UNIVERSIDAD TECNOLÓGICA DE LA MIXTECA

"CURVAS ELÍPTICAS Y SU APLICACIÓN EN CRIPTOGRAFÍA"

TESIS

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN MATEMÁTICAS APLICADAS

PRESENTA:

FLAVIA REYES PÉREZ

DIRECTOR:

M. C. ADOLFO MACEDA MÉNDEZ

HUAJUAPAN DE LEÓN, OAXACA, ENERO 2015

A mis padres y a mis hermanos

Agradecimientos

Agradezco a mis padres *Susana y Jesús* y a mis hermanos *Juan, Abraham, Jacob* y*Martha* quienes nunca dejaron de creer en mi y que a pesar de las dificultades siempre me brindaron apoyo incondicional, por sus palabras de aliento y consejos.

A mis amigos por hacer amena mi estancia en la universidad e hicieron superables los momentos tristes y angustiantes. Y a mis compañeros y grandes amigos quienes compartieron cinco años agradables conmigo.

A mi director de tesis el M. C. Adolfo Maceda Méndez, gracias por compartir conmigo sus conocimientos, por las asesorías y orientaciones, por su motivación, apoyo y tiempo dedicado en la realización de este trabajo. Agradezco a mis revisores, M.C. Luz del Carmen Álvarez Marín, M.C. Vulfrano Tochihuitl Bueno y M.C. Mario Lomelí Haro, por el tiempo dedicado a la revisión de este trabajo y, quienes con sus observaciones y comentarios hicieron de éste un mejor trabajo.

Mi agradecimiento a todos los profesores que me compartieron sus conocimientos a lo largo de la carrera. También quiero agradecer a la Universidad Tecnológica de la Mixteca por permitirme formarme profesionalmente.

Índice general

Introducción

A lo largo de la historia de la humanidad, el ser humano ha tenido la necesidad de comunicarse, de transmitir mensajes, de tal manera que si éste es interceptado por aquellas personas a las que no va dirigido el mensaje, no conozcan el contenido del mismo. Es por ello que se ha visto en la necesidad de diseñar sistemas y métodos para cifrar mensajes, de esto se encarga la criptografía.

La criptografía, de acuerdo a la historia se divide en dos partes: *clásica* y *moderna*. Todos los sitemas de cifrado anteriores a la segunda guerra mundial, o bien al nacimiento de las computadoras, son los que se conocen como criptografía clásica. Estos sistemas pueden ser empleados usando lápiz y papel, por ello los mensajes que son cifrados con estos algoritmos pueden ser descifrados de manera rápida con ayuda de una computadora, por lo que fueron dejándose de usar [9]. Además, la seguridad de estos algoritmos está basada en mantener en secreto la forma en que trabajan. De esta manera, un gran número de usuarios o cadenas de grupos de usuarios no pueden utilizarlos, debido a que si alguien abandona el grupo o revela accidentalmente el secreto del algoritmo todos tienen que cambiar sus algoritmos a uno distinto. Algunos ejemplos de este tipo de sistemas son: el cifrado por sustitución que utiliza la técnica de sustituir cada carácter o grupo de caracteres del texto claro por otro carácter o grupo de caracteres que corresponde al alfabeto cifrado, como ejemplo tenemos el cifrado de César; y el sistema de cifrado por transposición que utiliza la técnica de permutación de tal manera que los caracteres del texto se reordenan mediante un algoritmo.

La criptografía moderna nace junto con las computadoras. Los algoritmos de este tipo de criptografía basan su seguridad en algoritmos matemáticos que se consideran computacional-

mente difíciles, estos es, que no se conocen algoritmos eficientes para su resolución y resuelve el problema que presenta la clásica con una *clave*. Algunos ejemplos de este tipo de criptografía son: sistema de clave secreta o simétrica y el sistema de clave pública o asimétrica. En un sistema simétrico se utiliza algún método matemático que se conoce como *sistema de cifrado* que se utiliza para cifrar y descifrar el mensaje haciendo uso de una sola clave para ambas tareas, esto es, tanto el emisor como el receptor deben tener conocimiento de la misma.

Por otro lado, en un sistema asimétrico o de clave pública, se tiene una clave para cifrar y otra para descifrar el mensaje. La clave para cifrar se conoce como *clave pública del receptor* y ésta se encuentra disponible para cualquier emisor. La clave que se utiliza para descifrar se conoce como *clave privada del receptor* y como su nombre lo dice, esta clave es conocida únicamente por el receptor. En este tipo de criptosistemas, basta con que el o los emisores conozcan la clave pública del receptor para que este reciba los mensajes. Algunos ejemplos de este tipo de criptosistemas son el sistema RSA, ElGamal, Massey-Omura y curvas elípticas.

Otra de las diferencias entre los algoritmos simétricos y los asimétricos es que los asimétricos generalmente emplean longitudes de clave mucho mayores que los simétricos (excepto aquellos basados en curvas elípticas).

El objetivo de este trabajo de tesis es explicar la forma en que las curvas elípticas se utilizan para crear sistemas criptográficos, mostrando la evolución del concepto de curva elíptica desde su origen geométrico hasta su estado actual. Para lograr este objetivo, en el primer capítulo de este trabajo definimos a las curvas elípticas en el plano, analizando las propiedades que satisfacen. Además definimos una operación suma en el conjunto de puntos que forman una curva elíptica. Observando que esta operación junto con el conjunto de puntos de una curva elíptica no forman un grupo, pero es similar.

En el segundo capítulo definimos al plano proyectivo, después damos la definición de curva elíptica sobre este nuevo plano, y de manera similar al primer capítulo definimos un análogo a la operación suma y describimos algunas propiedades. Obteniendo que el conjunto de puntos de una curva elíptica junto con la operación forman un grupo.

Con el objetivo de definir una curva elíptica en un campo finito, en el tercer capítulo damos algunos conceptos y resultados del álgebra. Después describimos la forma de construir más campos finitos además de los enteros módulo un primo.

En el cuarto capítulo, extendemos la definición de una curva elíptica a un campo finito, analizamos las propiedades que satisfacen, y de manera similar extendemos la defincón de la operación suma que se definió en el primer capítulo a los campos finitos.

En el quinto capítulo describimos a los sistemas criptográficos simetricos y asimétricos. Para describir el funcionamiento de algunos sistemas criptográficos definimos a las funciones de un sólo sentido, el logaritmo discreto y el intercambio de claves propuesto por Diffie y Hellman en 1976.

Finalmente en el sexto capítulo describimos el análogo al intercambio de claves con curvas elípticas y la aplicación de las curvas elípticas en los sistemas criptográficos.

Capítulo 1

Curvas elípticas en el plano

En este capítulo introducimos el estudio de las curvas elípticas en el campo de los números reales, algunas características y propiedades que satisfacen. Observando que las características dependen del campo en que se definen.

Definición. Sean a_1, a_2, a_3, a_4 y a_6 elementos de $\mathbb{R}$. Una *curva elíptica general sobre* $\mathbb{R}$ es el conjunto de puntos $(x, y) \in \mathbb{R} \times \mathbb{R}$ que satisfacen la *ecuación de Weierstrass*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

Esta ecuación puede transformarse en una de la forma $y^2 = x^3 + ax + b$ mediante el siguiente procedimiento. Primero realizamos la siguiente transformación $y = y - \frac{1}{2}(a_1x + a_3)$. Sustituimos y desarrollamos

$$\begin{aligned} y^2 &= x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{4}(a_1x + a_3)^2 \\ &= x^3 + \left(a_2 + \frac{1}{4}a_1^2\right)x^2 + \left(\frac{1}{2}a_1a_3 + a_4\right)x + \left(a_6 + \frac{1}{4}a_3^2\right). \end{aligned}$$

De donde podemos observar que se tiene una ecuación de la forma

$$y^2 = x^3 + A_2x^2 + A_4x + A_6. \tag{1.2}$$

Por último, realizamos la siguiente transformación $x = x - \frac{1}{3}A_2$. Luego

$$\begin{aligned} y^2 &= \left(x - \frac{1}{3}A_2\right)^3 + A_2\left(x - \frac{1}{3}A_2\right)^2 + A_4\left(x - \frac{1}{3}A_2\right) + A_6, \\ &= x^3 + \frac{1}{3}(A_2^2 - \frac{2}{3}A_2 + A_4)x + \frac{2}{3^3}A_2^3 - \frac{1}{3}A_2A_4 + A_6. \end{aligned}$$

Teorema 1.1. *Sea* $\mathbb{R}$ *el campo de los números reales. Una* curva elíptica $\mathcal{E}$ sobre $\mathbb{R}$ *es el conjunto de puntos* (x, y) *con* $x, y \in \mathbb{R}$ *que satisfacen una ecuación de la forma*

$$y^2 = x^3 + ax + b. \tag{1.3}$$

De la ecuación (1.3) se observa que si (x, y) está en la curva, $(x, -y)$ también lo está. De aquí en adelante trabajaremos con ecuaciones de la forma como en (1.3).

Ejemplo 1.1. Consideremos la curva $y^2 = x^3 - 5x + 3$. Gráficando se tiene la siguiente figura.

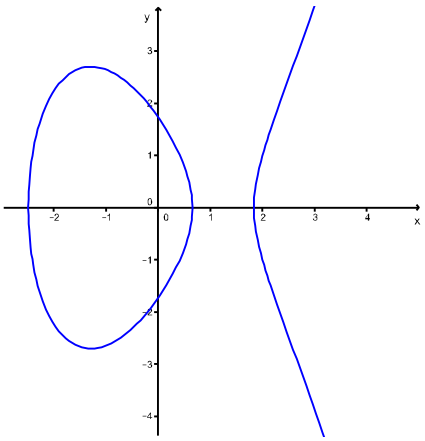


Figura 1.1: Curva elíptica cuya ecuación es $y^2 = x^3 - 5x + 3$.

Ejemplo 1.2. Consideremos la curva cuya ecuación está dada por $y^2 = x^3 - 3x + 2$.

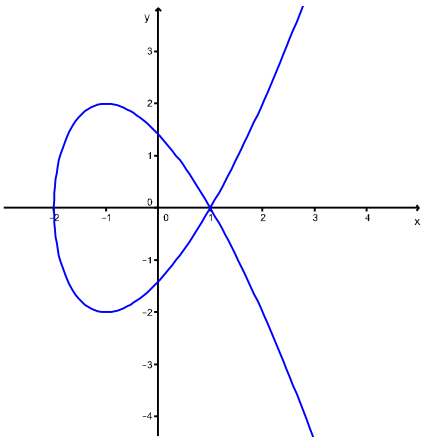


Figura 1.2: Curva elíptica cuya ecuación es $y^2 = x^3 - 3x + 2$.

Para poder introducir otras definiciones que nos ayuden a clasificar a las curvas elípticas, consideremos la ecuación implícita $F(x,y)=0$ para y en función de x en (1.3) como:

$$F(x,y)=y^2-x^3-ax-b=0. \tag{1.4}$$

Definición. Dado un punto (x,y) en una curva elíptica $\mathcal{E}$, se dice que (x,y) es un punto *no singular* de $\mathcal{E}$, si al menos una de las derivadas parciales $\partial F/\partial x$, $\partial F/\partial y$ no se anula en (x,y). Cuando ambas se anulan, (x,y) es un punto *singular* de $\mathcal{E}$.

Definición. Una curva elíptica $\mathcal{E}$ es *no singular* si todos sus puntos son no singulares, y se dice que es *singular* si contiene un punto singular.

Ahora veamos qué condiciones se deben imponer a los coeficientes de la ecuación de una curva elíptica que tiene la forma como en la ecuación (1.3) para que sea singular.
Sea (x,y) un punto singular en la curva elíptica $\mathcal{E}$, entonces $\frac{\partial F}{\partial x}(x,y)=0$ y $\frac{\partial F}{\partial y}(x,y)=0$, luego

$$\frac{\partial F}{\partial x}=-3x^2-a, \quad \frac{\partial F}{\partial y}=2y,$$

entonces

$$-3x^2-a=0, \quad 2y=0. \tag{1.5}$$

Así, se obtiene que

$$x=\pm(-a/3)^{1/2} \qquad y=0 \tag{1.6}$$

Esto muestra que la curva tiene a lo más dos puntos singulares si $a<0$. Si $a>0$, la curva no tiene puntos singulares. Sustituimos (1.6) en la ecuación (1.4),

$$\frac{a}{3}x-ax-b=0, \tag{1.7}$$

de las ecuaciones (1.5) y (1.7) obtenemos $9b^2/4a^2=-a/3$ o bien

$$27b^2+4a^3=0 \tag{1.8}$$

Por tanto, si los coeficientes satisfacen la relación (1.8) y $a>0$ se tiene un único punto singular.

Ahora supongamos que los coeficientes de una curva elíptica cumplen que $\frac{a}{3}x-ax-b=0$ y que el punto $(x,0)$ satisface la ecuación implícita (1.4). Derivamos implícitamente (1.4), se tiene que

$$\frac{\partial F}{\partial x}=-3x^2-a, \quad \frac{\partial F}{\partial y}=2y,$$

tenemos que en el punto $(x, 0)$, $\frac{\partial F}{\partial y} = 2y = 0$. Por otro lado

$$\frac{\partial F}{\partial x} = -3x^2 - a = -3\left(\frac{9b^2}{4a^2}\right) - a = -3\left(\frac{-a}{3}\right) - a = a - a = 0.$$

Tenemos que ambas derivadas parciales se anulan, por tanto se tiene que la curva tiene un punto singular.

Teorema 1.2. *Una curva elíptica $\mathcal{E}$ es no singular si y sólo si sus coeficientes satisfacen la relación* $27b^2 + 4a^3 \neq 0$.

A la cantidad $27b^2 + 4a^3$ se le conoce como *discriminante del polinomio cúbico.*
Para ilustrar lo anterior, notemos que la curva del ejemplo (1.2) está descrita por la ecuación $y^2 = x^3 - 3x + 2$. En este caso, $a = -3$ y $b = 2$, los cuales cumplen que $27(2)^2 + 4(-3)^3 = 0$, por tanto la curva es singular, donde el punto singular es (1,0). De manera geométrica se tienen dos rectas tangentes en este punto dadas por las ecuaciones $y = \sqrt{3}(x-1)$ y $y = -\sqrt{3}(x-1)$, las cuales intersecan a la curva únicamente en el punto $(1, 0)$.

Por otro lado, se tiene que la curva del ejemplo (1.1) descrita por la ecuación $y^2 = x^3 - 5x + 3$ es no singular. Puesto que, $a = -5$, $b = 3$ y $-257 = 27(3)^2 + 4(-5)^3 \neq 0$.

Nota. En este trabajo, nos enfocaremos al estudio de curvas elípticas no singulares.

1.1. Operación en la curva

De la sección anterior, se tiene que una curva elíptica es un conjunto de puntos de la forma (x, y) que satisfacen la ecuación (1.3). Sobre este conjunto se puede definir una operación binaria mediante el método conocido como *el método de la cuerda y la tangente.* El método de la cuerda y la tangente consiste en tomar dos puntos en una curva elíptica, considerar la recta que pasa por ellos y determinar el tercer punto de intersección. Si ambos puntos coinciden, entonces se considera la recta tangente al punto para calcular el otro punto de intersección de la recta con la curva.

En otras palabras, sean P y Q dos puntos diferentes en la curva elíptica $\mathcal{E}$ con coordenadas (x_1, y_1), (x_2, y_2), respectivamente, con P y Q puntos que no se encuentran en la misma recta vertical, esto es, cumplen que $x_1 \neq x_2$. Consideremos $\mathcal{L}$ como la recta que pasa por los puntos

P y Q. Pongamos R con coordenadas, digamos, (x_3, y_3) de tal manera que éste sea un punto de intersección de $\mathcal{L}$ con $\mathcal{E}$.

Supongamos que la ecuación de $\mathcal{L}$ tiene la forma $y = \alpha x + \beta$, y consideremos la ecuación de la recta que pasa por dos puntos,

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1),$$

$$y = \frac{y_2 - y_1}{x_2 - x_1}x - \frac{y_2 - y_1}{x_2 - x_1}x_1 + y_1.$$

Así, se tiene

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}, \quad \beta = y_1 - \alpha x_1.$$

De aquí, un punto (x, y) de la recta $\mathcal{L}$, esto es, un punto de la forma $(x, \alpha x + \beta)$ está en la curva $\mathcal{E}$ si y sólo si satisface la ecuación (1.3), es decir,

$$(\alpha x + \beta)^2 = x^3 + ax + b. \tag{1.9}$$

Desarrollamos

$$\begin{aligned} \alpha^2 x^2 + 2\alpha\beta x + \beta^2 &= x^3 + ax + b, \\ x^3 + ax + b - \alpha^2 x^2 - 2\alpha\beta x - \beta^2 &= 0, \\ x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 &= 0. \end{aligned} \tag{1.10}$$

Observemos que para cada raíz de la ecuación (1.10) se tiene un punto de intersección de $\mathcal{L}$ con $\mathcal{E}$.

