilde{y} + a_1 \widetilde{x} + a_3)} \mod p$$

2. **$(h_j)_{1 \leq j \leq i} \rightarrow h_{i+1}$**

   We suppose the p-adic expansion known to the term h_i and we show how to find h_{i+1} such that $f(\widetilde{x}, \widetilde{y} + h_1 p + \cdots + h_{i+1} p^{i+1}) \equiv 0$ (mod p^{i+2}). Again, we consider the Taylor expansion

   $$f(\widetilde{x}, \widetilde{y} + h_1 p + \cdots + h_i p^i + h_{i+1} p^{i+1}) = f(\widetilde{x}, \widetilde{y} + h_1 p + \cdots h_i p^i)$$

   $$+ \frac{\partial f(\widetilde{x}, \widetilde{y} + \cdots h_i p^i)}{\partial y} h_{i+1} p^{i+1} + \text{terms divisible by } p^i.$$

   Since $f(\widetilde{x}, \widetilde{y} + h_1 p + \cdots + h_i p^i)$ is divisible by p^{i+1}, we have

   $$\frac{f(\widetilde{x}, \widetilde{y} + \cdots + h_i p^i)}{p^{i+1}} + h_{i+1}(2(\widetilde{y} + h_1 p + \cdots + h_i p^i) + a_1 \widetilde{x} + a_3)) \equiv 0 \quad (\text{mod } p).$$

   Thus,

   $$h_{i+1} = -\frac{f(\widetilde{x}, \widetilde{y} + \cdots + h_i p^i)}{p^{i+1}(2(\widetilde{y} + h_1 p + \cdots + h_i p^i) + a_1 \widetilde{x} + a_3)} \mod p.$$

We then have a method to approximate the p-adic expansion of a lift.

8 Computation of the discrete logarithm

Let $\widetilde{E}$ be a non-singular elliptic curve of trace one defined over a finite field $\mathbb{F}_p$ with p prime, i.e.,

$$\#\widetilde{E}(\mathbb{F}_p) = p \tag{13}$$

Moreover, since p is prime, $\widetilde{E}(\mathbb{F}_p)$ is a cyclic group and therefore $\widetilde{E}(\mathbb{F}_p) \simeq \mathbb{F}_p^+$.

We provide now the algorithm proposed by Nigel Smart (see [5]) which allows to solve the discrete logarithm problem on such curves very rapidly. This problem can be described as following, given two points $\widetilde{P}, \widetilde{Q} \in \widetilde{E}(\mathbb{F}_p)$ with $\widetilde{Q} \in \{ [k]\, \widetilde{P} \mid k \in \mathbb{N} \}$ find m such that

$$\widetilde{Q} = [m]\, \widetilde{P}. \tag{14}$$

At first, we compute the lifts $P, Q \in E(\mathbb{Q}_p)$ of the points $\widetilde{P}, \widetilde{Q}$, using the method explained in Section 7. Since the reduction modulo p is an homomorphism and from (14), we have

$$Q - [m]\, P = R \in E_1(\mathbb{Q}_p). \tag{15}$$

According to Proposition 14, we have

$$\widetilde{E}(\mathbb{F}_p) \simeq E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \tag{16}$$

and by (12) we notice that

$$E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \simeq \mathbb{F}_p^+. \tag{17}$$

Claim 17. *The multiplication by $[p]$ maps the elements of $E(\mathbb{Q}_p)$ to $E_1(\mathbb{Q}_p)$ respectively the elements of $E_1(\mathbb{Q}_p)$ to $E_2(\mathbb{Q}_p)$.*

Proof. Let S an element of $E(\mathbb{Q}_p)$. By (13), the two quotient groups $E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$, $E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p)$ have order p. Then, if we multiply an element of one of these quotient groups by p, we obtain the neutral element. In particular,

$$E_1(\mathbb{Q}_p) = [p]\, (S + E_1(\mathbb{Q}_p)) = [p]\, S + E_1(\mathbb{Q}_p).$$

From this, we conclude that $[p]\, S \in E_1(\mathbb{Q}_p)$. A similar argument works for an element of $E_1(\mathbb{Q}_p)$. $\qquad\square$

Hence, multiplying (15) by p gives

$$[p]\,Q - [m]\,([p]\,P) = [p]\,R \in E_2(\mathbb{Q}_p). \tag{18}$$

Since $[p]\,P$ and $[p]\,Q$ lie in $E_1(\mathbb{Q}_p)$, we can apply the isomorphism

$$\begin{aligned}\psi_p : E_1(\mathbb{Q}_p) &\longrightarrow p\mathbb{Z}_p \\ P &\longmapsto \log_{\mathcal{F}} \circ \vartheta_p^{-1}(P)\end{aligned}$$

on (18) and we get

$$\psi_p\,([p]\,Q) - m\psi_p\,([p]\,P) \in p^2\mathbb{Z}_p. \tag{19}$$

So, this expression can be written in the form

$$c_1 \cdot p + c_2 \cdot p^2 + \cdots - m(d_1 \cdot p + d_2 \cdot p^2 + \cdots) = b_2 \cdot p^2 + \cdots,$$

where c_i's are the coefficients of the p-adic expansion of $\psi_p\,([p]\,Q)$ and d_i's are the coefficients of the p-adic expansion of $\psi_p\,([p]\,P)$. Thus, we finally obtain

$$m = \frac{\psi_p\,([p]\,Q)}{\psi_p\,([p]\,P)} \bmod p = \frac{c_1}{d_1} \bmod p.$$

