# Introduction to the Mathematical Foundations of Elliptic Curve Cryptography

Youssef El Housni

# Introduction to the Mathematical Foundations of Elliptic Curve Cryptography

Youssef El Housni

EY Wavespace LAB - Paris

*youssef.el.housni@fr.ey.com*

November 7, 2018

# Contents

**1 Elliptic curves** **3**
1.1 Weistrass equations . . . . . 3
1.2 Elliptic curve isomorphims . . . . . 6

**2 The group of elliptic curves** **8**
2.1 Geometric addition . . . . . 8
2.2 Algebraic addition . . . . . 11
2.3 Scalar multiplication . . . . . 15
2.4 The logarithm problem . . . . . 16

**3 Elliptic curves over finite fields** **17**
3.1 Group order . . . . . 18
3.2 A cyclic subgroup . . . . . 19
3.3 Subgroup order . . . . . 20
3.4 Discrete logarithm problem . . . . . 21

**4 Examples of ECC algorithms** **22**
4.1 ECDH: Elliptic Curve Diffie-Hellman . . . . . 22
4.2 ECDSA: Elliptic Curve Digital Signature . . . . . 23

**Appendices** **25**

**A Hasse's theorem** **26**

**B Chinese remainder theorem** **28**

# Introduction

The history of cryptography can be split into two eras: the classical era and the modern era. The turning point between the two occurred when asymetric cryptography was introduced. These new algorithms were revolutionary because they represented the first viable cryptographic schemes where security was based on the theory of numbers; it was the first to enable secure communication between two parties without a shared secret. Cryptography went from being about securely transporting messages around the world to being able to have provably secure communication between any two parties without worrying about someone listening in on the key exchange. The founding idea is that the key you use to encrypt your data can be made public while the key that is used to decrypt your data can be kept private. What you need for an asymetric cryptographic system to work is a set of algorithms that is easy to process in one direction, but difficult to undo. The first, and still most widely used, algorithm introduced was RSA. Its security relies on the fact that multiplying two prime numbers is easy, but factoring the product into its two component primes is difficult. After RSA, researchers explored other mathematics-based cryptographic solutions looking for other algorithms beyond factoring that serve asymetric schemes. Elliptic curve cryptography was then proposed.
What is an elliptic curve? And how can it be deployed to build an asymetric cryptographic algorithm ?

# Chapter 1

# Elliptic curves

The mathematical objects of ECC are -of course- elliptic curves. For cryptographic purposes we are mainly interested in curves over finite fields but we will study elliptic curves over an arbitrary field $\mathbb{K}$ because most of the theory is not harder to study in a general setting - it might even become clearer.

## 1.1 Weistrass equations

An elliptic curve over a a field $\mathbb{K}$ is a pair $(E, \mathcal{O})$, where $E$ is a cubic equation in the projective geometry and $\mathcal{O} \in E$ a point of the curve called the *base point*, on the line at $\infty$ (in projective geometry two parallel lines meet in a point at $\infty$).

$$(E) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ + a_6Z^3 \tag{1.1.1}$$

Here $\mathcal{O} = [0, 1, 0]$ is the base point and $a_1, ..., a_6 \in \mathbb{K}$ and $X, Y, Z$ are the homogenous coordinates in the projective geometry.
To ease notations we generally write Weistrass equations for our elliptic curve using non-homogenous coordinate (affine geometry) $x = X/Z$ and $y = Y/Z$,

$$(E) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1.2}$$

Considering $\mathbb{K} = \mathbb{R}$, figure (1.1) gives examples of plots in the affine plane of $(E)$ with given values $a_1, ..., a_6 \in \mathbb{R}$.

---

**Question:** Elliptic curves do not resemble ellipses in any way. So why are they called "elliptic" ?
**Answer:** They are solutions to elliptic functions used to find an ellipse's arc length.

---

**Definition:** For a field $\mathbb{K}$ with multiplicative identity $1_{\mathbb{K}}$ and addition identity $0_{\mathbb{K}}$, the field characteristic $p = char(\mathbb{K})$ satisfies: $\underbrace{1_{\mathbb{K}} + 1_{\mathbb{K}} + ... + 1_{\mathbb{K}}}_{\text{p times}} = 0_{\mathbb{K}}$.

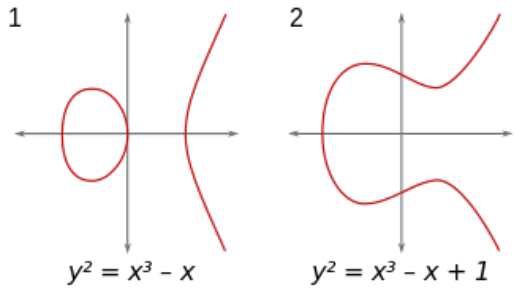


Figure 1.1: Graph of curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$

The equation of $(E)$ can be simplified over $\mathbb{K}$, by the following subsitutions. If the field characteristic $char(\mathbb{K}) \neq 2$, we substitute:

$$y \mapsto y - \frac{a_1}{2}x - \frac{a_3}{2}$$

We have then:

$$(y - \frac{a_1}{2}x - \frac{a_3}{2})^2 + a_1x(y - \frac{a_1}{2}x - \frac{a_3}{2}) + a_3(y - \frac{a_1}{2}x - \frac{a_3}{2}) = x^3 + a_2x^2 + a_4x + a_6$$

$$y^2 + \frac{a_1^2}{4}x^2 + \frac{a_3^2}{4} - a_1xy - a_3y + \frac{a_1a_3}{2}x + a_1xy - \frac{a_1^2}{2}x^2 - \frac{a_1a_3}{2}x + a_3y - \frac{a_1a_3}{2}x - \frac{a_3^2}{2}$$
$$= x^3 + a_2x^2 + a_4x + a_6$$

$$y^2 = x^3 + \underbrace{\left(a_2 + a_1^2/4\right)}_{a_2'}x^2 + \underbrace{\left(a_4 + a_1a_3/2\right)}_{a_4'}x + \underbrace{\left(a_6 + a_3^2/4\right)}_{a_6'}$$