Dado que la suma de las raíces de un polinomio mónico es el negativo del coeficiente de la segunda potencia más alta, tenemos que x_3 está dada de la forma $x_3 = \alpha^2 - x_1 - x_2$, puesto que x_1 y x_2 son raíces de la ecuación (1.10).
De aquí que, $y_3 = y_1 + \alpha(x_3 - x_1)$. Por tanto,

$$(x_3, y_3) = (\alpha^2 - x_1 - x_2,\ y_1 + \alpha(x_3 - x_1)). \tag{1.11}$$

Hacemos un desarrollo similar para el caso en que $P = Q$. Para ello, consideremos la recta tangente a la curva en P cuya pendiente α está dada por dy/dx. Derivando implícitamente la

ecuación (1.3) se tiene

$$2y\frac{dy}{dx} = 3x^2 + a,$$

o bien

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y},$$

evaluando en P se tiene que

$$\frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}. \tag{1.12}$$

Observemos que x_1 es una raíz de multiplicidad 2 de la ecuación $y^2 - x^3 - ax - b = 0$. Por lo tanto, el otro punto de intersección tiene la forma

$$(x_3, y_3) = \left(\left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1,\ y_1 + \frac{3x_1^2 + a}{2y_1}(x_3 - x_1) \right) \tag{1.13}$$

Podemos observar que se requiere que la curva sea no singular, ya que si suponemos lo contrario, entonces esta misma tiene un punto singular. Sea $P = (x_0, y_0)$ este punto singular y es tal que satisface la ecuación implícita de la ecuación (1.3), esto es, satisface

$$F(x, y) = y^2 - x^3 - ax - b = 0$$

además satisface que

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

La expansión en serie de Taylor está dada por

$$F(x,\ y) - F(x_0,\ y_0) = -3x_0(x - x_0)^2 + (y - y_0)^2 - (x - x_0)^3$$

la parte derecha de la ecuación previa se puede escribir de la forma

$$((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3$$

por tanto, se tiene la ecuación

$$F(x,\ y) - F(x_0,\ y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3 \tag{1.14}$$

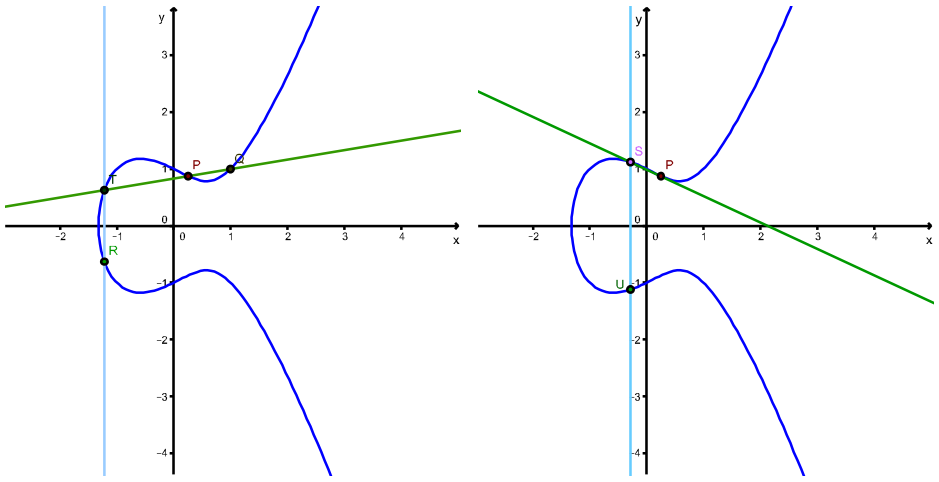
Definición. Con la notación como en (1.14), el punto singular P es un *nodo* si $\alpha \neq \beta$. En este caso, las rectas tangentes en P son $y - y_0 = \alpha(x - x_0)$ y $y - y_0 = \beta(x - x_0)$. De manera inversa, si $\alpha = \beta$, entonces decimos que P es una cúspide, en tal caso la recta tangente en P está dada por $y - y_0 = \alpha(x - x_0)$.

Así geométricamente se tiene una curva con un nodo o una cúspide, cuyas rectas tangentes no intersecan a la curva más que en el punto singular. Por lo tanto, cuando se tiene una curva singular y se desea obtener la suma del punto consigo mismo, no es posible definirlo. Es por ello que se pide que la curva sea no singular. Con lo anterior, pasamos a definir una operación suma, $\oplus$, en una curva elíptica como sigue.

Definición. Sean P y Q dos puntos en una curva elíptica no singular $\mathcal{E}$ con coordenadas (x_1, y_1) y (x_2, y_2), respectivamente. Definimos y escribimos la *suma de P y Q* como $P \oplus Q = R$, donde R tiene como coordenadas $(x_3, -y_3)$, con x_3, y_3 definidos como

$$\begin{cases} x_3 = \alpha^2 - x_1 - x_2, & \text{si } x_1 \neq x_2 \\ y_3 = y_1 + \alpha(x_3 - x_1) & \\ & \\ x_3 = \alpha^2 - 2x_1, & \text{si } P = Q \\ y_3 = y_1 + \alpha(x_3 - x_1) & \end{cases} \quad \text{donde} \quad \begin{cases} \alpha = \frac{y_2 - y_1}{x_2 - x_1}, & \text{si } x_1 \neq x_2 \\ & \\ \alpha = \frac{3x_1^2 + a}{2y_1}, & \text{si } P = Q \end{cases}$$

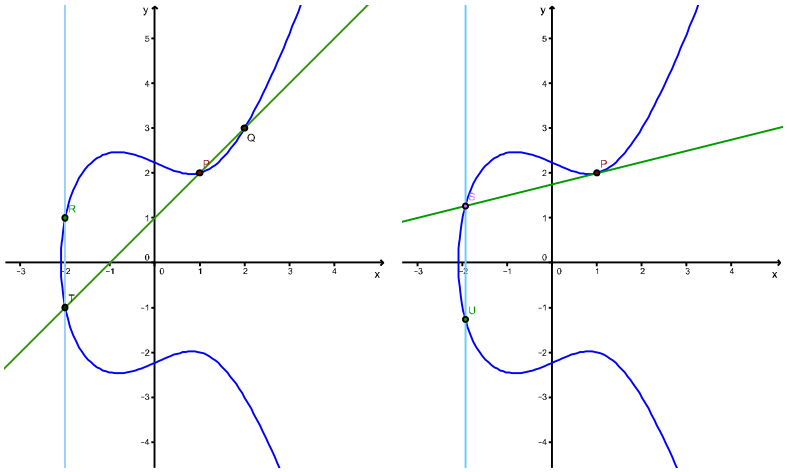
Ejemplo 1.3. En la figura (1.3) se tiene una curva elíptica cuya ecuación es $y^2 = x^3 - x + 1$ y en esta curva consideremos los puntos $P = (1/4, 7/8)$ y $Q = (1, 1)$. En el inciso (a), tenemos la suma de P y Q, donde $R = P \oplus Q$, con coordenadas $(-11/9, -77/108)$. En el inciso (b), observamos la suma de P consigo mismo, donde $U = 2P$, con coordenadas $(-233/784, -24655/21952)$.



(a) Suma de P y Q. (b) Suma de P consigo mismo.

Figura 1.3: Ejemplo de la operación $\oplus$ en una curva elíptica cuya ecuación es $y^2 = x^3 - x + 1$.

Ejemplo 1.4. En la figura (1.4) tenemos una curva elíptica cuya ecuación es $y^2 = x^3 - 2x + 5$. En esta curva consideremos los puntos $P = (1, 2)$ y $Q = (2, 3)$. En el inciso (a), observamos la suma de P y Q, donde $R = P \oplus Q$, con coordenadas $(-2, 1)$. En el inciso (b), tenemos la suma de P consigo mismo, donde $U = 2P$, con coordenadas $(-31/16, -81/64)$.



(a) Suma P y Q. (b) Suma de P consigo mismo.

Figura 1.4: Ejemplo de la operación $\oplus$ en una curva elíptica cuya ecuación es $y^2 = x^3 - 2x + 5$.

1.2. Propiedades de la operación

Ahora que ya tenemos definida la operación $\oplus$ en una curva elíptica, deseamos conocer qué propiedades cumple, para esto, realizamos lo siguiente.

Dados dos puntos $P = (x_1, y_1), Q = (x_2, y_2)$ en una curva elíptica $\mathcal{E}$, nos podemos preguntar qué sucede si fijamos el punto $P = (x_1, y_1)$ y hacemos tender el punto $Q = (x_2, y_2)$ al infinito, esto es, hacemos que x_2 tienda al infinito y calculamos el límite de x_3 y de y_3. Observemos que,

si $Q \in \mathcal{E}$, entonces y_2 tiene la forma $y_2 = \sqrt{x_2^3 + ax_2 + b}$. Esto es,

$$\begin{aligned}
\lim_{x_2 \to \infty} x_3 &= \lim_{x_2 \to \infty} \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \right) \\
&= \lim_{x_2 \to \infty} \left(\left(\frac{\sqrt{x_2^3 + ax_2 + b} - y_1}{x_2 - x_1} \right)^2 - (x_1 + x_2) \right) \\
&= \lim_{x_2 \to \infty} \left(\frac{(\sqrt{x_2^3 + ax_2 + b} - y_1)^2 - (x_1 + x_2)(x_2 - x_1)^2}{(x_2 - x_1)^2} \right) \\
&= \lim_{x_2 \to \infty} \left(\frac{ax_2 + b - 2y_1\sqrt{x_2^3 + ax_2 + b} + y_1^2 + x_1^2 x_2 + x_1 x_2^2 - x_1^3}{x_2^2 - 2x_1 x_2 + x_1^2} \right) \\
&= x_1.
\end{aligned}$$

Para y_3 se tiene

$$\begin{aligned}
\lim_{x_2 \to \infty} y_3 &= \lim_{x_2 \to \infty} (y_1 + \alpha(x_3 - x_1)) \\
&= \lim_{x_2 \to \infty} (y_1) + \alpha \lim_{x_2 \to \infty} (x_3 - x_1) \\
&= y_1.
\end{aligned} \tag{1.15}$$

Por lo tanto, $(x_3, y_3) \to (x_1, y_1)$ cuando $x_2 \to \infty$. De aquí, se tiene que

$$\lim_{x_2 \to \infty} ((x_1, y_1) \oplus (x_2, y_2)) = (x_1, y_1). \tag{1.16}$$

De la ecuación anterior se puede observar que la idea de que el segundo punto se aleje del primero, nos da la noción de la existencia del neutro para la suma en una curva elíptica $\mathcal{E}$.

Por otro lado, si $Q = (x_2, -y_2)$ y hacemos que x_2 tienda a x_1, calculando el límite de x_3 cuando x_2 tiende a x_1, tenemos que

$$\begin{aligned}
\lim_{x_2 \to x_1} x_3 &= \lim_{x_2 \to x_1} \left(\left(\frac{-y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \right) \\
&= \lim_{x_2 \to x_1} \left(\left(\frac{-\sqrt{x_2^3 + ax_2 + b} - y_1}{x_2 - x_1} \right)^2 - (x_1 + x_2) \right) \\
&= \lim_{x_2 \to x_1} \left(\frac{\sqrt{x_2^3 + ax_2 + b} + \sqrt{x_1^3 + ax_1 + b}}{x_2 - x_1} \right)^2 - 2x_1 \\
&= \infty
\end{aligned}$$

De aquí, $y_3 \to \infty$. Por lo tanto, $\lim_{x_2 \to x_1}(P \oplus Q) = \infty$. De manera similar, esta propiedad nos da la idea de la existencia de inverso aditivo.

Para mostrar que se satisface la asociatividad, realizar la prueba de manera análitica se hace tedioso, por ello lo haremos de manera gráfica. Trabajamos con una curva cuya ecuación es $y^2 = x^3 - 2x + 5$.
En la siguiente figura se muestra la suma $(P \oplus Q) \oplus R$, donde $T1$ es la suma de P y Q, mientras que $T22$ es la suma de $P \oplus Q$ con R.

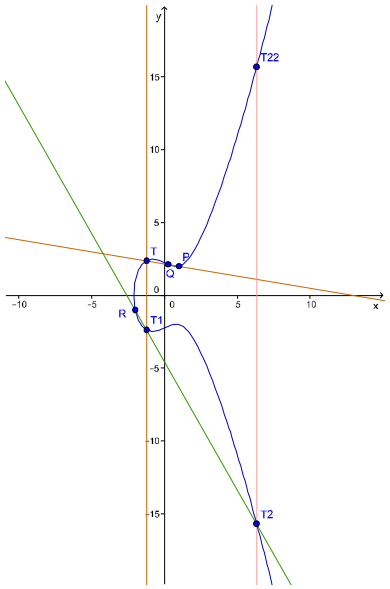


Figura 1.5: Asociatividad de la suma $(P \oplus Q) \oplus R$.

Por otro lado, la siguiente figura muestra la suma $P \oplus (Q \oplus R)$, donde $S1$ es la suma de Q con R y $S22$ es la suma de P con $Q \oplus R$.

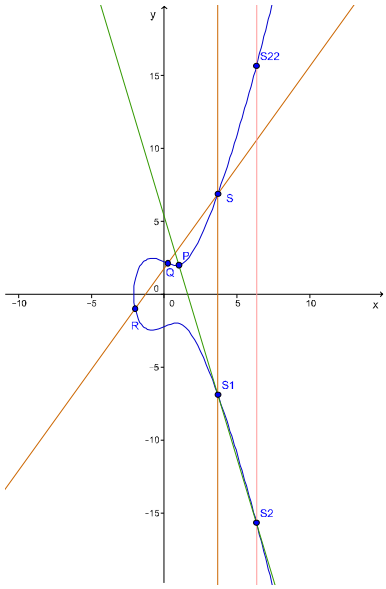


Figura 1.6: Asociatividad de la suma $P \oplus (Q \oplus R)$.

En las dos figuras previas las coordenadas de los puntos con los que se trabajaron son $P = (1, 2)$, $Q = (1/4, 17/8)$ y $R = (-2, -1)$. Realizando los cálculos se obtiene que $T22$ y $S22$ tienen las mismas coordenadas, esto es, $(310/49, 5375/343)$. Las propiedades anteriores se resumen en la siguiente proposición, donde ∞ representa el punto (∞, ∞).

Proposición 1. *Sean P, Q y R puntos de una curva elíptica $\mathcal{E}$. Se cumple que*

- $P \oplus Q = Q \oplus P$,
- $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$,
- $\lim_{Q \to \infty} P \oplus Q = P$,
- $\lim_{Q \to P} P \oplus Q = \infty$.

Con esta última propiedad podemos observar que en cuanto uno de los puntos se acerca lo suficientemente al opuesto del otro, la suma tiende al infinito. Por tanto, cuando ambos puntos se encuentran en la misma vertical, no se puede definir la suma, es por ello que en el siguiente capítulo estudiamos al plano proyectivo y las curvas elípticas sobre este mismo.

Capítulo 2

Curvas elípticas en el plano proyectivo

Considerando el conjunto de puntos de una curva elíptica junto con la operación suma, $\oplus$, estudiados en el capítulo previo, nos ha llevado a cuestionarnos si es que se puede, cómo definir un elemento neutro y, consecuentemente, un inverso aditivo de los elementos de este conjunto. Para ello en este capítulo nos enfocamos a definir y estudiar al plano proyectivo. Después, introducimos una definición similar a una curva elíptica y a la operación suma.

2.1. Plano proyectivo

El problema de representar figuras tridimensionales en el plano, ha interesado mucho tiempo a matemáticos, así como a pintores.

A comienzos del siglo XV en Italia comenzó un conocimiento de la geometría proyectiva, de la óptica y de la visión en sí misma, a lo que se llamó perspectiva natural. Alberto Durero quien ha sido el artista más reconocido y estudiado del Renacimiento alemán, pasó sus últimos siete años de vida trabajando en Nüremberg, donde pintó, entre otras muchas cosas, dos célebres retablos que regaló al Ayuntamiento de la ciudad, publicó los libros de geometría y perspectiva; y escribió una notable obra sobre proporciones humanas que apareció un año después de su muerte.

La *geometría proyectiva* es una rama de la geometría que trata las propiedades que se conservan bajo proyecciones. Tiene aplicaciones en visión artificial, funcionamiento de cámaras, reconstrucción de imágenes bidimensionales en tres dimensiones, etc. Podemos decir que es la geometría que está asociada al modo en que el ojo humano puede percibir el mundo. Esta geometría tiene sus orígenes en la época del Renacimiento, cuando los pintores observaron que tenían que comprender cómo se pueden representar escenas tridimensionales en lienzos que son bidimensionales.

Por ejemplo, pensemos en dibujar los dos rieles de una vía de tren. Podemos notar que a la vista del ojo humano, en el horizonte parece que los dos rieles se juntan en un sólo punto. A este punto llamaremos *punto al infinito*. Observemos que, para realizar el dibujo de esta escena en un lienzo o en el plano se está realizando una proyección al plano. Esto es, lo que el artista pinta es el resultado de proyectar este objeto o escena que se encuentra en tres dimensiones, sobre el plano o lienzo utilizando una fuente de luz que en este caso es el ojo, como se observa en la siguiente figura.