It suffices now to show how $\psi_p(P)$ can be computed for a point $P \in E_1(\mathbb{Q}_p)$. In order to find m, we only have to compute this modulo p^2. According to the definition of ϑ_p, we have

$$\vartheta_p^{-1}(P) = -\frac{x(P)}{y(P)} \in p\mathbb{Z}_p,$$

where $x(P)$, $y(P)$ denote the x-, y-coordinates of P. Hence, by (11) and the definition of ψ_p, we get

$$\psi_p(P) \equiv -\frac{x(P)}{y(P)} \pmod{p^2}. \tag{20}$$

As conclusion, we notice that the composition of the calculations performed above corresponds in fact to a group homomorphism ϕ_p that sends elements of $\widetilde{E}(\mathbb{F}_p)$ to $\mathbb{Z}/p\mathbb{Z}$,

$$\phi_p : \widetilde{E}(\mathbb{F}_p) \xrightarrow{\text{lift}} E(\mathbb{Q}_p) \xrightarrow{[p]} E_1(\mathbb{Q}_p) \xrightarrow{\vartheta_p^{-1}} \widehat{E}(p\mathbb{Z}_p) \xrightarrow{\log_{\mathcal{F}}} p\mathbb{Z}_p \xrightarrow{\bmod p^2} \mathbb{Z}/p\mathbb{Z}$$

and in particular

$$\phi_p : \mathcal{O} \xrightarrow{\text{lift}} E_1(\mathbb{Q}_p) \xrightarrow{[p]} E_2(\mathbb{Q}_p) \xrightarrow{\vartheta_p^{-1}} \widehat{E}(p^2\mathbb{Z}_p) \xrightarrow{\log_{\mathcal{F}}} p^2\mathbb{Z}_p \xrightarrow{\text{mod } p^2} 0.$$

Finally, we notice that $c_1 = \phi_p(Q)$ and $d_1 = \phi_p(P)$.

Remark
i) This algorithm requires only $O(\log p)$ group operations on $E(\mathbb{Q}_p)$ because the more difficult step in terms of computation is the multiplication with p in (18) that we compute thanks to a square and multiply algorithm.
ii) If $\psi_p([p]\, P) \equiv 0 \pmod{p^2}$, the above calculation fails. In this case, we have to choose an other elliptic curve which reduces to $\widetilde{E}(\mathbb{F}_p)$ modulo p. Fortunately, this occurs only with probability $\frac{1}{p}$.

Example To illustrate the above method, we give here an example over a small field, namely $\mathbb{F}_{1019}$. We consider the curve

$$\widetilde{E} : y^2 = x^3 + 373x + 837$$

and the points $\widetilde{P} = (293, 914)$, $\widetilde{Q} = (794, 329)$. The lifts are computed with the method given in Section 7.

$$P = (293, 914 + 308 \cdot 1019 + 857 \cdot 1019^2 + \cdots)$$

$$Q = (794, 329 + 561 \cdot 1019 + 465 \cdot 1019^2 + \cdots)$$

Using the square and multiply algorithm, we obtain

$[1019]\, P = (867 \cdot 1019^{-2} + 309 \cdot 1019^{-1} + \cdots, 950 \cdot 1019^{-3} + 16 \cdot 1019^{-2} + \cdots)$
$[1019]\, Q = (210 \cdot 1019^{-2} + 952 \cdot 1019^{-1} + \cdots, 300 \cdot 1019^{-3} + 17 \cdot 1019^{-2} + \cdots)$.

By (20), we then get

$$\psi_{1019}([1019]\, P) = 367 \cdot 1019 + 257 \cdot 1019^2 + \cdots$$
$$\psi_{1019}([1019]\, Q) = 305 \cdot 1019 + 431 \cdot 1019^2 + \cdots,$$

and so

$$m = \frac{305}{367} \text{ mod } 1019 = 123.$$

References

1. Ian Blake, Gadiel Seroussi and Nigel Smart, *Eliptic Curves in Cryptography* , London Mathematical Society Lecture Note Series **265**, Cambridge Press.
2. Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions* , Springer-Verlag.
3. Alfred J. Menezes, *Elliptic Curve Public Key Cryptosystem*, Kluwer Academic Publishers.
4. Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106** .
5. Nigel P. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, Journal of Cryptology (**1999**) 12: 193-196.