

Desarrollo de Aplicación Funcional para la Validación de Curvas Elípticas y la Suma Algebraica de Puntos sobre Curvas Elípticas

I.C. Guadalupe Hernández Salmerón¹, Dr. Fidel González Gutiérrez²

Resumen: En este trabajo se presenta primeramente una introducción con los antecedentes y fundamentos matemáticos del álgebra abstracta aplicados a las curvas elípticas definidas mediante una ecuación diofántica o de Weierstrass como $y^2 = x^3 + ax + b$ y sus propiedades algebraicas. Se plantea una metodología para determinar las propiedades aritméticas y algebraicas de las curvas elípticas así como la implementación funcional de tres algoritmos desarrollado en el lenguaje de alto nivel Mathematica©. El primer algoritmo ValidacionParametrosCE verifica el determinante $4a^3 + 27b^2 \neq 0$ con los coeficientes a y b para comprobar que la curva es racional; el segundo algoritmo Suma2PuntosCE calcula la suma de dos puntos $P + Q = R$ sobre la curva elíptica racional y el tercer algoritmo SumakVecesPuntoPCE calcula la suma de k veces un punto P sobre la curva elíptica racional. Los resultados de esta investigación son particularmente significativos ya que proporcionan una implementación eficiente y detallada de tres algoritmos fundamentales en el ámbito del álgebra abstracta y las curvas elípticas, ampliando así la comprensión y las posibles aplicaciones en áreas de alto impacto como la factorización de números compuestos para la generación de llaves públicas y privadas, el proceso de cifrar/descifrar en los sistemas criptográficos y el proceso de crear/validar las firmas digitales los cuales son empleados en la transmisión de información a través del internet. Actualmente las Curvas Elípticas son utilizadas para la generación de llaves públicas y privadas en sistemas criptográficos: sus propiedades algebraicas son aplicadas en diversos algoritmos y estándares de firmas digitales como ECDSA para las firmas digitales de la Bitcoin.

Palabras clave: Problema del logaritmo discreto, curvas elípticas, propiedades algebraicas, suma de puntos, Mathematica©.

Introducción

La Criptografía es el arte y una técnica de crear mensajes codificados con claves secretas con la finalidad de que solamente el destinatario final pueda descifrar el mensaje enviado a través de un canal de comunicación seguro o no seguro (Biddle et al., 2021). La palabra se forma a través del término griego κρυπτός (*kryptós*) que significa oculto y el sufijo *-graphos* que quiere decir escritura, su definición etimológica sería *escritura oculta* (Rouse, 2015).

Existe un problema en teoría de números llamado el problema del logaritmo discreto donde su importancia radica en la obtención de la inversa de la exponenciación en un grupo y que ha tenido su aplicación en los sistemas criptográficos. En el artículo "New directions in Cryptography" publicado en 1976, Whitfield Diffie y Martin E. Hellman presentan las ideas de la criptografía y las firmas digitales de clave pública, que son la base de los protocolos de seguridad más utilizados regularmente en el Internet actual (Diffie & Hellman, 1976). El protocolo Diffie-Hellman protege las comunicaciones por Internet y billones de dólares en transacciones financieras diarias.

En 1978 Ronald Linn Rivest, Adi Shamir y Leonard Adleman desarrollan el sistema criptográfico de llave pública RSA basado en la factorización de números enteros, su funcionamiento se basa en un cifrado asimétrico (Linn Rivest et al., 1978). Posteriormente Taher Elgamal en 1985 propone el esquema del Cifrado ElGamal basado en el problema de Logaritmo Discreto, éste cifrado es aplicado principalmente tanto para generar llaves digitales como para cifrar o descifrar (ElGamal, 1985). En 1986-1987, Victor Miller y Neal Koblitz propusieron de forma independiente las curvas elípticas en la criptografía, donde argumentaban que este método es más eficaz con lo cual la seguridad sería equivalente además que el tamaño de las llaves llega a ser hasta 3 veces menores que los criptosistemas RSA (Koblitz, 1987; Miller, 1986).