If further $char(\mathbb{K}) \neq 2, 3$ the substitution

$$x \mapsto x - \frac{a_2'}{3}$$

eliminates the $x^2$ term, yielding the simpler equation

$$y^2 = (x - a_2/3)^3 + a_2'\,(x - a_2'/3)^2 + a_4'\,(x - a_2'/3) + a_6'$$
$$y^2 = x^3 - \frac{a_2'^3}{27} - a_2'x^2 - a_2'x^2 + a_2'x^2 + \frac{a_2'^3}{9} - \frac{2}{3}a_2'^2x + a_4'x - \frac{a_2'a_4'}{3} + a_6'$$
$$y^2 = x^3 + \underbrace{\left(a_4' - a_2'^2/3\right)}_{a_4"}x + \underbrace{\left(a_6' + 2a_2'^3/27 - a_2'a_4'/3\right)}_{a_6"}$$

The properties of a field $\mathbb{K}$ with $char(\mathbb{K} = 2)$ is of interest in cryptography as we will see later. With the substitution

$$x \mapsto a_1^2x + a_3/a_1$$
$$y \mapsto a_1^3y + (a_1^2a_4 + a_3^2)/a_1^3$$

we get

$$\left(a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3\right)^2 + a_1\left(a_1^2 x + a_3/a_1\right)\left(a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3\right) + a_3\left(a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3\right)$$
$$= \left(a_1^2 x + a_3/a_1\right)^3 + a_2\left(a_1^2 x + a_3/a_1\right)^2 + a_4\left(a_1^2 x + a_3/a_1\right) + a_6$$

Keeping in mind that $2a_i = 0\,\forall a_i \in \mathbb{K}$ because $char(\mathbb{K}) = 2$ we find

$$y^2 + xy = x^3 + \underbrace{\left(a_1 a_3 + a_1^2 + a_2\right) a_1^{-3}}_{a_2'} x^2$$
$$+ \underbrace{\left(\frac{a_1^4 a_4^2 + a_3^4}{a_1^6} + \frac{a_1^2 a_4 + a_3^2}{a_1^2} + \frac{a_3(a_1^2 a_4 + a_3^2)}{a_1^2} + \frac{a_2 a_3^2}{a_1^2} + \frac{a_4 a_3}{a_1} + a_6\right)}_{a_6'}$$

Let us remind the Weistrass short forms of elliptic curves we have found:

| $char(\mathbb{K})$ | Weistrass Short Form |
|---|---|
| $\neq 2, 3$ | $y^2 = x^3 + ax + b$ |
| $2$ | $y^2 + xy = x^3 + ax^2 + b$ |

Table 1.1: Weistrass short forms for elliptic curves

Note that, in case $char(\mathbb{K}) = 2$ and $a_1 = 0$, we can find another short form $y^2 + ay = x^3 + bx + c$ with the substitution $x \mapsto x + a_2$.
Fields with $char$ 3 are not of interest in ECC and thus there is no need to find short forms in this case.

**Definition:**
A curve $f(x, y)$ is singular in a point $P(x_P, y_P)$ if $\frac{df(x_P,y_P)}{dx} = \frac{df(x_P,y_P)}{dy} = 0$

Our curves have to be non-singular (we will see why later). Rather than studying the singularity of elliptic curves in a general setting, we take a look at our short forms from Table 1.1.
When $char(\mathbb{K}) \neq 2, 3$ we have

$$(E_1) : y^2 = x^3 + ax + b \tag{1.1.3}$$

The curve is singular in a point $P(x_P, y_P)$ if

$$\frac{dE_1(x_P, y_P)}{dx} = 3x_P^2 + a = 0$$
$$\frac{dE_1(x_P, y_P)}{dy} = 2y_P = 0$$

substituing in (1.1.3)

$$0 = (\frac{-a}{3})^{\frac{3}{2}} + a(\frac{-a}{3})^{\frac{1}{2}} + b$$
$$b^2 = (\frac{-a}{3})^3 - \frac{a^3}{3} + \frac{2a^3}{9}$$
$$b^2 = \frac{-4a^3}{27}$$

So our curve of equation (1.1.3) is non-singular if $4a^3 + 27b^2 \neq 0$.
When $char(\mathbb{K}) = 2$ we have

$$(E_2) : y^2 + xy = x^3 + ax^2 + b \tag{1.1.4}$$

The curve is singular in a point $P(x_P, y_P)$ if

$$\frac{dE_2(x_P, y_P)}{dx} = y_P - 3x_P^2 - 2ax_P = y_P + x_P^2 = 0$$
$$\frac{dE_2(x_P, y_P)}{dy} = 2y_P + x_P = x_P = 0$$

substituing in (1.1.4)

$$b = 0$$

So our curve of equation (1.1.4) is non-singular if $b \neq 0$.

**NB:** Note that we can actually find a general condition to define non-singular elliptic curves by computing the discriminat $\Delta$ of (1.1.2) and solving the equation $\Delta = 0$, where

$$\Delta = -(a_1^2 + 4a_2)^2(a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 8(2a_4 + a_1a_3)^3 - 27(2a_4 + a_1a_3)^2$$
$$+ 9(a_1^2 + 4a_2)(2a_4 + a_1a3)(a_3^2 + 4a_6)$$

The calculus is tedious and it is easier to understand the singularities of the curves the way we did.

## 1.2 Elliptic curve isomorphims

In the sequel, we only consider elliptic curves defined over fields $\mathbb{K}$ of characteristic $char(\mathbb{K}) \neq 2, 3$ or $char(\mathbb{K}) = 2$. Let $E$ and $E'$ be two Weistrass elliptic curves of equations

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

**Theorem 1.** $E$ and $E'$ are $\mathbb{K}$-isomorphic if and only if there exists $u \in \mathbb{K}^*$ and $r, s, t \in \mathbb{K}$ such that the change of variables

$$(x, y) \leftarrow (u^2x + r, u^3y + u^2sx + t) \tag{1.2.1}$$

transforms equation $E$ into equation $E'$. Furthermore,

$$\begin{cases} ua'_1 = a_1 + 2s \\ u^2a'_2 = a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 = a_3 + ra_1 + 2t \\ u^4a'_4 = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a'_6 = a_6 + ra_4 - ta_3 + r^2a_2 - rta_1 + r^3 - t^2 \end{cases} \tag{1.2.2}$$