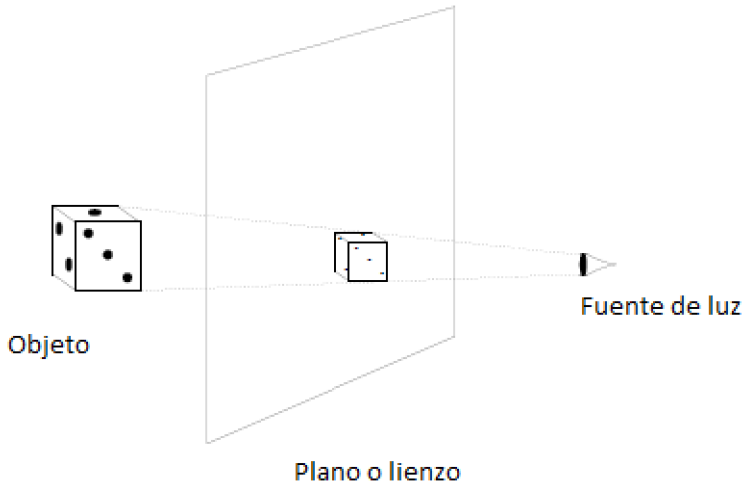


Figura 2.1: Idea del plano proyectivo

Para formalizar esta idea, consideremos la fuente de luz como el origen en $\mathbb{R}^3$; los rayos de luz como las rectas que pasan por el objeto en tres dimensiones, por el lienzo y por el origen. Notemos que este conjunto de rectas cumplen las siguientes propiedades

- Hallaremos al menos cuatro puntos en el espacio, de los cuales tres no se encuentran en la misma recta.
- Para cada par de puntos que tomemos en el espacio, siempre hallaremos una única recta que pasa por ellos.
- Cada par de rectas, se intersecan en un punto.

Observemos que el punto de intersección que indica esta última propiedad es el origen, o bien la fuente de luz. Estas tres últimas propiedades, son las que definen al plano proyectivo.

Consideremos el conjunto $\mathbb{R}^3 \setminus \{(0,0,0)\}$ y definamos la relación

$$(X_1, Y_1, Z_1) \sim (X, Y, Z) \text{ si y sólo si } (X_1, Y_1, Z_1) = t(X, Y, Z) \text{ con } t \in \mathbb{R} \setminus \{0\} \tag{2.1}$$

Proposición 2. *La relación definida en* (2.1) *es de equivalencia.*

Demostración. Sean (X_1, Y_1, Z_1), (X_2, Y_2, Z_2) y (X_3, Y_3, Z_3) elementos de $\mathbb{R}^3 \setminus \{(0,0,0)\}$.
Reflexividad: El punto (X_1, Y_1, Z_1) está relacionado consigo mismo, basta tomar $t = 1$.
Simetría: Supongamos que $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ entonces existe $t \in \mathbb{R} \setminus \{0\}$, tal que, $(X_1, Y_1, Z_1) = t(X_2, Y_2, Z_2)$, de aquí podemos ver que $(X_2, Y_2, Z_2) = \frac{1}{t}(X_1, Y_1, Z_1)$, así se tiene que $(X_2, Y_2, Z_2) \sim (X_1, Y_1, Z_1)$.
Transitividad: Supongamos que $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ y que $(X_2, Y_2, Z_2) \sim (X_3, Y_3, Z_3)$, entonces existen $t_1, t_2 \in \mathbb{R} \setminus \{0\}$ tal que $(X_1, Y_1, Z_1) = t_1(X_2, Y_2, Z_2)$ y $(X_2, Y_2, Z_2) = t_2(X_3, Y_3, Z_3)$. Como $t_1 \neq 0$ y $t_2 \neq 0$, se tiene que $t_1 t_2 \neq 0$, por tanto $(X_1, Y_1, Z_1) = t_1 t_2 (X_3, Y_3, Z_3)$. Así, $(X_1, Y_1, Z_1) \sim (X_3, Y_3, Z_3)$.
Por lo tanto, la relación dada es de equivalencia. □

La relación $\sim$ define clases de equivalencia en $\mathbb{R}^3 \setminus \{(0,0,0)\}$.

Definición. El *plano proyectivo* $\mathbb{P}$ se define como el conjunto de clases de equivalencia en $\mathbb{R}^3$

$$\mathbb{P} = \{[(X, Y, Z)] : (X, Y, Z) \in \mathbb{R}^3 \setminus \{(0,0,0)\}\}.$$

A $[(X,Y,Z)] \in \mathbb{P}$ se le conoce como *punto proyectivo* y está dada por

$$\begin{aligned}[(X,\ Y,\ Z)] &= \{(X_1,Y_1,Z_1) \in \mathbb{R}^3 \setminus \{(0,0,0)\} : (X,\ Y,\ Z) = \lambda(X_1,\ Y_1,\ Z_1),\ \lambda \in \mathbb{R} \setminus \{0\}\} \\ &= \{(X_1,Y_1,Z_1) \in \mathbb{R}^3 \setminus \{(0,0,0)\} : (X_1,\ Y_1,\ Z_1) = \frac{1}{\lambda}(X,\ Y,\ Z),\ \lambda \in \mathbb{R} \setminus \{0\}\}\end{aligned}$$

Observemos que el plano proyectivo se puede visualizar como puntos de la forma $[(X,Y,Z)]$ en los cuales $Z \neq 0$ o bien $Z = 0$.

Sea $[(X,Y,Z)]$ un punto proyectivo. Supongamos $Z \neq 0$, entonces $[(X,Y,Z)] = [(X/Z,\ Y/Z,\ 1)]$. De aquí que $(X,Y,Z) \sim (x,y,1)$, donde

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}. \tag{2.2}$$

Haciendo uso de las transformaciones dadas en (2.2), el espacio se proyecta al plano $Z = 1$, como se ilustra en la siguiente figura.

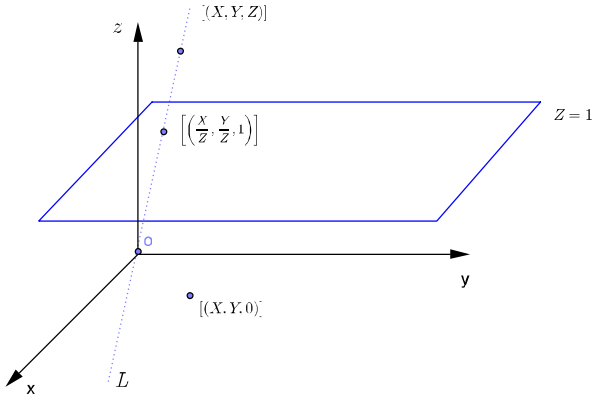


Figura 2.2: Plano proyectivo, $Z = 1$.

Además, definen una biyección entre el conjunto $\{[(X,Y,Z)]\ : (X,Y,Z) \in \mathbb{R}^3 \setminus \{(0,0,0)\}\}$, con $Z \neq 0$ y el conjunto $\{(x,y) : (x,y) \in \mathbb{R}^2\}$, dada de la siguiente manera

$$f : \mathbb{R}^3 \setminus \{(0,0,0)\}/\sim \longrightarrow \mathbb{R}^2$$

$$[(X,Y,Z)] \longmapsto (x,y)$$

Su inversa está dada por

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^3 \setminus \{(0,0,0)\}/\sim$$

$$(x, y) \longmapsto [(X, Y, 1)]$$

Por tanto, el plano proyectivo $\mathbb{P}$ se puede visualizar como los puntos $(x, y) \in \mathbb{R}^2$, donde x, y están dadas como en (2.2), más los puntos en los cuales Z es igual con cero.

2.2. Curvas elípticas

Supongamos que $(X, Y, Z) \sim (X_1, Y_1, Z_1)$ entonces $(X_1, Y_1, Z_1) = t(X, Y, Z) = (tX, tY, tZ)$ con $t \in \mathbb{R} - \{0\}$. Luego, sustituimos las ecuaciones dadas en (2.2) en la ecuación (1.3). De donde se obtiene lo siguiente

$$(Y/Z)^2 - (X/Z)^3 - a\,(X/Z) - b = 0. \tag{2.3}$$

o bien

$$Y^2Z - X^3 - aXZ^2 - bZ^3 = 0 \tag{2.4}$$

A la expresión del lado izquierdo de la igualdad en (2.4) se le conoce como *polinomio proyectivo.* Ahora, sustituimos $(X_1, Y_1, Z_1) = (tX, tY, tZ)$ en el polinomio proyectivo, esto es,

$$P(X_1, Y_1, Z_1) = (tY/tZ)^2 - (tX/tZ)^3 - a\,(tX/tZ) - b = (Y/Z)^2 - (X/Z)^3 - a\,(X/Z) - b = P(X, Y, Z)$$

,

por tanto, $P(X_1, Y_1, Z_1) = P(X, Y, Z)$. De aquí, concluimos que el polinomio proyectivo no depende de los representantes de las clases de puntos del plano proyectivo. Por tanto, los puntos proyectivos que tienen la forma $(X_1/Z_1,\, Y_1/Z_1,\, 1)$ con $Z_1 \neq 0$ también satisfacen que $P(X, Y, Z) = 0$.

Definición. Una *curva elíptica en el plano proyectivo* es el conjunto de puntos proyectivos $[(X, Y, Z)]$ en los cuales se anula el polinomio proyectivo, esto es,

$$\{[(X, Y, Z)] \in \mathbb{P} \ : \ P(X, Y, Z) = 0\},$$

donde $P(X, Y, Z)$ es un polinomio proyectivo.

A continuación definiremos una operación en una curva elíptica del plano proyectivo a partir de la operación definida anteriormente en el plano ordinario. Para esto, consideremos los puntos $(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$ y $(x_2, y_2) = (X_2/Z_2, Y_2/Z_2)$ en el plano, con $Z_1 \neq 0$ y $Z_2 \neq 0$. De las ecuaciones en (1.11) y de (1.13) se obtiene que las coordenadas de la suma, (x_3, y_3), están dadas

como sigue
$\left(\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)^2-\left(\frac{X_1Z_2+X_2Z_1}{Z_1Z_2}\right),\ \frac{Y_1}{Z_1}+\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)\left(\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)^2-\frac{2X_1Z_2+X_2Z_1}{Z_1Z_2}\right)\right)$
y
$\left(\left(\frac{3X_1^2+aZ_1^2}{2Y_1Z_1}\right)^2-2\frac{X_1}{Z_1},\ \frac{Y_1}{Z_1}+\left(\frac{3X_1^2+aZ_1^2}{2Y_1Z_1}\right)\left(\left(\frac{3X_1^2+aZ_1^2}{2Y_1Z_1}\right)^2-2\frac{X_1}{Z_1}\right)\right),$
respectivamente.

Así, tenemos que para los puntos $(X_1,\ Y_1,\ Z_1)$ y $(X_2,\ Y_2,\ Z_2)$ de una curva elíptica en el plano proyectivo, con $Z_1 \neq 0$ y $Z_2 \neq 0$, se puede definir una operación suma, basandonos en la operación suma definida en el capítulo anterior. Por tanto, la suma lo escribimos como $[(X_1/Z_1,\ Y_1/Z_2,\ 1)] \oplus [(X_2/Z_2,\ Y_2/Z_2,\ 1)]$ definida de la siguiente manera

- Si $X_1Z_2 \neq X_2Z_1$
  $\left[\left(\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)^2-\left(\frac{X_1Z_2+X_2Z_1}{Z_1Z_2}\right),\ -\frac{Y_1}{Z_1}-\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)\left(\left(\frac{Y_2Z_1-Y_1Z_2}{X_2Z_1-X_1Z_2}\right)^2-\frac{2X_1Z_2+X_2Z_1}{Z_1Z_2}\right),\ 1\right)\right]$
- Si $X_1Z_2 = X_2Z_1$ y $Y_1Z_2 = Y_2Z_1$
  $\left[\left(\left(\frac{3X_1^2+aZ_1^2}{2Y_1Z_1}\right)^2-2\frac{X_1}{Z_1},\ -\frac{Y_1}{Z_1}-\left(\frac{3X_1^2+aZ_1^2}{2Y_1Z_1}\right)\left(\left(\frac{3X_1^2+aZ_1^2}{2Y_1Z_1}\right)^2-\frac{2X_1}{Z_1}\right),\ 1\right)\right].$

Para obtener una expresión de manera general, multipliquemos cada una de las entradas por $Z_1Z_2(X_2Z_1 - X_1Z_2)^3$. Realizando manipulaciones algebraicas, se obtiene que $[(X_1, Y_1, Z_1)] \oplus [(X_2, Y_2, Z_2)] = [(X_3, Y_3,\ Z_3)]$, con $X_3,\ Y_3,$ y $\ Z_3$ como sigue

$$X_3 = (X_2Z_1 - X_1Z_2)\left(Z_1Z_2(Y_2Z_1 - Y_1Z_2)^2 - (X_2Z_1 + X_1Z_2)(X_2Z_1 - X_1Z_2)^2\right), \quad (2.5)$$

$$Y_3 = -Y_1Z_2(X_2Z_1 - X_1Z_2)^3 + X_1Z_2(Y_2Z_1 - Y_1Z_2)(X_2Z_1 - X_1Z_2)^2$$
$$-(Y_2Z_1 - Y_1Z_2)\left(Z_1Z_2(Y_2Z_1 - Y_1Z_2)^2 - (X_2Z_1 + X_1Z_2)(X_2Z_1 - X_1Z_2)^2\right), \quad (2.6)$$

$$Z_3 = Z_1Z_2(X_2Z_1 - X_1Z_2)^3. \quad (2.7)$$

Teorema 2.1. *Sean $P_1 = [(X_1, Y_1, Z_1)]$ y $P_2 = [(X_2, Y_2, Z_2)]$ puntos proyectivos. Entonces las coordenadas de $P_1 \oplus P_2$ están dadas como en las ecuaciones* (2.5)-(2.7).

2.3. Punto al infinito

En la sección previa, realizamos un análisis para los puntos proyectivos $[(X, Y, Z)]$ donde $Z \neq 0$. Ahora supongamos que $Z = 0$. Al sustituir en la ecuación (2.4) se tiene que $X^3 = 0$, esto es, $X = 0$, como $[(X, Y, Z)] \in \mathbb{P}$, entonces $[(X, Y, Z)] = [(0, 1, 0)]$, puesto que es el único punto en

$\mathbb{P}$ que satisface que $X = 0$ y $Z = 0$. A este punto lo llamaremos el *punto al infinito* y escribiremos $\mathcal{O}$ para hacer referencia a este punto. Notemos que el punto al infinito es la proyección de los puntos que se encuentran en el plano $Z = 0$.

En adelante describiremos la importancia de definir el punto al infinito, para ello pensemos en cómo se define el negativo de un punto en una curva elíptica. Consideremos un punto $P = (x_0, y_0)$ en una curva elíptica y tomemos la recta que pasa por el punto P y el punto al infinito $\mathcal{O}$, esto es,

$$L : x - x_0 = 0$$

sustituimos ésta en la ecuación (1.3)

$$\begin{aligned} f(x_0, y) &= y^2 - x_0^3 - ax_0 - b \\ &= y^2 - y_0^2 \end{aligned} \tag{2.8}$$

de aquí podemos notar que $f(x_0, y)$ tiene dos raíces. Hacemos $-P = (x_0, y_0^{'})$. Luego, se tiene que $y_0^{'} = -y_0$. De esta manera obtenemos que el negativo de P está definido como $-P = (x_0, -y_0)$, esto es, el negativo de un punto en una curva elíptica, se obtiene cambiando de signo la segunda entrada del mismo.

Retomando las fórmulas dadas en (2.5)-(2.7) para la suma de dos puntos proyectivos en los cuales $Z \neq 0$, y sumando $P = [(X, Y, Z)]$ con su negativo, se tiene que $X_3 = 0$, $Y_3 = (2YZ)^3Z^2$ y $Z_3 = 0$. Así, se tiene que $[(X, Y, Z)] \oplus [(X, -Y, Z)] = [(0, (2YZ)^3Z^2, 0)] = [(0, 1, 0)]$ con la restricción de que $Y \neq 0$.
Por tanto, tenemos que

$$P \oplus (-P) = \mathcal{O}$$

De esta manera, definimos el punto al infinito $\mathcal{O}$ como el neutro aditivo. Como consecuencia tenemos que

$$\mathcal{O} \oplus P = P = P \oplus \mathcal{O}$$

Con estas dos últimas propiedades y las dos primeras propiedades de la proposición (1) se tiene que *el conjunto de puntos que forman una curva elíptica junto con el punto al infinito y la operación binaria* $\oplus$ *definen un grupo abeliano.*

Capítulo 3

Campos finitos

En los capítulos anteriores hemos estudiado a las curvas elípticas en el plano y en el plano proyectivo. Notemos que en ambos casos, se construyen usando números reales. Dado que muchas de estas construcciones sólo depende de las operaciones + y $\cdot$ en $\mathbb{R}$, se puede tratar de generalizar usando otro tipo de objetos.
En este capítulo se mostrará cómo construir estructuras algebraicas similares a $\mathbb{R}$ pero con un número finito de elementos. A partir de esto, surge la interrogativa acerca de cómo se definen las curvas elípticas en campos finitos, si es que se puede definir.

3.1. Preliminares

Las operaciones en $\mathbb{R}$ satisfacen las siguientes propiedades

C1: Para $a, b \in \mathbb{R}$ se cumple que $a + b \in \mathbb{R}$.

C2: Para $a, b \in \mathbb{R}$, $a + b = b + a$.

C3: Para $a, b, c \in \mathbb{R}$ se cumple que $(a + b) + c = a + (b + c)$.