La implementación de seguridad en aplicaciones en un ambiente web requiere de sistemas criptográficos que necesitan llaves públicas y privadas para garantizar la confiabilidad y seguridad en las transacciones, por lo que es importante garantizar en este proceso de encriptación-desencriptación un manejo adecuado en recursos de almacenamiento y velocidad de procesamiento lo cual es de suma importancia dentro de la criptografía, ya que la solidez de la seguridad depende del tamaño de la clave. Por tal motivo, la importancia de las curvas elípticas en la criptografía radica en la optimización de espacio y tiempo de procesamiento (Gupta & Rekha, 2021). El uso de curvas elípticas en esta fascinante área de la criptografía va enfocada a la generación de llaves pública y privada usando métodos de factorización eficientes, así como en sistemas para la transmisión de información a través de canales

¹ I.C. Guadalupe Hernández Salmerón es estudiante del programa de Maestría en Ciencias de la Computación de la Facultad de Informática en la Universidad Autónoma de Querétaro, Querétaro, México. ghersal@ieee.org

² Dr. Fidel González Gutiérrez es Profesor de Tiempo Completo en la Facultad de Informática de la Universidad Autónoma de Querétaro, Querétaro, México. fglez@uaq.mx (autor corresponsal).

inseguros. Actualmente se ha investigado sobre las aplicaciones de las curvas elípticas en sistemas criptográficos de llave pública, sin embargo, se sabe que las curvas elípticas son vulnerables en el entorno cuántico (Aggarwal et al., 2018).

En este artículo se presentan las propiedades y operaciones algebraicas realizadas sobre curvas elípticas y su aplicación a los sistemas criptográficos, así como la implementación funcional de operaciones de exponenciación rápida y modulares en curvas elípticas a través del desarrollo de una aplicación en el lenguaje de programación de alto nivel Mathematica®.

Antecedentes

Para comprender mejor los sistemas criptográficos y las firmas digitales es necesario establecer los fundamentos matemáticos sobre las cuales se ha desarrollado este campo de las ciencias de la computación. Las matemáticas de la criptografía moderna se basan especialmente en la teoría de números, álgebra abstracta, probabilidad, estadística y teoría de la información. A continuación, se presentan los conceptos del álgebra abstracta sobre los cuales se desarrolla este estudio: grupos, campos, campos finitos y el problema del logaritmo discreto. Las propiedades de las estructuras algebraicas de grupos y campos contribuyen en la creación de sistemas criptográficos robustos con un grado alto de seguridad y confiabilidad; así mismo, abordar el problema del logaritmo discreto garantiza que las llaves públicas y privadas utilizadas no sean triviales.

Grupos

Los grupos son estructuras algebraicas que tienen propiedades que son compartidas por sistemas matemáticos y tienen aplicación en la criptografía, teoría de códigos y métodos de conteo. Sea G un conjunto no vacío y \circ una operación binaria sobre G , entonces (G, \circ) es llamado un grupo si las siguientes condiciones se satisfacen:

- a) Cerradura de G bajo \circ .

$$\forall a, b \in G, a \circ b \in G \tag{1}$$
- b) Propiedad Asociativa.

$$\forall a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c \in G \tag{2}$$
- c) Elemento Identidad.

$$\exists e \in G \forall a \in G, a \circ e = e \circ a = a \tag{3}$$
- d) Elemento Inverso.

$$\forall a \in G \exists b \in G, a \circ b = b \circ a = e \tag{4}$$

Además, si $\forall a, b \in G, a \circ b = b \circ a$ entonces G es llamado un grupo Abelian o conmutativo en honor al matemático noruego Niels Henrik Abel (Trappe & Washington, 2006).

Campos

Un campo es una estructura algebraica formada por un conjunto F , dos operaciones binarias: adición y multiplicación, así como dos elementos neutros para las operaciones:

- a) Elemento 0: tal que $a + 0 = a$ para todo $a \in F$.
- b) Elemento 1: tal que $a \times 1 = a$ para todo $a \in F$.

Campos Finitos

Se define como un campo sobre un conjunto finito de elementos. Los campos finitos constan de un número $q = p^n$, siendo p un número primo y n un número entero positivo. Se denota el campo finito F_q con $p - 1$ elementos con las operaciones binarias multiplicación y adición módulo p .

Por ejemplo, considere el conjunto $s = \{0, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$ de elementos módulo 7, podemos ver que el conjunto s es un grupo aditivo por el elemento neutro 0 y el elemento unitario 1 también genera un grupo multiplicativo donde el 0 se excluye. Por lo tanto, las dos operaciones pertenecen al campo finito F_7 (Trappe & Washington, 2006).

Problema de Logaritmo Discreto.

El problema establece que se tiene un número primo p y dos enteros diferentes de cero α y β módulos p , estableciendo la siguiente relación modular:

$$\beta \equiv \alpha^x \pmod{p} \tag{5}$$

El problema de encontrar x es llamado el problema del logaritmo discreto. Si n es el entero positivo más pequeño tal que $\alpha^n \equiv 1 \pmod{p}$, se puede asumir que $0 \leq x < n$ y entonces $x = L_\alpha(\beta)$ lo cual define el logaritmo discreto de β con respecto a α (Trappe & Washington, 2006).