*Proof.* A sketch of the proof is as follows:
Let $(x, y) \in E$, $(x', y') \in E'$ and

$$f(x) = x^3 + a_2x^2 + (a_4 - a_1y)x + (a_6 - y^2 - a_3y)$$
$$g(y) = y^2 + (a_3 + a_1x)y - (x + a_2x + a_4x + a_6)$$

Evaluating $f$ and $g$ in the point at infinity $\mathcal{O}$ gives

$$f(\mathcal{O}) = -y^2 - a_3y + a_6$$
$$g(\mathcal{O}) = -x^3 - a_2x^2 - a_4x - a_6$$

Thus, $x$ and $x'$ have poles of order 2 at $\mathcal{O}$, so both $\{1, x\}$ and $\{1, x'\}'$ are bases of the vector space $\mathcal{L}(2(\mathcal{O}))$. Therefore, $\exists u_1, r \in \mathbb{K}$ such that $x = u_1x' + r$. By analogous reasoning in $\mathcal{L}(3(\mathcal{O}))$, since $y$ and $y'$ have poles of order 3 at $\mathcal{O}$, we prove $\exists u_2, s, t \in \mathbb{K}$ such that $y = sx + u_2y' + t$. □

**Corollary 1.1.** If $char(\mathbb{K}) \neq 2, 3$, the elliptic curves equations are reduced to the short form

$$E : y^2 = x^3 + ax + b$$
$$E' : y^2 = x^3 + a'x + b'$$

where $a_1 = a_2 = a_3 = 0$, $a_4 = a$ and $a_6 = b$.
$E$ and $E'$ are $\mathbb{K}$-isomorphic if $\exists u \in \mathbb{K}^*$ such that $u^4a' = a$ and $u^6b' = b$. Furthermore, we have

$$\begin{aligned} \phi : \quad & E \to E' \\ & (x, y) \to (u^{-2}x, u^{-3}y) \end{aligned}$$

*Proof.* From equation 1.2.2, we obtain $r = s = t = 0$ and so $u^4a' = a$ and $u^6b' = b$ given $u \in \mathbb{K}^*$. □

**Corollary 1.2.** If $char(\mathbb{K}) = 2$, the elliptic curves equations are reduced to

$$E : y^2 + xy = x^3 + ax^2 + b$$
$$E' : y^2 + xy = x^3 + a'x^2 + b'$$

where $a_3 = a_4 = 0$, $a_1 = 1$, $a_2 = a$ and $a_6 = b$.
$E$ and $E'$ are $\mathbb{K}$-isomorphic if $\exists s \in \mathbb{K}$ such that $a' = a + s + s^2$ and $b' = b$. Furthermore, we have

$$\begin{aligned} \phi : \quad & E \to E' \\ & (x, y) \to (x, y + sx) \end{aligned}$$

*Proof.* from equation 1.2.2, we obtain $u = 1, r = t = 0$ and so $a' = a + s + s^2$ and $b' = b$. □

# Chapter 2

# The group of elliptic curves

We refine out definition of elliptic curve as follows:

- if $char(\mathbb{K}) \neq 2, 3$

$$\{(x, y) \in \mathbb{K}^2 \,|\, y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{\mathcal{O}\}$$

- if $char(\mathbb{K}) = 2$

$$\{(x, y) \in \mathbb{K}^2 \,|\, y^2 + xy = x^3 + ax^2 + b, b \neq 0\} \cup \{\mathcal{O}\}$$

With $\mathcal{O}$ the point at $\infty$. We can define a group over elliptic curves. Specifically:

- the elements of the group are the points of an elliptic curve,
- the **identity element** is the point $\mathcal{O}$,
- the **inverse** of a point $P$ is the one symmetric about the $x$-axis,
- addition is given by the following rule: **given 3 aligned, non-zero points P, Q and R, their sum P+Q+R=0**.

Note that with the last rule, we only require three aligned points without respect to order. This means that, if $P$, $Q$ and $R$ are aligned, then $P + (Q + R) = Q + (P + R) + R + (P + Q) = ... = 0$. This way, we have intuitively proved that the **addition** operator is associative and commutative: We are in an **abelian group**.
*But how do we actually compute the sum of two arbitrary points?*

## 2.1 Geometric addition

Thanks to the the abelian group properties, we can write $P + Q + R = 0$ as $P + Q = -R$. This equation, in this form, lets us derive a geometric method to compute the sum between two points $P$ and $Q$: if we draw a line passing through $P$ and $Q$, this line will intersect a third point on the curve $R$. If we take

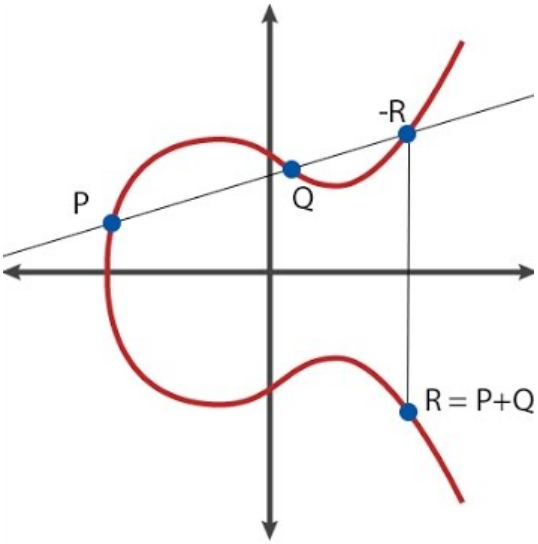


Figure 2.1: Points addition over elliptic curves

the inverse point (the symetric point about $x$-axis), $-R$, we have found the result of $P + Q$ (see figure 2.1).
This geometric method works but needs some refinement. Particularly we need to answer a few questions:

- **What if $P = 0$ or $Q = 0$?**
  We can't draw any line ($0 = \mathcal{O}$ is not on the $xy$-plane). But given that we have defined $0$ as the identity element, $P + 0 = P \, \forall P$.

- **What if $P = -Q$?**
  The line going through the two points is vertical, thus does not intersect the curve in a third point. But $P$ is the inverse of $Q$, then we have $P + Q = P + (-P) = 0$.

- **What if $P = Q$?** There are an infinite number of lines passing through the point. We take the line tangent to the curve, why? consider $Q' \neq P$, as $Q'$ tends towards $P$ the line passing through $P$ and $Q'$ becomes tangent to the curve (see figure 2.2).

