UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS

SECCIÓN DE POSGRADO Y SEGUNDA ESPECIALIZACIÓN PROFESIONAL

Tesis para Optar el Grado Académico de Maestro
en Ciencias con Mención en Matemática Aplicada

TÍTULO

CRIPTOGRAFÍA CON CURVAS ELÍPTICAS SOBRE CUERPOS p-ÁDICOS

POR

RUTH MEDINA APARCANA

ASESOR

DR. OSWALDO JOSÉ VELÁSQUEZ CASTAÑÓN

LIMA- PERU

2012

Agradecimientos

A Erlinda y Teodoro, mis padres, por su apoyo incondicional. A mi asesor Oswaldo Velásquez por su consejos, su paciencia y su tiempo. A mis colegas de la Universidad Nacional del Callao y a todas equellas personas que de una u otra manera contribuyeron a la realización de este trabajo.

Abstract

In the present work we study a cryptography algorithm with elliptic curves over p-adic fields proposed by MaoZhi et al.
Security of cryptography with elliptic curves is based on the discrete logarithm problem, being its two main applications the exchange of keys and the digital signature. We have considered some attacks to the discrete logarithm problem and we've implemented some examples using the calculation system PARI/GP. We define the p-adic field $\mathbb{Q}_p$ as the completion of the rational numbers with respect to the p-adic norm and we use the fact that an element $\alpha \in \mathbb{Q}_p$ has a unique p-adic expansion of the form

$$\alpha = \alpha_{-r}p^{-r} + \alpha_{-r+1}p^{\text{`}}-r+1+\cdots+\alpha_{-1}p^{-1}+\alpha_0+\alpha_1 p+\alpha_2 p^2+\cdots$$

Considering the elliptic curves defined over $\mathbb{Q}_p$ and using the formal group of this curve, we find a special finite group $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ that we call the *cryptographic group*, in which cryptography can be done as in $\mathbb{F}_p$, by using approximation theory we find a way to express the coordinates of the representatives of each element of the cryptographic group through finite approximations, and with these approximations we give an effective algorithm to calculate punctual multiplication. Finally we perform the respective security analysis.

Resumen

En el presente trabajo estudiamos un algoritmo de criptografía con curvas elípticas sobre cuerpos p-ádicos propuesto por MaoZhi et al.
La criptografía con curvas elípticas basa su seguridad en el problema de logaritmo discreto, siendo sus dos principales aplicaciones el intercambio de claves y la firma digital. Hemos considerado algunos ataques al logaritmo discreto y hemos implementado algunos ejemplos haciendo uso del sistema de cálculo PARI/GP.
Definimos el cuerpo p-ádico $\mathbb{Q}_p$ como la compleción de los números racionales respecto a la norma p-ádica y usamos el hecho de que un elemento $\alpha \in \mathbb{Q}_p$ tiene una única expansión p-ádica de la forma

$$\alpha = \alpha_{-r}p^{-r} + \alpha_{-r+1}p^{-r+1} + \cdots + \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$$

Considerando las curvas elípticas definidas sobre $\mathbb{Q}_p$ y usando el grupo formal de esta curva, encontramos un grupo finito especial $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ que denominamos *el grupo criptográfico*, en el que se puede hacer criptografía como en $\mathbb{F}_p$, pues usando la teoría de aproximaciones, encontramos una manera de expresar las coordenadas de los representantes de cada elemento del grupo criptográfico por aproximaciones finitas, y con estas aproximaciones damos un algoritmo efectivo para calcular la multiplicación puntual. Finalmente hacemos el análisis de seguridad respectivo.

Contenido

Introducción

La criptografía se puede definir como el arte o ciencia de cifrar y descifrar información, utilizando por ejemplo técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos. La finalidad de la criptografía es garantizar el secreto en la comunicación entre dos entidadaes (personas, organizaciones, etc) y asegurar que la información que se envía sea auténtica, esto es, que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado no haya sido modificado en su tránsito.

Un proceso criptográfico consiste en transformar un mensaje claro en otro que no lo es, para después devolverlo a su forma original, y cumple un rol fundamental en la protección de la información. Los criptosistemas clásicos (simétricos) son aquellos que usan una única clave para cifrar y decifrar los mensajes entre el emisor y el receptor.

En 1976, Whitfield Diffie y Martin Hellman revolucionan la criptografía al introducir el concepto de criptografía de clave pública (criptosistema asimétrico), que surge como una solución al problema de intercambiar claves privadas sobre un canal inseguro. Los sistemas asimétricos son aquellos en los cuales tanto el emisor como el receptor poseen un par de claves: una será de tipo público y la otra será de tipo privado (la cual se debe proteger) y para enviar mensajes el emisor tiene que cifrar el mensaje con la clave publica del receptor, para que así el receptor sea el único que pueda descifrar el mensaje usando su clave privada. Este novedoso sistema de encriptación, basa su seguridad en las funciones matemáticas cuya solución computacional sea difícil en el sentido que, aún conociendo los algoritmos para resolverlos, no es factible su ejecución en un tiempo razonable.

El primer criptosistema de clave pública y probablemente el más exitoso hasta ahora fue propuesto en 1978 por: Ronald Rivest, Adi Shamir y Leonard Adleman del *Massachussets Institute of Tecnology*. El criptosistema RSA basa su seguridad en que no existe una manera rápida y sencilla de factorizar cantidades que son producto de dos números primos grandes.

La criptografía de clave pública utiliza funciones que son sencillas de evaluar, pero difíciles de invertir, "one way function". Una de las más usadas es la *exponencial discreta*, $f : G \to G$, donde G es grupo finito y $f(x) = g^x$. Sin embargo, a partir de los valores conocidos $g^x (= h)$ y g, los cálculos para hallar x requieren un tiempo exponencial. *El problema del logaritmo discreto* es precisamente determinar tal valor de x. La dificultad de resolver el problema del logaritmo discreto radica en la naturaleza del grupo G al cual pertenece el elemento g, por lo que es de gran importancia trabajar con grupos que sean suficientemente complejos, pero que a su vez permitan realizar operaciones sin tener costos muy altos.

En 1985, Neal Koblitz y Victor Miller propusieron de manera independiente, la *criptografía con curvas elípticas*(ECC), cuya seguridad computacional también se basa en el problema del logaritmo discreto. Como los puntos racionales de una curva elíptica forman un grupo abeliano más complicado que el grupo de las unidades de un cuerpo finito, el problema del logaritmo discreto en curvas elípticas es más difícil que el problema del logaritmo discreto en cuerpos finitos. Sin embargo, trabajar con curvas elípticas permite el uso de claves más pequeñas y mantener el mismo nivel de seguridad, que se traduce en ahorro de banda en las redes de comunicación, consumo de memoria, tiempo y capacidad de procesador.

Sea E una curva elíptica sobre un cuerpo K en la forma de Weierstrass, esto es

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

el conjunto de puntos de E que satisfacen esta ecuación mas un punto del infinito $\mathcal{O}$, se denota por $E(K)$. Dados los puntos $P, Q \in E(K)$ y $k \in \mathbb{Z}$, la ecuación

$$Q = [k]P \tag{1}$$

donde la segunda expresión indica: sumar k veces el punto P (si $k > 0$), sumar $-k$ veces el punto $-P$ (si $k < 0$) y $\mathcal{O}$ para $k = 0$. El problema del logaritmo discreto para curvas elípticas consiste precisamente en hallar el valor de k en la ecuación (1) conociendo P y Q. Por esta razón la operación más importante de la criptografía con curvas elípticas es la *multiplicación puntual* dada en (1). En las investigaciones que se realizan sobre criptografía con curvas elípticas generalmente se aplican sobre cuerpos finitos, las curvas elípticas definidas sobre cuerpos infinitos generan grupos infinitos, lo que constituye un problema, por los recursos y el potencial limitado de las computadoras.

Considerando las curvas elípticas definidas sobre cuerpos p-ádicos $\mathbb{Q}_p$ y usando el grupo formal de esta curva, encontramos un grupo finito especial que llamamos *el grupo criptográfico*, en el que se puede hacer criptografía como en $\mathbb{F}_p$, pues usando la teoría de aproximaciones, encontramos una manera de expresar las coordenadas de los representantes de cada elemento del grupo criptográfico por aproximaciones finitas, y con estas aproximaciones damos un algoritmo efectivo para calcular la multiplicación puntual.

Este trabajo está organizado de la siguiente manera: En el primer capítulo damos la definición precisa de curvas elípticas dotandole de una estructura algebraica de grupo abeliano, hacemos un estudio particular de estas sobre cuerpos finitos y finalizamos este capítulo haciendo un estudio de los cuerpos p-ádicos.

En el segundo capítulo presentamos algunos fundamentos básicos de la criptografía como el protocolo de intercambio de claves de Diffie-Hellman, los criptosistemas tradicionales basados en criptografía de clave pública: el criptosistema RSA y el criptosistema ElGamal, vemos también el ataque de Pohlig-Hellman al problema del logaritmo discreto.

En el tercer capítulo hacemos un estudio del grupo formal de una curva elíptica y la reducción de curvas que nos permitirá determinar el grupo cociente $E(\mathbb{Q}_p)/\widehat{E}(\mathcal{M}^n)$ llamado el grupo criptográfico, donde

$$\widehat{E}(\mathcal{M}) = \{P(x, y) \in E / v_p(x) < 0\} \cup \{\mathcal{O}_E\} \subseteq E(\mathbb{Q}_p)$$

y

$$\mathcal{M}^n = \{ z \in \mathcal{M} \ / \ v_p(z) \geq n \ \ \}$$

En el último capítulo, hallamos una forma de encontrar un generador del grupo criptográfico o *grupo de cifrado* a partir de un generador de $\widetilde{E}(F_p)$, luego definimos la aproximación n-ésima de los elementos de $\mathbb{Q}_p$ y probamos que todo punto del grupo de cifrado esta determinado por un punto con coordenadas de aproximación finita de la forma $([x]_{n-3m}, [y]_{n-4m})$, luego calculamos la suma de los puntos en este grupo de cifrado teniendo en cuenta el algebra de las aproximaciones finitas, damos un algoritmo eficiente para el cálculo de $[k]P$ y finalmente demostramos que resolver el problema del logaritmo discreto en el grupo de cifrado es equivalente a resolver el problema del logaritmo discreto en $\widetilde{E}(F_p)$.

Capítulo 1

Teoría básica

1.1 El plano proyectivo

Sea K un cuerpo. Dados (x_1, y_1, z_1) y (x_2, y_2, z_2) en K^3, distintos de $(0, 0, 0)$, diremos que son *equivalentes* si existe un elemento $\alpha \in K$ no nulo tal que

$$(x_1, y_1, z_1) = \alpha(x_2, y_2, z_2)$$

si ese es el caso lo denotaremos así $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ y la clase de (x, y, z) la denotaremos por $(x : y : z)$.
Definimos el *plano proyectivo* $\mathbb{P}^2_K$ o simplemente $\mathbb{P}^2$ como el conjunto constituido por las clases de equivalencia de ternas (x, y, z) con $x, y, z \in K$ donde al menos uno de ellos x, y ó z es no nulo. Entonces

$$\mathbb{P}^2 := \frac{K^3 \setminus \{(0,0,0)\}}{\sim} = \left\{ (x : y : z) \;\; ; \;\; (x, y, z) \in K^3 \setminus \{(0,0,0)\} \right\}$$

Si $(x : y : z) \in \mathbb{P}^2$ con $z \neq 0$, entonces $(x : y : z) = (x/z : y/z : 1)$ y estos son llamados los puntos *finitos* de $\mathbb{P}^2$, y los puntos de la forma $(x : y : 0)$ son llamados *puntos infinitos* de $\mathbb{P}^2$.
Definimos el *plano afín* sobre K como el conjunto de pares ordenados de elementos de K, lo denotaremos por $\mathbb{A}^2(K)$ o simplemente así $\mathbb{A}^2$.

Tenemos entonces una identificación natural de $\mathbb{A}^2$ con $U = \{(x : y : z) \in P^2 \ / \ z \neq 0 \ \}$ dada por

$$\begin{array}{rccc} \varphi : & \mathbb{A}^2 & \longrightarrow & U \\ & (x, y) & \longmapsto & (x : y : 1) \end{array}$$

cuya inversa es

$$\begin{array}{rccc} \psi: & U & \longrightarrow & \mathbb{A}^2 \\ & (x:y:z) & \longmapsto & \left(\dfrac{x}{z}, \dfrac{y}{z}\right) \end{array}$$

de esta manera, el plano afín se identifica con los puntos finitos de $\mathbb{P}^2$. "Añadir" los puntos infinitos a $\mathbb{A}^2$ para obtener $\mathbb{P}^2$, se puede ver como una manera de compactificar el plano afín.

Un polinomio $F(x,y,z) \in K[x,y,z]$ es *homogéneo* de grado $d > 0$ si sus términos son de la forma $ax^iy^jz^k$ donde $a \in K$ e $i+j+k = d$. En este caso, para todo $\lambda \in K$

$$F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x,y,z).$$

Si $F(x,y,z)$ es un polinomio homogéneo de algún grado positivo y si $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$, entonces $F(x_1,y_1,z_1) = 0$ si y sólo si $F(x_2,y_2,z_2) = 0$. Por lo tanto, un cero de un polinomio homogéneo $F(x,y,z)$ en $\mathbb{P}^2$ no depende de la elección del representante de la clase de equivalencia, así tenemos la siguiente buena definición.

Definición 1.1.1 *Sea $F \in K[x,y,z]$ un polinomio homogéneo de grado positivo d. El punto $(x:y:z)$ de $\mathbb{P}^2$ es un cero de F, si $F(x,y,z) = 0$.*

Pero si $G(x,y,z)$ es un polinomio arbitrario, no podemos hablar de un punto $(a:b:c)$ en $\mathbb{P}^2_K$ donde $G(a,b,c) = 0$. Por ejemplo, consideremos el polinomio $G(x,y,z) = x^3 - 2xy + z$, que no es homogéneo y tenemos que $G(1,1,1) = 0$ y $G(2,2,2) = 2$ a pesar que $(1:1:1) = (2:2:2)$.

Si $f(x,y) \in K[x,y]$, podemos homogenizarlo insertando potencias apropiadas de z. Por ejemplo, si $f(x,y) = -y^2 + x^3 + Ax + B$ obtenemos el polinomio homogéneo $F(x,y,z) = -y^2z + x^3 + Axz^2 + Bz^3$. En general si $f(x,y) \in K[x,y]$ es de grado n, entonces

$$F(x,y,z) := z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$$

es un polinomio homogéneo de grado n es $K[x,y,z]$, llamado la *homogenización* de f. Recíprocamente si $F(x,y,z)$ es un polinomio homogéneo en x,y,z sobre K; el polinomio

$$f(x,y) := F(x,y,1)$$

es llamado la *deshomogenización* de F.

Ahora podemos ver lo que significa que dos rectas paralelas se intersecan en el infinito. En efecto: sean $\mathcal{L}_1 : y = mx + b_1$ y $\mathcal{L}_2 : y = mx + b_2$ dos rectas paralelas no verticales y distintas, por lo tanto $m \neq 0$ y $b_1 \neq b_2$, entonces estas tienen las formas homogéneas

$$y = mx + b_1 z, \quad y = mx + b_2 z,$$

y cuando resolvemos estas ecuaciones para encontrar la intersección, obtenemos $(b_1 - b_2)z = 0$ con $b_1 \neq b_2$, es decir

$$z = 0 \quad \text{e} \quad y = mx.$$

Como no podemos tener $(x, y, z) = (0, 0, 0)$, debemos tener que $x \neq 0$. Por lo tanto dividiendo por x encontramos que la intersección de estas rectas es el punto infinito

$$(x : mx : 0) = (1 : m : 0).$$

Análogamente, las rectas verticales distintas $x = c_1$ y $x = c_2$ se intersecan en el punto infinito

$$\mathcal{O} := (0 : 1 : 0).$$

1.2 Curvas elípticas

Sea $\overline{K}$ una clausura algebraica fija de un cuerpo K. Una *curva elíptica* sobre K es una curva proyectiva plana $E \subseteq \mathbb{P}^2(\overline{K})$ no singular definida por una ecuación de la forma

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3. \tag{1.1}$$

donde $a_1, a_2, a_3, a_4, a_6 \in K$.
Si afinizamos la curva elíptica E haciendo $z = 1$, obtenemos una curva dada por la ecuación afín

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1.2}$$

Si $car(K) \neq 2$, hacemos el siguiente cambio

$$\begin{cases} x &= x \\ y &= \frac{1}{2}(Y - a_1 x - a_3), \end{cases}$$

y conseguimos describir la curva con la ecuación

$$Y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \tag{1.3}$$

donde

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad \text{y} \quad b_6 = a_3^2 + 4a_6.$$

Si además $car(K) \neq 3$. En la ecuación (1.3), hacemos el cambio

$$\begin{cases} x &= X - \frac{1}{12}b_2 \\ Y &= Y, \end{cases}$$

obteniendo la ecuación

$$Y^2 = X^3 - \frac{c_4}{2^4 \cdot 3}X - \frac{c_6}{2^5 \cdot 3^3} \tag{1.4}$$

con

$$c_4 = b_2^2 - 24b_4, \quad \text{y} \quad c_6 = b_2^3 + 36b_2b_4 - 216b_6.$$

Y así tenemos que E esta dada por la ecuación

$$y^2 = x^3 + Ax + B \tag{1.5}$$

donde $A = -\frac{c_4}{2^4 \cdot 3}$ y $B = -\frac{c_6}{2^5 \cdot 3^3}$.

La ecuación dada en (1.5) es conocida como la **ecuación de Weierstrass** de la curva elíptica E, mientras (1.2) es llamada *ecuación general de Weierstrass*.

Por otro lado, supongamos que comenzamos con una ecuación de la forma

$$cy^2 = dx^3 + ax + b$$

con c y d no nulos. Multiplicando ambos lados de la ecuación por c^3d^2 obtenemos

$$(c^2dy)^2 = (cdx)^3 + (ac^2d)(cdx) + (bc^3d^2),$$

y haciendo el cambio de variables siguiente

$$Y = c^2dy \quad \text{y} \quad X = cdx$$

obtenemos de nuevo, una ecuación en la forma de Weierstrass.