Metodología

Material y Equipos

Para llevar a cabo la etapa de experimentación se utilizó un equipo de cómputo Dell Inspiron 14-3467 con un procesador Intel™ Core™ i5-7200U a 2.50GHz, 16GB de RAM y sistema operativo Windows 10. La implementación de los tres algoritmos propuestos en esta investigación se realizaron en el lenguaje de alto nivel *Mathematica*® versión 13 considerando las bondades y ventajas de su paradigma de programación funcional y símbolo, así como la robustez que tiene por el conjunto de funciones implementadas para el procesamiento matemático y de graficación.

Metodología o Procedimiento

El procedimiento general que se utilizó en este trabajo de investigación consistió en los siguientes pasos:

1. Investigación de las propiedades matemáticas de las estructuras algebraicas abstractas de grupos y campos con la finalidad de implementar algoritmos que permitieron comprobar las características de estas estructuras.
2. Determinar las características de los coeficientes de las ecuaciones de Weierstrass que definen las curvas elípticas adecuada para la criptografía a través del cálculo de su determinante.
3. Implementación de un algoritmo para la validación de una curva elíptica adecuada para un sistema criptográfico con base en las características de los coeficientes (Ver Algoritmo 1).
4. Determinar la aritmética relacionada con la operación de suma de dos puntos a través de una recta secante a la curva elíptica.
5. Implementación de un algoritmo para la suma de dos puntos en una curva elíptica con base en la aritmética obtenida (Ver Algoritmo 2).
6. Determinar la aritmética relacionada con la operación de suma de un punto a través de una recta tangente a la curva elíptica.

Implementación de un algoritmo para la suma de un punto en una curva elíptica con base en la aritmética obtenida (Ver Algoritmo 3).

Las características de los coeficientes de las curvas elípticas, así como la aritmética asociada a la suma de dos puntos y un punto sobre la curva elíptica se detallan a continuación:

Coeficientes de Curvas Elípticas y Sumas de Puntos.

Una curva elíptica E sobre un campo F (conocida también como *la ecuación de Weierstrass*) está definida como el conjunto de puntos (x, y) que satisfacen la ecuación:

$$E: y^2 = x^3 + ax^2 + b \quad (6)$$

donde a, b y x son elementos del campo F y existe un punto especial denominado *punto al infinito* denotado por \mathcal{O} . Donde sus coeficientes deben satisfacer el determinante: (Abhishek & Prakash Raj, 2021).

$$4a^3 + 27b^2 \neq 0 \quad (7)$$

En las **Figuras 1 y 2** se presentan las curvas elípticas de las **Ecuaciones 8 y 9** respectivamente, las cuales representan dos curvas elípticas características que tienen una estructura regular.

$$E: y^2 = x^3 - x \quad (8)$$

$$E: y^2 = x^3 - x + 1 \quad (9)$$

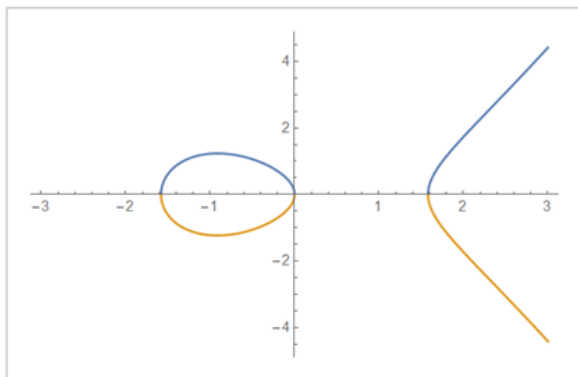


Figura 1. Curva Elíptica $y^2 = x^3 - x$

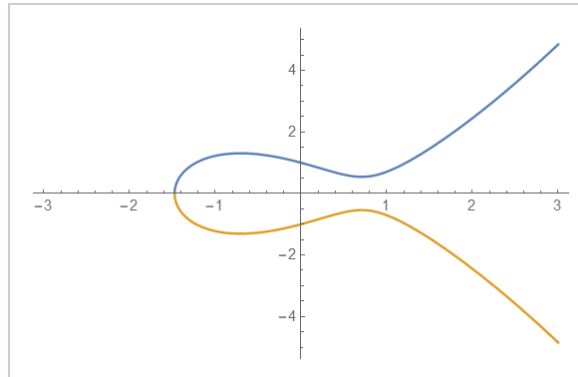


Figura 1. Curva Elíptica $y^2 = x^3 - x + 1$

Para que la curva elíptica sea racional es necesario que se cumpla que el determinante $4a^3 + 27b^2$ sea diferente de 0 para encontrar todos los valores racionales dentro de la curva elíptica. Para las curvas elípticas se define una aritmética especial para dos casos particulares: 1) la suma de dos puntos P y Q sobre la curva elíptica; o bien, 2) la suma de k veces el punto P sobre la curva elíptica.