C4: Existe un elemento $0 \in \mathbb{R}$ que cumple que $a + 0 = 0 + a = a$, para todo $a \in \mathbb{R}$.

C5: Para cada $a \in \mathbb{R}$ existe $-a \in \mathbb{R}$ tal que $a + (-a) = (-a) + a = 0$.

C6: Para $a, b \in \mathbb{R}$ se cumple que $a \cdot b \in \mathbb{R}$.

C7: Para $a, b \in \mathbb{R}$ se cumple que $a \cdot b = b \cdot a$.

C8: Para $a, b, c \in \mathbb{R}$ se cumple que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

C9: Existe un elemento $1 \in \mathbb{R}$ que cumple que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in \mathbb{R}$.

C10: Para cada $a \in \mathbb{R}$ distinto de 0, existe $a^{-1} \in \mathbb{R}$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

C11: Para cualesquiera $a, b, c \in \mathbb{R}$ se cumple que $a \cdot (b + c) = a \cdot b + a \cdot c$.

Existen otros conjuntos como los números racionales, $\mathbb{Q}$, y los números complejos $\mathbb{C}$, que de manera similar a $\mathbb{R}$ satisfacen las propiedades algebraicas previas.
Las propiedades de las curvas elípticas de los capítulos previos sólo dependen de estas propiedades algebraicas. En la siguiente sección se muestra cómo construir un conjunto finito con las operaciones + y $\cdot$ que tenga estas propiedades.

3.2. Los enteros módulo n

Hasta ahora hemos mencionado ejemplos de conjuntos infinitos que satisfacen las propiedades algebraicas de la sección previa.
Sabemos que en el conjunto de los números enteros, $\mathbb{Z}$, los únicos que tienen inversos multiplicativos son el 1 y el -1, por tanto, este conjunto no satisface la propiedad algebraica C10 de la sección previa, pero podemos encontrar subconjuntos finitos de $\mathbb{Z}$ que lo cumplan.

Definición. Sean $a,\ b$ números enteros. Se dice que a *divide a* b si existe un entero c, tal que $b = a \cdot c$.

Algunos ejemplos de la definición previa son: 3 divide a 12, 7 divide a 49, puesto que $12 = 3 \cdot 4$ y $49 = 7 \cdot 7$, respectivamente.

Definición. Sean a, b números enteros, se dice que a *es congruente con* b *módulo* n si n divide a $a - b$. Escribimos $a \equiv b \pmod{n}$ para indicar que a es congruente con b módulo n.

Como ejemplos tenemos que $35 \equiv 5 \pmod{6}$, puesto que $35 - 5 = 30 = 6 \cdot 5$; y $70 \equiv 6 \pmod{8}$, de manera similar, $70 - 6 = 64 = 8 \cdot 8$.
Definamos la siguiente relación:

$$a \sim b \ \text{ si y sólo si } a \equiv b \pmod{n} \tag{3.1}$$

Se puede verificar que la relación en (3.1) es de equivalencia. Por tanto, define clases de equivalencia en $\mathbb{Z}$. Escribiremos $[n]$ para referirnos a la clase de equivalencia de n, con n en $\mathbb{Z}$. A n se le conoce como *representante de la clase*.

Definición. Sea n un número natural. Se define el conjunto de los enteros módulo n, como el conjunto

$$\mathbb{Z}_n = \{[m] : \ m \in \mathbb{Z}\} \tag{3.2}$$

Teorema 3.1. *El conjunto de los enteros módulo n, es el conjunto*

$$\mathbb{Z}_n = \{[0],\ [1],\ [2], \ldots,\ [n-1]\}. \tag{3.3}$$

Demostración. Sea $m \in \mathbb{Z}$. Por el algoritmo de la división, existen dos enteros, q y r tales que $m = n\,q + r$, con $0 \leq r < n$. O bien $m - r = n\,q$, esto es, $r \sim m$. Por tanto, $[m] = [r]$, con $0 \leq r < n$. □

Notemos algo importante, si p es primo, para cada $[a] \in \mathbb{Z}_p \setminus \{[0]\}$ se tiene que a y p son primos relativos. Esto es, el máximo común divisor de a y p es 1.

En $\mathbb{Z}_n$ definimos las operaciones suma $(+)$ y producto $(\cdot)$ como sigue

$$[a] + [b] = [a + b], \tag{3.4}$$

$$[a] \cdot [b] = [a \cdot b]. \tag{3.5}$$

Las operaciones están bien definidas, es decir, las operaciones no dependen de los representantes de las clases.

Teorema 3.2. *La terna* $(\mathbb{Z}_n,\ +,\ \cdot)$ *cumple las propiedades* C1-C9 *y* C11.

Demostración. Sean $[a], [b], [c] \in \mathbb{Z}_n \setminus \{[0]\}$. Las propiedades C1, C2, C3, C6, C7 y C8 se obtienen de la definición de la operación y de la definición de $\mathbb{Z}_n$.
El neutro aditivo es la clase del cero, $[0]$ y es tal que $[a] + [0] = [a + 0] = [a]$, por tanto se satisface la propiedad C4. Para C5, esto es, el inverso aditivo $[a]$, supongamos que $[b]$ es tal que $[a] + [b] = [0]$, esto es, $[a + b] = [0]$, esto implica $b = -a$. Por tanto el inverso aditivo de $[a]$ es $[-a]$. Como $-a \equiv n - a \pmod{n}$, entonces se tiene que el inverso aditivo de $[a]$ es $[n - a]$.

El neutro multiplicativo es [1] , puesto que cumple que $[1][a] = [1 \cdot a] = [a \cdot 1] = [a]$, así se tiene la propiedad C9.
Por último probemos la propiedad C11. Luego,
$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a] \cdot [b + c] = [a \cdot (b + c)] = [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c]$.
Por tanto, $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$. Con todo lo anterior, queda probado el resultado. □

Ahora, nos cuestionamos acerca de qué debe cumplir n para que en $\mathbb{Z}_n$ se cumpla C10. Para responder a esta interrogativa tenemos el siguiente teorema.

Teorema 3.3. *Si p es primo, entonces $\mathbb{Z}_p$ se cumple* C10.

Demostración. Supongamos que p es primo. Por el teorema previo, basta probar que se satisface la propidedad C10. Esto es, dado $[a] \in \mathbb{Z}_p \setminus \{[0]\}$ resta probar que existe $[b]$ tal que $[a][b] = [1]$. Como p es primo, se tiene que el máximo común divisor de a y p es 1, esto es, $(a, p) = 1$, entonces existen enteros r, s, tales que $ar + ps = 1$. Así, $[1] = [ar] + [ps] = [a][r] + [p][s] = [a][r]$, por tanto, el inverso multiplicativo de $[a]$ es $[r]$.
Por tanto, se tiene que en $\mathbb{Z}_p$ sa satisface C10. □

Definición. Sea $\mathbb{F}$ un conjunto. Si en $\mathbb{F}$ junto con las operaciones $+$ y $\cdot$ se satisfacen las propiedades algebraicas C1-C11, se dice que $\mathbb{F}$ es un campo.

En estas estructuras de campo se pueden construir curvas elípticas.

3.3. Construcción de campos finitos mediante polinomios

De la sección previa tenemos tantos ejemplos de campos finitos como números primos se tengan. En esta sección veremos otra forma de construir campos finitos.

Definición. Sea $\mathbb{F}$ un campo y n un entero. Un *polinomio con coeficientes en $\mathbb{F}$ y en la variable x* es una expresión de la forma

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

donde $a_1,\ a_2,\ ...,\ a_n \in \mathbb{F}$, con $a_n \neq 0$. A n se le conoce como *el grado del polinomio.*

Escribiremos $\mathbb{F}[x]$ para denotar el conjunto de polinomios con coeficientes en $\mathbb{F}$ y en la variable x. Con $p(x)$, $q(x)$, $h(x)$, ... haremos referencia a los elementos de $\mathbb{F}[x]$. También escribiremos 0 para hacer referencia al polinomio cero.

Las operaciones de suma y producto de polinomios se definen como comúnmente se hace. De manera similar al caso de los números enteros, definimos una congruencia de polinomios.

Definición. Sean $p(x)$, $q(x)$, $h(x)$ elementos de $\mathbb{F}[x]$ con $p(x)$ distinto del polinomio cero. Decimos que $h(x)$ y $q(x)$ son *congruentes módulo* $p(x)$, si existe $r(x)$ en $\mathbb{F}[x]$ tal que $h(x) - q(x) = p(x)\ r(x)$. Escribimos $h(x) \equiv q(x) \bmod p(x)$ para indicar que $h(x)$ y $q(x)$ son congruentes módulo $p(x)$.

Definimos la siguiente relación

$$h(x) \sim q(x) \bmod p(x) \text{ si y sólo si } h(x) \equiv q(x) \bmod p(x) \tag{3.6}$$

La relación definida en (3.6) es de equivalencia. En efecto, sean $p(x)$, $q(x)$ y $h(x)$ elementos de $\mathbb{F}[x]$ con $p(x) \neq 0$. *Reflexividad*: Para $h(x)$, basta tomar $r(x) = 0$.
Simetría: Supongamos que $h(x) \equiv q(x) \bmod p(x)$, entonces existe $r(x)$ tal que $h(x) - q(x) = r(x)\ p(x)$, luego $-(h(x) - q(x)) = -r(x)\ p(x)$, así $q(x) - h(x) = r_1(x)\ p(x)$, donde $r_1(x) = -r(x)$. Por lo tanto, $q(x) \equiv h(x) \bmod p(x)$.
Transitividad: Supongamos que $h(x) \equiv q(x) \bmod p(x)$ y $q(x) \equiv r(x) \bmod p(x)$, entonces existen $r_1(x)$ y $r_2(x)$, tal que $h(x) - q(x) = r_1(x)\ p(x)$, $q(x) - r(x) = r_2(x)\ p(x)$. Por tanto, tenemos que $q(x) = r(x) + r_2(x)\ p(x)$. Así $h(x) = q(x) + r_1(x)\ p(x) = r(x) + r_2(x)\ p(x) + r_1(x)\ p(x)$, entonces $h(x) - r(x) = (r_2(x) + r_1(x))\ p(x)$, por lo tanto $h(x) - r(x) = r_3(x)\ p(x)$, donde $r_3(x) = r_2(x) + r_1(x)$. De aquí, $h(x) \equiv r(x) \bmod p(x)$. Así verificamos que la relación es de equivalencia.

La relación en (3.6) define clases de equivalencia en $\mathbb{F}[x]$. La clase de equivalencia módulo $p(x)$ del polinomio $h(x) \in \mathbb{F}[x]$, consiste de polinomios $r(x) \in \mathbb{F}[x]$ tal que $h(x) - r(x)$ es un múltiplo de $p(x)$ o divisible por $p(x)$. Esto es,

$$\begin{aligned} [h(x)] &= [p(x)q(x) + r(x)], \quad q(x) \in \mathbb{F}[x] \text{ y } r(x) \text{ de grado menor que } n, \\ &= [r(x)]. \end{aligned}$$

Con $\mathbb{F}[x]/(p(x))$ indicamos el conjunto de clases de equivalencia módulo $p(x)$. Es decir,

$$\mathbb{F}[x]/(p(x)) = \{\left[b_0 + b_1 x \cdots + b_{n-1}x^{n-1}\right] : b_i \in \mathbb{F}\},$$

donde los coeficientes $b_0, b_1, \ \ldots, \ b_{n-1}$ son únicos. Dado que los polinomios $q(x)$ y $r(x)$, se hallan mediante el algoritmo de la división, se tiene que los coeficientes $b_0, b_1, \ \ldots, \ b_{n-1}$ son únicos por la unicidad de $r(x)$.

Observemos que si $\mathbb{F}$ es finito entonces $\mathbb{F}[x]/(p(x))$ es finito, además $\mathbb{F}[x]/(p(x))$ tiene m^n elementos, donde m es el número de elementos de $\mathbb{F}$. En efecto, consideremos la función biyectiva, $\Phi : \mathbb{F}^n \longmapsto \mathbb{F}[x]/(p(x))$ definida como sigue

$$(b_0, \ b_1 \ , \ldots, b_{n-1}) \longmapsto [b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}]$$

si $\mathbb{F}$ tiene m elementos, se tiene que $\mathbb{F}^n$ tiene m^n elementos.

De manera análoga a $\mathbb{Z}_n$, en $\mathbb{F}[x]/(p(x))$ definimos las operaciones suma y producto como sigue

$$[h_1(x)] + [h_2(x)] = [h_1(x) + h_2(x)]$$

$$[h_1(x)][h_2(x)] = [h_1(x)h_2(x)]$$

Es decir, la suma de las clases de residuo de h_1 y h_2 módulo $p(x)$ es la clase de residuo de $h_1 + h_2$ módulo $p(x)$; y el producto de las clases de residuo de h_1 y h_2 módulo $p(x)$ es la clase de residuo de $h_1 h_2$ módulo $p(x)$.

Notemos que al igual que la operación suma de polinomios que comúnmente se conoce, se tiene que la suma definida previamente es asociativa y conmutativa. Y similarmente, de la multiplicación común de polinomios se tiene que la operación producto previamente definido cumple con la propiedad asociativa.

El neutro aditivo es la clase de residuo $[p(x)]$, puesto que cumple que para $[h(x)] \in \mathbb{F}[x]/(p(x))$

$$\begin{aligned} [h(x)] + [p(x)] &= [p(x) \ q(x) + r(x)] + [p(x)] \\ &= [p(x) \ q(x) + r(x) + p(x)] \\ &= [p(x) \ (q(x) + 1) + r(x)] \ = \ [h(x)] \end{aligned}$$

El inverso aditivo de la clase de residuo de $[h(x)]$ es la clase de residuo $[p(x)-h(x)]$, puesto que cumple con

$$\begin{aligned}[h(x)]+[p(x)-h(x)] &= [h(x)+(p(x)-h(x))] \\ &= [p(x)]\end{aligned}$$

Por último consideremos $[h(x)]$, $[q(x)]$ y $[r(x)]$ clases de residuos módulo $p(x)$, luego

$$\begin{aligned}[h(x)]\ ([q(x)]+[r(x)]) &= [h(x)][q(x)+r(x)] = [h(x)\ (q(x)+r(x))] \\ &= [h(x)\ q(x)]+[h(x)\ r(x)] = [h(x)]\ [q(x)]+[h(x)][r(x)] \quad (3.7)\end{aligned}$$

Por otro lado se tiene que

$$\begin{aligned}([h(x)]+[q(x)])\ [r(x)] &= [h(x)+q(x)]\ [r(x)] = [(h(x)+q(x))\ r(x)] \\ &= [h(x)\ r(x)]+[q(x)\ r(x)] = [h(x)][r(x)]+[q(x)][r(x)] \quad (3.8)\end{aligned}$$

De (3.7) y (3.8) se tiene la distributividad del producto sobre la suma. De esta manera tenemos que $\mathbb{F}[x]/(p(x))$ junto con la suma, satisfacen las propiedades C1-C5 y C11.

Definición. Un polinomio no constante $f(x) \in \mathbb{F}[x]$ es *irreducible sobre* $\mathbb{F}$ o es un *polinomio irreducible en* $\mathbb{F}[x]$ si $f(x)$ no se puede expresar como producto de dos polinomios $g(x)$ y $h(x)$ en $\mathbb{F}[x]$, ambos de grado menor que el grado de $f(x)$.

El conjunto de clases de equivalencia $\mathbb{F}[x]/(p(x))$ no necesariamente es un campo. Pero, si $p(x)$ es irreducible, del Teorema (A.2) se tiene que $\mathbb{F}[x]/(p(x))$ es campo. Donde el neutro multiplicativo es la clase de residuo $[1]$, o bien, la clase $[1+p(x)q(x)]$. Para hallar el inverso multiplicativo de una clase de residuo $[g(x)]$ con $g(x)$ no cero, aplicamos el análogo al algoritmo de Euclides, para hallar dos polinomios $r(x)$ y $s(x)$ tal que $g(x)\cdot r(x)+p(x)\cdot s(x)=1$ de donde $[g(x)]\ [r(x)]+[p(x)]\ [s(x)]=[1]$. Así, obtenemos que el inverso de $[g(x)]$ es $[r(x)]$.

De esta manera tenemos más ejemplos de campos finitos. Si consideramos $\mathbb{F}$ como $\mathbb{Z}_p$, con p primo, $\mathbb{Z}_p$ es isomorfo a $\mathbb{F}[x]/(p(x))$ y por tanto se puede considerar a $\mathbb{Z}_p$ como un subcampo de $\mathbb{F}[x]/(p(x))$.

Ejemplo 3.1. Consideremos $\mathbb{Z}_2$ y $p(x)=1+x+x^2$. Notemos que $p(x)$ es irreducible sobre $\mathbb{Z}_2[x]$. Los elementos de $\mathbb{Z}_2[x]/(p(x))$ es el conjunto

$$\{[1],\ [x],\ [1+x],\ [p(x)]\} = \{[0],\ [1],\ [x],\ [1+x]\}$$

Observemos que $[1+x]$ es su propio inverso aditivo. Puesto que para hallar el inverso aditivo de $[1+x]$, hacemos lo siguiente

$$[p(x)-(x+1)] = [x^2+x+1-x-1] = [x^2],$$

dividiendo x^2 entre x^2+x+1 obtenemos que $x^2 = (x^2+x+1)(1)+(-x-1)$, con residuo $-x-1$, pero sabemos que $-1 \equiv 1 \pmod 2$, por tanto $[x^2] = [x+1]$.
De manera similar se obtiene que el inverso aditivo de $[x]$ es $[x]$ y el inverso aditivo de $[1]$ es $[1]$. Además notemos que $[1+x]$ y $[x]$ son inversos multiplicativos, puesto que utilizando el similar al algoritmo de Euclides, tenemos que $[x^2+x+1]+[x(x+1)] = [1]$, o bien $[1] = [x][x+1]$.