- **What if $P \neq Q$, but there is no third point $R$?**
  We are in a case very similar to the previous one. In fact, we are in the case where the line passing through $P$ and $Q$ is tangent to the curve. Let us assume that $P$ is the tangency point, then $P + Q = -P$. If $Q$ were the tangency point, then $P + Q = -Q$.

  ***Proof:***

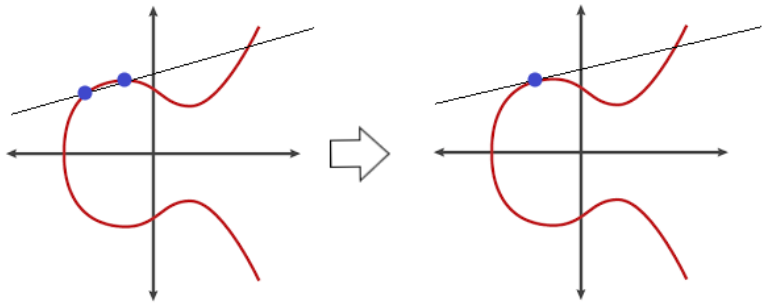

Figure 2.2: Points doublement over elliptic curves

Let $(E)$ be the curve and $(L)$ the line passing through $P$ and $Q$

$$(E) : y^2 = x^3 + ax + b$$
$$(L) : y = mx + n$$

*Lemma:* Let $f$ be a function differentiable in $x = x_P$, $g$ is a function tangent to $f$ in $x = x_P$ if and only if

$$\begin{cases} g(x_P) = f(x_P) \\ g'(x_P) = f'(x_P) \end{cases}$$

Suppose the line $(L)$ passes only through $P$ and $Q$ and let $f$ be the function of $(E)$ and $g$ the function of $(L)$

$$f(x) = \pm\sqrt{x^3 + ax + b}$$
$$g(x) = mx + n$$

The instersection points are solutions to

$$f(x) = g(x)$$

and consequently to

$$f^2(x) = g^2(x) \tag{2.1.1}$$

Because the intersection is supposed to occur only in two points, the cubic equation (2.2.1) has a root $a_1$ and a double root $a_2$

$$g^2(x) - f^2(x) = (x - a_1)^2(x - a_2)$$

Thus, if we differentiate at a point $x$ we obtain

$$2g'(x)g(x) - 2f'(x)f(x) = (x - a_1)(2(x - a_2) + x - a_1) \tag{2.1.2}$$

Evaluating (2.1.2) at $x = a_1$, yields:

– if $f(a_1), g(a_1) \neq 0$, then $f$ is differentiable at $x = a_1$ and

$$\begin{cases} g(a_1) = f(a_1) \\ g'(a_1) = f'(a_1) \end{cases}$$

– if $f(a) = g(a) = 0$, then $f$ is not differentiable at $x = a_1$, and in fact either

$$\lim_{x \to a_1^+} f'(x) = \infty \text{ or}$$
$$\lim_{x \to a_1^-} f'(x) = \infty$$

either way, evaluating the limit in (2.1.2) we find that

$$\lim_{x \to a_1^-} g'(x) = \infty$$

Which implies that $(L)$ must be a vertical line at $x = a_1$, and since $f(a_1) = 0$ the curve $(E)$ is passes through the $x$-axis at $x = a_1$. Keeping in mind that $(E)$ is symetric about $x$-axis, we conclude that $(E)$ must be tangent to $(L)$, as claimed.

The goemetric method is now complete and covers all cases, but if we want a computer to perform point addition, we need to turn the geometric method into an algebraic method.

## 2.2 Algebraic addition

Given an elliptic curve $(E)$ and two points $P(x_P, y_P)$ and $Q(x_Q, y_Q)$, we try here to transform the rules described in the geometric addition section into a set of equation. We first derive equations for a curve over $\mathbb{K}$ with $char(\mathbb{K}) \neq 2, 3$ and then with $char(\mathbb{K}) = 2$. In the first case we have

$$(E) : y^2 = x^3 + ax + b$$

Let $(L)$ be the line passing through $P$ and $Q$

- if $x_P \neq x_Q$

$$(L) : y = mx + n$$

Where

$$m = \frac{y_P - y_Q}{x_P - x_Q}$$
$$n = y_P - mx_P$$
$$= y_Q - mx_Q$$

The intersection points of $(E)$ and $(L)$ are the solutions to the equation

$$\begin{aligned}
&(mx+n)^2 = x^3+ax+b \\
&(mx+y_P-mx_P)^2 = x^3+ax+b \\
&(m(x-x_P)+y_P)^2 = x^3+ax+b \\
&m^2(x^2+x_P^2-2xx_P)+y_P^2+2y_Px-2y_Px_P = x^3+ax+b \\
&x^3-m^2x^2+(a-2m^2x_P-2y_P)x+(b+2y_Px_P-y_P^2-mx_P^2) = 0 \qquad (2.2.1)
\end{aligned}$$

Finding the points of intersection requires solving the cubic equation (2.2.1), which can be tedious (e.g. Tschirnhaus method). But since we know two roots out of the three we can use Vieta's formulas.

**Vieta's Formulas:**
Let $P(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ be a polynomial of degree $n$ with $a_n \neq 0$. By fundamental theorem of algebra, $P(x)$ is known to have $n$ roots $x_1, x_2, ..., x_n$. The formulas relate the coefficients to sums and products of the roots as follows:

$$x_1 + x_2 + ... + x_n = \frac{-a_{n-1}}{a_n} \qquad (2.2.2)$$

$$x_1x_2x...x_n = (-1)^n\frac{a_0}{a_n} \qquad (2.2.3)$$

The polynomial (2.2.1) has three solutions $x_P, x_Q$ and $x_R$. Thus, according to equation (2.2.2) of Vieta's formulas:

$$x_P + x_Q + x_R = \frac{-(-m^2)}{1} = m^2$$

which means

$$x_R = m^2 - x_P - x_R$$

using the equation of $(L)$ we find

$$y_R = m(x_R - x_P) + y_P$$

Keeping in mind that $P+Q = -R$ and that $-R$ is symetric about $x$-axis we write

$$-R(x,y) = R(x,-y)$$

Then the coordinate of $P+Q$ are

$$x = m^2 - x_P - x_Q \qquad (2.2.4)$$

$$y = -m(x - x_P) - y_P \qquad (2.2.5)$$

- if $x_P = x_Q$

$$(L) : y = f'(x_P)(x - x_P) + f(x_P)$$

Where $f(x) = \pm\sqrt{x^3 + ax + b} = y$ the function of elliptic curve $(E)$ and

$$\begin{aligned} f'(x) &= \frac{1}{2}\frac{\pm(3x^2 + a)}{\pm\sqrt{x^3 + ax + b}} \\ &= \frac{3x^2 + a}{2y} \end{aligned}$$