En el caso particular de la suma de dos puntos P y Q sobre la curva elíptica, los puntos se unen a través de una recta como se puede apreciar en la **Figura 3**. La línea recta se prolonga hasta el punto S donde se vuelve a cortar la curva elíptica, y se trazará una recta vertical hasta el punto R donde vuelve a cortar la curva elíptica, este punto R se define como la suma de P y Q encontrando un punto racional dentro de la curva como se muestra en la **Figura 4**. Si se suma P y Q que estén alineados verticalmente la recta no cortará la curva elíptica en otro punto, lo que determina que se encuentra en un punto neutro de la suma y este tercer punto se define como un punto al infinito \mathcal{O} como se aprecia en la **Figura 5** (Trappe & Washington, 2006).

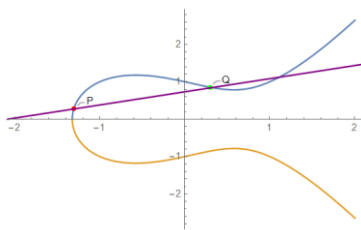


Figura 2. Recta uniendo puntos P y Q .

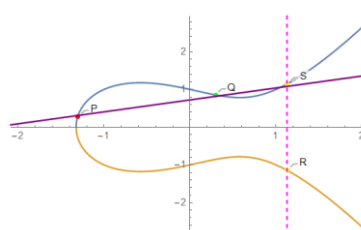


Figura 3. Suma: $P + Q = R$.

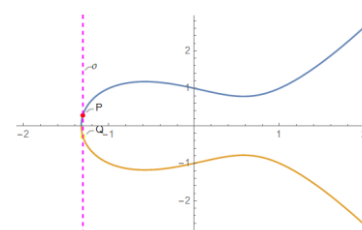


Figura 4. Punto \mathcal{O} de la suma P y Q .

Si sumamos el punto P con el punto \mathcal{O} , esto no cambiará el resultado, esto significa que hay número finito de soluciones para encontrar los puntos racionales dentro de esta curva. Por otro lado, también hay curvas que tienen puntos racionales infinitos. Para determinar cuántos puntos racionales tiene la curva elíptica se considera la siguiente ecuación:

$$E: y^2 = x^3 + ax + b \quad a, b \in \mathbb{Q} \tag{10}$$

Por lo que, el conjunto de todos los puntos racionales dentro de una curva elíptica con la operación suma ya definida tiene estructura de *grupo Abelian* o *grupo Conmutativo* y esto nos lleva a una relación entre la geometría algebraica y teoría de grupos (Trappe & Washington, 2006).

En el caso de sumar dos veces el punto P tenemos el caso particular de $k = 2$. Se tomamos el punto P y se traza una recta tangente para poder encontrar el punto $2P$ véase en la **Figura 6**. Cuando $k = 3$, se suman los puntos P y $2P$ para encontrar $3P$ como se aprecia en la **Figura 7**.

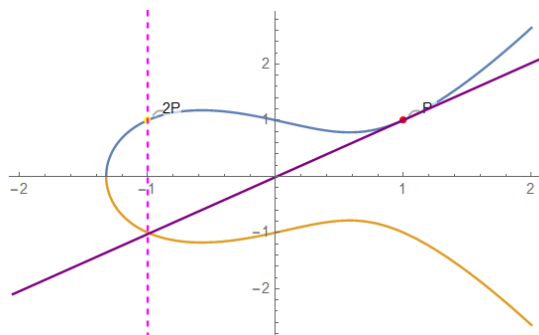


Figura 5. Suma de $P + P = 2P$ trazo de tangente

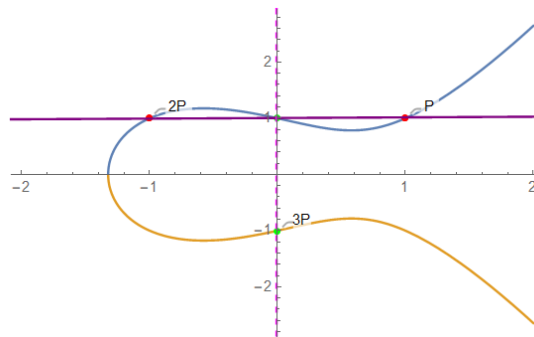


Figura 6. Suma de $P + 2P = 3P$

Resultados y Análisis

Diseño de Algoritmos.