Para ver qué puntos de E pertenecen al infinito, hacemos $z = 0$ en (1.1) y obtenemos que $x^3 = 0$, por lo tanto $x = 0$ e y puede ser cualquier elemento no nulo

de K, y dividiendo por y encontramos que $\mathcal{O} = (0 : 1 : 0)$ es el **único** punto del infinito, en E. Así

$$E(K) = \left\{(x : y : z) \in \mathbb{P}^2; \quad y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\right\},$$

o bien

$$E(K) = \left\{(x, y) \in A^2(K); \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \left\{\mathcal{O}\right\}.$$

Como podemos observar, al afinizar de esta forma sólo perdemos un punto de la curva, el punto $\mathcal{O}$. Es decir todos los puntos pueden encontrarse en esta afinización salvo el punto del infinito $\mathcal{O}$. Todos los puntos de $E(K)$, excepto el $\mathcal{O}$, son llamados puntos finitos.

Y como vimos al final de la sección (1.1) el punto $\mathcal{O} = (0 : 1 : 0)$ pertenece a toda recta vertical. Luego toda recta vertical interseca a la curva elíptica E en este punto del infinito.

En adelante, casi siempre trabajaremos con coordenadas afines y tratamos el punto del infinito como un caso especial, siempre que sea necesario.
Un punto $P = (x_0 : y_0 : z_0) \in E(K)$ es un *punto singular* si

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

donde F es el polinomio homógeneo que define la curva proyectiva $E(K)$, es decir

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3).$$

Si la curva no tiene puntos singulares se dice que es una *curva no singular*, regular o lisa. Por ejemplo, el punto $\mathcal{O}$ es no singular, ya que

$$\frac{\partial F}{\partial z}(\mathcal{O}) = y^2 + a_1xy + 2a_3yz - (a_2x^2 + 2a_4xz + 3a_6z^2)\Big|_{(0,1,0)} = 1 \neq 0$$

La *recta tangente* a la curva proyectiva $E(K)$, en un punto no singular $P \in E(K)$, es la recta de ecuación

$$\frac{\partial F}{\partial x}(P) \cdot x + \frac{\partial F}{\partial y}(P) \cdot y + \frac{\partial F}{\partial z}(P) \cdot z = 0.$$

Por ejemplo, la recta tangente a $E(K)$ en el punto $\mathcal{O}$ es $z = 0$.
Ahora si

$$\begin{aligned} E(K) &= \{(x : y : z) \in \mathbb{P}^2 / y^2z = x^3 + Axz^2 + Bz^3\} \\ &= \{(x, y) \in \mathbb{A}^2 / y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}. \end{aligned}$$

El discriminante y el invariante j de $E(K)$ son respectivamente

$$\triangle := -16(4A^3 + 27B^2) \qquad \text{y} \qquad j := 1728\frac{(4A)^3}{\triangle}. \tag{1.6}$$

Supongamos que

$$f(x) = x^3 + Ax + B = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

con $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$. Se demuestra que el *discriminante* de esta cúbica

$$d := \left[(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\right]^2$$

es igual a $-(4A^3 + 27B^2)$. Por lo tanto,

$$d = -(4A^3 + 27B^2) \qquad \text{y} \qquad \triangle = 16 \cdot d \tag{1.7}$$

Teorema 1.1 *Sea $\mathcal{C}$ la curva cúbica dada por $y^2 = x^3 + Ax + B$. Entonces*

$$\begin{aligned} \mathcal{C} \text{ es singular} \quad & \text{si y sólo si} \quad \triangle = 0 \\ & \text{si y sólo si} \quad d = 0 \\ & \text{si y sólo si} \quad f \text{ tiene raíces multiples} \end{aligned}$$

Por lo tanto, $\mathcal{C}$ es no singular si y sólo si $4A^3 + 27B^2 \neq 0$.

Prueba. Es obvio, por la definición del discriminante, que $d = 0$ es equivalente a que $f(x)$ tenga raíces multiples. También es obvio que $\triangle = 0$ si y solo si $d = 0$, por la relación (1.7). Por lo tanto, sólo nos queda ver que $\mathcal{C}$ es singular si y sólo si $d = 0$. Nuestra curva viene dada por

$$\mathcal{C} : y^2z = x^3 + Axz^2 + Bz^3.$$

Sabemos que el único punto de intersección de $\mathcal{C}$ con la recta del infinito, $z = 0$, es $\mathcal{O}$ (que es no singular). Por lo tanto, si un punto $P = (x_0 : y_0 : z_0) \in \mathcal{C}$ es singular se tiene que $z_0 \neq 0$. Así que podemos suponer que $z_0 = 1$. Ahora bien, si un punto $P = (x_0 : y_0 : 1) \in \mathcal{C}$ es singular, se ha de tener que

$$\frac{\partial F}{\partial x}(x_0, y_0, 1) = \frac{\partial F}{\partial y}(x_0, y_0, 1) = \frac{\partial F}{\partial z}(x_0, y_0, 1) = 0.$$

donde $F(x, y, z) = y^2z - (x^3 + Axz^2 + Bz^3)$. Es decir,

$$\begin{cases} -3x_0^2 - A &= 0, \quad (i) \\ 2y_0 &= 0, \quad (ii) \\ y_0^2 - 2Ax_0 - 3B &= 0. \quad (iii) \end{cases}$$

La ecuación (ii) nos dice que $y_0 = 0$. Ahora vamos a distinguir dos casos, cuando $A \neq 0$ y cuando $A = 0$.

1. $A \neq 0$.

   Entonces por (iii) tenemos que $x_0 = -\frac{3B}{2A}$, y sustituyendo esto en (i) obtenemos

   $$\frac{1}{4A^2}(27B^2 + 4A^3) = 0 \text{ si y solo si } d = 0$$

2. $A = 0$.

   Tenemos

   $$\begin{cases} -3x_0^2 = 0 \\ -3B = 0 \end{cases} \text{ si y solo si } \begin{cases} x_0 = 0. \\ B = 0. \end{cases}$$

   Con lo que llegamos a que esto ocurre si y sólo si $d = 27B^2 = 0$. □

Sea $\triangle$ el discriminante de la curva definida por

$$\mathcal{C} = \left\{(x, y) \in \mathbb{A}^2 \ / \ y^2 = f(x) = x^3 + Ax + B \ \right\} \cup \left\{\mathcal{O}\right\}$$

1. $\triangle \neq 0$, entonces $\mathcal{C}$ es **no singular**, por lo tanto $\mathcal{C}$ es una curva elíptica. Se tienen los dos casos siguientes:

   (a) $\triangle > 0$, entonces la ecuación $f(x) = 0$ tiene tres raíces reales distintas, y el grafo real afín de la curva tiene dos componentes conexa: una no compacta, que es la componente de la curva cuyo cierre proyectivo contiene a $\mathcal{O}$, y una compacta de forma oval.

   (b) $\triangle < 0$, entonces la ecuación $f(x) = 0$ tiene una sola raíz real, y el grafo real afín de la curva tiene una sola componente conexa.

2. $\triangle = 0$, entonces $\mathcal{C}$ **es singular** y contiene un sólo punto singular. Este caso se divide en tres subcasos. Como el polinomio $f(x)$ tiene al menos una raíz doble, escribimos $f(x) = (x - \alpha)^2(x - \beta)$ y como $f(x) = x^3 + Ax + B$ obtenemos que $2\alpha + \beta = 0$, por lo tanto $f(x) = (x - \alpha)^2(x + 2\alpha)$.

   (a) $\alpha > 0$ entonces el grafo real afín tiene una única componente conexa, que posee un punto doble en $x = \alpha$. Las tangentes en el punto doble tienen pendientes reales distintas

   (b) $\alpha < 0$ entonces el grafo real afín tiene dos componentes conexas. una no compacta, y un punto aislado de coordenadas $(\alpha, 0)$. De hecho este punto es de nuevo un punto doble, pero con tangentes distintas de pendientes complejas

(c) $\alpha = 0$ entonces la curva tiene una cúspide en $(0, 0)$, es decir las tangentes en el punto singular $(0, 0)$ son la misma

1.2.1 Suma de puntos en una curva elíptica

Las curvas elípticas definen de manera natural una operación llamada suma, con la cual se obtiene un grupo abeliano sobre el conjunto de sus puntos; y es a partir de esta suma, que quedará definido el múltiplo de un punto, que es la suma del punto consigo mismo, un número determinado de veces.
Dados dos puntos $P, Q \in E(K)$, el teorema de Bezout asegura la existencia de un tercer punto de intersección entre la recta $\mathcal{L}$ que une los puntos P y Q; y $E(K)$.

Sea E una curva elíptica con ecuación $y^2 = x^3 + Ax + B$ y sean P_1, P_2 puntos en E tales que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$. Definiremos un nuevo punto P_3.

Sea la recta $\mathcal{L}$ que pasa por P_1 y P_2, en el espacio proyectivo veremos más adelante que $\mathcal{L}$ interseca a E en un tercer punto P_3', que reflejamos con respecto del eje x y obtenemos P_3; luego definimos

$$P_1 + P_2 = P_3.$$

Consideremos primero $P_1 \neq P_2$ y que ambos sean distintos de $\mathcal{O}$. La recta $\mathcal{L}$ a través de P_1 y P_2 tiene pendiente igual a

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Supongamos que $x_1 \neq x_2$. La ecuación de $\mathcal{L}$ es $y = m(x - x_1) + y_1$. Para encontrar la intersección con E, sustituímos para obtener

$$[m(x - x_1) + y_1]^2 = x^3 + Ax + B.$$

Esto se puede escribir de la forma

$$x^3 - m^2x^2 + ax + b = 0$$

Las tres raíces de esta cúbica corresponden a los tres puntos de intersección de $\mathcal{L}$ con E, pero en este caso ya conocemos dos raíces x_1 y x_2, pues P_1 y P_2 son puntos de E y $\mathcal{L}$. Por lo tanto, si $P_3' = (x_3', y_3')$, obtenemos

$$x_3' = m^2 - x_1 - x_2$$

e

$$y_3' = m(x_3' - x_1) + y_1.$$

Ahora, reflejamos con respecto al eje x para obtener el punto $P_3 = (x_3, y_3)$ donde

$$x_3 = m^2 - x_1 - x_2 \quad \text{e} \quad y_3 = m(x_1 - x_3) - y_1.$$

En el caso que $x_1 = x_2$, pero $y_1 \neq y_2$, la recta a través de P_1 y P_2 es vertical, y por lo tanto interseca a E en $\mathcal{O}$. Reflejando $\mathcal{O}$ con respecto al eje x obtenemos el mismo punto $\mathcal{O}$ (es por esto que ponemos $\mathcal{O}$ al tope y al fondo del eje y). Por lo tanto, en este caso

$$P_1 + P_2 = \mathcal{O}.$$

Ahora consideremos el caso $P_1 = P_2 = (x_1, y_1)$. Cuando los dos puntos coinciden tomamos la recta $\mathcal{L}$ a través de ellos como la recta tangente, y la diferenciación implícita nos permite encontrar la pendiente m de esta recta

$$m = \frac{3x_1^2 + A}{2y_1} \quad \text{si } y_1 \neq 0$$

(cuando $y_1 = 0$, la recta es vertical y $P_1 + P_2 = \mathcal{O}$, como antes). Por lo tanto, asumiendo que $y_1 \neq 0$, la ecuación de $\mathcal{L}$ es

$$y = m(x - x_1) + y_1,$$

y como antes obtenemos la ecuación cúbica

$$x^3 - m^2x^2 + \alpha x + \beta = 0.$$

Esta vez, conocemos sólo una raíz x_1, pero es una raíz doble pues $\mathcal{L}$ es tangente a E en P_1. Procediendo como antes obtenemos que

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

Finalmente, supongamos que $P_2 = \mathcal{O}$. La recta a través de P_1 y $\mathcal{O}$ es una recta vertical que interseca a E en el punto P_1' que es la reflexión de P_1 con respecto al eje x. Cuando reflejamos P_1' con respecto al eje x para obtener $P_3 = P_1 + P_2$, regresamos a P_1. Luego,

$$P_1 + \mathcal{O} = P_1$$

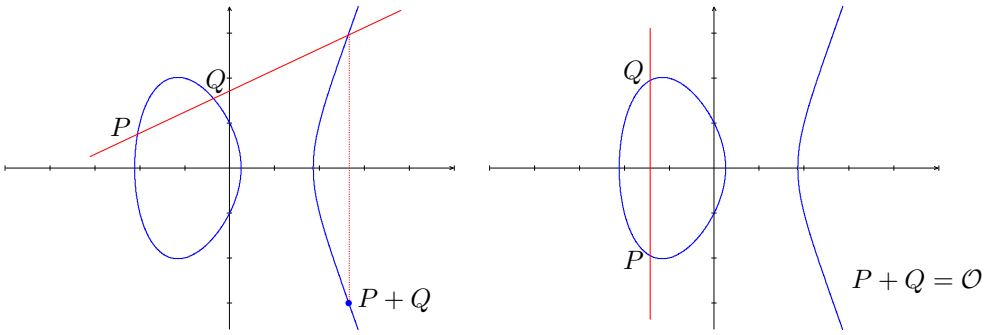
para todo punto $P_1 \in E$.
Resumamos esta discusión en la siguiente proposición.

Proposición 1.1 (Suma de puntos en una curva elíptica)
Sea E una curva elíptica sobre un cuerpo K definida por $y^2 = x^3 + Ax + B$. Sean $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ puntos en E con $P \neq \mathcal{O}$ y $Q \neq \mathcal{O}$. Entonces $P + Q = (x_3, y_3)$ es como sigue:

i) Si $x_1 \neq x_2$, entonces

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{donde } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

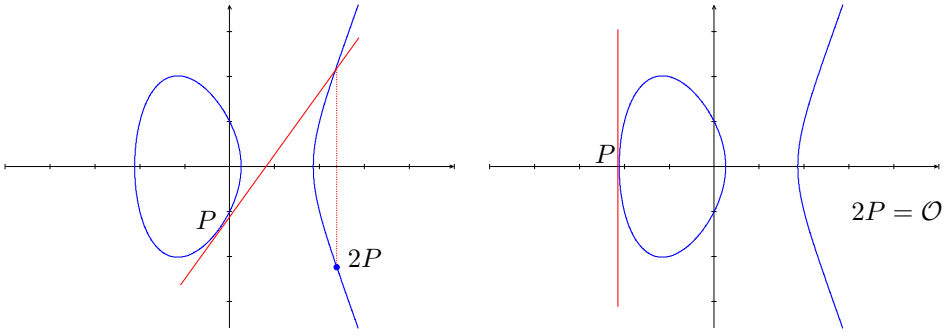
ii) Si $x_1 = x_2$ pero $y_1 \neq y_2$, entonces $P + Q = \mathcal{O}$.



iii) Si $P = Q$ y $y_1 \neq 0$, entonces

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{donde } m = \frac{3x_1^2 + A}{2y_1}.$$

iv) Si $P = Q$ y $y_1 = 0$, entonces $P + Q = \mathcal{O}$.



Además, definimos

$$P + \mathcal{O} = P \quad \text{para todo } P \text{ en } E.$$

Por lo tanto $E(K)$ es cerrado bajo la ***suma de puntos***.

Teorema 1.2 *La suma de puntos en una curva elíptica E, satisface las siguientes propiedades:*

1. *Conmutatividad:* $P_1 + P_2 = P_2 + P_1$ *para todo* $P_1, P_2 \in E$.
2. *Existencia del neutro:* $P + \mathcal{O} = P$ *para todo* $P \in E$.
3. *Existencia de inverso: Dado* $P \in E$, *existe* $P' \in E$ *tal que* $P + P' = \mathcal{O}$.
4. *Asociatividad:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ *para todo* $P_1, P_2, P_3 \in E$.

Esto significa que los puntos de E forman un grupo abeliano aditivo con $\mathcal{O}$ como elemento neutro.

Prueba. La conmutatividad, es obvia pues la recta que une P_1 y P_2 es la misma que la recta que une P_2 y P_1.

La propiedad de existencia del elemento neutro $\mathcal{O}$, se cumple por definición. Ahora, si P está en E y P' es la reflexión de P con respecto al eje x, entonces $P + P' = \mathcal{O}$.

La asociatividad es la propiedad menos obvia de la suma de puntos de E, los detalles de la prueba los podemos encontrar en [Was03] pág. 20.

Observación: En la ecuación de Weierstrass, si $P = (x, y)$, entonces $-P = (x, -y)$. Para la ecuación general de Weierstrass (1.2), si $P = (x, y)$, se prueba que

$$-P = (x, -a_1x - a_3 - y).$$

Ejemplo 1.1 Dada la curva elíptica definida sobre $\mathbb{Q}$

$$E : y^2 = x^3 - 82x,$$

si estos son puntos en $E(\mathbb{Q}) : (-8, 12), (-1, 9), (0, 0)$, tenemos que

$$[2](-8, 12) = (-8, 12) + (-8, 12) = \left(\frac{5329}{144}, -\frac{377191}{1728}\right).$$

También tenemos

$$(0, 0) + (-8, 12) = \left(\frac{41}{4}, \frac{123}{8}\right), \quad [2](-1, 9) = \left(\frac{6889}{324}, \frac{517339}{5832}\right).$$

Estos resultados se han obtenido utilizando el sistema de cálculo PARI/GP.

1.2.2 Multiplicación Puntual

Si P es un punto de una curva elíptica E, y k es un entero , entonces $[k]P$ denota $P + P + \cdots + P$ (con k sumandos, $k > 0$).
Si $k < 0$, entonces $[k]P = (-P) + (-P) + \cdots + (-P)$, con $|k|$ sumandos.
Para calcular *la multiplicación puntual o multiplicación escalar* $[k]P$, cuando k es un entero muy grande, es más rápido y eficiente usar el método de las *doblar y sumar*(double and add) puntos elípticos.
Este algoritmo se basa en la idea de que para multiplicar k veces el punto P, se considera la representación binaria del escalar k y se realiza de izquierda a derecha de tal manera que a cada paso se dobla el punto; y el resultado se suma con el punto, si fuera necesario por ejemplo: Consideremos $k = 15$ y su representación binaria es $15 = 2^3 + 2^2 + 2 + 1$ entonces tenemos que $[15]P = ([2]([2]([2]P + P) + P) + P$ y $[40]P = [2]([2](([2]([2]([2]P)) + P)))$ siendo la representación binaria de $40 = 2^5 + 2^3$.

Este método nos permite calcular $[k]P$ para k grande, más rápidamente. La dificultad es que el tamaño de las coordenadas de los puntos se incrementa velozmente (como en el ejemplo 1.1) si trabajamos por ejemplo sobre los números racionales.
Sin embargo, cuando trabajamos sobre un cuerpo finito, por ejemplo $\mathbb{F}_p$, este no es un problema, porque podemos reducir módulo p continuamente y por tanto los números implicados son relativamente pequeños.
Este método se puede implementar mediante el siguiente algoritmo.