Lo anterior se resume en las siguientes tablas.

$+$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[0]$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[1]$	$[1]$	$[0]$	$[1+x]$	$[x]$
$[x]$	$[x]$	$[1+x]$	$[0]$	$[1]$
$[1+x]$	$[1+x]$	$[x]$	$[1]$	$[0]$

Cuadro 3.1: Suma de elementos de $\mathbb{Z}_2/(1+x+x^2)$.

$\cdot$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[x]$	$[0]$	$[x]$	$[1+x]$	$[1]$
$[1+x]$	$[0]$	$[1+x]$	$[1]$	$[x]$

Cuadro 3.2: Multiplicación de elementos de $\mathbb{Z}_2/(1+x+x^2)$.

Capítulo 4

Curvas elípticas sobre campos finitos

En capítulos anteriores, hemos visto la definición de una curva elíptica en el plano y en el plano proyectivo. También construimos campos finitos. Ahora mostraremos cómo se pueden extender las definiciones y la operación definida en una curva elíptica a un campo finito.

Definición. Sea $\mathbb{F}_q$ un campo finito con q elementos, donde $q = p^n$ para algún p primo y sean a_1, a_2, a_3, a_4, a_6 elementos de $\mathbb{F}_q$. Una *curva elíptica sobre* $\mathbb{F}_q$ es el conjunto de puntos $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ que cumplen la ecuación $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. [11] [8] Escribiremos $\mathcal{E}\ (\mathbb{F}_q)$ para indicar que $\mathcal{E}$ es una curva elíptica sobre $\mathbb{F}_q$, es decir,

$$\mathcal{E}\ (\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}$$

De manera similar a las curvas elípticas en el plano, aplicamos las transformaciones similares para obtener una relación de la forma

$$y^2 = x^3 + ax + b \tag{4.1}$$

Notemos que la relación del Teorema (1.2) depende de la operación del campo, por tanto lo podemos extender a campos finitos. Así, diremos que una curva en un campo finito es no singular si y sólo si $27b^2 + 4a^3 \neq 0$. Observemos que esta relación no se satisface si la característica del campo es 2 o 3. Por ello, en adelante trabajaremos con campos finitos de característica distinta de 2 y de 3. Además trabajaremos con una ecuación de la forma como en (4.1).

Para ilustar la definición previa veamos algunos ejemplos de curvas elípticas sobre $\mathbb{Z}_p$ como campo. En este caso, la igualdad $[a] = [b]$ en $\mathbb{Z}_p$ con p primo, es equivalente a la congruencia $a \equiv b \bmod p$

Ejemplo 4.1. Consideremos $\mathbb{Z}_{11}$ y $y^2 \equiv x^3 - 5x + 3 \pmod{11}$. Así, $\mathcal{E}(\mathbb{Z}_{11}) = \{(0,5),(0,6),(2,1),(2,10),(3,2),(3,9),(4,5),(4,6),(5,2),(5,9),(7,5),(7,6),(9,4),(9,7)\}$.
Consideremos la pareja $(4,5)$ y verifiquemos que este punto está en la curva. Sustituimos 4 en $x^3 - 5x + 3$, así $(4)^3 - 5(4) + 3 = 64 - 20 + 3 = 47$. Tenemos que $47 \equiv 3 \pmod{11}$. Además $3 \equiv 25 \pmod{11}$ por tanto $y^2 \equiv 25 \pmod{11}$. Así $y = \pm 5$, de donde obtenemos que $(4,5)$ y $(4,6)$ están en la curva.
Los puntos de la curva se obtuvieron utilizando las funciones *Flatten, Table* y *Solve* del programa *Wolfran Mathematica*, como sigue

```
Clear[x, y];
p = 11;
Flatten[Table[Solve[y^2 == x^3 - 5x + 3, x == u, Modulus== p], u, 0, p - 1], 4]
```

Cuadro 4.1: Código en Mathematica para obtener los puntos de la curva $y^2 \equiv x^3 - 5x + 3 \pmod{11}$.

Obteniendo lo siguiente

$\{Modulus \to 11, y \to 5, x \to 0$	$Modulus \to 11, y \to 6, x \to 0$
$Modulus \to 11, y \to 1, x \to 2$	$Modulus \to 11, y \to 10, x \to 2$
$Modulus \to 11, y \to 2, x \to 3$	$Modulus \to 11, y \to 9, x \to 3$
$Modulus \to 11, y \to 5, x \to 4$	$Modulus \to 11, y \to 6, x \to 4$
$Modulus \to 11, y \to 2, x \to 5$	$Modulus \to 11, y \to 9, x \to 5$
$Modulus \to 11, y \to 5, x \to 7$	$Modulus \to 11, y \to 6, x \to 7$
$Modulus \to 11, y \to 4, x \to 9$	$Modulus \to 11, y \to 7, x \to 9\}$

Cuadro 4.2: Puntos de la curva $y^2 \equiv x^3 - 5x + 3 \pmod{11}$.

Gráficando se tiene la siguiente figura

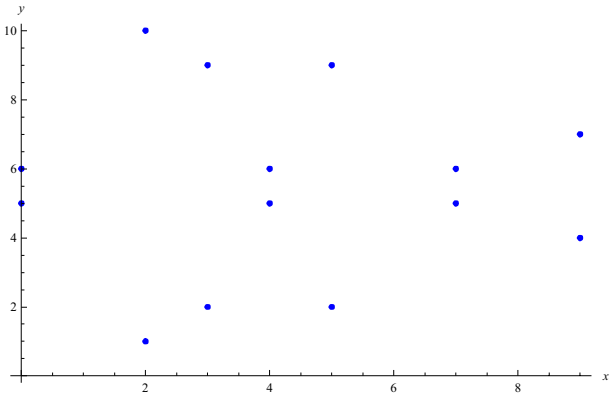


Figura 4.1: Gráfica de una curva elíptica en $\mathbb{Z}_{11}$.

Ejemplo 4.2. Consideremos $\mathbb{Z}_5$ y $y^2 \equiv x^3+3 \pmod 5$. Así, $\mathcal{E}(\mathbb{Z}_5) = \{(1,2),(1,3),(2,1),(2,4),(3,0)\}$. Los puntos de esta curva se obtuvieron de manera similar al ejemplo anterior. E igualmente se puede verificar que los puntos pertenecen a la curva.

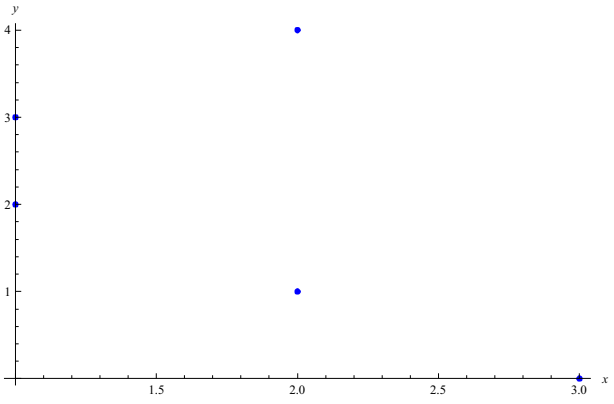


Figura 4.2: Gráfica de una curva elíptica en $\mathbb{Z}_5$.

4.1. Operación en la curva elíptica

En el primer capítulo, se definió la suma de dos puntos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ de una curva elíptica no singular $\mathcal{E}$, como sigue

$$\begin{cases} x_3 = \alpha^2 - x_1 - x_2, & \text{si } x_1 \neq x_2 \\ y_3 = y_1 + \alpha(x_3 - x_1) & \end{cases} \quad \text{donde} \quad \begin{cases} \alpha = \frac{y_2 - y_1}{x_2 - x_1}, & \text{si } x_1 \neq x_2 \\ \alpha = \frac{3x_1^2 + a}{2y_1}, & \text{si } P = Q \end{cases}$$

$$\begin{cases} x_3 = \alpha^2 - 2x_1, & \text{si } P = Q \\ y_3 = y_1 + \alpha(x_3 - x_1) & \end{cases}$$

donde x_3 y $-y_3$ son las coordenadas de la suma.

Notemos que las operaciones que se realizan dependen de las propiedades de campo, los cuales se pueden extender en campos finitos, tomando en cuenta que la característica del campo sea distinto de 2, dado que se tiene una división entre cero si lo es.

Ejemplo 4.3. Del ejemplo (4.1), consideremos los puntos $P = (0, 5)$, $Q = (2, 1)$. Para sumarlos realizamos las siguientes operaciones. Consideremos $P = (x_1, y_1) = (0, 5)$ y $Q = (x_2, y_2) = (2, 1)$. Así $\alpha = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1-5}{2-0} = -2 \equiv 9 \pmod{11}$. Por tanto, $\alpha^2 = 9^2 \pmod{11} = 81 \pmod{11} = 4$. Luego, $x_3 = \alpha^2 - x_1 - x_2 = 4 - 0 - 2 = 2$ y $y_3 = y_1 + \alpha(x_3 - x_1) = 5 + 9(2 - 0) = 5 + 18 = 23 \equiv 1 \pmod{11}$. De esto último se obtiene que $-y_3 = -1 \equiv 10 \pmod{11}$, por tanto $-y_3 = 10$. Obteniendo como resultado el punto $P \oplus Q = (2, 10)$. Gráficamente se tiene como se observa en la siguiente figura.

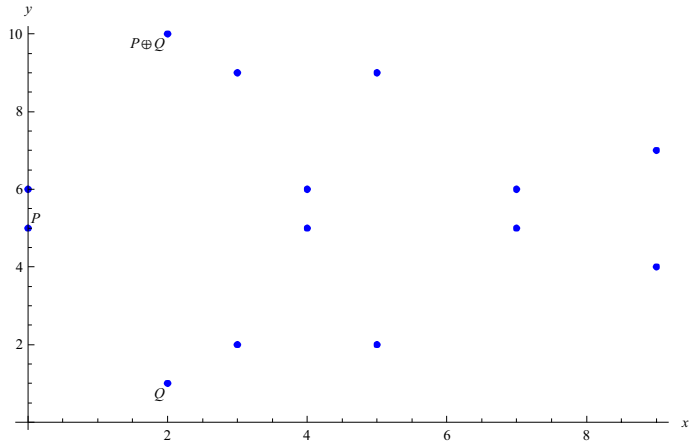


Figura 4.3: Suma de dos puntos distintos en $\mathbb{Z}_{11}$.

De manera similar a lo anterior, veamos los cálculos que se realizan para hallar la suma del punto $P = (3, 9)$ consigo mismo. Para esto, recurrimos a las fórmulas que se tienen cuando los dos puntos coinciden. Como consideramos la curva del ejemplo (4.1), se tiene que $a = -5$. Luego $\alpha = \frac{3x_1^2+a}{2y_1} = \frac{3(3)^2-5}{2(9)} = \frac{27-5}{18} = \frac{22}{18}$. Notemos que $22 \equiv 0 \pmod{11}$. Por tanto, $\alpha = 0$. Consecuentemente, $x_3 = \alpha^2 - 2x_1 = 0 - 2(3) = -6 \equiv 5 \pmod{11}$, y $y_3 = y_1 + \alpha(x_3 - x_1) = 9$, de donde, $-y_3 = -9 \equiv 2 \pmod{11}$. Así se obtiene que $P \oplus P = 2P$ tiene como coordenadas $(5, 2)$. Esto se ilustra en la siguiente figura.

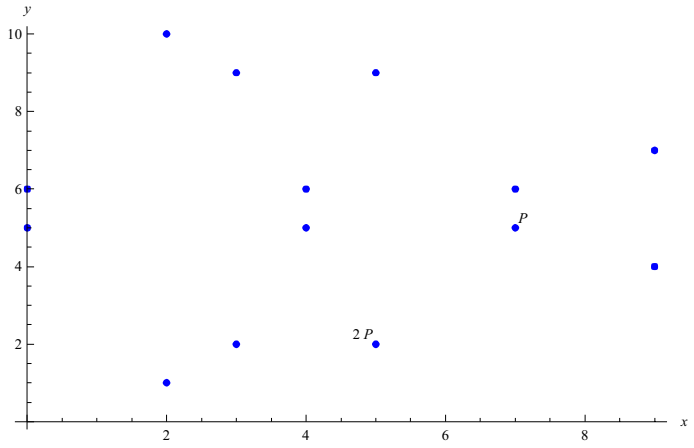


Figura 4.4: Suma de un punto consigo mismo en $\mathbb{Z}_{11}$.

Ejemplo 4.4. Del ejemplo (4.2), consideremos los puntos $P = (2, 4)$ y $Q = (1, 3)$, sumando se tiene que $P \oplus Q = (3, 0)$. De manera gráfica se tiene la figura (4.5).

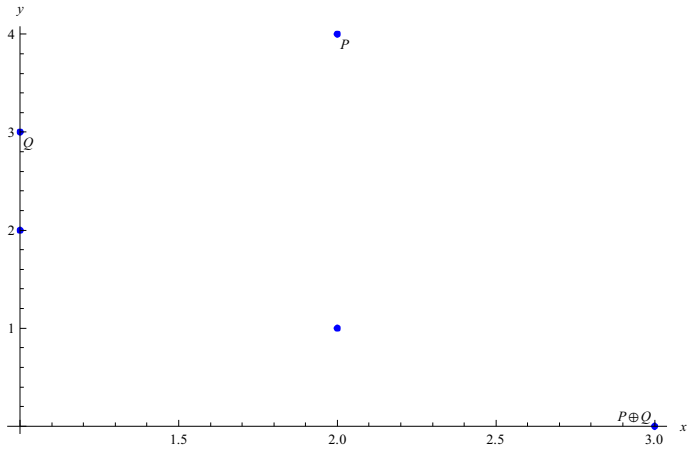


Figura 4.5: Suma de dos puntos diferentes en $\mathbb{Z}_5$.

Por otro lado, en la figura (4.6) tenemos la gráfica que nos muestra la suma de P consigo mismo dos veces, donde $P = (2,\ 1)$ y $2P = (2, 4)$.

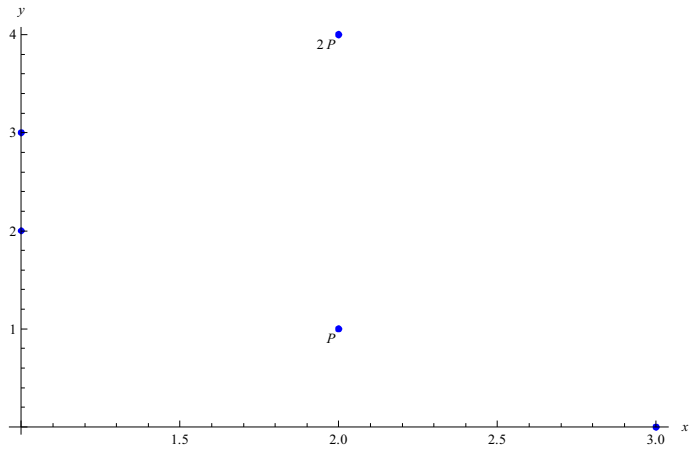


Figura 4.6: Suma de un punto consigo mismo en $\mathbb{Z}_5$.

Los cálculos que se realizan para las sumas de dos puntos distintos y de un punto consigo mismo, son similares al ejemplo anterior, sólo que en este caso se trabaja con enteros módulo 5.

4.2. Plano proyectivo para un campo finito

Definimos una relación de equivalencia en $\mathbb{F}_q$ de manera similar a como se definió en la sección 2.1 . Consideremos $X,\ Y,\ Z \in \mathbb{F}_q$ y la terna (X, Y, Z). Diremos que (X, Y, Z) y (X_1, Y_1, Z_1) con $X_1, Y_1, Z_1 \in \mathbb{F}_q$, están relacionados si existe $\lambda \in \mathbb{F}_q$ distinto de 0 tal que

$$(X, Y, Z) = \lambda(X_1, Y_1, Z_1)$$

Por tanto la relación previa define clases de equivalencia en $\mathbb{F}_q^3 \setminus \{(0, 0, 0)\}$.