En esta sección se presentan los algoritmos que se diseñaron para llevar a cabo la validación de parámetros, así como el álgebra desarrollada para las curvas elípticas

El **Algoritmo 1:** *ValidacionParametrosCE* recibe como parámetros de entrada los coeficientes a y b para calcular el determinante $4a^3 + 27b^2$, como salida el algoritmo indicara si la curva es racional o no con *True* o *False* respectivamente, así como la gráfica correspondiente.

Algoritmo 1: *ValidacionParametrosCE*

Validar si una Curva Elíptica es Racional o no.

Entrada: Coeficientes a, b

Salida: Aceptar o rechazar los parámetros

1. Calcular $s \leftarrow 4a^3 + 27b^2$
 2. Si $s \neq 0$ mostrar gráfico e indicar que la Curva Elíptica es racional: *True*
 en otro caso mostrar gráfico e indicar que la Curva Elíptica no es racional: *False*.
-

En la **Tabla 1** se muestran cinco casos de validación de coeficientes de curvas, solamente tres coeficientes válidos corresponden a curvas elípticas racionales mientras que dos casos no son curvas elípticas racionales.

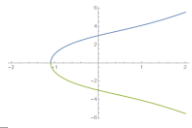
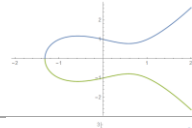
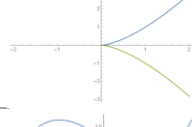

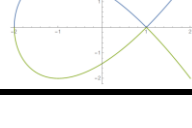
Caso	a	b	Determinante $4a^3 + 27b^2$	¿Curva Racional?	$y^2 = x^3 + ax + b$
1	7	9	3559	True	
2	-1	1	23	True	
3	0	0	0	False	
4	-3	1	-81	True	
5	-3	2	0	False	

Tabla 1. Validación de Coeficientes en Curvas Elípticas.

El **Algoritmo 2**: *Suma2PuntosCE* recibirá como parámetros a , b , P y Q donde a y b son los coeficientes correspondientes a una curva elíptica racional (validados por el **Algoritmo 1**), mientras que P y Q representan los puntos sobre la curva a través de sus coordenadas (x, y) . Se calcula la pendiente de la recta que une los puntos P y Q (Línea 1), posteriormente se calcula la coordenada $\{x_3, y_3\}$ del punto R que corresponde a la suma de los puntos P y Q (Línea 2). El **Algoritmo 2** como salida proporciona el punto R y el gráfico con la suma.

Algoritmo 2: *Suma2PuntosCE*

Calcular el punto $R = \{x_3, y_3\}$ al sumar los puntos $P = \{x_1, y_1\}$ y $Q = \{x_2, y_2\}$

Entrada: Coeficientes a, b y Puntos P, Q

Salida: Representación gráfica de la suma de los puntos P y Q sobre la curva elíptica $y^2 = x^3 + ax + b$.

1. $m \leftarrow \frac{y_2 - y_1}{x_2 - x_1}$
2. $x_3 \leftarrow m^2 - x_1 - x_2, y_3 \leftarrow m(x_1 - x_3) - y_1$
3. $R \leftarrow \{x_3, y_3\}$

En la **Tabla 2** se presentan cinco resultados obtenidos con el Algoritmo 2. Se consideró la curva elíptica racional $y^2 = x^3 - x + 1$ tomando para cada caso dos puntos racionales P y Q sobre la curva elíptica. Se puede observar el resultado de la suma de P y Q en la columna R , así como la gráfica del proceso realizado.

Caso	a	b	P	Q	R	$y^2 = x^3 + ax + b$
1	-1	1	{-1.305, 0.289}	{0.3, 0.853}	{1.128, -1.143}	
2	-1	1	{-1, 1}	{0.4, 0.815}	{2.28, 3.253}	
3	-1	1	{1.314, 1.398}	{-0.706, 1.164}	{-0.594, -1.176}	
4	-1	1	{3, -5}	{0, -1}	{-1.222, -0.6296}	
5	-1	1	{0, 1}	{1.314, 1.398}	{-1.222, -0.629}	

Tabla 2. Suma de Punto P y Q en Curvas Elípticas Racionales.