Algoritmo para calcular $[k]P$

Sea k un entero positivo y sea P un punto en una curva elíptica E. El siguiente procedimiento genera, el punto $[k]P$.
Inicio: Dados: un entero $a = k$, los puntos $A = \mathcal{O}$ y $B = P$.
Paso 1. Si a es par, sea $a = a/2$, y sean $A = A$, $B = 2B$.
Paso 2. Si a es impar, sea $a = a - 1$, y sean $A = A + B$, $B = B$.
Paso 3. Si $a \neq 0$, ir al paso 2.
Salida: A. (El valor A, es $[k]P$).

1.3 Curvas elípticas sobre cuerpos finitos

Dado un cuerpo K y E/K una curva elíptica, sabemos que $E(K)$ es un grupo abeliano con la suma elíptica. En 1922, Mordel, demostró el siguiente teorema

Teorema 1.3 *(Mordell-Weil). $E(K)$ es un grupo abeliano generado por un número finito de puntos racionales.*

Encontramos una prueba detallada de este teorema en [Sil09],capítulo VIII, pág. 189. Este resultado es válido por ejemplo para $\mathbb{Q}$, para un cuerpo finito F_q, etc.
El teorema de Mordell-Weil, y el teorema fundamental de clasificación de grupos abelianos finitamente generados, implican que para toda curva elíptica E/K el grupo de puntos racionales tiene la siguiente forma:

$$E(K) = E(K)_{torsion} \bigoplus \mathbb{Z}^r$$

donde $E(K)_{torsion} = \{P \in E(K)/\text{existe}m \in \mathbb{N} \text{ tal que } \ m.P = \mathcal{O}\}$ el conjunto de los puntos de torsión (o de orden finito), y r que depende de la curva E a estudiar, es un entero no negativo que es llamado *el rango* de la curva elíptica. Si la curva elíptica E está dada sobre un cuerpo $\mathbb{F}$ con un número finito de elementos, genera un grupo abeliano finito $E(\mathbb{F})$, pues las coordenadas x,y de sus puntos, se escogen de una cantidad finita de elementos. En criptografía generalmente se trabaja con curvas elípticas sobre cuerpos finitos como $\mathbb{F}_p$ y $\mathbb{F}_{2^m}$, donde p es un primo y m es un entero positivo.
Las curvas elípticas sobre cuerpos finitos tienen aplicaciones en el reconocimiento de primos (elliptic curve primality proving ECPP) y la factorización de enteros (Elliptic curve method ECM), y el interés de las curvas elípticas para la criptografía es que por el momento no se conoce ningún algoritmo subexponencial para resolver el PLD.

Ejemplo 1.2 Sea E la curva $y^2 = x^3 + x + 6$ sobre $\mathbb{F}_7$.
Para determinar los puntos en E, primero hacemos una lista de posibles valores de x, luego una lista de los valores de $x^3+x+6 \pmod 7$, y una lista de raíces cuadradas

y de $x^3 + x + 6 \pmod 7$. Esto nos lleva a los puntos de E.

x	$x^3 + x + 6$	y	puntos
0	6	$--$	$----$
1	1	± 1	$(1,1),(1,6)$
2	2	± 4	$(2,4),(2,3)$
3	1	± 1	$(3,1),(3,6)$
4	4	± 2	$(4,2),(4,5)$
5	3	$--$	$----$
6	4	± 2	$(6,2),(6,5)$

Por lo tanto, $E(\mathbb{F}_7)$ es un grupo de orden 11, isomorfo a $\mathbb{Z}_{11}$.
Ahora consideremos el elemento $\alpha = (2,4)$ de la curva E, entonces $2\alpha = (2,4) + (2,4)$.
La pendiente de la recta que une los dos puntos es

$$m = \frac{3.2^2 + 1}{2.4} = 6(\mod 7).$$

Entonces tenemos que

$$x_3 = m^2 - 2 - 2 = 4, (\mod 7)$$

y

$$y_3 = 6(2 - 4) - 4 = 5(\mod 7)$$

Luego $2\alpha = (x_3, y_3) = (4,5)$

En los siguientes teoremas veremos dos importantes restricciones para el grupo $E(\mathbb{F}_q)$.

Teorema 1.4 (Cassels) *Sea E una curva elíptica definida sobre el cuerpo finito $\mathbb{F}_q$, entonces*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad o \quad E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

para algún entero $n \geq 1$, o enteros $n_1, n_2 \geq 1$ con $n_1 \mid n_2$.

Prueba. Como todo grupo abeliano finito es isomorfo a una suma directa de grupos cíclicos

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r},$$

con $n_i \mid n_{i+1}$ para $i \geq 1$ y como para cada i el grupo $\mathbb{Z}_{n_i}$ tiene n_1 elementos de orden que divide a n_1, encontramos que $E(\mathbb{F}_q)$ tiene n_1^r elementos de orden que divide a n_1. Existen a lo más n_1^2 puntos con esta propiedad (aún si permitimos coordenadas en la clausura algebraica de $\mathbb{F}_q$). Por lo tanto $r \leq 2$. Este es el resultado deseado (el grupo es trivial si $r = 0$; este caso está cubierto por $n = 1$ en el teorema). □

Teorema 1.5 (Hasse) *Sea E una curva elíptica definida sobre el cuerpo finito $\mathbb{F}_q$. Entonces el orden de $E(\mathbb{F}_q)$ satisface*

$$\left|q + 1 - \#E(\mathbb{F}_q)\right| \leq 2\sqrt{q}.$$

La prueba de este teorema la podemos encontrar con todo detalle en [Was03]pág.100.

Teorema 1.6 *Sea $q = p^n$ una potencia de un primo p y sea $N = q + 1 - a$. Existe una curva elíptica E definida sobre $\mathbb{F}_q$ tal que $\sharp E(\mathbb{F}_q) = N$ si y sólo si $|a| \leq 2\sqrt{q}$ y a satisface una de las siguientes condiciones:*

1. *$mcd(a, p) = 1$*
2. *n es par y $a = \pm 2\sqrt{q}$*
3. *n es par, $p \not\equiv 1 \mod 3$ y $a = \pm\sqrt{q}$*
4. *n es impar, $p = 2$ ó 3 y $a = \pm p^{(n+1)/2}$*
5. *n es par, $p \not\equiv 1 \mod 4$ y $a = 0$*
6. *n es impar y $a = 0$.*

Teorema 1.7 *Sea N un entero que es el orden de una curva elíptica sobre un cuerpo finito $\mathbb{F}_q$, como en el teorema 1.6. Escribimos $N = p^e n_1 n_2$ con $p \nmid n_1 n_2$ y $n_1 \mid n_2$ (posiblemente $n_1 = 1$). Existe una curva elíptica E sobre $\mathbb{F}_q$ tal que*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

si y sólo si

1. *$n_1 \mid q - 1$ en los casos 1, 3, 4, 5, 6 del teorema 1.6*
2. *$n_1 = n_2$ en el caso 2 del teorema 1.6.*

Estos son los únicos grupos que son los grupos $E(\mathbb{F}_q)$.

1.3.1 Orden del grupo de puntos de una curva elíptica

En esta sección veremos algunos resultados que nos permiten determinar el orden del grupo de puntos en una curva elíptica.

Por ejemplo dada una curva elíptica E definida sobre un cuerpo finito pequeño $\mathbb{F}_q$, quisieramos saber el orden de $E(\mathbb{F}_{q^n})$ para algún n, veamos el siguiente teorema.

Teorema 1.8 *Si* $\#E(\mathbb{F}_q) = q+1-a \;\; y \;\; X^2 - aX + q = (X-\alpha)(X-\beta)$, *entonces*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

para todo $n \geq 1$.

Prueba. Para probar que $\alpha^n + \beta^n$ es un entero haremos uso del siguiente resultado: Sea $s_n = \alpha^n + \beta^n$. Entonces $s_0 = 2$, $s_1 = a$ y $s_{n+1} = as_n - qs_{n-1}$ para todo $n \geq 1$.

En efecto, tenemos que $\alpha^2 - a\alpha + q = 0$, y multiplicando por α^{n-1} obtenemos que $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. Procediendo de manera análoga para β, tenemos también que $\beta^{n+1} = a\beta^n - q\beta^{n-1}$. Sumando estas igualdades obtenemos lo pedido. Sea

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Entonces $X^2 - aX + q = (X-\alpha)(X-\beta)$ divide a $f(X)$. Se sigue inmediatamente del algoritmo estándar para dividir polinomios que el cociente es un polinomio $Q(X)$ con coeficientes enteros (los puntos principales son que el coeficiente principal de $X^2 - aX + q$ es 1 y que este polinomio y $f(X)$ tienen coeficientes enteros). Por lo tanto aplicando el endomorfismo de Frobenius

$$(\phi_q^n)^2 - (\alpha^n - \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0,$$

como endomorfismos de E, este resultado lo podemos encontrar en [Was03]pág. 106. Note que $\phi_q^n = \phi_{q^n}$. Entonces, existe un único entero k tal que $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$, y tal k está determinado por $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$. Por lo tanto

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}).$$

Esto completa la prueba del teorema 1.8.

1.3.2 Cálculo del orden de un punto

Sea $P \in E(\mathbb{F}_q)$. El *orden* de P es el menor entero positivo k tal que $kP = 0$.
De la teoría básica de grupos, sabemos que el orden de un punto siempre divide al orden del grupo $E(\mathbb{F}_q)$ y por el teorema de Hasse, tenemos que $\#E(\mathbb{F}_q)$ está en un intervalo de longitud $4\sqrt{q}$, entonces, si podemos encontrar un punto de orden mayor que $4\sqrt{q}$, sólamente puede haber un múltiplo de este orden en el intervalo correcto, y debe ser $\#E(\mathbb{F}_q)$. Aún si el orden del punto es menor que $4\sqrt{q}$, obtenemos una pequeña lista de posibilidades para $\#E(\mathbb{F}_q)$.

Proposición 1.2 *Sea E una curva elíptica sobre $\mathbb{F}_q$ y supongamos que*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

para algún entero n. Entonces $q = n^2 + 1$, $q = n^2 \pm n + 1$ o $q = (n \pm 1)^2$.

La prueba e este resultado se puede encontrar en [Was03]pág.108.

1.4 Cuerpos p-ádicos

1.4.1 Orden p-ádico y métricas sobre los racionales

Definición 1.4.1 *Sea X un conjunto no vacío. Una métrica sobre X es una función $d : X \times X \to \mathbb{R}_{\geq 0}$ tal que para todo $x, y \in X$ se cumple*

(d1) $d(x, y) = 0$ *si y sólo sí* $x = y$.

(d2) $d(x, y) = d(y, x)$.

(d3) $d(x, y) \leq d(x, z) + d(z, y)$ *para todo $z \in X$ (desigualdad triangular).*

Al par (X, d) con X un conjunto no vacío y d una métrica en X, se le denomina *espacio métrico.*
$(\mathbb{Q}, d)$ es un espacio métrico, donde $d(x, y) = |x - y|$ y $|\cdot|$ es el valor absoluto usual. Ésta es la distancia usual en $\mathbb{Q}$.

Definición 1.4.2 *Una norma $\|.\|$ sobre un cuerpo K es una aplicación $\|.\| : K \to \mathbb{R}_{\geq 0}$ tal que para todo $x, y \in K$ se tiene:*

(n1) $\|x\| = 0$ *si y sólo sí* $x = 0$.

(n2) $\|x \cdot y\| = \|x\| \cdot \|y\|$.

(n3) $\|x + y\| \leq \|x\| + \|y\|$ *(desigualdad triangular).*

Si $K = \mathbb{Q}$, es fácil ver que el valor absoluto $|.|$ es una norma en $\mathbb{Q}$. Diremos que d es una distancia si

$$d(x, y) = \|x - y\| \text{ para todo } x, y \in K$$

Nota. Podemos definir otras normas sobre $\mathbb{Q}$ que a pesar de satisfacer las propiedades $(d1), (d2), (d3)$, van a diferir bastante de las nociones intuitivas de la distancia inducida por el valor absoluto. Todas estas normas cumplen una relación más fuerte que la desigualdad triangular.

Definición 1.4.3 *Una norma se dice no arquimediana si para todo* $x, y \in K$ *se tiene que*

$$\|x + y\| \leq \max\{\|x\|, \|y\|\}.$$

Una métrica en un conjunto X se dice no arquimediana si

$$d(x, y) \leq \max\{\ d(x, z);\ d(z, y)\} \text{ (desigualdad ultramétrica)}$$

para todo $x, y, z \in X$.
La propiedad no arquimediana de una norma implica la desigualdad triangular, por ello podríamos llamar a esta propiedad como: desigualdad triangular fuerte. La distancia inducida por una norma no euclidiana es llamada *ultramétrica.*
Definiremos métricas sobre $\mathbb{Q}$, una para cada número primo; y como se verá más adelante, toda métrica no trivial sobre $\mathbb{Q}$ es equivalente a una de éstas.

Proposición 1.3 *Los siguientes enunciados son equivalentes*

1. $\|.\|$ *es no arquimediana.*
2. $\|n\| \leq 1$ *para todo entero* n.

Sea $m \in \mathbb{Z}$ y p un número primo. Denotaremos por $v_p(m)$, a la máxima potencia de p que divide a m, es decir, el mayor n tal que $m \equiv 0 \mod p^n$. Entonces, si $m \neq 0$, tenemos que

$$\text{si } \ 0 \leq v_p(m) \ \text{ y } \ p^a | m \ \text{ entonces } \ a \leq v_p(m) \text{ y } p^{v_p(m)} | m. \tag{1.8}$$

Es claro que $p|m$ si y solo si $v_p(m) > 0$.

Definición 1.4.4 *$v_p(m)$ se denomina el orden p-ádico (o valuación) de m con respecto a p. Definimos también $v_p(0) = \infty$.*

Por ejemplo $v_5(45) = 1$, $v_3(45) = 2$ y $v_2(45) = 0$, pues $45 = 5 \cdot 3^2$,$v_3(27) = 3$ y $v_5(100) = 2$.

Observación:

Dado un $m \in \mathbb{Z}$, por el teorema fundamental de la aritmética podemos escribir $m = \varepsilon p_1^{n_1} \cdot p_2^{n_2} \cdots p_t^{n_t}$ de manera única como potencias de primos distintos, claramente, la mayor potencia de p_i que divide a m es n_i, entonces, $n_i = v_{p_i}(m)$ para todo $1 \leq i \leq t$. Entonces

$$m = \varepsilon p_1^{v_{p_1}(m)} \cdot p_2^{v_{p_2}(m)} \cdots p_t^{v_{p_t}(m)} = \prod_{p \in \mathcal{P}} p^{v_p(m)} \quad \text{para todo } \ m \in \mathbb{Z}$$

donde $\varepsilon = \pm 1$, $\mathcal{P}$ el conjunto de los números primos y $v_p(m) = 0$ si $p \nmid m$.

Proposición 1.4 *Para todo $m, n \in \mathbb{Z}$ se tiene*

1. $v_p(m \cdot n) = v_p(m) + v_p(n)$
2. $v_p(m + n) \geq \min\{ v_p(m), v_p(n)\}$
3. *Si* $v_p(m) \neq v_p(n)$ *entonces* $v_p(m + n) = \min\{v_p(m); v_p(n)\}$

Prueba

1. Siendo $m = \prod_{p \in \mathcal{P}} p^{v_p(m)}$ y $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$, implica que

$$m \cdot n = \prod_{p \in \mathcal{P}} p^{v_p(m) + v_p(n)} = \prod_{p \in \mathcal{P}} p^{v_p(m \cdot n)}$$

luego, por el teorema fundamental de la aritmética tenemos que $v_p(m \cdot n) = v_p(m) + v_p(n)$.

2. Sabemos que $p^{v_p(m)}\big|m$ y $p^{v_p(n)}\big|n$. Si $t_p = \min\{v_p(m), v_p(n)\}$, entonces $p^{t_p}|p^{v_p(m)}, p^{t_p}|p^{v_p(n)}$ y por ende $p^{t_p}|m$ y $p^{t_p}|n$. Luego, $p^{t_p}|(m+n)$, de donde se sigue que $v_p(m+n) \geq \min\{v_p(m), v_p(n)\}$.

3. Supongamos que $v_p(m) \neq v_p(n)$ digamos que $v_p(n) < v_p(m)$.
   Por (2.) sabemos que $v_p(m+n) \geq v_p(n)$. Probemos la otra desigualdad.
   Si $v_p(n) = v_p(n+m-m) \geq \min\{v_p(n+m), v_p(m)\}$, de (2.); si el mínimo fuera $v_p(m)$ entonces $v_p(n) \geq v_p(m)$, lo que es una contradicción. Por lo tanto $v_p(n) = v_p(n+m-m) \geq \min\{v_p(n+m), v_p(m)\} = v_p(n+m)$.
   Lo prueba que $v_p(n) \geq v_p(m+n)$. Así $v_p(m+n) = \min\{v_p(n), v_p(m)\}$.

Ahora extenderemos el orden p-ádico para los números racionales

Si $x = a/b \in \mathbb{Q}$, $(a,b) = 1$, definimos

$$v_p(x) = v_p(a) - v_p(b)$$

Por ejemplo : $v_3(2/9) = -2$, $v_5(3/7) = 0$ y $v_7(14/5) = 1$.

Ahora, $v_p : \mathbb{Q} \to \mathbb{Z}$ y las propiedades se mantienen

1. $v_p(r) = \infty$ si y sólo sí $r = 0$
2. $v_p(r \cdot s) = v_p(r) + v_p(s)$
3. $v_p(r+s) \geq \min\{\ v_p(r), v_p(s)\}$

Notar que esta definición del orden sobre $\mathbb{Q}$ no depende de la escritura de x, pues si $x = ac/bc$ entonces

$$v_p(ac/bc) = v_p(ac) - v_p(bc) = v_p(a) - v_(b).$$

Definición 1.4.5 *Dado p un número primo la aplicación $|.|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ dada por*

$$|x|_p = \begin{cases} p^{-v_p(x)} & si \quad x \neq 0 \\ p^{-\infty} = 0 & si \quad x = 0 \end{cases}$$

Es llamada la norma p-ádica de x.

Proposición 1.5 *La norma p-ádica satisface las siguientes propiedades*

(a) $|.|_p = 0$ *si y solo si* $x = 0$*;*

(b) $|xy|_p = |x|_p|y|_p$*;*

(c) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$*; se da la igualdad si* $|x|_p \neq |y|_p$

Nota

1.Denotaremos por $|.|_\infty$ al valor absoluto usual. Cabe aclarar que ésta es sólo una convención y no implica una relación directa entre $|.|_\infty$ y $|.|_p$.