So we have

$$\begin{aligned} f(x_P) &= y_P \\ f'(x_P) &= \frac{3x^2 + a}{2y} \end{aligned}$$

And

$$(L) : y = \underbrace{\frac{3x_P^2 + a}{2y_P}}_{m} x + \underbrace{\left(y_P - \frac{3x_P^2 + a}{2y_P} x_P\right)}_{n}$$

As previously we prove that $P + Q$ coordinates are the same with the new calculated $m$. Where

$$\begin{aligned} m &= \frac{3x_P^2 + a}{2y_P} \\ &= \frac{3x_Q^2 + a}{2y_Q} \end{aligned}$$

In case we have $char(\mathbb{K}) = 2$ we have

$$(E) : y^2 + xy = x^3 + ax^2 + b$$

- if $x_P \neq x_Q$

$$(L) : y = mx + n$$

Where

$$\begin{aligned} m &= \frac{y_P + y_Q}{x_P + x_Q} \\ n &= y_P + mx_P \\ &= y_Q + mx_Q \end{aligned}$$

We are in case $char(\mathbb{K}) = 2$, so $2x_i = 0 \, \forall x_i \in \mathbb{K}$. Thus $-x_i = x_i$.
the $y$ coordinate of $R$ the aligned point with $P$ and $Q$ is

$$y_R = m(x_R + x_P) + y_P$$

Let us call $R^{-1}$ the symetric point of $R$ and find its $y$ coordinate, we have

$$\begin{aligned} y_R^2 + x_R y_R &= x_R^3 + ax_R^2 + b \\ y_{R^{-1}}^2 + x_{R^{-1}} y_{R^{-1}} &= x_{R^{-1}}^3 + ax_{R^{-1}}^2 + b \end{aligned}$$

Thus a quadratic equation

$$y_{R^{-1}}^2 + x_{R^{-1}} y_{R^{-1}} + (x_R y_R + y_R^2) = 0$$

And according to Vieta's formulas, the sum of the two roots $y_R$ and $y_{R^{-1}}$ is equal to

$$y_R + y_{R^{-1}} = -x_R = x_R$$

Thus

$$y_{R^{-1}} = y_R + x_R$$

So the $y$ coordinate of $P + Q$ is

$$y = m(x_R + x_P) + y_P + x_R$$

Let's find the $x$ coordinate using the equation of $(E)$

$$\begin{aligned}(m(x + x_P) + y_P + x_R)^2 + x_R\,(m(x_R + x_P) + y_P + x_R) &= x_R^3 + a x_R^2 + b \\ x_R^3 + (m^2 + am)x_R^2 + (b + m^2 x_P^2 + y_P^2) + (m x_P + y_P)x_R &= 0\end{aligned}$$

using Vieta's formulas, we have

$$\begin{aligned}x_P + x_Q + x_R &= m^2 + m + a \\ x_R &= m^2 + m + a + x_P + x_Q\end{aligned}$$

- if $x_P = x_Q$

We have to find the equation of the tangent $(L) : y = f'(x_P)(x - x_P) + f(x_P)$.
let us derivate $(E)$:

$$\begin{aligned}\frac{d}{dxdy}\left(y^2 + xy\right) &= \frac{d}{dxdy}\left(x^3 + ax^2 + b\right) \\ 2y.dy + y.dx + x.dy &= 3x^2.dx + 2a.x.dx \\ dy\,(2y + x) &= dx(3x^2 + 2ax - y) \\ \frac{dy}{dx} &= \frac{3x^2 + 2ax - y}{2y + x} \\ f'(x) &= \frac{x^2 + y}{x} \\ &= x + \frac{y}{x}\end{aligned}$$

Thus the equation of $(L)$ is

$$(L) : y = \underbrace{\left(x_P + \frac{y_P}{x_P}\right)}_{m} x + \underbrace{(y_P + m x_P)}_{n}$$

As previously the coordinates of $P + Q$ are

$$x = m^2 + m + a + 2x_P = m^2 + m + a$$
$$y = m(x + x_P) + y_P + x$$

Finally let us recapitulate the results in the table below:

| $char(\mathbb{K})$ | Condition | $m$ | Coordinates of $P + Q$ |
|---|---|---|---|
| $\neq 2, 3$ | $x_P \neq x_Q$ | $\frac{y_P - y_Q}{x_P - x_Q}$ | $x = m^2 - x_P - x_Q$<br>$y = -m(x - x_P) - y_P$ |
| $\neq 2, 3$ | $x_P = x_Q$ | $\frac{3x_P^2 + a}{2y_P}$ | $x = m^2 - 2x_P$<br>$y = -m(x - x_P) - y_P$ |
| $= 2$ | $x_P \neq x_Q$ | $\frac{y_P + y_Q}{x_P + x_Q}$ | $x = m^2 + m + a + x_P + x_Q$<br>$y = m(x + x_P) + y_P + x$ |
| $= 2$ | $x_P = x_Q$ | $x_P + \frac{y_P}{x_P}$ | $x = m^2 + m + a$<br>$y = m(x + x_P) + y_P + x$ |

Table 2.1: Algebraic addition equations

## 2.3 Scalar multiplication

Other than addition, we can define another operation: scalar multiplication, that is:

$$nP = \underbrace{P + P + ... + P}_{n\ times}$$

where $n$ is a natural number. It may seem that nomputing $nP$ requires $n$ additions, but if $n$ has $k$ digits the algorithm would be $O(2^k)$. However there is a fast algorithm called **double and add**. Its principle can be better explained with an example. Take $n = 151$, its binary representation is $10010111_2$ and can be turned into a sum of powers of two:

$$151 = 2^7 + 2^4 + 2^2 + 2^1 + 2^0$$

In view of this, we can write:

$$151P = 2^7P + 2^4P + 2^2P + 2^1P + 2^0P$$

What the double-and-add algorithm tells us to do is:

- Take $P$
- Double it to get $2P$
- Add $2P$ to $P$
- Double $2P$ to get $2^2P$

- Add it to the result
- ...