El **Algoritmo 3**: *SumakVecesPuntoPCE* recibirá como parámetros a , b , k y P ; donde a y b son los coeficientes correspondientes a una curva elíptica racional (validados por el **Algoritmo 1**), mientras que P representa el punto sobre la curva a través de sus coordenadas (x, y) . La variable k representa la cantidad de veces que se sumara el punto P .

La coordenada del punto P se asignan a $\{xc, yc\}$ (Línea 1). Se calcula la pendiente de la recta tangente sobre la coordenada $\{xc, yc\}$ y el coeficiente a (Línea 2). Posteriormente se calcula kP , para el caso particular con la condición $k = 2$ se realiza la suma de $P + P = 2P$ para obtener las coordenadas del tercer punto $\{x3, y3\}$ asignandolas a las coordenadas $\{xc, yc\}$ (Líneas 3-4). Para la suma de kP donde $k > 2$ se inicializa la variable $i \leftarrow 3$ (Línea 5). Mientras que $i \leq k$ se utilizan los puntos $\{x1, y1\}$ y $\{xc, yc\}$ para calcular la pendiente de la línea que une los puntos y posteriormente las coordenadas $\{x3, y3\}$, asignandolas a las coordenadas $\{xc, yc\}$ (Líneas 6-10).

El **Algoritmo 3** como salida arrojará la coordenada al sumar k veces el punto P y el gráfico de la suma de k veces P sobre la Curva Elíptica.

Algoritmo 3: SumakVecesPuntoPCE

Calcular la suma de k veces el punto $P = (x1, y1)$

Entrada: Coeficientes a, b ; cantidad de veces para suma k y Punto P

Salida: Representación gráfica del punto R que corresponde a la suma de k veces P sobre la curva elíptica

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

1. $(xc, yc) \leftarrow (x1, y1)$
2. $m \leftarrow \frac{3(xc)^2 + a}{2(yc)}$
3. $x3 \leftarrow m^2 - 2(xc), y3 \leftarrow m(xc - x3) - yc$
4. $(xc, yc) \leftarrow (x3, y3)$
5. $i \leftarrow 3$
6. Mientras $i \leq k$ hacer
7. $m \leftarrow \frac{yc - y1}{xc - x1}$
8. $x3 \leftarrow m^2 - x1 - xc, y3 \leftarrow m(x1 - x3) - y1$
9. $(xc, yc) \leftarrow (x3, y3)$
10. $i \leftarrow i + 1$

En la **Tabla 3** se muestran los resultados obtenidos por el **Algoritmo 3** para cinco casos de *Suma de k veces P* sobre curvas elípticas racionales.

Caso	a	b	k	P	kP	$y^2 = x^3 + ax + b$
1	-1	1	2	{1, 1}	{-1, 1}	
2	-1	1	3	{1, 1}	{0, -1}	
3	-1	1	4	{1, 1}	{3, -5}	
4	-1	1	5	{1, 1}	{5, 11}	
5	-1	1	6	{1, 1}	{0.25, 0.875}	

Tabla 3. Suma de k veces el punto P en Curvas Elípticas Racionales.

Diseño de Aplicación

En la **Figura 8** se presenta la interfaz de la aplicación desarrollada para calcular el determinante (ver Ecuación 7) de la curva elíptica con sus coeficientes a y b , los cuales son seleccionados a través de menú como se puede observar en la parte superior izquierda de la interfaz. Se puede visualizar en la interfaz: 1) La ecuación diofántica $E: y^2 = x^3 + ax + b$, 2) La validación ¿La Curva Elíptica $y^2 = x^3 - 10x$ es Racional? con los valores de coeficientes $a = -10$ y $b = 0$, 3) La respuesta True y 4) La gráfica de la Curva Elíptica.

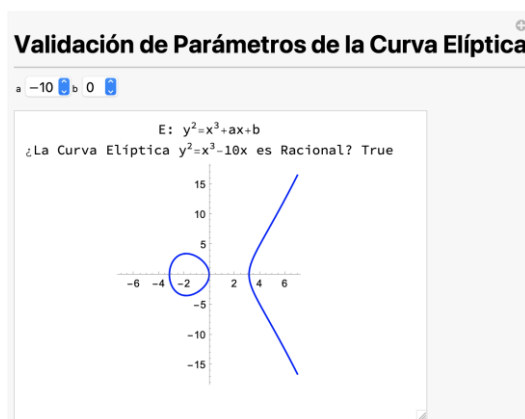


Figura 8. Aplicación de Validación de Parámetros.