2. $d_p(r, s) = |r - s|_p$ es una métrica sobre $\mathbb{Q}$, la cual induce una topología sobre $\mathbb{Q}$.

3.$(\mathbb{Q}, d_p)$ es un espacio métrico incompleto.

Proposición 1.6 *Para todo p primo,* $|.|_p$ *es una norma no arquimediana sobre* $\mathbb{Q}$.

Prueba. Veremos que $|.|_p$ es una norma según la definición (1.4.2).

Sea $x \in \mathbb{Q}$. Claramente por definición $|x|_p \neq 0$ si y sólo si $x \neq 0$. Luego, $|.|_p$ verifica $(n1)$.

Sea $y \in \mathbb{Q}$. Si $x = 0$ ó $y = 0$, entonces $|xy|_p = 0 = |x|_p|y|_p$. Si $x \neq 0$ y $y \neq 0$, entonces por el lema anterior tenemos que $|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)} \cdot p^{-v_p(y)} = |x|_p|y|_p$, lo que implica que se cumple $(n2)$.

Probemos ahora $(n3)$. Si $x = 0$ o $y = 0$ o si $x + y = 0$, la propiedad $(n3)$ se verifica trivialmente. Por lo tanto, podemos suponer que x, y, $x + y$ son no nulos. Escribamos $x = a/b$, $y = c/d$ tales que $(a, b) = 1 = (c, d)$. Entonces $x + y = (ad + bc)/bd$ y $v_p(x + y) = v_p(ad + bc) - v_p(b) - v_p(d)$. Luego, del lema se sigue que

$$\begin{aligned} v_p(x+y) &\geq \min\{v_p(ad), v_p(bc)\} - v_p(b) - v_p(d) \\ &= \min\{v_p(a) + v_p(d); v_p(b) + v_p(c)\} - v_p(b) - v_p(d) \\ &= \min\{v_p(a) - v_p(b); v_p(c) - v_p(d)\} \\ &= \min\{v_p(x), v_p(y)\} \end{aligned}$$

Por lo tanto

$$|x + y|_p = p^{-v_p(x+y)} \leq p^{-\min\{v_p(x),v_p(y)\}} = \max\{p^{-v_p(x)}, p^{-v_p(y)}\} = \max\{|x|_p, |y|_p\},$$

y esto es menor o igual que $|x|_p + |y|_p$. En particular, hemos probado que la norma es no arquimediana.

Más aún, toda norma no trivial $\|.\|$ sobre $\mathbb{Q}$ es equivalente a $|.|_p$ para algún primo p o $p = \infty$, la prueba de este resultado la encontramos en [Kob84]Th1pág.3-5.

1.4.2 El cuerpo de los números p-ádicos

Uno de los grandes problemas al trabajar con $\mathbb{Q}$ es que no toda sucesión de Cauchy con el valor absoluto $|.|$ es convergente en $\mathbb{Q}$, es decir, una sucesión de Cauchy puede no converger a un número racional; estos "agujeros" en $\mathbb{Q}$ son llenados por el proceso de compleción que da como resultado $\mathbb{R}$.
De manera análoga, si consideramos a $\mathbb{Q}$ con la norma p-ádica, donde p un número primo, resulta que $\mathbb{Q}$ tampoco es completo. Su compleción dará lugar al cuerpo $\mathbb{Q}_p$ de números p-ádicos.
Veamos algunas definiciones previas, antes de hacer la construcción de la compleción de un cuerpo general K y luego particularizar cuando $K = Q$

Definición 1.4.6 *Sea K un cuerpo y $|.|$ una norma en K. Decimos que una sucesión $(a_n)_{n\in\mathbb{N}}$ es convergente a un elemento $\alpha \in K$ si, para todo número real $\varepsilon > 0$ existe $n \in \mathbb{N}$ tal que $|a_n - \alpha| < \varepsilon$ para todo $n \geq N$.*
En términos de la distancia d inducida por la norma esto se traduce en $d(a_n, \alpha) \to 0$ cuando $n \to \infty$.

Definición 1.4.7 *Un cuerpo K se dice completo con respecto a una norma, si toda sucesión de Cauchy en K es convergente con respecto dicha norma.*

Ejemplo 1.3 *Si $K = \mathbb{Q}$ y $|.|$ es el valor absoluto usual, la sucesión dada por $a_n = (1 + 1/n)^n$ es una sucesión de Cauchy que converge al número real e, que no es racional, por lo que tenemos que $\mathbb{Q}$ no es completo con respecto al valor absoluto usual, mientras que $\mathbb{R}$ y $\mathbb{C}$ si son completos con sus valores absolutos usuales.*

Construcción de la compleción. Sea K un cuerpo con una norma $\|.\|$ y sean (a_n) y (b_n) dos sucesiones de Cauchy de K con respecto a $\|.\|$. Se define la suma y el producto entre sucesiones de Cauchy por la suma y el producto término a término, esto es,

$$(a_n) + (b_n) = (a_n + b_n) \quad \text{y} \quad (a_n)(b_n) = (a_n b_n)$$

Veamos, que el conjunto de sucesiones de Cauchy es cerrado con respecto a estas operaciones. Claramente, $(a_n) + (b_n)$ es una sucesión de Cauchy.

Además, como toda sucesión de Cauchy es acotada, se deduce que la sucesión $(a_n b_n)$ también es de Cauchy. En efecto:

$$\begin{aligned} \|a_n b_n - a_m b_m\| &= \|a_n(b_n - b_m) + b_m(a_n - a_m)\| \\ &\leq \|a_n\|.\|b_n - b_m\| + \|b_m\|.\|a_n - a_m\| \\ &\leq M\|b_n - b_m\| + M'\|a_n - a_m\| \end{aligned}$$

donde $\|a_n\| \leq M$ para todo $n \in \mathbb{N}$ y $\|b_n\| \leq M'$ para todo $n \in \mathbb{N}$.
Esto implica que si dos sucesiones (a_n) y (b_n) son de Cauchy, entonces su producto también lo es.
Más aún, si (a_n) es una sucesión de Cauchy, entonces la sucesión $-(a_n) = (-a_n)$ definida por el inverso aditivo en cada coordenada, es una sucesión de Cauchy.
Luego, el conjunto $\mathcal{SC}$ de sucesiones de Cauchy de K con estas dos operaciones es un anillo, cuya unidad está dada por la sucesión (u_n), $u_n = 1$ para todo $n \in \mathbb{N}$ (al ser constante), claramente es de Cauchy.

Definición 1.4.8 *Una sucesión (a_n) se dice una sucesión nula con respecto a una norma $\|.\|$ si para todo número real $\varepsilon > 0$, existe un número natural N tal que $\|a_n\| < \varepsilon$ para todo $n \geq N$.*

Es decir, una sucesión se llama *nula* con respecto a $\|.\|$, si es convergente a 0 con respecto a esta norma.
Denotaremos por $\mathcal{SN}$ el conjunto de sucesiones nulas con respecto a $\|.\|$. Una sucesión nula con respecto a $\|.\|$, es una sucesión de Cauchy en K con respecto a $\|.\|$.

En lo que sigue, consideramos un cuerpo K con una norma $\|.\|$. En general diremos que una sucesión es nula, sin referirnos a la norma, cuando es claro a qué norma nos referimos.

Sean (a_n) y (b_n) dos sucesiones nulas. Entonces, la sucesión dada por $(a_n) + (b_n)$ es también una sucesión nula, pues por la desigualdad triangular tenemos que

$$\|a_n + b_n\| \leq \|a_n\| + \|b_n\|$$

También tenemos que si (c_n) es una sucesión de Cauchy y (a_n) es una sucesión nula, entonces la sucesión $(a_n c_n)$ dada por el producto de ambas es una sucesión nula, ya que toda sucesión de Cauchy es acotada y

$$\|a_n c_n\| = \|a_n\|\|c_n\| \leq \|a_n\| C$$

donde $c_n \leq C$ para todo $n \in N$.

Por lo tanto, hemos probado que el conjunto $\mathcal{SN}$ de sucesiones nulas es un ideal del anillo $\mathcal{SC}$. Más aún, este ideal es un ideal maximal de $\mathcal{SC}$ y , el cociente $\mathcal{SC}/\mathcal{SN}$ es un cuerpo. Definimos entonces $\widehat{K} = \frac{\mathcal{SC}}{\mathcal{SN}}$

Sea ahora $a \in K$, por (a) denotamos la sucesión constante igual a a, que obviamente es de Cauchy. Luego, definimos la aplicación

$$f : K \to \widehat{K}$$

dada por $f(a) = (a) + \mathcal{SN}$, para todo $a \in K$.
Esta aplicación resulta ser claramente un morfismo de cuerpos que es inyectivo, pues si $f(a) = 0$, esto implica que $0 = (a) + \mathcal{SN}$ y por lo tanto $(a) \in \mathcal{SN}$ es una sucesión nula, pero esto sucede si y sólo si $a = 0$. Así, si definimos

$$\widetilde{K} = \{(a) + \mathcal{SN} \ / \ a \in K \ \}$$

así, resulta que $K \cong \widetilde{K}$. Por lo tanto, identificamos a K con $\widetilde{K}$.

Teorema 1.9 *Dado un cuerpo K con una norma $\|.\|$, existe un cuerpo $\widehat{K}$, único salvo congruencia, llamado la compleción de K, tal que $\widehat{K}$ es completo con respecto a la norma inducida por la norma $\|.\|$ y K es denso en $\widehat{K}$.*

Prueba. La construcción del cuerpo $\widehat{K}$ fue dada anteriormente. Falta probar que la norma de K induce una norma en $\widehat{K}$, el morfismo f , dado antes, respeta la norma, K es denso en $\widehat{K}$ y $\widehat{K}$ es completo con la norma inducida,veamos.

Sea $(a_n) + \mathcal{SN} \in \widehat{K}$. Entonces, la sucesión de números reales dada por $(\|a_n\|)$ es una sucesión de Cauchy en $\mathbb{R}$, pues (a_n) es una sucesión de Cauchy en K y de la desigualdad triangular se deduce que $\big|\|a_n\| - \|a_m\|\big| \leq \|a_n - a_m\|$

Como $\mathbb{R}$ es completo con respecto a $|.|$, la sucesión $(\|a_n\|)$ tiene límite en $\mathbb{R}$. Definimos entonces la norma en $\widehat{K}$ como

$$\|(a_n) + \mathcal{SN}\| = \lim_{n\to\infty} \|a_n\|$$

Esta norma está bien definida: sea $(b_n) \in \mathcal{SC}$ tal que $(a_n) + \mathcal{SN} = (b_n) + \mathcal{SN}$. Entonces $(a_n - b_n) = (a_n) - (b_n) \in \mathcal{SN}$. Usando nuevamente la desigualdad triangular, tenemos que $\big|\|a_n\| - \|a_m\|\big| \leq \|a_n - a_m\| \longrightarrow 0$,

esto es, $\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|b_n\|$, y la norma resulta bien definida.
Demostremos ahora que el morfismo f , respeta la norma, es decir, $\|f(a)\| = \|a\|$ para todo $a \in K$. Pero $\|f(a)\| = \|(a) + M\| = \lim_{n\to\infty} \|a\| = \|a\|$. En particular, el morfismo f induce un isomorfismo isométrico entre K y su imagen por f.

Veamos ahora que $K = \widetilde{K}$ es denso en $\widehat{K}$, esto es, para todo elemento $\{a_n\}+M \in \widehat{K}$, y todo número real $\epsilon > 0$, existe $b \in K$ tal que $\| (\{a_n\} + M) - (b + M)\| < \epsilon$.

Definición 1.4.9 *La compleción del cuerpo de los números racionales $\mathbb{Q}$ respecto a la norma p- ádica se denomina* ***el cuerpo de los números p-ádicos*** *y se denota por $\mathbb{Q}_p$.*

Observación 1.1 *El conjunto $\mathbb{Q}_p$ está formado por clases de equivalencia de sucesiones de cauchy, que constituye un cuerpo con la suma y, multiplicación definidas; y más aún, podemos identificar $\mathbb{Q}$ con el subcuerpo de $\mathbb{Q}_p$, formado por las clases de equivalencia de sucesiones de Cauchy constantes.*

Observación 1.2 *Si denotamos $[(a_n)] \in \mathbb{Q}_p$. Definimos*

$$\big|[(a_n)]\big|_p = \lim_{n\to\infty} |a_n|_p$$

Observación 1.3 *La bola cerrada, de centro 0 y radio 1 en $\mathbb{Q}_p$ se denota y define por* $\mathbb{Z}_p =: B_1[0] = \{x \in \mathbb{Q}_p \ / \ |x|_p \leq 1\}$
$\mathbb{Z}_p$ constituye un subanillo de $\mathbb{Q}_p$, pues $|rs|_p = |r|_p|s|_p \leq 1$,
$|r \pm s|_p \leq \max\{|r|_p, |s|_p\} \leq 1$ *y es llamado* Anillo de los Enteros p-ádicos.

Ahora, describiremos los elementos de $\mathbb{Q}_p$, usando expansiones p-ádicas.

Teorema 1.10 *Dado $\alpha \in \mathbb{Z}_p$ existe una única sucesión de Cauchy $\{a_i\}$ que satisface:*

1. *$0 \leq a_i \leq p^i$, para $i = 1, 2, 3, \cdots$*

2. *$a_i \equiv a_{i+1}(\mod p^i)$, para $i = 1, 2, 3, \cdots$*

Prueba. La prueba de este resultado la podemos encontrar en [Kob84]Th 2. pág. 11-12.

Según el teorema anterior, tenemos que la sucesión $\{a_n\}$ es de Cauchy y su término $n-$ésimo es $a_n = a_0 + a_1p + a_2p^2 + \cdots + a_np^n$; y además es convergente a α, pues $|\alpha - a_n|_p < \frac{1}{p^n}$, entonces:

$$\alpha = a_0 + a_1p + a_2p^2 + \cdots$$

Esta expresión es llamada *la expansión p-ádica de* $\alpha \in \mathbb{Z}_p$ y los a_n son llamados *los dígitos p-ádicos de* $\alpha \in \mathbb{Z}_p$. Un elemento de $\mathbb{Z}_p$ es llamado un entero p-ádico.

Teorema 1.11 *Todo* $\alpha \in \mathbb{Q}_p$ *tiene una única expansión p-ádica*

$$\alpha = \alpha_{-r}p^{-r} + \alpha_{-r+1}p^{-r+1} + \cdots + \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1p + \alpha_2p^2 + \cdots$$

donde los $\alpha_i \in \mathbb{Z}$ *y* $0 \leq \alpha_i < p$. *Además* $\alpha \in \mathbb{Z}_p$ *si y sólo sí* $\alpha_{-r} = 0$ *para todo* $r > 0$, *es decir*

$$\alpha \in \mathbb{Z}_p \text{ si solo si } \alpha = \alpha_0 + \alpha_1p + \alpha_2p^2 + \cdots$$

Prueba. Dado algún número p-ádico $\alpha \in \mathbb{Q}_p$.
Si $|\alpha|_p \leq 1$, tenemos que $\alpha \in \mathbb{Z}_p$ y segun el teorema anterior, ya hemos obtenido su expansión p-ádica. Si $|\alpha|_p > 1$, supongamos que $|\alpha|_p = p^k$, $k > 0$. Consideremos $\beta = p^k\alpha$, tenemos que $|\beta|_p \leq 1$, entonces β tiene una expansión p-ádica de la forma

$$\beta = b_0 + b_1p + b_2p^2 + \cdots$$

Luego, $\alpha = p^{-k}\beta$, entonces tenemos que:

$$\alpha = \frac{b_0}{p^k} + \frac{b_1}{p^{k-1}} + \cdots + \frac{b_{k-1}}{p} + b_k + b_{k+1}p + \cdots + b_{k+r}p^r \cdots$$

donde $0 \leq b_n \leq p-1$ para cada n.

Observación 1.4 $p\mathbb{Z}_p$ *es un ideal de* $\mathbb{Z}_p$ *y más aún es el único ideal maximal de* $\mathbb{Z}_p$, *esto es,* $\mathbb{Z}_p$ *es un* anillo local, *con ideal maximal* $p\mathbb{Z}_p$ *y su cuerpo residual es isomorfo a* $\mathbb{F}_p$, *lo denotamos así*

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$$

La *Aritmética en* $\mathbb{Q}_p$, es decir la suma, resta, multiplicación y división de números p-ádicos es muy parecida a la que se emplea para las operaciones con decimales.

Capítulo 2

Fundamentos de la criptografía

Para comprender mejor el alcance de la criptografía moderna es conveniente tener en cuenta sus objetivos más importantes, que son los siguientes:

1. Confidenciabilidad. A envía a B un mensaje no puede ser leido por nadie más.
2. Autenticidad. Cuando B recibe un mensaje de A, sabe que es realmente A quien lo envía.
3. Integridad. B puede detectar si el mensaje que le ha enviado A ha sido alterado por un tercero.
4. No repudio. Después de haber enviado un mensaje a B, A no puede afirmar que el mensaje no es suyo.

Los criptosistemas clásicos, se basaban en el uso de una clave secreta que A y B compartían y que era la que se usaba tanto para cifrar como para descifrar (***criptosistemas simétricos***). Estos criptosistemas estaban diseñados pensando en mantener la información secreta, pero carecían de mecanísmos para alcanzar los objetivos restantes.

Por ejemplo, para que B pueda convencer a una tercera persona de que un cierto mensaje recibido procede de A, se necesita una ***firma digital***, que es el análogo a una firma escrita; dado que en un criptosistema de clave secreta A y B tienen la misma capacidad para cifrar y descifrar, B podría haber falsificado el mensaje y atribuírselo a A, o un intruso puede copiar la firma y anexarla a otro documento. Por lo tanto, se deben tomar acciones para atar la firma al documento, de tal forma

de que no se pueda volver a utilizar. Sin embargo, debe ser posible verificar que la firma es válida, y debe ser posible mostrar que A debe haber sido la persona que firmó el documento.

Los criptosistemas simétricos también tienen otra deficiencia, es que no son adecuados, por sí solos, para proteger las comunicación entre múltiples personas que probablemente no se conozcan y nunca han estado en contacto; el uso de una clave secreta requiere que haya sido compartida a través de un *canal seguro*, que no es factible en ésta situación.

En una red con n usuarios, un criptosistema clásico requiere que cada par de usuarios compartan una clave secreta, lo que hace un total de $\frac{n(n-1)}{2}$ claves, que, para n grande, no es manejable.