In the end we compute $151P$ performing just seven doublings and four additions. If doubling and adding are both $O(1)$ operations, then this algorithm is $O(\log n)$ which is better than $O(n)$.

## 2.4 The logarithm problem

Given a natural number $n$ and a point $P$ on the elliptic curve, we can compute $Q = nP$ in a polynomial time using the add-and-double algorithm. But what about the other way round? What if we know $Q$ and $P$ and need to find out $n$? This problem is known as the **logarithm problem**. This problem is believed to be a "hard" one to solve and there are no "easy" algorithms that run in polynomial times to do so. To make the problem even harder, a variant is called the **discrete logarithm problem**. As we will see in the next post, if we reduce the domain of our elliptic curves, scalar multiplication remains "easy" while the discrete logarithm becomes "hard". This duality is the key brick of ECC.

# Chapter 3

# Elliptic curves over finite fields

In this section we restrict our curves to finite fields. A finite field is a set of a finite number of elements. An example of finite field we use in cryptography is the set of integers modulo $p$, where $p$ is a prime number. It is generally denoted $GF(p)$ or $\mathbb{F}_p$, and $char(\mathbb{F}_p) = p$.
An elliptic curve is now defined as:

$$\{(x, y) \in \mathbb{F}_p^2 \,|\, y^2 \equiv x^3 + ax + b \pmod p, 4a^3 + 27b^2 \not\equiv 0 \pmod 0\} \cup 0$$

where $0$ is still the point at $\infty$, and $a$ and $b$ are two integers in $\mathbb{F}_p$. This forms a group over $\mathbb{K} = \mathbb{F}_p$ and the equations for addition law are the same as in Table 2.1. Note that the prime $p$ is usually taken very large ($\neq 2, 3$), so we consider that the addition equations are those for $char(\mathbb{K}) \neq 2, 3$.
The figure 3.1 shows points addition over the curve $y^2 \equiv x^3 - x + 3 \pmod{127}$ with $P = (16, 20)$ and $Q = (41, 120)$. Note that the line $y \equiv 4x + 83 \pmod{127}$ that connects thes points "repeats" itself in the plane ("the modulo effect").

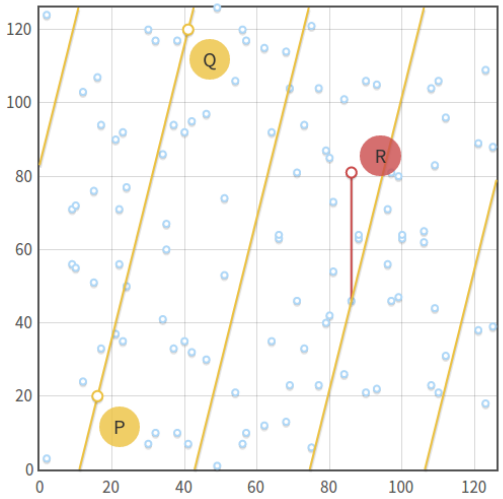


Figure 3.1: Points addition over $E/GF(p)$

## 3.1 Group order

We said that an elliptic curve defined over a finite field has a finite number of points. An important question that we need to answer is: how many points are there exactly? Firstly, let's say that the number of points in a group is called the order of the group. Trying all the possible values for $x$ from $0$ to $p1$ is not a feasible way to count the points, as it would require $O(p)$ steps, and this is "hard" if $p$ is a large prime. Luckily, there's a faster algorithm for computing the order: **Schoof's algorithm**. The algorithm was the first deterministic polynomial time algorithm for counting points on elliptic curves. Before Schoof's algorithm, approaches to counting points on elliptic curves such as the naive and baby-step-giant-step algorithms were, for the most part, tedious and had an exponential running time.
Let $E$ be an elliptic curve over a finite field $\mathbb{F}_p$ where $p$ is a prime $\neq 2, 3$. The short Weistrass equation is given by:

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

with $a, b \in \mathbb{F}_p$.
In order to count the points on an elliptic curve, we compute the cardinality of $E(\mathbb{F}_p)$. Schoof's approach to computing the cardinality $\#E(\mathbb{F}_p)$ makes use of Hasse's theorem on elliptic curves (see appendix A) along with the Chinese remainder theorem (see appendix B) and division polynomials.
Hasse's theorem tells us that the cardinality of the group of points is

$$|p + 1\#E(\mathbb{F}_p)| \leq 2\sqrt{p}$$

or equivalently

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

with $|t| \leq 2\sqrt{p}$ we now have that computing the cardinality of $t$ modulo $N$ where $N > 4\sqrt{p}$ is sufficient for determining $t$, and thus $\#E(\mathbb{F}_p)$. While there is no efficient way to directly compute $t \pmod N$ for general $N$ , it is possible to compute $t \pmod l$ for $l$ a small prime. We choose $S = \{l_1, l_2, ..., l_r\}$ to be a set of distinct primes such that $\prod_{i=1}^{r} l_i = N > 4\sqrt{p}$. Given $t \pmod{l_i}$ for all $l_i \in S$, the chinese remainder theorem allows us to compute $t \pmod N$. In order to compute $t \pmod l$ for a prime $l \neq p$, we make use of the theory of the Frobenius endomorphism $\phi_p$

$$\begin{aligned} \phi_p : E(\mathbb{F}_p) &\to E(\mathbb{F}_p) \\ (x, y) &\to \phi_p(x, y) = (x^p, y^p) \end{aligned}$$

which has the following property:

$$\phi_p^2 - t\phi_p + p = 0 \quad \forall P \in E(\mathbb{F}_p)$$

## 3.2 A cyclic subgroup

We will try here to construct a cyclic subgroup using scalar multiplication

$$nP = \underbrace{P + P + ... + P}_{n\ times}$$

This multiplication has interesting properties in $\mathbb{F}_p$. Take for example the curve $y^2 \equiv x^3 + 2x + 3 \pmod{97}$ and the point $P = (3, 6)$. Now calculate all the multiples of $P$:

- $0P = 0$
- $1P = (3, 6)$
- $2P = (80, 10)$
- $3P = (80, 87)$
- $4P = (3, 91)$
- $5P = 0$
- $6P = (3, 6)$
- $7P = (80, 10)$
- $8P = (80, 87)$
- $9P = (3, 91)$
- ...