Definición. Consideremos $\mathbb{F}_q$ un campo finito. Definimos el *plano proyectivo en* $\mathbb{F}_q$ como el conjunto de clases de quivalencia en $\mathbb{F}_q^3$

$$\{[(X, Y, Z)] : (X, Y, Z) \in \mathbb{F}_q^3\}$$

La clase de equivalencia $[(X, Y, Z)]$ es el conjunto

$$\begin{aligned}[(X,Y,Z)] &= \{(X_1,Y_1,Z_1) \in \mathbb{F}_q^3 : (X,Y,Z) = \lambda(X_1,Y_1,Z_1),\ \lambda \in \mathbb{F}_q^3 \setminus \{0\}\} \\ &= \{(X_1,Y_1,Z_1) \in \mathbb{F}_q^3 : (X_1,Y_1,Z_1) = \frac{1}{\lambda}(X,Y,Z),\ \lambda \in \mathbb{F}_q^3 \setminus \{0\}\}\end{aligned} \tag{4.2}$$

Observemos que para $[(X_1, Y_1, Z_1)]$ y $[(X_2, Y_2, Z_2)]$ en el plano proyectivo, las operaciones que se realizan en las ecuaciones (2.5)-(2.7), únicamente dependen de las operaciones de campo, por tanto se pueden extender a un campo finito. Así, en este caso, el punto al infinito se obtiene de manera similar y es el punto proyectivo $[(0, 1, 0)]$.

Veamos un ejemplo de plano proyectivo. Para esto, consideremos $\mathbb{Z}_5$ y por la notación trabajaremos con los representantes de las clases de equivalencia.

Ejemplo 4.5. Observemos que $\mathbb{Z}_5^3$ tiene 125 elementos, dentro de los cuales se tiene $(0, 0, 0)$. Por tanto, tiene 124 elementos diferentes de $(0, 0, 0)$. Dado que en $\mathbb{Z}_5$ se tienen 4 elementos distintos de 0, el plano proyectivo tiene 31 elementos. El plano proyectivo de $\mathbb{Z}_5$ es el siguiente conjunto

$\{[1,0,0],[0,1,0],[0,0,1],[1,1,0],[1,0,1],[1,2,0],[1,3,0],[1,4,0],[1,1,1],[1,1,2],[1,1,3],[1,1,4],$
$[1,2,1],[1,2,2],[1,2,3],[1,2,4],[1,3,1],[1,3,2],[1,3,3],[1,3,4],[1,4,1],[1,4,2],[1,4,3],[1,4,4],$
$[0,1,1],[0,1,2],[0,1,3],[0,1,4],[1,0,2],[1,0,3],[1,0,4]\}$

Observemos que del ejemplo (4.2), se tienen los puntos de la curva

$$\mathcal{E}\ (\mathbb{Z}_5) = \{(1,2),(1,3),(2,1),(2,4),(3,0)\}$$

los cuales en el plano proyectivo corresponden respectivamente a los siguientes puntos

$$[1,2,1],[1,3,1],[2,1,1] = [1,3,3],[2,4,1] = [1,2,3],[3,0,1] = [1,0,2]$$

junto con el punto al infinito $[0, 1, 0]$.

El siguiente teorema es de gran importancia, ya que nos permitirá construir curvas elípticas con un número grande de puntos. Y tener una idea de cuántos puntos tiene una curva elíptica nos será útil en el capítulo de criptosistemas basados en curvas elípticas. [17], [4], [8], [11]

Teorema 4.1. *Si N es el número de puntos de la curva elíptica $\mathcal{E}$ $(\mathbb{F}_q)$, entonces* $| N - (q+1) | \leqslant 2\sqrt{q}$.

La curva descrita en los ejemplos (4.1) y (4.2), junto con el punto al infinito tienen 15 y 6 elementos, y estas cantidades satisfacen $| 15 - (11+1) | \leqslant 2\sqrt{11}$ o bien $3 \leqslant 2\sqrt{11} \approx 6.6332$ y $| 6 - (5+1) | \leqslant 2\sqrt{5}$ o bien $0 \leqslant 2\sqrt{5} \approx 4.4721$, respectivamente.

Capítulo 5

Sistemas criptográficos

Supongamos que A y B que se encuentran en lugares distintos desean comunicarse por medio de mensajes de manera secreta y que existe un medio (canal) de comunicación el cual no es seguro, esto es, el mensaje puede ser observado por un tercero, digamos, C. Así, aunque C intercepte el mensaje, no tendrá conocimiento del contenido del mismo. La *criptografía* se encarga de estudiar métodos para enviar mensajes de manera encurbierta y segura de tal modo que sólo los destinatarios puedan quitar el disfraz y leer el mensaje. Por otro lado, estudiar los métodos para romper la seguridad de los métodos criptográficos se le conoce como *criptoanálisis*.

Parte de los objetivos de la criptografía, es proporcionar *privacidad, autenticidad, integridad y no rechazo*. La *privacidad* se refiere a que la información que contiene el mensaje sea accedida sólo por los destinatarios. La *autenticidad* hace posible que el receptor verifique que el mensaje vino de la persona quien dice ser y no de otra. La *integridad* hace posible que se verifique que el mensaje no ha sido modificado durante el trayecto. *No-rechazo* hace que el emisor no niegue que ha enviado el mensaje. Estas cuatro características hacen que la comunicación sea similar a una conversación realizada en persona, como también garantizan la seguridad de la transmisión de información.

El mensaje o información que se desea enviar lo llamaremos *texto claro* o *plaintext* y el mensaje disfrazado lo llamaremos *texto cifrado* o *ciphertext*. Estos textos están escritos en algún alfabeto con cierta cantidad N de letras o caracteres.

El proceso de cifrar un texto claro se le conoce como *cifrado* o *encriptación* y el proceso inverso se le conoce como *descifrado* o *desencriptación*.

Definición. Un *sistema criptográfico* es una quintupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ donde

1. $\mathcal{P}$ es un conjunto finito de posibles textos claros.
2. $\mathcal{C}$ es un conjunto finito de posibles textos cifrados.
3. $\mathcal{K}$ es el espacio de claves, conjunto de posibles claves.
4. $\mathcal{E} = \{e_k : k \in \mathcal{K}\}$ es una familia de funciones $e_k : \mathcal{P} \longrightarrow \mathcal{C}$. Sus elementos son llamados *funciones de encriptación*.
5. $\mathcal{D} = \{d_k : k \in \mathcal{K}\}$ es una familia de funciones $d_k : \mathcal{C} \longrightarrow \mathcal{P}$. Sus elementos son llamados *funciones de desencriptación*.
6. Para cada $k \in \mathcal{K}$ existe una función de encriptación $e_k \in \mathcal{E}$ y una correspondiente función de desencriptación $d_k \in \mathcal{D}$. Cada e_k y d_k son funciones tales que $d_k(e_k(p)) = p$, para todo $p \in \mathcal{P}$.

Ejemplo 5.1. Consideremos la asignación del conjunto de 27 letras, $\Omega = \{a,\ b, \ldots, z\}$ al conjunto de números $\{0, 1, \ldots,\ 26\}$, como se muestra en la tabla siguiente

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25	26

Si a un amigo le queremos transmitir el mensaje

iremos a la luna

primero escribimos el texto sin considerar espacios, así obtenemos la siguiente sucesión

iremosalaluna

Utilizando la asignación dada obtenemos

$$\gamma = 8\ 18\ 4\ 12\ 15\ 19\ 0\ 11\ 0\ 11\ 21\ 13\ 0$$

De aquí, podemos pensar en una regla r que cambia el orden de los números, de tal manera que la comprensión del mensaje sea aún más díficil para aquellas personas que lo intercepten, así obtenemos la siguiente asignación

0	1	2	3	4	5	6	7	8	9	10	11	12
26	25	24	23	22	21	20	19	18	17	16	15	14

13	14	15	16	17	18	19	20	21	22	23	24	25	26
13	12	11	10	9	8	7	6	5	4	3	2	1	0

Observemos que la regla r es una biyección y es tal que si aplicamos dos veces esta misma regla se obtiene el número original. Entonces aplicando esta regla a la suceción de números de γ obtenemos la nueva sucesión

18 8 22 14 11 7 26 15 26 15 5 13 26

Sustituyendo nuevamente por las letras de Ω se tiene lo siguiente

r i v ñ *l h z o z o f n z*

por tanto, cualquiera de las sucesiones previas será lo que le enviaremos a nuestro amigo.
En este caso, se tiene que $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{27}$, $\mathcal{K} = \{r\}$, $\mathcal{E} = \{e_r\}$, $\mathcal{D} = \{d_r\}$, donde $e_r : \mathcal{P} \longmapsto \mathcal{C}$ y $d_r : \mathcal{C} \longmapsto \mathcal{P}$ están definidas como $e_r(x) = 26 - x,\ x \in \mathcal{P}$ y $d_r(x) = 26 - y,\ y \in \mathcal{C}$. Podemos ver que $r = 26$ y que las claves de encripción como de desencripción coinciden.

En relación a las claves de encriptación y desencriptación, los criptosistemas se dividen en dos tipos: *criptosistema de clave privada* o *criptosistema simétrico* y *criptosistemas de clave pública* o *criptosistema asimétrico*.

5.1. Criptosistemas simétricos

En un *criptosistema simétrico* o *de clave privada*, A y B, utilizan una sola clave para cifrar y descifrar los mensajes. Esto es, si A utiliza la clave k para cifrar un mensaje, B usará k para descifrar el mismo. La seguridad de este tipo de criptosistemas se basa en que A y B intercambian la clave antes de separarse y mantenerlo en secreto o intercambiar la clave por medio de

un mensajero autorizado y seguro. [3]

Ahora supongamos que se tiene una cierta cantidad n de personas que desean estar comunicados unos con otros, esto implica que se deben tener $n(n-1)$ claves distintas y cada uno de ellos necesita conocer $(n-1)$ claves. De ahí surge uno de los problemas a los que se enfrenta este tipo de criptosistemas que es la administración de claves; y como su seguridad depende de mantener en secreto la clave, si alguna persona desea abandonar o alguna persona va a unirse al grupo, se tienen que generar nuevas claves.

5.2. Criptosistemas asimétricos

Para resolver el problema que presentan los criptosistemas de clave privada, en 1976 Martin Hellman y Whitfield Diffie propusieron la noción de criptosistemas de clave pública [2] [12] [8]. El siguiente diagrama ilustra el criptosistema propuesto por Diffie y Hellman [17].

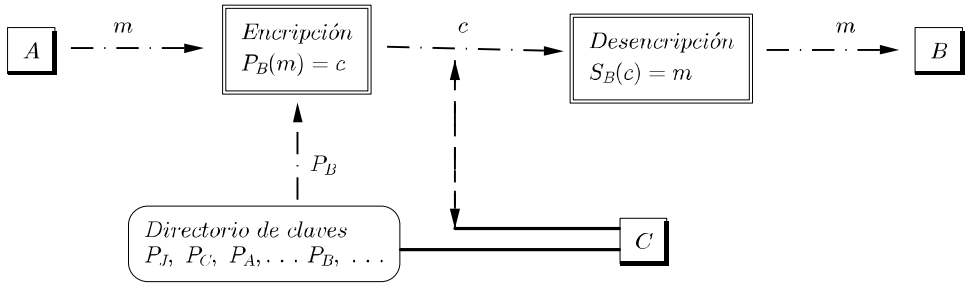


Figura 5.1: Diagrama de un criptosistema de clave pública.

En un *criptosistema asimétrico* o *de clave pública*, se tienen dos claves. Una de las claves se conoce como *clave pública* y la otra como *clave privada*. La clave pública es la que se utiliza para cifrar mensajes y se encuentra disponible para cualquier emisor. Mientras que la clave privada se utiliza para descifrar mensajes que es conocido únicamente por el receptor.

Nuevamente, si A le desea enviar un mensaje a B, A ocupa la clave pública de B, que se encuentra, digamos, en un directorio y B lo descifra utilizando su clave privada, esto es, la clave

que solamente B conoce. De esta manera, A y B no necesariamente tienen que reunirse para realizar dicho intercambio de claves.
Con el criptosistema de clave pública se resuelve el problema de administración y distribución de claves y el problema de autenficación.

La seguridad de este tipo de criptosistemas se basa en encontrar formas matemáticas que generen dos claves relacionadas, de tal manera que la clave privada no se pueda hallar a partir de la clave pública y del algoritmo de cifrado.

Cada usuario $\mathcal{U}$ genera un par de algoritmos, digamos, $P_{\mathcal{U}}$ y $S_{\mathcal{U}}$, donde el usuario $\mathcal{U}$ hace público $P_{\mathcal{U}}$ y mantiene en secreto $S_{\mathcal{U}}$. Dependiendo de la aplicación, estos algoritmos satisfacen las siguientes propiedades [17]

- PK1: $P_{\mathcal{U}}$ y $S_{\mathcal{U}}$ son eficientes, es decir, no necesitan mucho tiempo de cómputo y ni mucho espacio de memoria.
- PK2: $S_{\mathcal{U}}\ (P_{\mathcal{U}}(m)) = m$, para cada usuario y para cada posible mensaje m.
- PK3: No es factible encontrar un algoritmo $S^*_{\mathcal{U}}$ de $P_{\mathcal{U}}$ que satisfaga $S^*_{\mathcal{U}}\ (P_{\mathcal{U}}(m)) = m$, para todo m.
- PK4: $P_{\mathcal{U}}\ (S_{\mathcal{U}}(m)) = m$, para todo usuario $\mathcal{U}$ y para cada posible mensaje m.
- PK5: No es factible encontrar un algoritmo $P^*_{\mathcal{U}}$ de $S_{\mathcal{U}}$ tal que $P^*_{\mathcal{U}}\ (S_{\mathcal{U}}(m)) = m$, para todo m.

Dentro de los criptosistemas de claves públicas tenemos el famoso sistema RSA basado en la factorización de enteros, ElGamal basado en el problema de logaritmo discreto sobre el grupo multiplicativo de un campo finito, el criptosistema Massey-Omura, Rabin y curvas elípticas. Los más usados son el sistema RSA y ElGamal. [2].

5.2.1. Sistema RSA

Este criptosistema es conocido como RSA debido a sus creadores Ronald Rivest, Adi Shamir y Leonard Adleman cuya seguridad se basa en la factorización de números enteros en factores primos, cuando estos son muy grandes.

Generación de claves

Hemos mencionado que el sistema RSA es de clave pública, mostraremos cómo se generan las claves pública y privada.
Algoritmo para generar las claves.

1. Generar dos números primos grandes, p y q.
2. Calcular $n = p \cdot q$ y $\varphi(n) = (p-1)(q-1)$.
3. Elegir e tal que $1 < e < \varphi(n)$ y $\text{mcd}(e, \varphi(n)) = 1$.
4. Determinar d tal que $ed \equiv 1 \text{ mod} \varphi(n)$.

El par $(n,\ e)$ es la clave pública y d es la privada. Observemos que la cantidad $\varphi(n)$ generada en el segundo paso es la función φ de Euler, cuyo valor en n es el número de enteros positivos menores que n que son primos relativos con n.

Notemos que no se necesita mucho espacio de memoria para realizar este tipo de algoritmo, y también dado un número entero no es fácil hallar sus factores primos. Por tanto, este algoritmo satisface las propiedades mencionadas en el párrafo previo.

Ejemplo 5.2. Consideremos $p = 17$ y $q = 11$. Calculamos $n = 17{\cdot}11 = 187$, $\varphi(n) = 16{\cdot}10 = 160$. Luego, elegimos $e = 7$ puesto que cumple con $\text{mcd}(7, 160) = 1$. Resolvemos la congruencia $7d \equiv 1 \text{ mod } 160$, de donde obtenemos $d = 23$. Por tanto, la clave pública es $(187,\ 7)$ y la clave privada es 23.

Encripción

Representamos el mensaje en claro M como un entero en $m \in \mathbb{Z}_n$, y realizamos lo siguiente

1. Calcular $c = m^e \text{mod } n$.
2. Enviar c.

Ejemplo 5.3. Retomando el ejemplo (5.2), supongamos que A le desea enviar a B un mensaje representado por $M \in \mathbb{Z}_{160}$, digamos que $M = 88$. Calculamos $c = 88^7 \text{ mod } 187 = 11$ y enviamos $c = 11$.

Desencripción

Por último describimos la forma de desencriptar un mensaje. En este caso, B desea recuperar el mensaje m a partir del mensaje encriptado c. Para esto, realiza el siguiente cálculo

$$m = c^d \bmod n$$

Del ejemplo anterior, B recibe el mensaje $c = 11$. Así, para recuperar m, realiza lo siguiente:

$$m = 11^{23} \bmod 187 = 88,$$

de donde recupera el mensaje original.

Considerando nuevamente el mensanje *iremos a la luna* del ejemplo (5.1), desarrollaremos un ejemplo desde la generación de claves hasta la desencripción.

Ejemplo 5.4. Pensemos que alguien desea enviarnos el mensaje *iremos a la luna* del ejemplo (5.1). Consideremos $\mathbb{Z}_{26}$ y la siguiente asignación

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Así, en $\mathbb{Z}_{26}$ se tiene la siguiente sucesión que representa el mensaje *iremos a la luna*

$$\gamma = 8\ 17\ 4\ 12\ 14\ 18\ 0\ 11\ 0\ 11\ 20\ 13\ 0$$

Por tanto, para lograr nuestro objetivo iniciemos calculando las claves pública y privada. Tenemos que 26 es el producto de los primos $p = 13$ y $q = 2$. De donde, $n = p \cdot q = 26$ y $\varphi(26) = 12$. Elegimos $e = 5$, tal que cumple $1 < e < 12$ y $\text{mcd}(5, 12) = 1$. Utilizando el algoritmo de Euclides, hallamos que la clave privada d es igual a 5. Observemos que este caso, e y d coinciden. Una vez hallado las claves, hacemos público el par $(n,\ e) = (26,\ 5)$. Así, esta persona que desea enviarnos el mensaje procederá a encriptar la sucesión que se tiene en γ. Esto es, cada elemento de γ lo elevará a la potencia $e = 5$ módulo $n = 26$. Realizando esto último se obtiene la siguiente sucesión

$$\omega = 8\ 23\ 10\ 12\ 14\ 18\ 0\ 7\ 0\ 7\ 24\ 13$$

Si volvemos a sustituir las letras que corresponden esta sucesión de números, se tiene la siguiente

$$i\ x\ k\ m\ o\ s\ a\ h\ a\ h\ v\ n\ a$$

Así, ya sea esta última o la sucesión en ω es el texto cifrado que nosotros recibiremos.
Finalmente, teniendo el mensaje cifrado, nostros procedemos a desencriptar el mensaje, realizando una operación similar, debido a que e y d coinciden. Esto es, a cada elemento de la sucesión en ω se eleva a la quinta potencia módulo 26, de donde obtenemos el mensaje orginal.