Otro aspecto insatisfactorio, de los criptosistemas tradicionales, es la falta de criterios rigurosos para evaluar su seguridad, es decir, su resistencia al *criptoanálisis*. De la misma forma que la criptografía es la ciencia para diseñar sistemas para proteger la información y las comunicaciones (criptosistemas), existe la disciplina que se trata de encontrar métodos para "romper" o criptoanalizar, dichos sistemas : el criptoanálisis.

La confianza en un criptosistema se basa en el tiempo que pasa sin que haya sido roto, por ello la idea de basar los criptosistemas en problemas matemáticos "difíciles" dió lugar al desarrollo de un nuevo tipo de criptografía. Más adelante veremos, que en 1976 se produce una revolución en la criptografía con la aparición de criptografía de clave pública.

2.1 El problema del logaritmo discreto

Sea $(G, .)$ un grupo multiplicativo, $a \in G$ un elemento de orden n y $b \in < a >$. El *problema del logaritmo discreto* consiste en encontrar k, $0 \leq k \leq n-1$, tal que $a^k = b$. Se tiene que $k = log_a b$ es llamado el logaritmo discreto.

Por ejemplo, G podría ser el grupo multiplicativo $\mathbb{F}_p^\times$ de un cuerpo finito, también podría ser el conjunto de los puntos racionales de una curva E definida sobre K, que forman un grupo abeliano, que en general es un grupo abeliano mas complejo. En este caso P y Q son puntos en $E(K)$ e intentamos hallar un entero k con $kP = Q$, a esto se le conoce como ***el problema del Logaritmo Elíptico*** y por tanto se puede esperar que el problema del logaritmo discreto sobre curvas elípticas

(PLDCE) sea más difícil que el problema de logaritmo discreto sobre cuerpos finitos (PLDCF). Un problema se considera difícil, si uno no puede resolverlo en un tiempo razonable con un buen ordenador.
La seguridad de los criptosistemas dependerá de la dificultad para resolver el problema del logaritmo discreto y esto depende de la naturaleza del grupo, por lo que si el grupo es mas complejo, el problema de logaritmo es más complejo también.

2.2 Algunos ataques al problema del logaritmo discreto

La seguridad del logaritmo discreto en curvas elípticas radica en la dificultad de resolver el problema

$$\text{dados} \quad P, Q \in E(\mathbb{F}_q) \quad \text{con} \quad < P >= E(\mathbb{F}_q) \quad \text{encontrar } k \text{ talque} \quad Q = k.P$$

Una manera de atacar un problema de logaritmo discreto es simple fuerza bruta: probar todos los posibles valores de k hasta que uno funcione. Esto no es práctico cuando la respuesta k pueda ser un entero de muchos cientos de dígitos, que es un tamaño típico usado en criptografía.

Se conoce algunos algoritmos que convierten el PLDCE en problemas más sencillos, como el PLDCF, donde si existe un algoritmo de ataque subexponencial, el Index-Calculus.
Para una curva E definida sobre $\mathbb{F}_q$ con un primo grande, algunos de los ataques más importantes son:
Anomalous Attack: Cuando $\sharp E(\mathbb{F}_p) = p$ y éste ataque reduce el problema,

$$LDCE \leftrightarrow LDCF$$

$$E(\mathbb{F}_p) \leftrightarrow (\mathbb{F}_p, +)$$

Pohlig-Hellman :
Cuando $\sharp E(\mathbb{F}_p)$ descompone en primos pequeños, entonces podemos reducir el problema del LDCE a muchos problemas sencillos del LDCF, procediendo de la siguiente manera:
Consideremos dos puntos P y $Q \in G = E(\mathbb{F}_p)$, si el orden de P es N y $N = \prod_i q_i^{e_i}$.

Entonces para determinar $k \mod N$, debemos determinar $k \mod q_i^{e_i}$ para cada i, y luego aplicar el teorema chino del resto.

Consideremos un primo q genérico y supongamos que q^e la potencia exacta en que q que divide a N. Luego, escribimos k como una serie de potencias de q , de la siguiente manera $k = k_0 + k_1 q + k_2 q^2 + \cdots$ con $0 \leq k_i < q$.
Evaluaremos $k \mod q^e$ determinando sucesivamente $k_0, k_1, \ldots, k_{e-1}$. El procedimiento es el siguiente

1. Debemos calcular los valores; $j\left(\frac{N}{q}P\right) : 0 \leq j \leq q-1$;
2. Luego calculamos $\frac{N}{q}Q$; este será un elemento $k_0\left(\frac{N}{q}P\right)$ de los calculados en 1.;
3. Si $e = 1$, termina, si no, continuamos;
4. Hacemos $Q_1 = Q - k_0 P$;
5. Ahora calculamos $\frac{N}{q^2}Q_1$; este será un elemento $k_1\left(\frac{N}{q}P\right)$ de los calculados en 1.;
6. Si $e = 2$, termina, si no, continuamos;
7. Procediendo de manera inductiva podemos calcular $k_0, k_1, \ldots, k_{r-1}$ y $Q_1, \ldots, Q_{r-1}$;
8. Hacemos $Q_r = Q_{r-1} - k_{r-1} q^{r-1} P$;
9. Luego determinamos k_r tal que $\frac{N}{q^{r+1}}Q_r = k_r\left(\frac{N}{q}P\right)$;
10. Si $r = e - 1$, termina, si no, regresamos al paso 7.

Entonces

$$k \equiv k_0 + k_1 q + \cdots + k_{e-1} q^{e-1} \mod q^e.$$

Esto funciona porque:

$$\frac{N}{q}Q = \frac{N}{q}(k_0 + k_1 q + \cdots)P$$
$$= k_0 \frac{N}{q}P + (k_1 + k_2 q + \cdots)NP = k_0 \frac{N}{q}P,$$

pues $NP = 0$. Por lo tanto, el paso 2 encuentra a k_0. Entonces

$$Q_1 = Q - k_0 P = (k_1 q + k_2 q^2 + \cdots)P,$$

luego

$$\frac{N}{q^2}Q_1 = (k_1 + k_2 q + \cdots)\frac{N}{q}P$$
$$= k_1\frac{N}{q}P + (k_2 + k_3 q + \cdots)NP = k_1\frac{N}{q}P.$$

Por lo tanto, encontramos k_1. Procediendo de manera análoga, el método produce $k_2, k_3, \ldots$.

Nos detenemos después de $r = e-1$, pues N/q^{e+1} ya no es un entero, y no podemos multiplicar Q_e por algo que no es entero N/q^{e+1}. Además, no necesitamos continuar, porque ya conocemos $k \mod q^e$.

Veamos un ejemplo de aplicación

Ejemplo 2.1 *Sea $G = E(\mathbb{F}_{101})$, donde E es la curva elíptica dada por $y^2 = x^3 + 7x + 1$. Sean $P = (0,1)$ y $Q = (0,3)$ puntos en G. Como P tiene orden $N = 116$ y $116 = 2^2 \cdot 29$.*

Calcularemos $k \mod 4$ y $k \mod 29$, luego aplicaremos el teorema chino del resto y obtendremos $k \mod 116$.

Haciendo los los cálculos en sistema PARI/GP, tenemos que

```
e2=ellinit([0,0,0,Mod(7,101),Mod(1,101)])
%5 = [0, 0, 0, Mod(7, 101), Mod(1, 101), 0, Mod(14, 101), Mod(4, 101),
 Mod(52, 101), Mod(68, 101), Mod(45, 101), Mod(38, 101),
 Mod(51, 101), 0, 0, 0, 0, 0, 0]
ellpow(e2,[Mod(0,101),Mod(1,101)],58)
%6 = [Mod(18, 101), Mod(0, 101)]
ellpow(e2,[Mod(1,101),Mod(3,101)],29)
%7 = [Mod(18, 101), Mod(0, 101)]
```

k mod 4 . *Calculamos $j\left(\frac{N}{2}P\right)$, $\quad 0 \le j \le 1$; entonces: $\mathcal{O}, 58P = (18,0)$.*

Como

$$(N/2)Q = 58Q = (18,0) = 1 \cdot (58P),$$

tenemos $k_0 = 1$. Por lo tanto,

$$Q_1 = Q - 1P = \mathcal{O}.$$

Como $(N/4)Q_1 = 29Q_1 = \mathcal{O} = 0 \cdot \frac{N}{2}P$, tenemos $k_1 = 0$.

Por lo tanto,

$$k = 1 + 0 \cdot 2 + \equiv 1 \mod 4.$$

k mod 29 . *Calculamos* $j\left(\frac{N}{4}P\right) : 0 \leq j \leq 28$*; entonces calculando los puntos tenemos.*

```
 ellpow(e2,[Mod(0,101),Mod(1,101)],4)
%2 = [Mod(96, 101), Mod(12, 101)]
ellpow(e2,[Mod(1,101),Mod(3,101)],4)
%8 = [Mod(41, 101), Mod(78, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],2)
%5 = [Mod(35, 101), Mod(87, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],3)
%6 = [Mod(54, 101), Mod(92, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],4)
%7 = [Mod(27, 101), Mod(73, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],5)
%9 = [Mod(49, 101), Mod(5, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],6)
%10 = [Mod(61, 101), Mod(19, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],7)
%11 = [Mod(41, 101), Mod(78, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],8)
%12 = [Mod(22, 101), Mod(81, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],9)
%13 = [Mod(2, 101), Mod(15, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],10)
%14 = [Mod(98, 101), Mod(16, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],11)
%15 = [Mod(12, 101), Mod(55, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],12)
%16 = [Mod(99, 101), Mod(22, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],13)
%17 = [Mod(63, 101), Mod(98, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],14)
```

```
%18 = [Mod(19, 101), Mod(23, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],15)
%19 = [Mod(19, 101), Mod(78, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],16)
%20 = [Mod(63, 101), Mod(3, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],17)
%21 = [Mod(99, 101), Mod(79, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],18)
%22 = [Mod(12, 101), Mod(46, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],19)
%23 = [Mod(98, 101), Mod(85, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],20)
%24 = [Mod(2, 101), Mod(86, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],21)
%25 = [Mod(22, 101), Mod(20, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],22)
%26 = [Mod(41, 101), Mod(23, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],23)
%27 = [Mod(61, 101), Mod(82, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],24)
%28 = [Mod(49, 101), Mod(96, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],25)
%29 = [Mod(27, 101), Mod(28, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],26)
%30 = [Mod(54, 101), Mod(9, 101)]
ellpow(e2,[Mod(96,101),Mod(12,101)],27)
%31 = [Mod(35, 101), Mod(14, 101)]
 ellpow(e2,[Mod(96,101),Mod(12,101)],28)
%32 = [Mod(96, 101), Mod(89, 101)]
```

los puntos son: $4P = (96, 12), 2(4P) = (35, 87), (54, 92), (27, 73), (49, 5),$
$(61, 19), 7(4P) = (41, 78), (22, 81), \cdots, (35, 14), (96, 89)$
Como $(N/29)Q = 4Q = (41, 78) = 7 \cdot (4P)$, *entonces* $k_0 = 7$. *Así,* $k \equiv 7 \mod (29)$

Ahora tenemos el sistema de congruncias

$$\begin{cases} k \equiv 2 \mod 4 \\ k \equiv 7 \mod 29. \end{cases}$$

por el teorema chino del resto $k \equiv 94 \mod 116$*, luego* $k = 94$.

El método Pohlig-Hellman funciona bien si todos los primos, que dividen a N, son pequeños. Sin embargo, si q es un primo muy grande que divide a N, es difícil listar los elementos indicados en el paso (1), que contiene q elementos.

Side channel attack :

En este ataque se basa en aprovechar que el dispositivo criptográfico presenta escapes de información física, durante el proceso de un algoritmo criptográfico. Estos escapes que pueden consistir en disipación de energía, información del tiempo de un algoritmo, emanción electromagnética y ruido; estos elementos pueden ser capturados exteriormente y peuden ser utilizados para obtener información de claves secretas de algoritmos criptográficos con la ayuda de herramientas estadísticas. Generalmente, todos los algoritmos criptográficos pueden ser vulnerables a éste ataque si no se toman la medidas de seguridad al implementar el algoritmo, como son el utilizar materiales de alta calidad y con protección electromagnética, llenar el canal con ruido, sea con señal sonora o electromagnética y seguridad física para evitar la instalación de micrófonos y censores de radiación. Algunos casos generales de Side channel attack:

1. Timin attack: ataques que se basan en el tiempo de ejecución del algoritmo, cononciendo el tiempo en que se transfieren las claves, podrían calcularse la longitud de las claves.

2. Power monitoring attack: basado en el análisis de energía consumido por el hardware mientras se ejecuta el proceso.

3. Radiation monitoring: ataque basado en escape de radiación electromagnética del harward.

4. Acoustic crytanalysis: consiste en analizar acústicamente el sonido generado electrónicamente al digitar una tecla, logrando saber que tecla fue utilizada.

2.3 El intercambio de claves de Diffie-Hellman

En 1976, William Diffie y Martin Hellman propusieron un sistema de encriptación en que se empleaban diferentes claves para el cifrado y el descifrado, sin realizar intercambio de claves; estas claves deben estar relacionadas mediante un algoritmo o función matemática de dirección única. Una "*one way function*", es una función $f : X \to Y$ tal que $f(x)$ es (computacionalmente) "fácil" de calcular para cada $x \in X$, pero que , para la mayoría de los $y \in Y$ es "difícil" de calcular $f^{-1}(y)$, "difícil", significa "computacionalmente no factible ", es decir, no factible usando los mejores algoritmos conocidos y el mejor hardware. Pero podría suceder que si se usa una función de dirección única para cifrar, ni siquiera el destinatario legítimo del mensaje, pueda ser capaz de descifrar; por ello es interesante concepto de *función única con trampa*, que es una función de dirección única para la cual existe una información adicional que permita invertirla de modo eficiente.
Para establecer el intercambio de claves, según Diffie y Hellman procedemos de la siguiente manera:

Primero, A y B acuerdan en una curva elíptica E sobre un cuerpo finito $\mathbb{F}_q$ y un punto $P \in E(\mathbb{F}_q)$ cuyo orden sea un primo grande.
Luego, A elige un entero a, calcula aP y envía aP a B.
También B elige un entero b, calcula bP y envía bP a A. Con lo enviado, A determina abP y B determina baP.

Si un intruso puede resolver logaritmos discretos en $E(\mathbb{F}_q)$, entonces puede usar P y aP para encontrar a. Después, puede calcular $a(bP)$ para hallar abP.

2.4 El Criptosistema de Rivest, Shamir y Adleman

En 1978, Ron Rivest, Adi Shamir y Len Adleman, propusieron el primer criptosistema de clave pública, y quizá el que más éxito ha tenido, conocido con el nombre de RSA.
El criptosistema RSA se basa en la hipótesis, de que, para n y e enteros positivos dados, donde n es, usualmente, el producto de dos primos grandes, la función

$m \to m^e \pmod n$ es de dirección única con trampa.
La trampa, que permite invertir la función, es precisamente conocer la descomposición en factores primos de n, por lo que se puede decir que el RSA está basado en la dificultad del problema de factorización de números enteros.
Un usuario del RSA construye su clave de la siguiente manera:
Primero construye un entero $n = pq$ donde p y q son dos primos grandes, aproximadamente del mismo tamaño y que no estén muy próximos(para dificultar al máximo la factorización n).
Luego calcula $\phi(n) = (p-1)(q-1)$ y elige un entero e tal que
$1 < e < \phi(n)$ y $\text{mcd}(e, \phi(n)) = 1$.
Finalmente, calcula el inverso multiplicativo de e módulo $\phi(n)$, es decir el único entero d tal que $1 < d < \phi(n)$ y $e.d \equiv 1 \pmod{\phi(n)}$.
Así,el par (n, e) constituye la clave pública para el usuario; y d es su clave privada. n recibe el nombre de *módulo*, e es el *exponente de encriptación* y d el *exponente de desencriptación*
Para enviar un mensaje a este usuario sólo hay que conocer su clave pública (n, e), si el texto claro es m (donde m es un entero menor que n), éste se encripta calculando:

$$c = m^e \pmod{n}$$

Como antes se ha mencionado, la función encriptación que proporciona el criptotexto c a partir de m es una función de dirección única con trampa. El usuario por su parte, descifra el mensaje haciendo uso de su clave privada calculando:

$$c^d = m \pmod{n}$$

Si se conoce la factorización de n en producto de primos, es fácil invertir esta función y desencriptar, pues entonces se puede obtener $\phi(n)$ y luego d de la misma forma que lo ha hecho el usuario.
Veamos a continuación un ejemplo de aplicación.

Ejemplo 2.2

1. *Primero tomemos dos números primos $p = 61$ y $q = 53$, entonces $n = 61 \times 53 = 3233$.*

2. *Calculemos el valor de $\phi(n) = 60 \times 52 = 3120$.*

3. *Si tomamos el valor de $e = 17$ que es primo relativo con $\phi(n)$,*

4. *Debemos determinar el valor de* d , $0 < d < 3120$ *tal que* $17d \equiv 1(\mod 3120)$, *entonces* $d = 2753$.

La clave privada es $(17, 3233)$ *y la clave pública es* $(2753, 3233)$.

Si tenemos un texto claro $m = 64$ *entonces debemos determinar* $64^{17} \mod 3233$, *para encriptarlo. Podemos usar la aritmética modular para determinarlo, también podemos aplicar el sistema de cálculo de PARI/gp de donde obtenemos que*

$$64^{17} \equiv 1577 \mod 3233$$

Entonces, $c = 1577$ *es el texto encriptado. Para descifrar* $c = 1577$ *calcularemos* $c^{2753} \mod 3233$
luego $1577^{2753} \equiv 64 \mod 3233$. *Como vemos hemos obtenido el texto claro inicial* m

2.5 Criptosistema ElGamal

El procedimiento de ElGamal es un algoritmo basado en el problema del logaritmo discreto en $\mathbb{F}_q$ creado por Taher ElGamal en 1984. Consiste en lo siguiente:
Primero, B establece su clave pública eligiendo una curva elíptica E sobre un cuerpo finito $\mathbb{F}_q$; y un punto P sobre E cuyo orden sea un primo grande.
Luego, B elige un número entero secreto b y calcula $Q = bP$.
Entonces, la curva elíptica E, el cuerpo finito $\mathbb{F}_q$ y los puntos P y Q son la clave pública de B. El entero b es su clave privada. Si A quiere mandar un mensaje a B, primero A expresa su mensaje como un punto $R \in E(\mathbb{F}_q)$, elige un entero a y calcula $N = aP$, $M = R + aQ$ y envía N y M a B.
Para desencriptar el mensaje, B calcula: $M - bN$, pues $M - bN = (R + aQ) - b(aP) = R + a(bP) - b(aP) = R$.