Here we can immediately spot two things: firstly, the multiples of $P$ are just five: the other points of the elliptic curve never appear. Secondly, they are repeating cyclically. We can write:

- 5kP=0
- (5k+1)P=P
- (5k+2)P=2P
- (5k+3)P=3P
- (5k+4)P=4P

Not only that, but we can immediately verify that these five points are closed under addition. Which means: however I add $0, P, 2P, 3Por4P$, the result is always one of these five points. Again, the other points of the elliptic curve

never appear in the results. The same holds for every point, not just for $P = (3, 6)$. In fact, if we take a generic $P$:

$$\begin{aligned} nP + mP &= \underbrace{P + P + ... + P}_{n\ times} + \underbrace{P + P + ... + P}_{m\ times} \\ &= \underbrace{P + P + ... + P}_{n+m\ times} \\ &= (n + m)P \end{aligned}$$

Which means: if we add two multiples of $P$, we obtain a multiple of $P$ (i.e. multiples of $P$ are closed under addition). This is enough to prove that the set of the multiples of $P$ is a cyclic subgroup of the group formed by the elliptic curve. The point $P$ is called generator or base point of the cyclic subgroup.

## 3.3 Subgroup order

A question to ask is: what is the order of the subgroup generated by a point $P$? or, equivalently, what the order of $P$ is? To answer this question, we need to consider the following:

- The order is the number of points of the subgroup. So it is the smallest positive integer $n$ such that $nP = 0$.
- The order of the subgroup is linked to the order group by Lagrange's theorem.

**Lagrange's theorem:**
For any finite group $G$, the order of every subgroup $H$ of $G$ divides the order of $G$.
These two information give us a way to find out the order of a subgroup with base point $P$:

- Calculate the elliptic curve's $N$ using Schoof's algorithm.
- Find out all the divisors of $N$.
- For every divisor $n$ of $N$, compute $nP$.
- The smallest $n$ such that $nP = 0$ is the order of the subgroup.

*Example:*
Let $(E) : y^2 = x^3 - x + 3$ be an elliptic curve over $\mathbb{F}_3 7$. $(E)$ forms a group of order $N = 42$ (Schoof's algorithm). Thus, its subgroups may have order $n = 1, 2, 3, 6, 7, 14, 21$ or $42$. **If we try** $P = (2, 3)$ we can see that $P \neq 0, 2P \neq 0, ..., 7P = 0$, hence the order of the generated subgroup is $n = 7$.

In view of this example, it is clear that the hardest step is to find a suitable point $P$ to generate the subgroup. That is: we won't choose a point and then

calculate its order, but we will do the opposite; we will first choose an order that looks good enough anf then we will look for a suitable point. How?

Lagrange's theorem implies that the number $h = \frac{N}{n}$ is always an integer (because $n$ is a divisor of $N$). This number is called the **cofactor** of the subgroup. For every point $P$ of an elliptic curve we have $NP = 0$ because $N$ is a multiple of any candidate $n$. Thus,

$$n(hP) = 0$$

which means that the point $G = hP$ generates a subgroup of order $n$ if $n$ is prime (otherwise the order will be one of the divisors of $n$) and if $G \neq 0$ in which case the subgroup has order $1$.
In the light of this, we can outline the following algorithm:

- Calculate ther order $N$ of an elliptic curve.
- Choose a prime order $n$ of the subgroup.
- Compute the cofactor $h = N/n$.
- Choose a random point $P$ on the curve.
- Compute $G = hP$.
- If $G = 0$, then go to the fourth step. Otherwise we have found a generator of a subgroup with order $n$ and cofactor $h$.

## 3.4 Discrete logarithm problem

As we did when working with continuous elliptic curves, we are now going to discuss the question: if we know $P$ and $Q$, what is $k$ such that $Q = kP$?
This problem, which is known as the discrete logarithm problem for elliptic curves, is believed to be a "hard" problem, in that there is no known polynomial time algorithm that can run on a classical computer. There are, however, no mathematical proofs for this belief.

# Chapter 4

# Examples of ECC algorithms

Our elliptic curve algorithms will work in a cyclic subgroup of an elliptic curve over a finite field. Therefore, our algorithms will need the following parameters:

- The prime $p$ that specifies the size of the finite field
- The coefficients $a$ and $b$ of the elliptic curve equation.
- The base point $G$ that generates our subgroup.
- The order $n$ of the subgroup.
- The cofactor $h$ of the subgroup.

In conclusion, the domain parameters for our algorithms are the sextuple $(p, a, b, G, n, h)$. Actually, the coefficients $a$ and $b$ are genrated using a seed and hash functions in order to give some sort of assurance that the curve has not been specially crafted to expose vulnerabilities known to the author.

**Algorithm scheme:**

- The **private key** is a random integer $d$ chosen from $\{1, ..., n-1\}$.
- The **public key** is the point $H = dG$.

If we know $d$ and $G$ finding $H$ is easy. But if we know $H$ and $G$, finding $d$ is hard (the discrete logarithm problem).

## 4.1 ECDH: Elliptic Curve Diffie-Hellman

ECDH is a variant of the Diffie-Hellman algorithm for elliptic curves. It is actually a key-agreement protocol. The problem it solves is the following: two parties, Alice and Bob, want to exchange information securely, so that a third party, the Man In the Middle, may intercept them, but may not decode them. Here's how it works:

- First, Alice and Bob generate their own private and public keys. We have the private key $d_A$ and the public key $H_A = d_A G$ for Alice, and the keys $d_B$ and $H_B = d_B G$ for Bob. Note that both Alice and Bob are using the same domain parameters: the same base point $G$ on the same elliptic curve on the same finite field.
- Alice and Bob exchange their public keys $H_A$ and $H_B$ over an insecure channel. The Man In the Middle would intercept $H_A$ and $H_B$, but won't be able to find out neither $d_A$ nor $d_B$ without solving the discrete logarithm problem.
- Alice calculates $S = d_A H_B$ (using her own private key and Bob's public key), and Bob calculates $S = d_B H_A$ (using his own private key and Alice's public key). Note that $S$ is the same for both Alice and Bob, in fact:

$$S = d_A H_B = d_A(d_B G) = d_B(d_A G) = d_B H_A$$

## 4.2 ECDSA: Elliptic Curve Digital Signature

The scenario is the following: Alice wants to sign a message with her private key $(d_A)$, and Bob wants to validate the signature using Alice's public key $(H_A)$. Nobody but Alice should be able to produce valid signatures. Everyone should be able to check signatures. Again, Alice and Bob are using the same domain parameters. ECDSA works on the hash of the message, rather than on the message itself. The choice of the hash function is up to us, but it should be obvious that a cryptographically secure hash function should be chosen. The hash of the message ought to be truncated so that the bit length of the hash is the same as the bit length of $n$ (the order of the subgroup). The truncated hash is an integer and will be denoted as $z$.
The algorithm performed by Alice to sign the message works as follows:

- Take a random integer $k$ chosen from $\{1, ..., n_1\}$ (where $n$ is still the subgroup order).
- Calculate the point $P = kG$ (where $G$ is the base point of the subgroup).
- Calculate the number $r = x_P \pmod n$ (where $x_P$ is the $x$ coordinate of $P$).
- If $r = 0$, then choose another $k$ and try again.
- Calculate $s = k^{-1}(z + rd_A) \pmod n$ (where $d_A$ is Alice's private key and $k^{-1}$ is the multiplicative inverse of $k$ modulo $n$).
- If $s = 0$, then choose another $k$ and try again.

The pair $(r, s)$ is the signature.
In order to verify signatures we'll need Alice's public key $H_A$ , the (truncated) hash $z$ and the signature $(r, s)$.

- Calculate the integer $u_1 = s^{-1}z \pmod{n}$.
- Calculate the integer $u_2 = s^{-1}r \pmod{n}$.
- Calculate the point $P = u_1G + u_2H_A$.

The signature is valid only if $r = x_P \pmod{n}$.

# Appendices

# Appendix A

# Hasse's theorem

Let $E(\mathbb{F}_p)$ be an elliptic curve over the finite field $\mathbb{F}_p$ with $p$ prime. Then there exists a unique $t \in \mathbb{Z}$ such that

$$\#E(\mathbb{F}_p) = p + 1 - t \qquad \text{where } |t| < 2\sqrt{p}$$

**Sketch of the proof:**
Define the Frobenius map $f_p : E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ where $(x, y) \to (x^p, y^p)$, then $f_p(P) = P \, \forall P \in E$ because $x^p \equiv x \pmod{p}$ (Little Fermat's Thoerem). Thus, $(f_p - 1)(P) = 0$ which means $ker(f_p - 1) = E(\mathbb{F}_p)$. Further:

$$\#E(\mathbb{F}_p) = \#ker(f_p - 1) = deg(f_p - 1)$$

Now let $t = p + 1 - \#E(\mathbb{F}_p)$. Then by Washington proposition $3.16$ in **[?]**, for $r, s \in \mathbb{Z}$ and $gcd(s, p) = 1$ we have

$$\begin{aligned} deg(rf_p - s) &= r^2 deg(f_p) + s^2 deg(-1) + rs\,(deg(f_p - 1) - deg(f_p) - deg(-1)) \\ &= r^2 p + s^2 + rs(\#E(\mathbb{F}_p) - p - 1) \\ &= r^2 p + s^2 + rs\,(p + 1 - t - p - 1) \\ &= r^2 p + s^2 - rst \end{aligned}$$

Since $deg(rf_p - s) \geq 0$ and $s \neq 0$ then dividing through by $s^2$ gives

$$p\left(\frac{r}{s}\right)^2 - t\left(\frac{r}{s}\right) + 1 \geq 0$$

Having that the set of rational numbers $\frac{r}{s}$ with $gcd(s, p) = 1$ is dense in $\mathbb{R}$ implies that for all $x \in \mathbb{R}$ we have

$$px^2 - tx + 1 \geq 0 \tag{A.0.1}$$

So quadratic equation (A.0.1) has no real roots, hence its discriminant $\Delta$ is non-positive. Thus

$$\Delta = t^2 - 4p \leq 0 \Rightarrow |t| < 2\sqrt{p}$$

Completing the proof.

Or alternatively, one can use Cauchy-Swartz inequality defining the inner product

$$< f, g >= deg(f) + deg(g) - deg(f - g)$$

This yields:

$$| < f, g > |^2 \leq < f, f > . < g, g >$$
$$|deg(f) + deg(g) - deg(f - g)|^2 \leq 2deg(f)2deg(g)$$

subsituing $f$ and $g$ with $f_p$ and $-1$ completes the proof.

# Appendix B

# Chinese remainder theorem

Let $n_1, n_2, ..., n_k$ be pairwise relatively primes($pgcd(n_i, n_j) = 1 \forall i \neq j$). For all $a_1, a_2, ..., a_k$, there exists a unique integer $x$ modulo $n = \prod_{i=1}^{k} n_i$, such that:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &... \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{B.0.1}$$

A solution $x$ might be computed as the following: For every $i$, the integers $n_i$ and $\hat{n_i} = \frac{n}{n_i} = n_1...n_{i-1}n_{i+1}...n_k$ are pairwise relatively primes, and according to BÃl'zout theorem there are integers $u_i$ et $v_i$ such that $u_i n_i + v_i \hat{n_i} = 1$. Let $e_i = v_i \hat{n_i}$, thus we have:

$$\begin{aligned} e_i &\equiv 1 \pmod{n_i} \\ e_i &\equiv 0 \pmod{n_j} \quad \text{pour } j \neq i \end{aligned}$$

A particular solution to this system of equations is:

$$x = \sum_{i=1}^{a_i e_i}$$

This is a unique solution modulo $n = \prod_{i=1}^{k} n_i$.
Proof:
Suppose there are 2 solutions x et y to the system (B.0.1). We have:

$$\begin{aligned} x - y &\equiv 0 \pmod{n_1} \\ x - y &\equiv 0 \pmod{n_2} \\ &... \\ x - y &\equiv 0 \pmod{n_k} \end{aligned}$$

Thus:

$$
\begin{aligned}
(x-y)^k &\equiv 0 \pmod{\prod_{i=1}^{k} n_i} \\
x-y &\equiv 0 \pmod{n} \\
y &\equiv x \pmod{n}
\end{aligned}
$$