En la **Figura 9** se presenta la interfaz de la aplicación desarrollada para calcular la suma de dos puntos P y Q sobre una Curva Elíptica Racional. Los parámetros son seleccionados a través de un menú como se puede observar en la parte superior izquierda de la interfaz, los cuales incluyen los coeficientes a y b , así como las coordenadas de los

puntos P y Q respectivamente. Se puede visualizar en la interfaz para un caso particular: 1) La validación de la Curva Elíptica Racional $E: y^2 = x^3 - x + 1$, 2) Las coordenadas de los puntos $P = \{-1.305, 0.289\}$ y $Q = \{0.3, 0.853\}$, 3) El resultado de la suma de los puntos P y Q a través de las coordenadas del punto $R = \{1.12848, -1.14413\}$ y 4) La gráfica de la Curva Elíptica, las coordenadas de los puntos P, Q y R así como las líneas que se unen los puntos P, Q y R .

En la **Figura 10** se presenta la interfaz de la aplicación desarrollada para calcular la suma de kP sobre una Curva Elíptica Racional. Los parámetros son seleccionados a través de un menu como se puede observar en la parte superior izquierda de la interfaz, los cuales incluyen los coeficientes a y b , el valor de k y las coordenadas del punto P respectivamente. Se puede visualizar en la interfaz para un caso particular: 1) La validación de la Curva Elíptica Racional $E: y^2 = x^3 - x + 1$, 2) El valor de $k = 2$ que corresponde al número de veces que se sumará el punto P , 3) Las coordenadas de los puntos $P = \{1, 1\}$, 3) El resultado de la suma de $2P$ a través de las coordenadas del punto $R = 2P = \{-1, 1\}$ y 4) La gráfica de la Curva Elíptica, las coordenadas de los puntos P y R así como las líneas que se unen los puntos P y R .

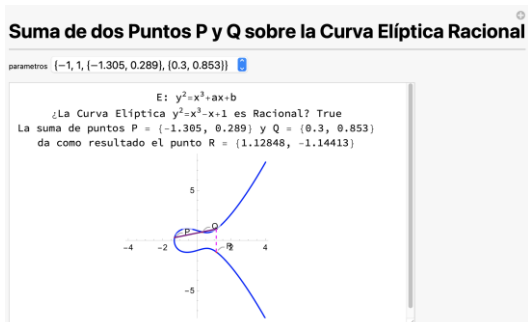


Figura 9. Aplicación de Suma de dos Puntos.

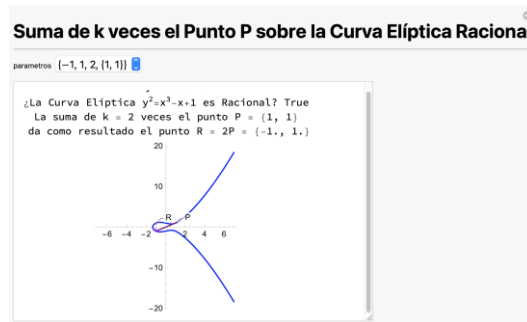


Figura 10. Aplicación de Suma de kP .

Conclusiones

Finalmente, como producto de este trabajo se logro construir tres aplicaciones basados en el desarrollo, implementación, verificación y análisis de resultados de algoritmos de curvas elípticas. Estas aplicaciones desarrolladas para la validación de las curvas elípticas mediante el cálculo de su determinante; así como las las operaciones de suma de dos puntos y de un punto sobre la curva elíptica representan una base importante en los sistemas criptográficos.

Este trabajo tiene un impacto importante en el campo de la criptografía el uso de curvas elípticas puede ser utilizado para la generación de llaves públicas y privadas, desarrollo de sistemas criptográficos para el envío y recepción de información, así como la generación y validación de firmas digital. El desarrollo de aplicaciones que requieren realizar transacciones economicas o simplemente el envío de información confidencial a través del internet requiere de un sistema robusto y confiable como las curvas elípticas por sus propiedades matemáticas sólidas que tiene. El uso de sistemas criptograficos y firmas digitales usando curvas elípticas ha tenido una gran importancia en los últimos años por garantizar la seguridad, mejorar tiempos de procesamiento y menor costo de almacenamiento. Además de esto, la investigación ha revelado una serie de oportunidades para futuros trabajos. En particular, se identificaron varios algoritmos que utilizan curvas elípticas y que podrían ser objeto de futuras investigaciones. Estos incluyen el Algoritmo Baby-Step Giant Step, el Algoritmo Cifrado ElGamal, el Algoritmo para Firma Digital, el Algoritmo de Firma Digital de Curva Elíptica (ECDSA), el Algoritmo de Diffie-Hellman, y el Algoritmo de Massey Omura. Todos estos algoritmos juegan un papel importante en la criptografía moderna y serán cruciales en el diseño de sistemas seguros para la transmisión de información en el futuro.