Una tercera persona que conoce la información pública de B y los puntos M y N; si puede calcular logaritmos discretos, él puede usar P y Q para hallar b, y desencriptar el mensaje $M - bN$.

Firmas digitales con curvas elípticas

El uso de comunicaciones electrónicas y sobre todo del comercio electrónico han motivado la necesidad de hallar una forma de poder garantizar la identidad del remitente del mensaje recibido (*no repudio*). Es entonces que ha surgido la firma digital como el análogo de la firma manual.
Para que la longitud de la firma digital sea mucho menor que el mensaje que se firma, se utilizan funciones *hash*, llamadas funciones resumen. Entonces, la firma digital será una función del hash del mensaje y de la clave privada del firmante, así, se podrá comprobar la veracidad de tal firma a partir de a clave pública del firmante.

Para obtener el esquema de firmas digitales de ElGamal se hace uso idea similar a la del criptosistema de ElGamal. Una variante de este esquema es el llamado Algoritmo de firmas digitales (Digital Signature Algorithm, DSA), cuyo algoritmo es la base del Digital Signature Standard (DSS) que fue adoptado como estándar para firmas digitales en los Estados Unidos.

Algoritmo (*Generación de firma digital del ECDSA*)
Entrada : Los parámetros (p,a,b,P,n), la clave pública Q, la clave privada d y el mensaje en claro m.
Salida : El mensaje m con la firma (r,s).

Paso 1 Calcular el *Hash* del mensaje: $h = H(m)$.

Paso 2 Elegir un valor de k tal que $1 \leq k \leq n-1$

Paso 3 Calcular el punto $[k]P = (x, y)$ en $E(\mathbb{F}_p)$.

Paso 4 Calcular $r = x(\mod n)$.

Paso 5 Calcular $s = k^{-1}(h + dr) \quad (\mod n)$.

Paso 6 Devolver m y (r, s).

Capítulo 3

Grupo formal de curvas elípticas

Antes de introducir el concepto de grupo formal, haremos primero un estudio del desarrollo en series de potencias de la suma de dos puntos de una curva elíptica alrededor del punto $\mathcal{O}$.

3.1 Expansiones alrededor de 0

Sea E la curva elíptica definida sobre un cuerpo K,con la siguiente ecuación de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.1}$$

Queremos representar los puntos racionales de E en series de potencias alrededor del punto $\mathcal{O}$ con un parámetro en K, para ello consideremos el siguiente cambio de variable, para que el punto $\mathcal{O}$ sea el par $(0, 0)$ en el plano (z, w):

$$z = -\frac{x}{y},\ w = -\frac{1}{y}.$$

Así, tendremos que

$$x = \frac{z}{w},\ y = -\frac{1}{w}. \tag{3.2}$$

Con este cambio, la ecuación (3.1) se convierte en

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 \quad (= f(z, w)\ ) \tag{3.3}$$

Sustituyendo w, en la parte derecha de la igualdad por su misma fórmula recursivamente, obtenemos una expresión de w como serie de potencias en z.

$$w(z) = z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + 2a_3)z^6 + \cdots \tag{3.4}$$

Luego, podemos reescribirla así:

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]. \tag{3.5}$$

donde : $A_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, para todo valor de $n \in \mathbb{N}$.
Quisiéramos que la serie dada en (3.4) sea convergente, para ello recurrimos al siguiente resultado dado por Kurt Hensel.

Decimos que un anillo R es completo respecto a un ideal I, si toda sucesión de cauchy es convergente, a un elemento de R, en el sentido de la topología I-ádica.

Lema 3.1 *(Hensel) Sea R un anillo que es completo con respecto al ideal $I \subset R$, y sea $F(\omega) \in R[\omega]$ un polinomio. Si $a \in R$ satisface*

$$F(a) \in I^k \text{ y } F'(a) \in R^*, \quad \textit{(para algún enterok} \geq 1)$$

Entonces, para cualquier $\alpha \in R$ tal que $\alpha \equiv F'(a) \mod I$, la sucesión

$$\omega_0 = a, \ \omega_{m+1} = \omega_m - F(\omega_m)/\alpha$$

converge según el sentido de la topología I-ádica, a un elemento $b \in R$ que satisface

$$F(b) = 0 \text{ y } b \equiv a \mod I^k.$$

Si R es un dominio integral, estas condiciones determinan b unívocamente.

Aplicando este lema cuando $R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$ que es completo respecto de $I = \langle z \rangle$,

$$F(w) = f(z, w) - w = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 - w$$

y tomando $a = 0$, $F(0) = z^3 \in I^3$

$$F'(0) = a_1 z + a_2 z^2 - 1 \equiv -1 \ (mod I), \text{ así } \alpha = -1.$$

La sucesión converge a un valor de $b = b(z) \in R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$ tal que $f\big(z, b(z)\big) - b(z) = F(b) = 0$. Así $b(z) = f\big(z, b(z)\big)$
Más aun $b(z) \equiv 0 \mod I^3$, es decir $b(z) = z^3(T(z))$ donde $T \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$.

Entonces, por el lema de Hensel, la serie dada en (3.5) es convergente en $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$ y más aun $w(z)$ es la única serie de potencias que satisface que $w(z) = f\big(z, w(z)\big)$. La prueba de este lema la podemos encontrar en [Sil09]pág.155

Ahora, como la serie $1 + A_1 z + A_2 z^2 + \cdots$ es invertible, calculemos las z-series de potencias de x e y usando las ecuaciones (3.2) y (3.4)

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 + \cdots, \tag{3.6}$$

$$y(z) = \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 z + (a_4 + a_1 a_3) z^2 + \cdots. \tag{3.7}$$

Ahora, en el plano (z, w) consideremos la recta que une los puntos $P_1 = (z_1, w_1)$ y $P_2 = (z_2, w_2)$, cuya pendiente es

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{w_2^n - w_1^n}{z_2 - z_1} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!]$$

puesto que $w_i = w(z_i) = A_0 z_i^3 + A_1 z_i^4 + A_2 z_i^5 + \cdots$ para $i = 1, 2$.
La ecuación de la recta que pasa por P_1 y P_2 es $w = \lambda z + v$, donde $v = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, a_2, \cdots a_6][\![z_1, z_2]\!]$
Considerando la intersección de la recta con la curva en la ecuación de Weierstrass dada por (3.3)

$$w = z^3 + a_1 z(\lambda z + v) + a_2 z^2(\lambda z + v) + a_3(\lambda z + v)^2 + a_6(\lambda z + v)^3$$

obtenemos la siguiente cúbica,

$$w = (1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3) z^3 + (a_1\lambda + a_2 v + a_3\lambda^2 + 2a_4\lambda v + 3a_6\lambda^2 v) z^2 + \cdots$$

tal que dos de sus 3 raíces son z_1, z_2, y su tercera raíz z_3 es tal que

$$z_3 = -z_1 - z_2 - \frac{a_1\lambda + a_2 v + a_3\lambda^2 + 2a_4\lambda v + 3a_6\lambda^2 v}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3}.$$

Así, z_3 es la coordenada del tercer punto P_3 donde la recta corta a E; más aún, dicho punto es $-P_1 - P_2$, por la ley de grupo de E y $z_3 = z_3(z_1, z_2) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!]$

Como el opuesto de (x, y) es $(x, -y - a_1 x - a_3)$, el opuesto aditivo de (z, w) tiene z-coordenada

$$i(z) = \frac{x(z)}{y(z) + a_1 x(z) + a_3} = \frac{z^{-2} - a_1 z^{-1} - \cdots}{-z^{-3} + 2a_1 z^{-2} + \cdots} = -z + \cdots \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$$

Para nuestro caso tenemos que

$$z(P_1 + P_2) = i(z_3(z_1, z_2)) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - \cdots$$

Luego, definimos

$$F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - (2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \cdots \tag{3.8}$$

Observamos que $F(z_1, z_2) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!]$; y de la geometría de la curva E, se tienen las siguientes propiedades:

1. $F(z_1, z_2) = F(z_2, z_1)$
2. $F(z_1, F(z_2, z)) = F(F(z_1, z_2), z)$
3. $F(z, i(z)) = 0$

3.1.1 Grupo formal de curvas elípticas

Sea R un anillo. Un *grupo formal* $\mathfrak{F}$ definido sobre R que denotaremos así $\mathfrak{F}/R$, es una serie de potencias $F(X, Y) \in R[\![X, Y]\!]$ que satisface las siguientes propiedades:

1. $F(X, Y) = X + Y +$ (términos de grado ≥ 2);
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$; (Asociatividad)
3. $F(X, Y) = F(Y, X)$; (Conmutatividad)
4. Existe una única serie de potencias $i(T) \in R[\![T]\!]$ tal que $F(T, i(T)) = 0$; (inversa)
5. $F(X, 0) = X$ y $F(0, Y) = Y$.

Veamos algunos ejemplos de grupos formales:

1. El *grupo formal aditivo*, denotado por $\widehat{\mathbb{G}}_a$ es

$$F(X, Y) = X + Y$$

obviamente cumple con las propiedades de la definición y $i(X) = -X$.

2. El *grupo formal multiplicativo*, denotado por $\widehat{\mathbb{G}}_m$ es

$$F(X,Y) = X + Y + XY \quad , \quad i(X) = \frac{1}{1+X} - 1 = \sum_{n=1}^{\infty} (-1)^n X^n$$

3. Sea E una curva elíptica dada por la ecuación de Weierstrass (3.1), con coeficientes en R. El *grupo formal asociado a* E, denotado por $\widehat{E}$, es dado por la serie $F(z_1, z_2)$ descrita en la ecuación (3.8).

Observación 3.1 *1. La serie dada en (3.8), que obtuvimos a partir de la suma de puntos de una curva elíptica dada por la ecuación de Weierstrass, con coeficientes* a_1, a_2, a_3, a_4, a_6*; es un grupo formal.*

2. La serie $i(T)$ *dada en la difinición de grupo formal es única, pues si existiera otra serie* $i'(T)$ *tal que* $F(T, i'(T)) = 0$ *entonces tendríamos que* $i'(T) = F(i'(T), 0) = F(i'(T), F(T, i(T))) = F(F(T, i'(T)), i(T)) = F(0, i(T)) = i(T)$.

Sea R un anillo local y completo, $\mathcal{M}$ el ideal maximal de R y $\mathfrak{F}/R$ el grupo formal definido sobre R, con ley de grupo formal $F(X,Y)$.

Definición 3.1.1 El grupo asociado a $\mathfrak{F}/R$, *denotado por* $\mathfrak{F}(\mathcal{M})$ *es el conjunto* $\mathcal{M}$ *con las operaciones de grupo*

$$x \oplus_{\mathfrak{F}} y = F(x,y), \quad \textit{para } x, y \in \mathcal{M};$$

$$x \ominus_{\mathfrak{F}} y = i(x), \qquad \textit{para } x, y \in \mathcal{M}.$$

Como R es completo, las series $F(x,y)$ y $i(x)$ convergen en R para $x, y \in \mathcal{M}$; y los axiomas de grupo formal implican que $\mathfrak{F}(\mathcal{M})$ es un grupo y $\mathfrak{F}(\mathcal{M}^n)$ es su subgrupo, para $n \geq 1$, con la ley de adición inducida por F, $z_1 \oplus z_2 = F(z_1, z_2)$ dada por la ecuación (3.8), donde $\mathcal{M}^n = \{z \in \mathcal{M} / v_p(z) \geq n\}$.

En particular, consideraremos el anillo local y completo $\mathbb{Z}_p$, con cuerpo de fracciones $\mathbb{Q}_p$ y $\mathcal{M} = p\mathbb{Z}_p$ su único ideal maximal. Tenemos que $\widehat{E}(\mathcal{M})$ es el grupo asociado a $\widehat{E}$, que es el conjunto $\mathcal{M}$ con la ley de adición inducida por F, $z_1 \oplus z_2 = F(z_1, z_2)$ dada por la ecuación (3.8).

Si $z \in \mathcal{M}$, la serie de potencias (3.4) converge y $P(\frac{z}{w(z)}, -\frac{1}{w(z)})$ es un punto en $E(\mathbb{Q}_p)$, es decir tenemos un mapeo de $\mathcal{M} \to E(\mathbb{Q}_p)$ tal que $z \mapsto (x(z), y(z))$; donde $x(z) = \frac{z}{w(z)}, y(z) = -\frac{1}{w(z)}$, con $v_p(x(z)) = -2v_p(z) < 0$; así las series de potencias para $\widehat{E}$ están definidas, y éste mapeo nos da un homomorfismo de $\widehat{E}(\mathcal{M})$ a $E(\mathbb{Q}_p)$.

Recíprocamente, para un punto arbitrario $P(x, y)$ en $E(\mathbb{Q}_p)$ que satisface $v_p(x) < 0$, existe un único valor $z \in \mathcal{M}$ correspondiente a este P, $z = -\frac{x(z)}{y(z)}$.
Luego, este tipo de puntos junto con el punto infinito $\mathcal{O}$ es isomorfo a $\widehat{E}(\mathcal{M})$.Así

$$\widehat{E}(\mathcal{M}) = \{P(x, y) \in E / v_p(x) < 0\} \cup \{\mathcal{O}_E\} \subseteq E(\mathbb{Q}_p)$$

se convierte en un subgrupo de $E(\mathbb{Q}_p)$.
$\mathcal{M}^n = \{z \in \mathcal{M} | v_p(z) \geq n\}$ con la suma formal definida antes y denotada por $\oplus$, constituye en un subgrupo de $(\mathcal{M}, \oplus)$ y denotamos por $\widehat{E}(\mathcal{M}^n)$ a los correspondientes puntos con $z \in \mathcal{M}^n$ y $\mathcal{O}$ en E, que forman un subgrupo de $\widehat{E}(\mathcal{M})$. Para mas detalles sobre el tema podemos revisar [Sil09]pág 117-118,capítulo IV.

3.2 Logaritmo formal

El logaritmo formal es una función que nos permite transformar el grupo $\hat{E}(\mathcal{M})$ en el grupo $\mathcal{M}$ con su suma usual; para ver ello, daremos antes, algunas definiciones.

Definición 3.2.1 *Una forma diferencial es una expresión del siguiente tipo:* $P(T)dT \quad$ *donde* $P(T) \in R[\![T]\!]$

Definición 3.2.2 *Sea* R *un anillo y el* grupo formal $\mathfrak{F}$ *definido sobre* R.
Una forma diferencial $w(T) = P(T)dT \in R[\![T]\!]dT$ *es una* diferencial invariante sobre $\mathfrak{F}/R$ *si* $\quad w \circ F(T, S) = w(T)$.

Es decir, una diferencial invariante es una diferencial que satisface que

$$P(F(T, S))F_X(T, S) = P(T)$$

donde $F_X(T, S)$ es la derivada parcial de F con respecto a la primera variable.
Más aún, si $P(0) = 1$, decimos que w es una diferencial invariante normalizada.

Teorema 3.1 *Dado $\mathfrak{F}/R$ un grupo formal, entonces*
Existe una única forma diferencial invariante normalizada sobre $\mathfrak{F}/R$ y es

$$w = F_X(0,T)^{-1}dt$$

Ahora, considerando $\widehat{E}$ el grupo formal asociado a la curva elíptica E, existe una única diferencial invariante normalizada ω,

$$\omega = \frac{dx}{2y + a_1x + a_3}. \tag{3.9}$$

sustituyendo x e y dados en las acuaciones (3.6) y (3.7), ω se transforma en

$$\omega(z) = \big(1 + a_1z + (a_1^2 + a_2)z^2 + \cdots\big)dz.$$

Definición 3.2.3 *El logaritmo formal es la integral de ω:*

$$\log_E(T) = \int \omega(T) = T + \frac{1}{2}a_1T^2 + \frac{1}{3}(a_1^2 + a_2)T^3 + \cdots \in \mathbb{Q}[\![T]\!].$$

La exponencial formal es la inversa del logaritmo formal bajo la composición.

Los llamados *logaritmo formal* y *exponencial formal* son isomorfismos de grupos de $(\mathcal{M}, \oplus)$ a $(\mathcal{M}, +)$ y vicecersa, la exponencial formal es la única serie de potencias $\exp_E(T) \in \mathbb{Q}[\![T]\!]$ que satisface

$$\log_E(\exp_E(T)) = \exp_E(\log_E(T)) = T;$$

Mas aún, tenemos el siguiente resultado cuya demostración la podemos encontrar en [Sil09]Prop.5.5 pág. 123

Teorema 3.2 *Sea R un anillo con característica 0, y $\mathfrak{F}/R$ un grupo formal, entonces*

$$\log_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{a_n}{n}T^n \quad y \quad \exp_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!}T^n$$

con $a_n, b_n \in R$ y $a_1 = b_1 = 1$.

Observación 3.2 *Dado un $P \in \widehat{E}(\mathcal{M})$, queremos calcular $[m]P$.*
Para ello basta con calcular su z-coordenada y aplicar el logaritmo formal, hacer multiplicación puntual en $\mathbb{Z}_p$ y regresar con la exponencial, así

$$z([m]P) = \exp_E(m \log_E(z(P))).$$

Los coeficientes del logaritmo formal y exponencial formal se pueden calcular con anticipación, de tal forma que la multiplicación puntual en $\widehat{E}(\mathcal{M})$ se convierta en dos cálculos de series de potencia y una multiplicación en $\mathbb{Z}_p$, estos nos permite mejorar la eficiencia del cálculo de $[m]P$.