En este último ejemplo vimos que las claves e y d coincidieron, mientras que en ejemplo (5.2), e y d son distintos.

5.3. Funciones de un sólo sentido

Sabemos que desarmar un rompecabezas es una tarea fácil de realizar, pero armarlo no lo es en general. Esto es un ejemplo de un proceso que es fácil de realizar en un sólo sentido. Entonces, si pensamos en una función que asigne a cada pieza del rompecabezas a la posición que le corresponde en el rompecabezas, podemos observar que es una función cuya inversa es difícil de hallar. A las funciones que son fáciles de calcular en un sentido y cuya inversa es difícil de calcular, se les conoce como *funciones de un sólo sentido* o *one-way functions*. [8][4] Esta noción de funciones de un sólo sentido es de gran utilidad en la criptografía. Por ejemplo, si escribimos un mensaje claro en las piezas del rompecabezas armado y después dárselo a alguien una vez que lo hayamos desarmado, éste le será difícil descifrarlo.

En matemáticas, tenemos funciones de un sólo sentido, por ejemplo, multiplicar dos números primos es fácil de realizar, pero si nos dan un número y nos piden hallar sus factores primos ya no lo es, más aún si se nos da un número "grande"; elevar un número a una potencia dada es fácil de realizar, pero si nos dan dos números a y b, no es fácil determinar a qué potencia n se tiene que elevar a para obtener b. Este último ejemplo es una función de un sólo sentido en campos finitos. En $\mathbb{R}$, sabemos que la inversa de la función exponenciación es el logaritmo natural y que ambas son procesos fáciles de realizar, mientras que en campos finitos se complica. En este caso, hablamos de lo que se conoce como *logaritmo discreto*. [4]

5.4. Logaritmo discreto

En la sección previa hemos mencionado a las funciones de un sólo sentido, ahora definiremos una función de este tipo, el logaritmo discreto.

Definición. Sean G un grupo cíclico multiplicativo con n elementos y g un generador de G. Sea A un elemento de G, entonces existe un exponente $a \in \{0,\ 1,\ 2, \ldots,\ n-1\}$ tal que $A = g^a$. Este exponente se le conoce como *logaritmo discreto de A en la base g* o *índice de A en base g*. *El problema de logaritmo discreto* consiste en hallar el exponente a, a partir de A y g. [3]

Ejemplo 5.5. Consideremos el campo $\mathbb{Z}_{11}$. Sea $g = 2$ elemento de $\mathbb{Z}_{11}$. Notemos que g es generador del grupo cíclico multiplicativo de $\mathbb{Z}_{11}$, puesto que si calculamos g^a para cada $a \in \{1,\ 2, \ldots,\ 10\}$ tenemos lo siguiente

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 5, \quad 2^5 = 10$$
$$2^6 = 9, \quad 2^7 = 7, \quad 2^8 = 3, \quad 2^9 = 6, \quad 2^{10} = 1$$

Luego, por el corolario (A.9.1) se tiene que el conjunto que es generado por $g = 2$ junto con el producto es un grupo cíclico. Si consideramos $A = 3$, de los cálculos previos se tiene que $x = 8$ satisface que $g^x = A$.

Del ejemplo previo, observemos que la tarea de tomar cada uno de los elementos del grupo multiplicativo e ir probando para ver cuál de ellos es el logaritmo discreto del elemento que se conoce, es tedioso y nos tomará tiempo, más aún cuando el grupo multiplicativo tenga un número grande de elementos.

5.5. Intercambio de claves privadas

Ahora veamos la aplicación del logaritmo discreto, para esto describimos el intercambio de claves que plantearon Diffie y Hellman. [3]

Supongamos que A y B desean acordar una clave común y que únicamente se pueden comunicar por medio de un canal no seguro. Para esto ellos se ponen de acuerdo en un número primo grande p y una raíz primitiva g mod p, donde $2 \leq g \leq p-2$. No hay problema si otras personas llegan a conocer estos dos elementos.

Luego, A elige un entero $a \in \{0,\ 1,\ 2, \ldots,\ p-2\}$ de manera arbitraria. Después calcula

$$A_1 \equiv g^a \bmod p,$$

una vez calculado esto, A le envía este resultado a B, pero mantiene en secreto a.
De manera similar, B elige un entero, digamos, $b \in \{0,\ 1,\ 2, \ldots,\ p-2\}$, de manera arbitraria. Después realiza el siguiente cálculo

$$B_1 = g^b \bmod p.$$

Luego B le envía B_1 a A manteniendo b en secreto.
Para obtener la clave en común, A calcula $B_1^a \bmod p = g^{ab} \bmod p$ y B realiza un cálculo similar, $A_1^b \bmod p = g^{ab} \bmod p$.
Así, la clave común es

$$K = g^{ab} \bmod p.$$

Ejemplo 5.6. Consideremos $p = 17$ y $g = 3$. Supongamos que A elige $a = 7$ y calcula

$$g^a \bmod p = 3^7 \bmod 17 = 11.$$

Así, A le envía $A_1 = 11$ a B. Ahora supongamos que B elige $b = 4$, después calcula

$$g^b \bmod p = 3^4 \bmod 17 = 13.$$

Entonces, B le envía $B_1 = 13$ a A. Por último, A realiza el cálculo

$$B_1^a \bmod p = 13^7 \bmod 17 = 4,$$

y B realiza

$$A_1^b \bmod p = 11^4 \bmod 17 = 4.$$

Así, obtienen que la clave común es 4.

5.5.1. Sistema ElGamal

En 1984 Taher ElGamal propuso un esquema que permite tanto el cifrado de mensajes como la implementación de firmas digitales [4]. Este sistema está basado en el problema de logaritmo discreto y está estrechamente relacionado con el intercambio de claves de Diffie-Hellman.[3]

Generación de claves

Supongamos que A y B desean intercambiar mensajes. Así, para generar las claves, A elige un número primo p y una raíz primitiva $g \bmod p$.

Entonces A elige un exponente $a \in \{1, \ldots, p-2\}$ de manera aleatoria y realiza el siguiente cálculo

$$A_1 = g^a \bmod p$$

Por tanto, la clave pública de A es la terna $(p,\ g,\ A_1)$ y la clave secreta es el exponente a. Observemos que el entero A_1 es la clave de A en el protocolo de intercambio de claves de Diffie-Hellman.

Encripción

El espacio de texto claro es el conjunto $\{0,\ 1, \ldots,\ p-1\}$. Para encriptar un mensaje en claro m, B adquiere la clave pública de A. De manera similar, elige arbitariamente un exponente $b \in \{1, \ldots,\ p-2\}$ y realiza el cálculo

$$B_1 = g^b \bmod p$$

El número B_1 es la clave de B en el protocolo de Diffie-Hellman. Por último B determina

$$C = A_1^b m \bmod p.$$

Por tanto, el texto cifrado es el par $(B_1,\ C)$. Observemos que B encripta el mensaje en claro multiplicandolo por la clave de Diffie-Hellman.

Desencripción

Sabemos que A conoce su clave secreta a y una vez que obtiene el texto cifrado $(B_1,\ C)$ procederá a desencriptar este mismo. Para construir el texto claro, A determina el exponente $x = p - 1 - a$. Como $1 \leq a \leq p-2$, tenemos que $1 \leq x \leq p-2$. Entonces A calcula $m = B_1^x C \bmod p$. Podemos ver que este es el texto en claro original. En efecto,

$$B_1^x C \equiv (g^b)^{p-1-a} A^b m \equiv (g^{p-1})^b (g^{-a})^b A^b m \equiv g^{-b} g^b m \equiv m \bmod p.$$

Capítulo 6

Criptosistemas basados en curvas elípticas

Hemos estudiado algunos criptosistemas públicos, notemos que una de las características de este tipo de criptosistemas es que su seguridad reside en problemas matemáticos que se conjeturan computacionalmente difíciles, esto es, problemas para los cuales no se conocen algoritmos eficientes para resolverlos.
Debido al avance en la eficiencia de algoritmos de factorización y el criptoanálisis del problema del logaritmo discreto han provocado la necesidad de aumentar el tamaño de las claves. Para esto, los criptosistemas basado en curvas elípticas hacen su aparición como una alternativa a los criptosistemas estudiados [2].

6.1. Múltiplos de puntos

En un grupo multiplicativo se realizan multiplicaciones de dos elementos, su análogo en el grupo de curvas elípticas es sumar dos puntos de la curva; así, elevar a una potencia n un elemento del grupo multiplicativo, su análogo en una curva elíptica es sumar n veces un punto consigo mismo.

Para hallar la multiplicación escalar de un punto P de una curva elíptica, digamos $n \cdot P$, tomamos la representación binaria de n y de izquierda a derecha recorremos cada bit doblando

el punto P en cada paso y si el bit actual es 1 sumamos P. [13]

Por ejemplo, supongamos que queremos calcular $70P$, entonces hallamos la representación binaria de 70, esto es, 1 0 0 0 1 1 0. En la siguiente tabla mostramos el cálculo correspondiente en cada paso.

No. Paso	**Bit**	**Expresión**
1	1	P
2	0	$2P$
3	0	$2(2P)$
4	0	$2(2(2P))$
5	1	$2(2(2(2P))) + P$
6	1	$2(2(2(2(2P))) + P) + P$
7	0	$2(2(2(2(2(2P))) + P) + P) = 70P$

Cuadro 6.1: Ejemplo de multiplicación escalar.

Observemos que para este ejemplo, realizar la suma 70 veces se hace tedioso, por lo que lo anterior es un método eficiente, que como se observa en la tabla se reduce a realizar 7 pasos.

6.2. Problema de logaritmo discreto sobre curvas elípticas

Con la noción de la multiplicación escalar de un punto de una curva elíptica, podemos definir el análogo del problema de logaritmo discreto en una curva elíptica.

Definición. Sea $\mathcal{E}$ una curva elíptica y sea P un punto de $\mathcal{E}$. El *problema de logaritmo discreto en* $\mathcal{E}$ es el problema de, dado un punto Q de $\mathcal{E}$, hallar un entero n tal que $n \cdot P = Q$, si tal entero existe. [8]

Definición. El *orden* n de un punto P de una curva elíptica es el entero positivo más pequeño tal que $n \cdot P = \mathcal{O}$. Claramente, este entero finito n puede no existir. [8]

Consecuentemente, describimos el análogo al intercambio de claves de Diffie y Hellman [17]. Como parámetros necesitamos una curva elíptica $\mathcal{E}$ sobre un campo finito $\mathbb{F}_q$ y un punto P en

$\mathcal{E}$ de orden mayor, digamos n.

Cada usuario U del sistema selecciona un escalar M_u y calcula el punto $Q_U = M_U \cdot P$ y pública Q_U. Por tanto, los usuarios A y B pueden acordar una clave en común

$$K_{A,B} = M_A \cdot M_B \cdot P,$$

calculando $M_A \cdot Q_B$ y $M_B \cdot Q_A$, respectivamente.

Ejemplo 6.1. Consideremos $\mathbb{Z}_{197}$ y la curva descrita por la ecuación $y^2 \equiv x^3 + 10x + 1$. Se puede verificar que el punto $(2, 63)$ pertenece a la curva y que tiene orden 93. Ahora supongamos que A y B eligen los enteros 15 y 23, respectivamente y desean acordar una clave común. Calculando los múltiplos escalares, se tiene los siguientes puntos $Q_A = 15 \cdot (2, 63) = (57, 105)$ y $Q_B = 23 \cdot (2, 63) = (166, 89)$. Donde Q_A y Q_B son las claves públicas de A y B, respectivamente. Por tanto, para que ambos obtengan la clave común, A calcula $15 \cdot Q_B = 15 \cdot (166, 89)$ y B calcula $23 \cdot Q_A = 23 \cdot (57, 105)$. Realizando los cálculos se tiene que $15 \cdot Q_B = (35, 87)$ y $23 \cdot Q_A = (35, 87)$. Por tanto la clave común es $(35, 87)$.

6.3. Criptosistema del tipo ElGamal

Hemos descrito como realizar el intercambio de claves. Ahora describimos el análogo al sistema de ElGamal en curvas elípticas. Se necesita generar un número primo p para definir el campo $\mathbb{F}_p$, los parámetros a y b para la curva elíptica $\mathcal{E}$ sobre $\mathbb{F}_p$ y un punto P de $\mathcal{E}$ cuyo orden sea un entero n que tenga factor primo del tamaño de p. Se trabaja en el subgrupo de orden n generado por P. [3] [4]

Como clave privada se elige $d \in [1,\ n-1]$ y la clave que se hace pública es el punto $Q = d \cdot P$ de la curva. Para realizar el cifrado de un mensaje m se efectúan los siguientes pasos.

- Representar el mensaje m como un punto de M del sugrupo generado por P.
- Escoger un entero aleatorio $e \in [1,\ n-1]$
- Calcular $C_1 = e \cdot P$ y $C_2 = M \oplus e \cdot Q$.

De esta manera, se envía la pareja $(C_1,\ C_2)$ a la persona que va dirigida el mensaje.

Para realizar el descifrado, una vez que se recibe $(C_1,\ C_2)$, se realiza la siguiente tarea

- Calcular los puntos $d \cdot C_1 = d \cdot e \cdot P = e \cdot Q$ y $M = C_2 - e \cdot Q$ que se encuentra en el conjunto generado por P.
- Obtener el mensaje en claro m del punto M.

Como podemos observar, ambas partes, emisor y receptor, necesitan conocer los parámetros p, a, b, n y P.

Ejemplo 6.2. Consideremos nuevamente la curva del ejemplo (6.1) y supongamos que B le desea enviar a A el mensaje $M = (173, 11)$. El punto M se encuentra en el generado de $P = (2, 63)$. Supongamos que A tiene como clave privada $d = 15$, luego del ejemplo (6.1), se tiene que $Q_A = d \cdot P = (57, 105)$. Ahora supongamos que B elige $e = 65$.
Entonces B calcula

$$C_1 = e \cdot P = 65 \cdot (2, 63) = (96, 173),$$

$$C_2 = M \oplus e \cdot Q_A = (173, 11) \oplus 65 \cdot (57, 105) = (173, 11) \oplus (56, 16) = (155, 64).$$

Por último envía el par (C_1, C_2) a A.
Una vez que A recibe (C_1, C_2), para recuperar el mensaje M procede a calcular los siguientes

$$d \cdot C_1 = 15 \cdot C_1 = 15 \cdot (96, 173),$$

$$M = C_2 - e \cdot Q_A = (155, 64) - 65 \cdot (57, 105) = (155, 64) \oplus (56, -16) = (173, 11).$$

Recuperando así el mensaje original.