El presente trabajo se limita a la validación de curvas elípticas y a las operaciones de suma con uno y dos puntos sobre la curva elíptica lo cual representa la base para la generación de llaves públicas y privadas mediante la factorización de números compuestos así como el cifrado/decifrado de información y la creación/validación de firmas digital. Considerando la fundamentación matemática sobre las cuales se construyeron estos algoritmos una limitación era la elección del lenguaje de programación para desarrollarlo, finalmente el lenguaje Mathematica® ofrece un conjunto de instrucciones para este proposito debido a el paradigma funcional y símbolo que utiliza. La disponibilidad de recursos computacionales es un factor determinante, ya que el rendimiento y la eficiencia de los algoritmos criptográficos a menudo dependen en gran medida de la capacidad de procesamiento y la memoria disponible. La naturaleza altamente especializada y técnica de este campo de estudio es más amplia por lo que se seguirá trabajando en algoritmos de encriptación/descriptación, así como creación/validación de firmas digitales. Las pruebas de

experimentación realizadas se hicieron sobre computadoras portátiles, una alternativa sería realizarla sobre tarjetas embebidas como Raspberry Pi u Orange Pi con la finalidad de verificar el funcionamiento en sistemas que cuentan con menores recursos. En los últimos años ha sido de gran interés el desarrollo de aplicaciones en el campo del IoT (Internet de las Cosas), como trabajo a futuro se pretende emplear algoritmos de encriptación/descriptación basados en curvas elípticas para la transmisión de información utilizando una red de sistemas embebidos.

Referencias

- Abhishek, K., & Prakash Raj, E. G. D. (2021). *Computation of Trusted Short Weierstrass Elliptic Curves for Cryptography*. *21(2)*, 71–88.
- Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (2018). Quantum Attacks on Bitcoin, and How to Protect Against Them: Open Review. *Ledger*, *3*, 68–90. <https://doi.org/10.5915/LEDGER.2018.127>
- Biddle, G., McGoldrick, L., & Halamek, J. (2021). Non-traditional encryption methods: Moving toward electrochemical cryptography. *Electrochemical Science Advances*, 1–7. <https://doi.org/https://doi.org/10.1002/elsa.202100188>
- Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography Invited Paper. *IEEE Transactions on Information Theory*, *IT-22(6)*, 644–654.
- ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *Advances in Cryptology*, 10–18. https://doi.org/10.1007/3-540-39568-7_2
- Gupta, R., & Rekha. (2021). Elliptic Curve Cryptography based Secure Image Transmission in Clustered Wireless Sensor Networks. *International Journal of Computer Networks and Applications*, *8(1)*, 67–78. <https://doi.org/10.22247/ijcna/2021/207983>
- Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics Of Computation*, *48(177)*, 203–209. <https://doi.org/10.1090/S0025-5718-1987-0866109-5>
- Linn Rivest, R., Shamir, A., & Adleman, L. (1978). Programming Techniques A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *21(2)*, 120–12. <https://doi.org/10.1145/359340.359342>
- Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. *Advances in Cryptology --- CRYPTO '85 Proceedings*, 417–426. https://doi.org/10.1007/3-540-39799-X_31
- Rouse, M. (2015). *What is cryptography? - Definition from WhatIs.com*. TechTarget. <http://searchsoftwarequality.techtarget.com/definition/cryptography>
- Trappe, W., & Washington, L. C. (2006). *Introduction to Cryptography with Coding Theory* (Pearson Education. Inc., Ed.; 2nd ed.).

Notas Biográficas

La **I. C. Guadalupe Hernández Salmerón** es estudiante del programa de Maestría en Ciencias de la Computación de la Facultad de Informática en la Universidad Autónoma de Querétaro. Terminó sus estudios de licenciatura en Ingeniería en Computación en la Facultad de Informática en la Universidad Autónoma de Querétaro. Es miembro de IEEE.

El **Dr. Fidel González Gutiérrez** obtuvo su Doctorado en Ciencias de la Computación y su Maestría en Ciencias Computacionales en Sistemas Distribuidos por la Universidad Autónoma de Querétaro y su Ingeniería en Sistemas Computacionales por el Instituto Tecnológico de Querétaro. Es profesor titular a tiempo completo en la Facultad de Informática de la Universidad Autónoma de Querétaro, donde enseña a nivel licenciatura y posgrado. Su línea de investigación está orientada a problemas de optimización y criptografía. Es miembro de ACM e IEEE (IEEE Computer Society y IEEE Intelligent Systems Society).