3.3 Reducción de curvas elípticas

Dados un primo p y una curva elíptica E definida sobre $\mathbb{Q}_p$, por la ecuación de Weierstrass (3.1), con $a_i \in \mathbb{Z}_p$.
Diremos que E *tiene una buena reducción módulo* p, si al reducir los coeficientes modulo p de esta ecuación, obtenemos otra curva elíptica sobre $\mathbb{F}_p$, llamada *la curva reducción de E modulo p*, la denotaremos por $\tilde{E}$ y está dada por la siguiente ecuación:

$$\tilde{E}/\mathbb{F}_p : y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6,$$

donde $\overline{a}_i \equiv a_i \mod p$.
$\tilde{E}(\mathbb{F}_p)$ denotará el conjunto de los puntos $\mathbb{F}_p$-racionales de $\tilde{E}$ y $\tilde{\mathcal{O}}_{\tilde{E}}$ es el elemento identidad del grupo abeliano $\tilde{E}(\mathbb{F}_p)$, es decir

$$\tilde{E}(\mathbb{F}_p) = \left\{(\overline{x}_0 : \overline{y}_0) \in \mathbb{F}_p^2 \mid \overline{y}_0^2 + \overline{a}_1\overline{x}_0\overline{y}_0 + \overline{a}_3\overline{y}_0 = \overline{x}_0^3 + \overline{a}_2\overline{x}_0^2 + \overline{a}_4\overline{x}_0 + \overline{a}_6\right\} \cup \{\tilde{\mathcal{O}}_{\tilde{E}}\}$$

Dado un punto P en $E(\mathbb{Q}_p)$ podemos expresarlo en coordenadas homogéneas
$P = (X_0 : Y_0 : Z_0)$, donde X_0, Y_0, Z_0 son no todos cero.
Existe una aplicación reducción modulo p canónica de $E(\mathbb{Q}_p)$ a $\tilde{E}(\mathbb{F}_p)$:

$$\begin{aligned} \kappa : E(\mathbb{Q}_p) &\rightarrow \tilde{E}(\mathbb{F}_p), \\ (X_0 : Y_0 : Z_0) &\mapsto (\overline{X}_0 : \overline{Y}_0 : \overline{Z}_0), \end{aligned}$$

donde $(X_0 : Y_0 : Z_0)$ son las coordenadas homogéneas del punto P en $E(\mathbb{Q}_p)$, $X_0, Y_0, Z_0 \in \mathbb{Z}_p$ y al menos una de ellas no pertenece a $\mathcal{M}$, además $X_0 = \overline{X}_0 \mod p, Y_0 = \overline{Y}_0 \mod p, Z_0 = \overline{Z}_0 \mod p$. (Llamamos a esto buena representación de la reducción de las coordenadas homogéneas de P).
La aplicación κ está bien definida y es suryectiva. Si denotando por $E_1(\mathbb{Q}_p)$ el núcleo de este homomorfismo, obtenemos la siguiente sucesión exacta de grupos abelianos

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E(\mathbb{Q}_p) \xrightarrow{\kappa} \tilde{E}(\mathbb{F}_p) \longrightarrow 0. \tag{3.10}$$

más aún se tiene que $E_1(\mathbb{Q}_p)$ y $\hat{E}(\mathcal{M})$ son isomorfos; así tenemos la siguiente sucesión exacta

$$0 \longrightarrow \hat{E}(\mathcal{M}) \longrightarrow E(\mathbb{Q}_p) \xrightarrow{\kappa} \tilde{E}(\mathbb{F}_p) \longrightarrow 0. \tag{3.11}$$

3.4 Levantamiento de un curva elíptica

Sea $\tilde{E}$ una curva definida sobre $\mathbb{F}_p$. Una curva elíptica E definida sobre $\mathbb{Q}_p$ es llamada *levantamiento* de $\tilde{E}$, si $\tilde{E}$ es la curva reducción de E módulo p. Un punto $P \in \mathbb{Q}_p$ es llamado *el levantamiento del punto* $\overline{P} \in \tilde{E}(\mathbb{F}_p)$, si este se reduce a $\overline{P}$ módulo p.

Cabe resaltar que los levantamientos de una curva elíptica o de un punto no son únicos.

Para hallar el levantamiento de $\overline{P} \in \tilde{E}(\mathbb{F}_p)$, debemos considerar E, dada por la misma ecuación de Weierstrass que $\tilde{E}$. La x- coordenada de P permanecerá igual a la de $\overline{P}$, la y-coordenada puede calcularse considerando su expansión $p-$ádica y teniendo en cuenta que satisface la ecuación de Weierstrass, y por el lema de Hensel([Kob84]pág.16), si tenemos una solución de una ecuación polinomial modulo p^i, podemos hallar una solución modulo p^{i+1}.

Capítulo 4

Criptografía con curvas elípticas sobre cuerpos p-ádicos

La criptografía con curva elíptica (CCE) es una variante de la criptografía de clave pública basada en las propiedades matemáticas de las curvas elípticas, fue propuesta por Neal Koblitz y Victor Miller en 1985, y son importantes porque usa claves mas pequeñas que los métodos tradicionales como el RSA, lo que proporciona ahorro en ancho de banda en las redes de comunicación, ahorro en consumo de memoria y de capacidad del procesador, y con un nivel de seguridad equivalente al RSA.

4.1 El grupo criptográfico

Determinación del grupo critográfico

Queremos encontrar un subgrupo finito del grupo de puntos racionales de una curva elíptica definida en el cuerpo p-ádico $\mathbb{Q}_p$, en el que podamos trabajar como en $\mathbb{F}_p$.

Sea $\tilde{E}$ la curva elíptica definida sobre $\mathbb{F}_p$,con ecuación

$$\tilde{E} : y^2 = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6,\ \overline{a}_i \in \mathbb{F}_p. \tag{4.1}$$

y consideremos que el orden del grupo $\tilde{E}(\mathbb{F}_p)$ tiene un factor primo d grande, distinto de $p(p > 2)$.
Si levantamos $\tilde{E}(\mathbb{F}_p)$ dada por (4.1) a $\mathbb{Q}_p$, obtenemos otra curva elíptica con ecuación

$$E : y^2 = x^3 + a_2 x^2 + a_4 x + a_6, \tag{4.2}$$

donde $a_i \in \mathbb{Q}_p$, con $a_i \equiv \overline{a}_i \mod p$.

Como $\hat{E}(\mathcal{M}^n)$ es un subgrupo de $\hat{E}(\mathcal{M})$ y tenemos la sucesión exacta

$$0 \longrightarrow \hat{E}(\mathcal{M}) \longrightarrow E(\mathbb{Q}_p) \xrightarrow{\kappa} \tilde{E}(\mathbb{F}_p) \longrightarrow 0,$$

entonces la siguiente sucesión también es exacta

$$0 \longrightarrow \hat{E}(\mathcal{M})/\hat{E}(\mathcal{M}^n) \longrightarrow E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n) \xrightarrow{\kappa} \tilde{E}(\mathbb{F}_p) \longrightarrow 0,$$

Así por el teorema fundamental de homomorfismo de grupos, el grupo cociente $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$, es un grupo finito con orden igual a $\#\tilde{E}(\mathbb{F}_p) \times p^{n-1}$.

Observación 4.1 *Veremos la posiblilidad de aplicar criptografía en este grupo $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$, para ello debemos garantizar las siguientes condiciones: poder determinar el generador de grupo, establecer un método del cálculo de $[k]P$, y hacer el análisis de dificultad del problema de logaritmo discreto en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$.*

Generador de grupo de cifrado

Queremos determinar el elemento generador del grupo de cifrado y para ello empezamos tomando un punto $\overline{P}$ de $\tilde{E}(\mathbb{F}_p)$ tal que el orden del grupo $\overline{G} = \langle \overline{P} \rangle$ es un primo grande d.

Proposición 4.1 *Los puntos de $\overline{G} \setminus \{\tilde{\mathcal{O}}_{\tilde{E}}\}$ poseen y-coordenadas no nulas.*

Prueba. Si existiera un punto de $\tilde{E}(\mathbb{F}_p)$ con y-coordenada igual a cero, entonces según la suma de puntos de una curva elíptica el orden de este punto es 2. Pero en $\overline{G}$ no existen puntos de orden 2, de lo contrario 2 dividiría a d el orden de $\overline{G}$, que es un primo grande. □

Por lo tanto, como la y-cordenada de $\overline{P}$ es no nula podemos levantar $\overline{P}$ a $E(\mathbb{Q}_p)$, por el lema de Hensel, luego aplicando módulo $\hat{E}(\mathcal{M}^n)$, obtenemos un punto P en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$.

Proposición 4.2 *Sea $Q(x, y)$ el punto determinado por las ecuaciones (3.6) y (3.7) con $z = p$. Si P es un elemento en el grupo $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ con $o(P) \neq dp^{n-1}$, entonces $o(P + Q) = dp^{n-1}$.*

Prueba. Por la suma de grupos formales tenemos que los elementos en $\hat{E}(\mathcal{M})/\hat{E}(\mathcal{M}^n)$ deben tener orden de esta forma p^j para algún entero $j < n$. Como el orden del $\overline{P}$ es d tenmos que $d.\overline{P} = 0$ y de acuerdo por reducción de curvas elípticas, $[d]P$ debe pertenecer a $\hat{E}(\mathcal{M})$. Por lo tanto, el orden de P debe ser dp^j para algún $0 \leq j < n$. Por la suma de grupo formales dada en (3.8), Q debe ser un punto de orden p^{n-1} en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$. Como $(d, p) = 1$, sabemos que el orden de $P + Q$ es dp^{n-1}. Entonces, siempre tendremos un punto $P \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ cuyo orden es dp^{n-1}.

De este resultado vemos que siempre encontraremos un punto P' es el generador de nuestro grupo de cifrado. Sea $G = \langle P' \rangle$.

Corolario 4.1 *Sea $(x, y) \in E(\mathbb{Q}_p)$ un elemento representativo de un punto finito en G. Entonces $v_p(y)$ no es positivo.*

Algoritmo y complejidad de cálculo de$[k]P$

Daremos un algoritmo de multiplicación puntual que usa el logaritmo y exponencial formal en curvas elípticas definidas sobre cuerpos numéricos p-ádicos.

Inicio: Dados un punto P, y los enteros k; d;
Paso 1. Calcular q, r tales que $k = dq + r$;
Paso 2. calcular $P_1 = [r]P$;
Paso 3. calcular $n = \log(z([d]P))$
Paso 4. calcular $z_1 = q \times n$;
Paso 5. calcular $z_2 = \exp(z_1)$;
Paso 6. calcular $P_2(x, y)$ tal que $z(P_2(x, y)) = z_2$;
Paso 7. devolver $P_1 + P_2$.
Salida: obtenemos $[k]P$;

Se pueden calcular $[d]P$ y $[r]P$ simultáneamente; si calculamos $[d]P$ por métodos tradicionales, el tiempo de complejidad es $\mathcal{O}(\log(k))$.
Con este nuevo método, todos los pasos tienen un consumo de tiempo fijo, excepto el paso 2; así la complejidad del cálculo la determina el cálculo de $[r]P$, éste método disminuye grandemente el costo de tiempo, comparado con calcular directamente

$[k]P$ por métodos tradicionales. Presentamos una comparación entre el cálculo de la multiplicación puntual en $E(\mathbb{Q}_p)/\widehat{E}(\mathcal{M}^n)$ y n veces la multiplicación puntual en $E(\mathbb{F}_p)$ basándonos en la siguiente teoría de cálculo aproximado.
El número r tiene la misma longitud en bits que la longitud del escalar en la multiplicación puntual de $E(\mathbb{F}_p)$, pero debemos considerar la complejidad de las fórmulas de adición en curvas elípticas definidas sobre cuerpos numéricos p-ádicos.
La suma de puntos en $E(\mathbb{Q}_p)/\widehat{E}(\mathcal{M}^n)$ esta dado por sumas, restas, multiplicaciones y divisiones de números p-ádicos. Una multiplicación (o división) de números p-ádicos de n coeficientes requiere $\frac{n^2}{2}$ multiplicaciones en $\mathbb{F}_p$. El algoritmo de multiplicación de Karastsuba ([CP05] sec.9.5, pág. 473) la puede reducir a $n^{\log_2 3}$.
Luego, el tiempo que se necesita para calcular la multiplicación puntual en $E(\mathbb{Q}_p)/\widehat{E}(\mathcal{M}^n)$, consume $\frac{n}{2}(n^{\log_2 3-1})$ múltiplo del tiempo para calcular n veces multiplicaciones puntuales en $E(\mathbb{F}_p)$.
Afortunadamente, la comparación del tiempo de complejidad no es muy significativo cuando n es pequeño, en la práctica recomendamos $3 \leq n \leq 6$.

4.2 Teoría del cálculo de aproximación

Sabemos que los representantes de este grupo cociente $E(\mathbb{Q}_p)/\widehat{E}(\mathcal{M}^n)$ son elementos de $E(\mathbb{Q}_p)$ y las coordenadas de estos puntos pertenecen a $\mathbb{Q}_p$, pero la mayoría de elementos en $\mathbb{Q}_p$ no puden ser almacenados en computadoras reales, por lo que es necesario encontrar una manera de aproximar las coordenadas.

En lo que sigue consideraremos que $\#\tilde{E}(\mathbb{F}_p)$ es impar.
Sea la curva elíptica definada en $\mathbb{Q}_p$ en la forma de Weierstrass

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \quad \text{donde} \quad a_i \in \mathbb{Z}_p.$$

Definición 4.2.1 *Dado* $x = \sum_{i=-t}^{\infty} a_i p^i \in \mathbb{Q}_p$, *llamaremos la* n-ésima aproximación de x *a la expresión* $\sum_{i=-t}^{n-1} a_i p^i$; *y la denotaremos por* $[x]_n$ *ó* $(x)_n$.

Proposición 4.3 *Sean* $x, y \in \mathbb{Q}_p$, $v_p(x) = r < n$, $v_p(y) = s < n$. *Tenemos las siguientes igualdades:*

1. $(x \pm y)(n) \equiv x(n) \pm y(n) \mod p^n$;

2. $(x \cdot y)(n) \equiv x(n-s) \cdot y(n-r) \mod p^n$;

3. $\frac{1}{x}(n) \equiv \frac{1}{x(n+2r)} \mod p^n$;

4. $\frac{y}{x}(n) \equiv \frac{y(n+r)}{x(n+2r-s)} \mod p^n$.

Todas estas propiedades se pueden verificar directamente de la definición.

4.2.1 Representación finita de puntos

En los teoremas siguientes veremos que todo punto finito en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ puede ser determinado por las coordenadas de aproximación $([x]_{n-3m}, [y]_{n-4m})$ del punto de representación arbitrario $P(x,y)$, donde $m = -\frac{v_p(y)}{3}$. Mostraremos que estas coordenadas de aproximación son únicas y las llamaremos *representación reducción* de $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$.

Proposición 4.4 *Para todo $P(x,y) \in \hat{E}(\mathcal{M})$, existe un entero positivo m que satisface*

$$v_p(x) = -2m,\ v_p(y) = -3m,\ v_p(z) = m,\ v_p(w) = 3m,$$

donde z, w se definen en las ecuaciones 3.2 y 3.4.

Prueba. Dado el punto $P(x,y) \in \hat{E}(\mathcal{M})$, y considerando las representaciones como series potencias de x, y, w dadas por las ecuaciones 3.6, 3.7, 3.3, entonces si $v_p(z) = m$ entonces $v_p(x) = -2m,\ v_p(y) = -3m,$ y, $v_p(w) = 3m$, donde m es un entero positivo, pues por el corolario 4.1, $v_p(y) < 0$.

Notar que si $P(x,y) \in \hat{E}(\mathcal{M})$, de la proposición anterior tenemos que

$m = v_p(z) \geq n$, entonces $-2m \leq -2n$; así $v_p(x(z)) \leq -2n$.

Teorema 4.1 *Sea $\hat{P}$ un punto finito arbitrario, $\hat{P} \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ tal que $P \in E(\mathbb{Q}_p)$ y $\hat{P} = P(x,y) \mod \hat{E}(\mathcal{M}^n)$ con $v_p(y) = -3m \quad (0 \leq m < n)$, entonces $\hat{P}$ está determinado, de manera única, por $([x]_{n-3m}, [y]_{n-4m})$.*

Prueba. Supongamos que también existe $Q(x', y') \in E(\mathbb{Q}_p)$ que satisface

$$[x']_{n-3m} = [x]_{n-3m}, \quad [y']_{n-4m} = [y]_{n-4m}.$$

entonces $v_p(y') = -3m$. Debemos probar que su diferencia pertenece a $\hat{E}(\mathcal{M}^n)$, es decir que $v_p\big(x(P-Q)\big) \leq -2n$.
Supongamos que $P \neq Q$, por la suma de puntos en curvas elípticas, sabemos que

$$x(P-Q) = \left(\frac{y+y'}{x-x'}\right)^2 - x - x' - a_2,$$

Luego, como $p \neq 2$ y $[y']_{n-4m} = [y]_{n-4m}$, tenemos $v_p(y+y') = v_p(y) = -3m$.
Como $[x']_{n-3m} = [x]_{n-3m}$, entonces $v_p(x-x') \geq n-3m$.
Por lo tanto,

$$v_p\left(\left(\frac{y+y'}{x-x'}\right)^2\right) \leq -2n$$

También,tenemos

$$v_p(-x-x'-a_2) = v_p(-x-x') \geq -2m > -2n;$$

entonces

$$v_p\big(x(P-Q)\big) = min\left\{v_p\left(\left(\frac{y+y'}{x-x'}\right)^2\right), v_p(-x-x'-a_2)\right\} = v_p\left(\left(\frac{y+y'}{x-x'}\right)^2\right) \leq -2n,$$

Así, $\quad P-Q \in \hat{E}(\mathcal{M}^n)$. $\square$

Teorema 4.2 *Sean $P(x_1, y_1)$, $Q(x_2, y_2) \in E(\mathbb{Q}_p)$ dos puntos representates del punto finito $\hat{P} \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$, distintos. Entonces se cumple que*
$v_p(y_1) = v_p(y_2) = -3m$, $[x_1]_{n-3m} = [x_2]_{n-3m}$, $[y_1]_{n-4m} = [y_2]_{n-4m}$.

Prueba. Primero, supongamos que $\hat{P} \in \hat{E}(\mathcal{M}^m) \setminus \hat{E}(\mathcal{M}^{m+1}), (0 \leq m < n)$. Entonces como $P, Q \in E(\mathbb{Q}_p)$ tenemos que $v_p(y_1) = v_p(y_2) = -3m$. Además, $v_p(x_1)$ y $v_p(x_2)$ no deben ser menores que $-2m > -2n$.
Como $P-Q \in \hat{E}(\mathcal{M}^n)$, tenemos $v_p\Big(x(P-Q)\Big) \leq -2n$.
De la fórmula de adición puntual

$$x(P-Q) = \left(\frac{y_1+y_2}{x_1-x_2}\right)^2 - x_1 - x_2 - a_2,$$

haciendo uso del resultado obtenido en la prueba anterior, tenemos que

$$-2n \geq v_p\left(\left(\frac{y_1+y_2}{x_1-x_2}\right)^2 - x_1 - x_2 - a_2\right) = v_p\left(\left(\frac{y_1+y_2}{x_1-x_2}\right)^2\right).$$

Así, $v_p(x_1-x_2) \geq n + v_p(y_1+y_2) \geq n-3m$,entonces $[x_1]_{n-3m} = [x_2]_{n-3m}$.
De la ecuación de Weierstrass de la curva elíptica tenemos que $[y_1]_{n-4m} = \pm[y_2]_{n-4m}$. Si $[y_1]_{n-4m} = -[y_2]_{n-4m}$, entonces como P y Q tienen el mismo representante $\hat{P} = -\hat{P}$, entonces $\hat{P}$ debe ser igual al $\hat{\mathcal{O}}$. Esto contradice la condición de que $\hat{P}$ es finito. Por lo tanto, $[y_1]_{n-4m} = [y_2]_{n-4m}$. □

4.2.2 Suma de puntos

Para que la suma de puntos en $E(\mathbb{Q}_p)/\tilde{E}(\mathcal{M}^n)$, tenga la exactitud deseada, necesitamos valores más exactos que $[x]_{n-3m}$ o $[y]_{n-4m}$, por ello veremos un algoritmo de levantamiento de puntos en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ a puntos en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^{n_1})$, donde n_1 es un entero mayor que n.