Ejemplo 6.3. Veamos otro ejemplo, utilizando el texo *iremos a la luna*. Retomando $\mathbb{Z}_{197}$ y el punto $P = (2, 63)$ de orden 93 de la curva elíptica del ejemplo (6.1), se tiene el siguiente conjunto generado por P
$\{\mathcal{O},\ (2,63),\ (170,39),\ (21,193),\ (32,105),\ (31,54),\ (28,13),\ (11,121),\ (155,133),\ (174,139),\ (75,88),$
$(84,141),\ (148,72),\ (182,131),\ (29,45),\ (57,105),\ (45,94),\ (46,171),\ (142,59),\ (108,92),\ (179,80),$
$(97,67),\ (39,120),\ (166,89),\ (134,41),\ (165,194),\ (14,18),\ (35,110),\ (96,24),\ (196,160),\ (147,160),$
$(89,194),\ (130,136),\ (125,50),\ (51,160),\ (180,51),\ (136,39),\ (140,194),\ (88,158),\ (149,148),\ (173,11),$
$(26,86),\ (160,196),\ (25,71),\ (80,124),\ (56,16),\ (47,9),\ (47,188),\ (56,181),\ (80,73),\ (25,126),$
$(160,1),\ (26,111),\ (173,186),\ (149,49),\ (88,39),\ (140,3),\ (136,158),\ (180,146),\ (51,37),\ (125,147)$

$(130, 61),\ (89, 3),\ (147, 37),\ (196, 37),\ (96, 173),\ (35, 87),\ (14, 179),\ (165, 3),\ (134, 156),\ (166, 108),$
$(39, 77),\ (97, 130),\ (179, 117),\ (108, 105),\ (142, 138),\ (46, 26),\ (45, 103),\ (57, 92),\ (29, 152),\ (182, 66),$
$(148, 125),\ (84, 56),\ (75, 109),\ (174, 58),\ (155, 64),\ (11, 76),\ (28, 184),\ (31, 143),\ (32, 92),\ (21, 4),$
$(170, 158),\ (2, 134)\ \}$

Por otro lado, asignemos $a \longmapsto \mathcal{O}$, $b \longmapsto (2, 63)$, $c \longmapsto (170, 39)$ y así sucesivamente hasta $z \longmapsto (14, 18)$. De aquí, se obtiene que el mensaje *iremos a la luna* se transforma en la siguiente sucesión

$$\Omega = (155, 133)\ (142, 59)\ (32, 105)\ (148, 72)\ (57, 105)\ (108, 92)\ \mathcal{O}\ (84, 141)\ \mathcal{O}$$
$$(84, 141)\ (97, 67)\ (182, 131)\ \mathcal{O}$$

Consideremos también que la claves privadas de A y B son 15 y 23, respectivamente. De donde se obtiene que la clave pública de A es $Q_A = (57, 105)$. Supongamos que B le desea enviar el mensaje a A, por tanto realiza lo siguiente.
Primero calcula $C_1 = 23 \cdot (2, 63) = (166, 89)$ y también calcula $C_{2i} = \Omega_i + 23 \cdot Q_A$, donde Ω_i es el i-ésimo elemento de la sucesión Ω. Por tanto realizando los calculos, se obtiene la siguiente sucesión, que es el texto cifrado

$$\Gamma = (108, 105)\ (174, 58)\ (166, 108)\ (57, 92)\ (148, 125)\ (155, 64)\ (35, 87)$$
$$(45, 103)\ (35, 87)\ (45, 103)\ (28, 184)\ (29, 152)\ (35, 87)$$

Por tanto B le envía a A el par (C_1, Γ).
Para que A recupere el mensaje, realiza los siguientes
Calcula $15 \cdot C_1 = 15 \cdot (166, 89)$ y $M_i = \Gamma_i - 15 \cdot C_1$. Realizando los calculos se obtiene la sucesión como en Ω.

6.4. Seguridad de criptosistemas

Algunos métodos que resuelven logaritmo discreto, como Pollard-ρ, Pohlig-hellman, etc. se pueden describir de manera similar con curvas elípticas, cambiando únicamente exponenciación modular por multiplicación escalar en curvas elípticas. Pero el algoritmo conocido como *index-calculus*, no ha podido reescribirse, lo cual es bueno para los criptosistemas con curvas elípticas, ya que este algoritmo es el único con complejidad subexponencial. [17]

Por tanto, la ventaja principal que tienen los criptosistemas basados en curvas elípticas sobre el grupo multiplicativo de un campo finito es la ausencia de algoritmos de tiempo subexponencial que hallen logaritmos discretos sobre estos grupos.
Consecuentemente se pueden utilizar claves mucho más pequeñas que mantengan el mismo nivel de seguridad. Además se obtienen ahorros de ancho de banda e implementación rápida. [10]

La seguridad del protocolo de intercambio de claves de Diffie-Hellman con curvas elípticas está basada en la intratabilidad del Problema de Diffie-Hellman con curvas elípticas:
Dado una curva elíptica definida en $\mathbb{F}_q$ *y puntos* P, K_1P, K_2P *en* $\mathcal{E}$ $(\mathbb{F}_q)$, *calcular* K_1K_2P.
Boneh y Lipton probaron que si el problema de logaritmo discreto con curvas elípticas no puede ser resuelto en tiempo subexponencial, entonces tampoco se puede resolver el problema de Diffie-Hellman con curvas elípticas.

Existen ataques especiales sobre criptosistemas basados en el logaritmo discreto con curvas elípticas, estos hacen necesario evitar algunos tipos especiales de curvas, dentro de los cuales se encuentra las curvas singulares, las denominadas curvas supersingulares y las anómalas.
Las curvas anómalas son aquellas cuyo número de puntos es igual a q y las supersingulares son aquellas que tienen número de puntos igual a $q + 1$.

Conclusiones

En este trabajo de tesis, se estudiaron a las curvas elípticas sobre el plano, el plano proyectivo y en campos finitos. En el primer capítulo se ha definido sobre el conjunto de puntos de una curva elíptica en el plano una operación suma, $\oplus$, analizando las características y las propiedades que ésta posee. Observando que las operaciones que se realizan en esta definición de suma son similares, en cierta manera, a las propiedades de un grupo. Además, dependen únicamente de las operaciones de campo, lo cual facilita extender las curvas elípticas y sus propiedades al plano proyectivo y a campos finitos, obteniendo así fórmulas de la suma, $\oplus$, en cada uno de estos espacios.

Con las definiciones de curva elíptica y la suma en el plano proyectivo se pudo definir el *punto al infinito* y consecuentemente, el resultado de que *el conjunto formado por los puntos de una curva elíptica y el punto al infinito junto con la operación* $\oplus$*, forman un grupo.*
Con este resultado se puede definir el análogo al logaritmo discreto y por lo tanto el problema de logaritmo discreto sobre curvas elípticas.

Un aspecto importante que tienen las curvas elípticas en los sistemas criptográficos es que aparecen como una alternativa a otros criptosistemas que se han estudiado, por la disminución de tamaños de claves que se requieren, manteniendo el mismo nivel de seguridad computacional. Además de que tienen complejidad en la resolución del problema de logaritmo discreto.

Hemos visto cómo se pasa de objetos geométricos muy familiares como son las curvas a objetos más abstractos como los grupos finitos, manteniendo propiedades algebraicas, para resolver problemas de aplicación. Además, los sistemas criptográficos constituyen una de las aplicaciones más importantes que tiene la teoría matemática referente a grupos y campos finitos.

Como trabajo futuro se tienen los siguientes: implementación eficiente de los algoritmos en campos finitos, métodos para generar curvas elípticas que se puedan usar en aplicaciones reales y desarrollo de la teoría en campos finitos de característica 2 o 3.

Apéndice A

Conceptos de álgebra

Campos

Definición. Sea $\mathbb{K}$ un campo. Si existe algún entero positivo n, tal que $n \cdot x = 0$, donde $n \cdot x = \underbrace{x + x + \cdots + x}_{n-veces}$, para todo $x \in \mathbb{K}$, entonces el menor de dichos enteros positivos es la *característica de* $\mathbb{K}$. Si no existen dichos enteros positivos, entonces $\mathbb{K}$ es de característica 0.

A los campos que tienen un número finito de elementos se les llaman *campos finitos*.

Ejemplo A.1. Algunos ejemplos de campos son:

1. Los campos, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica cero.

2. El campo $\mathbb{Z}_p$, tiene característica p.

Definición. Sea $\mathbb{F}$ un campo. Un campo $\mathbb{K}$ se dice que es una *extensión de* $\mathbb{F}$ si $\mathbb{K}$ contiene a $\mathbb{F}$. Es decir, $\mathbb{K}$ es una extensión de $\mathbb{F}$ si $\mathbb{F}$ es un subcampo de $\mathbb{K}$.

Ejemplo A.2. El campo $\mathbb{R}$ es extensión de $\mathbb{Q}$ y $\mathbb{C}$ es extensión de $\mathbb{R}$.

Teorema A.1. *Sea* $\mathbb{E}$ *una extensión finita de grado* n *sobre un campo finito* $\mathbb{F}$. *Si* $\mathbb{F}$ *tiene* q *elementos, entonces* $\mathbb{E}$ *tiene* q^n *elementos.*

Corolario A.1.1. *Si* $\mathbb{E}$ *es un campo finito de característica* p, *entonces* $\mathbb{E}$ *contiene un subcampo isomorfo a* $\mathbb{Z}_p$.

Corolario A.1.2. *Si* $\mathbb{E}$ *es una extensión finita de grado* n *de* $\mathbb{Z}_p$, *entonces* $\mathbb{E}$ *tiene* p^n *elementos.*

Definición. Un elemento α de un campo es una raíz n-ésima del unitario si $\alpha^n = 1$. Es una raíz n-ésima primitiva del unitario si $\alpha^n = 1$ y $\alpha^m \neq 1$ para $0 < m < n$.

Polinomios

Definición. Un polinomio $P(x_0, x_1, ..., x_n)$ en $\mathbb{K}[x_0, x_1, ..., x_n]$ es homogéneo de grado d si $P(tx_0, tx_1, ..., tx_n) = t^d P(x_0, x_1, ..., x_n)$

Definición. Sean $p(x),\ h(x) \in \mathbb{F}[x]$ con $p(x) \neq o(x)$. Diremos que $p(x)$ divide a $h(x)$ si existe $q(x) \in \mathbb{F}[x]$ tal que $h(x) = p(x)\ q(x)$. Para indicarlo escribimos $p(x) \setminus q(x)$.

Teorema A.2. *Sea $\mathbb{F}$ un campo. El polinomio $p(x) \in \mathbb{F}[x]$ es irreducible sobre $\mathbb{F}$ si y sólo si $\frac{\mathbb{F}[x]}{(p(x))}$ es un campo.*

Proposición 3. *Si un polinomio es irreducible y divide un producto de polinomios, entonces el polinomio divide a uno de los dos polinomios.*

En los enteros se tiene la definición de primo relativo, de manera similar en $\mathbb{F}[x]$ se tiene la definición de irreducibles relativos.

Teorema A.3. *Sea $\mathbb{F}$ un campo. Para cualesquiera dos polinomios en $\mathbb{F}[x]$ no ambos cero siempre existe un máximo común divisor. Además si $m(x)$ es un máximo común divisor de $p(x)$ y $q(x)$, entonces $m(x) = p(x)\ l_1(x) + q(x)\ l_2(x)$ para algunos polinomios $l_1(x)$ y $l_2(x)$ en $\mathbb{F}[x]$.*

Con el teorema previo se tiene que si $p(x)$ y $q(x)$ en $\mathbb{F}[x]$ son irreducibles relativos, entonces se pueden hallar dos polinomios $r(x),\ s(x) \in \mathbb{F}[x]$ tales que $1 = p(x)\ r(x) + q(x)\ s(x)$.

Definición. Sean $p(x),\ q(x) \in \mathbb{F}[x]$. Diremos que $m(x) \in \mathbb{F}[x]$ distinto del polinomio cero, es un máximo común divisor de $p(x)$ y $q(x)$ si

1. $m(x) \setminus p(x)$ y $m(x) \setminus q(x)$,
2. si $m'(x) \setminus p(x)$ y $m'(x) \setminus q(x)$, entonces $m'(x) \setminus m(x)$.

Teorema A.4. *(Algoritmo de la división) Sea $\mathbb{F}$ un campo y $p(x),\ q(x) \in \mathbb{F}[x]$ con $p(x) \neq o(x)$. Entonces existen polinomios $q(x)$ y $r(x)$ en $\mathbb{F}[x]$ tales que $h(x) = p(x)\ q(x) + r(x)$ con $r(x) = o(x)$ o $grad(r(x)) < gradp(x)$*

El máximo común divisor de dos polinomios no nulos se puede obtener por el algoritmo de Euclides que se puede realizar de manera similar a los enteros.

Teorema A.5. *Sea $\mathbb{F}$ un campo y $p(x) \in \mathbb{F}[x]$. Supongamos que $p(x)$ es irreducuble, entonces $\mathbb{F}[x]/(p(x))$ no tiene divisores de cero.*

Del resultado previo se tiene que si $q(x)$, $r(x) \in \mathbb{F}[x]/(p(x))$ y cumplen que $[q(x)]\ [r(x)] = [p(x)]$ entonces se tiene que $[q(x)] = [p(x)]$ o $[r(x)] = [p(x)]$.

Grupos

Definición. Un *grupo* $(G, *)$ es un conjunto G junto con una operación binaria $*$ en G, tal que satisface los siguientes axiomas:

1. La operación biaria $*$ es asociativa.
2. Existe un elemento $e \in G$, tal que $e * x = x * e = x$, para todo $x \in G$. A este elemento e se le conoce como *elemento identidad.*
3. Para cada g en G existe un elemento $g^{'} \in G$ con la propiedad de que $g^{'} * g = g * g^{'} = e$

Si la operación biaria es conmutativa, se dice que el grupo es *abeliano.* Si G es finito y $g \in G$ definimos el *orden de g* como el mínimo entero m tal que $g^m = e$.

El conjunto de los enteros positivos con la operación suma no es un grupo. Puesto que no existe un elemento identidad.

Definición. Si H es un subconjunto de un grupo G, cerrado bajo la operación de grupo de G y si H es él mismo un grupo bajo esta operación inducida, entonces H es un subgrupo de G.

Teorema A.6. *Un conjunto H de un grupo G es un subgrupo de G si y sólo si*

1. *H es cerrado bajo la operación binaria de G.*
2. *la identidad e de G está en H.*
3. *para cada elemento $h \in G$, se cumple que $h^{-1} \in H$ también.*

Teorema A.7. *Sea G un grupo y a un elemento de G. Entonces*

$$H = \{a^n | n \in \mathbb{Z}\}$$

es un subgrupo de G y es el menor subgrupo de G que contiene a, esto es, cada subgrupo que contiene a contiene H.

Definición. El grupo H del teorema previo es el subgrupo cíclico de G generado por a y se denotará por $< a >$.

Definición. Un elemento a de un grupo G genera G y es un generador de G si $< a >= G$. Un grupo G es cíclico si existe algún elemento a de G que genere G.

Teorema A.8. *Todo grupo ciclico es abeliano.*

Teorema A.9. *Si G es un subgrupo finito multiplicativo del grupo multiplicativo $< F^*, \cdot >$ de los elementos distintos de cero de un campo $\mathbb{F}$, entonces G es cíclico.*

Corolario A.9.1. *El grupo multiplicativo de todos los elementos distintos de cero de un campo finito bajo la multiplicación de un campo es cíclico.*

Definición. Decimos que a y b elementos distintos de cero de un anillo R son *divisores de cero* si $ab = 0$.

Se tiene que la función φ de Euler cuyo valor en n es el número de enteros positivos menores que n que son primos relativos con n.
Para calcular $\varphi(n)$, se pueden utilizar las siguientes propiedades:

1. Si p es un primo, entonces $\varphi(p) = p - 1$.
2. Si p es un primo y $a > 0$ entonces $\varphi(p^a) = (p-1)p^{a-1}$.
3. Si a y b son primos relativos, entonces $\varphi(ab) = \varphi(a)\varphi(b)$.

Teorema A.10. *(Fermat) Si $a \in \mathbb{Z}$ y p es un primo que no divide a, entonces p divide $a^{p-1} - 1$, esto es, $a^{p-1} \equiv a\ 1 \pmod{p}$ para $a \not\equiv 0 \pmod{p}$.*

Corolario A.10.1. *Si $a \in \mathbb{Z}$, entonces $a^p \equiv a \pmod{p}$ para cualquier primo p.*

Bibliografía

[1] R. Anderson. *Security Engineering*. Willey, 2008.

[2] J. M. M. Biosca. Criptografía con curvas elípticas. *C/ Jaume II, 69, 25001-Leida*.

[3] J. A. Buchamann. *Introduction to cryptography*. Serie Undergraduate texts in mathematics. New York, N.Y. Editorial Spring-Verlag, 2001.

[4] J. G. Casas, A. Magidin. Introducción a la criptología. Vínculos matemáticos No. 15, Universidad Nacional Autónoma de México.

[5] I. Connell. Elliptic curve handbook, February 1999.

[6] J. B. Fraleigh. *Algebra abstracta: primer curso*. Mexico, Sitesa, 1988. Traducido de: A first course in abstract algebra, third edition.

[7] A. M. P. Jarama. Alberto Durero historia de las matemáticas, Diciembre 2006.

[8] N. Koblitz. *A course in number theory and cryptography*. Number 114 in Serie Graduate text in mathematics. New York, N.Y. Editorial Spring-Verlag, second edition, 1994.

[9] M. J. L. López. *Criptografía y seguridad en computadores*. Tercera edition, Junio 2001.

[10] A. Menezes, S. Vanstone, N. Koblitz. The state of elliptic curve cryptography. *Kluwer Academic Publisher, Boston*, 2000.

[11] L. M. D. Ordoñez, R. A. V. Villareal, W. F. M. Cantero, J. H. C. Gómez. La estructura de grupo de las curvas elípticas. *Revista Sigma*, IX:20–37, 2009.

[12] I. Peterson. *The Mathematical Tourist*. New York, N. Y. Freeman, 1988.

[13] S. M. H. Rodríguez. Multiplicación escalar en curvas elípticas empleando bisección de punto: una arquitectura de hardware reconfigurable. Departamento de Ingeniería Electronica, Sección de Computación. Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, Ciudad de México, Distrito Federal, Enero 2006.

[14] B. Schneier. *Applied criptography : protocols, algorithms, and source code in C.* The CRC press series on discrete mathematics and its applications. New York, N.Y. Editorial Willey, second edition, 1996.

[15] J. H. Silverman. *The arithmetic of elliptic curves.* Graduate texts in mathematics 106. Springer Dordrecht Heidelberg London New York, 2nd edition, November 2008.

[16] D. R. Stinson. *Cryptography: theory and practice.* Boca Raton, FL, CRC Press, 1995.

[17] H. C. V. Tilborg. *Fundamentals of criptology.* Kluwer Academic Publishers, Boston/Dordrecht/London, 2000.