Proposición 4.5 Algoritmo de levantamiento en la y-coordenada
Entrada: Dada (x_0, y_0) *la representación reducción de un punto finito* $P_0 \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$.
Salida: Obtenemos (x, y) *la representación reducción de un punto* $P_r \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^{n_1})$ *tal que satisface* $P_r \equiv P_0 \mod \hat{E}(\mathcal{M}^n)$.
Paso 1. *Sean* $F(y) = y^2 - x_0^3 - a_2x_0^2 - a_4x_0 - a_6$ *y* $m = -\frac{v_p(y_0)}{3}$;
Paso 2. $k = n, y = y_0$;
Paso 3. *mientras* $k < n_1$;
{
$y = y - \left[\frac{F(y)}{2y}\right]_{2k-5m}$;
$k = 2k - m$;
}
Paso 4. *retornar* $(x_0, [y]_{(n_1-4m)})$.

Prueba. Denotemos por k_i al valor de k y por y_i al valor de y cuando el programa termina en la i-ésima vuelta. Como p es un primo impar, se cumple que $v_p(2y_i) = v_p(y_i)$ en cada vuelta. Probaremos por inducción que

$$v_p(F(y_i)) \geq k_i - 7m, \quad v_p(y_i) = -3m.$$

Para $i = 0$, la conclusión es obviamente correcta. Ahora, supongamos que para $i = L$ es correcta, y la probaremos para $i = L + 1$. Como $v_p(F(y_L)) \geq k_L - 7m$, $v_p(y_L) = -3m$, tenemos $v_p\left(\frac{F(y_L)}{2y_L}\right) = v_p(y_{L+1} - y_L) \geq k_L - 4m$. Esto significa que y_{L+1} no cambia los coeficientes de y_L en los términos de p^{-3m} hasta p^{k_L-4m-1}, y $v_p(y_i) \equiv -3m$ para cualquier i. Tendremos

$$F(y_{L+1}) = F(y_L) - 2y_L \left[\frac{F(y_L)}{2y_L}\right]_{2k_L-5m} + \left(\left[\frac{F(y_L)}{2y_L}\right]_{2k_L-5m}\right)^2,$$

como $v_p\left(\left(\left[\frac{F(y_L)}{2y_L}\right]_{2k_L-5m}\right)^2\right) \geq 2k_L - 8m$,

y $\quad v_p\left(F(y_L) - 2y_L \left[\frac{F(y_L)}{2y_L}\right]_{2k_L-5m}\right) \geq 2k_L - 8m$,

obtenemos $v_p(F(y_{L+1})) \geq 2k_L - 8m = k_{L+1} - 7m$.

Por inducción, vemos que nuestra conclusión es cierta para $i = L + 1$.

Sea $y = \lim_{i\to\infty} y_i$, veremos que

$$\lim_{i\to\infty} v_p(F(y_i)) = \infty \text{ si y sólo si } \lim_{i\to\infty} F(y_i) = 0\ , \qquad \text{entonces} \qquad F(y) = 0.$$

Es decir, $P(x_0, y)$ satisface la ecuación de Weierstrass y $P_i(x_0, y_i) = P(x_0, y)$ mod $\hat{E}(\mathcal{M}^{k_i})$. Por el teorema del punto representación sabemos que $(x_0, [y]_{n_1-4m})$ es lo que queremos.

Suma de puntos

Sean $\hat{P}(x_1, y_1)$ y $\hat{Q}(x_2, y_2)$ dos puntos finitos en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$, y sea $\hat{R}(x_3, y_3) = \hat{P}(x_1, y_1) + \hat{Q}(x_2, y_2)$. Denotemos por $P, Q,$ y $R = P + Q$ a sus puntos representantes en $E(\mathbb{Q}_p)$. Tomaremos en cuenta los siguientes casos.

Caso 1. $v_p(y_1) = v_p(y_2) = v_p(x_1 - x_2) = 0$. Es obvio que $P \neq \pm Q$ en esta situación. Consideremos las fórmulas de suma puntual

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 - a_2,$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

Supongamos que $v_p(y_2 - y_1) = t \geq 0$, entonces tendremos

$$[y_3]_n = \frac{[y_2 - y_1]_n}{[x_2 - x_1]_{n-t}}[x_1 - x_3]_n - [y_1]_n,$$

$$[x_3]_n = \left(\frac{[y_2 - y_1]_{n-t}}{[x_2 - x_1]_{n-2t}}\right)^2 - [x_1]_n - [x_2]_n - [a_2]_n.$$

En este caso, x_1, x_2, y_1 y y_2 tienen nivel de exactitud n, por lo tanto el levantamiento no es necesario.

Caso 2. $v_p(y_1) = 0$, $v_p(y_2) < 0$. Sean $v_p(y_2) = -3m$, $v_p(x_2) = -2m$. Entonces

$$v_p(x_2 - x_1) = -2m,$$

$$v_p(y_2 - y_1) = -3m.$$

Como $P \in E\backslash\hat{E}(\mathcal{M})$, $Q \in \hat{E}(\mathcal{M}^m)$, tendremos $R = P+Q \in E\backslash\hat{E}(\mathcal{M})$, y $v_p(y_3) = 0$. Como $R - P = Q \in \hat{E}(\mathcal{M}^m)$, por el teorema de representación de puntos, sabemos que $v_p(x_3 - x_1) = m$. Aquí, $P \neq \pm Q$, luego

$$[y_3]_n = \frac{[y_2]_{n-3m} - [y_1]_{n-3m}}{[x_2]_{n-3m} - [x_1]_{n-2m}}([x_1]_n - [x_3]_{n+m}) - [y_1]_n,$$

Note que $[x_3]_{n+m}$ aparece en la fórmula para el cálculo de $[y_3]_n$. Se debería calcular $[x_3]_{n+m}$ en el siguiente paso en vez de $[x_3]_n$. Aquí, necesitamos levantar $[y_2]_{n-4m}$ a $[y_2]_n$. Este cálculo explota el hecho de que el algoritmo de levantamiento de la Y-coordenada mantiene invariante a x.

Caso 3. $v_p(y_1) = v_p(y_2) = 0$, $v_p(x_1 - x_2) = m$, $0 < m < n$. Aquí, $P \neq \pm Q$. Por teoría de representación de puntos, sabemos si $v_p(y_2 - y_1) \geq m$ o $v_p(y_2 - y_1) = 0$.

1. Si $v_p(y_2 - y_1) = s \geq m$, afirmamos que $v_p(x_3) \geq 0$. Porque $\#E(\mathbb{F}_p)$ es impar y $\kappa(R) = \kappa(P) + \kappa(Q) = [2]\kappa(P)$. Por lo tanto, R debe ser un punto finito.

$$[y_3]_n = \frac{[y_2 - y_1]_{n+m}}{[x_2 - x_1]_{n-s+2m}}[x_1 - x_3]_{n-s+m} - [y_1]_n,$$

$$[x_3]_n = \left(\frac{[y_2 - y_1]_{n-s+2m}}{[x_2 - x_1]_{n-2s+3m}}\right)^2 - [x_1]_n - [x_2]_n - [a_2]_n.$$

Ahora, se necesita levantar $[y_1]_n, [y_2]_n$ a $[y_1]_{n+m}, [y_2]_{n+m}$.

2. Si $v_p(y_2 - y_1) = 0$, entonces R debe estar en $\hat{E}(\mathcal{M}) \setminus \hat{E}(\mathcal{M}^{m+1})$.

$$[y_3]_{n-4m} = \frac{[y_2 - y_1]_{n-m}}{[x_2 - x_1]_n}[x_3 - x_1]_{n-3m} - [y_1]_{n-4m} \mod p^n,$$

$$[x_3]_{n-3m} = \left(\frac{[y_2 - y_1]_{n-m}}{[x_2 - x_1]_n}\right)^2 - [x_1]_{n-3m} - [x_2]_{n-3m} - [a_2]_{n-3m} \mod p^n.$$

Caso 4. $v_p(y_1) = v_p(y_2) = 0$, $v_p(x_1 - x_2) = m \geq n$. Aquí, $P \equiv Q \mod \hat{E}(\mathcal{M}^n)$ o $P \equiv -Q \mod \hat{E}(\mathcal{M}^n)$. $\hat{R}$ debe ser $\hat{\mathcal{O}}_E$ en la segunda situación. Las fórmulas para la duplicación de un punto se usan en esta primera situación. Tenemos $v_p(x_3) = 0$ y

$$[y_3]_n = \frac{3[x_1]_n^2 + 2[a_2]_n[x_1]_n + [a_4]_n}{2[y_1]_n}[x_1 - x_3]_n - [y_1]_n,$$

$$[x_3]_n = \left(\frac{3[x_1]_n^2 + 2[a_2]_n[x_1]_n + [a_4]_n}{2[y_1]_n}\right)^2 - 2[x_1]_n.$$

No necesitamos levantamiento.

Caso 5. $P \in \hat{E}(\mathcal{M})$, $Q \in \hat{E}(\mathcal{M})$. (O calculamos $[m]P, P \in \hat{E}(\mathcal{M})$ directamente.) Podemos usar el logaritmo formal y la exponencial formal para acelerar el cálculo en este caso. Se necesitan los siguientes lemas.

Lema 4.1 *Sea P un punto en $\hat{E}(\mathcal{M}^m) \setminus \hat{E}(\mathcal{M}^{m+1})$. Entonces, $([x]_{n-3m}, [y]_{n-4m})$ y $[z]_n$ se determinan el uno al otro.*

Prueba. Del teorema 4.3 tenemos

$$[z]_n = -\left[\frac{x}{y}\right]_n = -\frac{[x]_{n-3m}}{[y]_{n-6m+2m}} = -\frac{[x]_{n-3m}}{[y]_{n-4m}}.$$

Por lo tanto, $[z]_n$ se puede determinar de $([x]_{n-3m}, [y]_{n-4m})$. Por otro lado, si $[z]$ tiene aproximación n-ésima, entonces w tiene aproximación $n + 2m$-ésima. Por lo tanto,

$$[y]_{n-4m} = -\left[\frac{1}{w}\right]_{n-4m} = -\frac{1}{[w]_{n-4m+6m}} = -\frac{1}{[w]_{n+2m}},$$
$$[x]_{n-3m} = [zy]_{n-3m} = [z]_{n-3m+3m}[y]_{n-3m-m} = [z]_n[y]_{n-4m}.$$

Esto muestra que $([x]_{n-3m}, [y]_{n-4m})$ también se puede determinar por $[z]_n$.

Podemos solamente extender la serie de potencias $w(z)$ al término z^{n+1}. Los coeficientes de z^i $(i > 3)$ pueden ser con $\{n + 2m - im\}$-ésima aproximación.

Observaciones.

1. Hacemos notar que esta suma de puntos aproximada es la que se considera en el algoritmo que dimos antes para el cálculo de $[k]P$.

2. Por el teorema 3.2, $\log_E$ y $\exp_E$ estan dados por series de potencias, y si se requiere resultados con aproximación de orden n-ésimo, sus entradas también deberían tener aproximación de orden n-ésimo. Las dos series de potencias se tienen que extender al término T^{n-1} y el coeficiente de cada término T^i se debe almacenar con aproximación $\{n-i\}$-ésima.

3. En resumen, $P+Q$ y $[k]P$ se pueden calcular como sigue.
Empezamos transformando las X, Y-coordenadas en Z-coordenada.
luego, calculamos la operación $\log_E$ sobre Z.
después, realizamos la suma de puntos y la multiplicación puntual o escalar en el cuerpos numéricos p-ádicos.
a continuación, calculamos $\exp_E$ de los resultados obtenidos.
Finalmente, regresamos a las X, Y-coordenadas.

4. Si $p > 3$, el coeficiente a_2 en la ecuación de Weierstrass se puede omitir. Esto ahorra más tiempo de cálculo. Además, levantar la curva elíptica de $\mathbb{F}_p$ a $\mathbb{Q}_p$ también se puede hacer sin a_2. Levantar $\overline{a}_4$ y $\overline{a}_6$ en a_4 y a_6 tal que satisfagan $a_4 \mod p = \overline{a}_4$ y $a_6 \mod p = \overline{a}_6$ es suficiente.

4.3 Análisis de seguridad

En esta sección queremos sealar que resolver el problema del logaritmo discreto en curvas elípticas en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ es tan seguro como resolverlo en $\tilde{E}(\mathbb{F}_p)$

Teorema 4.3 *Resolver un logaritmo discreto en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ es tan difícil como resolver el problema del logaritmo discreto en $\tilde{E}(\mathbb{F}_p)$.*

Prueba. (1) Si existe un algoritmo que es rápido para resolver el problema del logaritmo diacreto en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$, entonces también existe en $\tilde{E}(\mathbb{F}_p)$.

En efecto, si tenemos $\overline{P}, \overline{Q} \in \tilde{E}(\mathbb{F}_p)$, el problema es encontrar un k que satisfaga $[k]\overline{P} = \overline{Q}$. Por lo tanto, primero levantamos $\overline{P}, \overline{Q}$ a puntos $P, Q \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$. Como por hipótesis, existe un algoritmo rápido para resolver el logarimo discreto entonces hallamos el valor de k que satisface $[k]P = Q$. Luego consideramos el

homomorfismode grupos reducción y obtenemos que $[k]\overline{P} = \overline{Q}$, lo que resuelve el problema del logaritmo discreto en $\tilde{E}(\mathbb{F}_p)$.
(2) Si existe un algoritmo para resolver rápidamente el problema del logaritmo discreto en $\tilde{E}(\mathbb{F}_p)$, entonces también existe en $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$.
En efecto, sean $P, Q \in E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$, queremos determinar el valor de un m que satisfaga $[m]P = Q$. Entonces, consideramos mediante el homomorfiamo reducción $\kappa(P)$ y $\kappa(Q) \in \widehat{E}(\mathbb{F}_p)$ y como por hipótesis, existe un algoritmo que resuelve el problema del logaritmo discreto en $\tilde{E}(\mathbb{F}_p)$, podemos encontrar un r que satisfaga $[r]\kappa(P) = \kappa(Q)$. Entonces $Q - [r]P$ debe estar en $\tilde{E}(\mathcal{M})$, luego calculamos el logaritmo formal de $Q - [r]P$ y de $[d]P$ y encontramos un q que satisface

$$(q \times \log(z([d]P))) \equiv \log(z(Q - [r]P)) \mod \mathcal{M}^n.$$

Luego, aplicando la exponencial formal obtenemos que $Q = [r + qd]P$. Por lo tanto existe, un entero $m = r + qd$ tal que $[m]P = Q$.

Conclusiones

- El conjunto de puntos racionales de una curva elíptica E definida sobre un cuerpo K constituye un grupo abeliano con la suma, siendo la multiplicación puntual $[k]P$ la operación más importante.

- El problema del logaritmo discreto sobre curvas elípticas consiste en, conocidos $P, Q \in E(K)$ tal que $Q = kP$ hallar el valor de k, es por ello la importancia de la multiplicación puntual.

- Es posible hacer criptografía con curvas elípticas sobre cuerpos infinitos, como $\mathbb{Q}_p$ pues usando la teoría de grupo formal de curvas elípticas es posible encontrar un grupo $E(\mathbb{Q}_p)/\hat{E}(\mathcal{M}^n)$ que tiene todas las características que se necesita para hacer criptografía.

- Mediante la teoría de aproximación, podemos calcular la suma de puntos y obtener un método de multiplicación puntual eficiente, que resuelve el problema de logaritmo discreto.

- Hacer critografía con curvas elípticas sobre $E(\mathbb{Q}_p)/\widehat{E}(\mathcal{M}^n)$ es tan seguro como el criptosistema con curvas elípticas definidas sobre $\mathbb{F}_p$.

- Los métodos de criptografía sobre grupos de curvas elípticas son tan seguros como los tradicionales, y con claves criptográficas con menores cantidades de bits, lo que genera una ganancia en el procesamiento, pues podemos tener criptografía con curvas elípticas en dispositivos con poco poder computacional, como tarjetas de banco, teléfonos celulares, etc.

Bibliografía

[Bac64] George Bachman. *Introduction to p-adic Numbers and Valuation Theory.* Academic Press, 1964.

[CP05] R. Crandall and C. Pomerance. *Prime Numbers, A computacional perspective.* Springer, 2005.

[Kna93] Anthony W. Knapp. *Elliptic Curves.* Princeton University Press, 1993.

[Kob84] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta- Function.* Springer-Verlag, 1984.

[Kul03] Leopoldo Kulesz. Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$. *Acta Arith.*, 108(4):339–356, 2003.

[Rob00] A. M. Robert. *A coursse in p-adic analysis.* Springer-Verlag, 2000.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[Was03] L . Washinton. *Elliptic Curves: Number Theory and criptography.* Boca Raton, 2003.

[XZF+08] MaoZhi Xu, ChunLai Zhao, Min Feng, ZhaoRong Ren, and JiQing Ye. Cryptography on elliptic curves over p-adic number fields. *Sci. China Ser. F*, 51(3):258–272, 2008.

[BGN00] I. Blake, G.Seroussi, N. Smart *Elliptic curves in Cryptography.* Cambrige University Press, 2000.

[DH76] W. Diffie, M.E. Hellman New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol.IT-22.1976,644-654.

[ElG85] T. ElGamal A public key cryptosystem and a signature scheme based on discret logarithms. *IEEE Transactions on Information Theory*, 31 n4,1985,469-472.

[RSA78] R. Rivest, A. Shamir, L. Adleman.
A method for obtaining digited signatures and PKC *Comunications of the ACM*, vol.21(2),1978,120-128.

[HMV03] D. Hankerson, A. Meneses, S. Vanstone *Guide to Elliptis Curve Criptography*. Springer, 2003.

[NK98] N. Koblitz. *Algebraic aspects of cryotgraphy.*, Springer-Verlag, 1998.

[MN93] A. Menezes. *Elliptic Curves Public Key Crytography*, Kluwer, 1993.

[MLL86] V. Miller.
Uses of elliptic curves in cryptography. *Advances in cryptology-CRYPTO'85,*, LNCS218,1986,417-426