

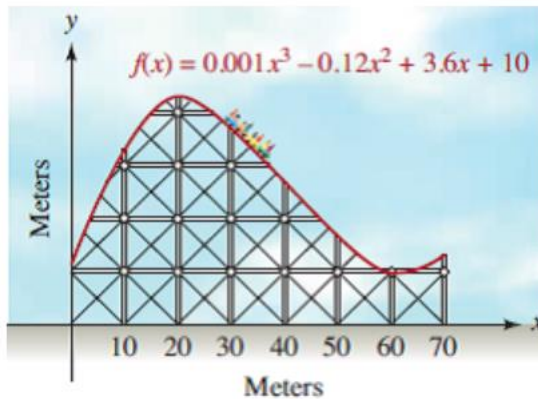


FORMATO DE PLANEACIÓN

Estrategia didáctica

DATOS GENERALES

Nombre del participante	Mario Alberto Terrés Palacios
Asignatura	Matemáticas IV
Año o semestre en que imparte	Cuarto semestre
Horas clase a la semana	5 horas
Unidad	Unidad 2. Funciones racionales y funciones con radicales
Aprendizajes	Resuelve problemas de aplicación (función con radicales)
Problemática que se abordará a través del problema.	Implementar un mecanismo de autenticación con firma digital mediante el uso de una curva elíptica
Justificación. (porque considera que el programa en python o Julia puede apoyar al alumno a entender o lograr el aprendizaje)	<i>La aplicación de las funciones polinomiales (en esta secuencia una función con radical como lo es una curva elíptica) son variados y se utilizan para resolver muchos problemas en otras ciencias, por mencionar los siguientes:</i> <i>-En construcción, ingeniería civil y arquitectura</i>



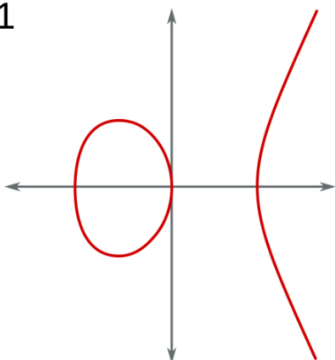
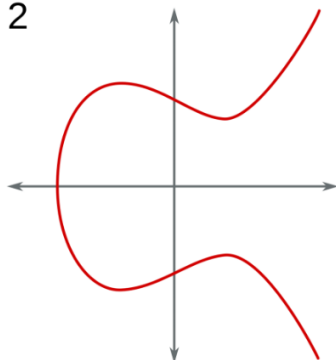
Diseñando una montaña rusa con
polinomios

-En Ingeniería forestal, por ejemplo, necesitamos la geometría para calcular áreas, pero también los polinomios en problemas como calcular cuántos árboles necesitamos replantar después de haber talado una zona de un bosque.

-El uso de polinomios en el área de la salud es amplio, desde el cálculo de las dosis más adecuadas de un medicamento, o el peso de un paciente enfermo en función del tiempo. Por poner solo un ejemplo, si queremos modelizar el ritmo circadiano en pacientes con hipertensión, buscamos la curva que mejor se adapte a nuestros datos, en este caso un polinomio de grado cuatro, lo que nos permite optimizar las dosis del medicamento contra la hipertensión.

-Finalmente, las curvas elípticas son usadas en criptografía, y no son más que expresiones polinómicas en dos variables, que también se pueden expresar como funciones con radicales, tal y como muestran estos dos ejemplos:






	<div><div><div>1</div>$y^2 = x^3 - x$</div><div><div>2</div>$y^2 = x^3 - x + 1$</div></div> <div><div>1.-</div>$y = \sqrt{x^3 - x}$</div> <div><div>2.-</div>$y = \sqrt{x^3 - x + 1}$</div> <p><i>Que es el problema de aplicación que utilizaremos para ejemplificar al alumno</i></p>
--	---

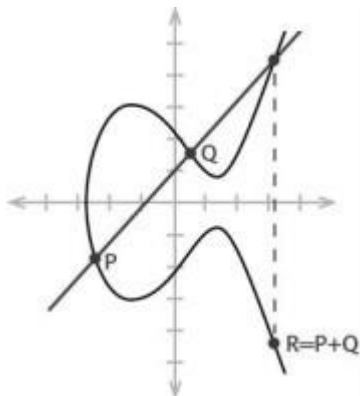


	<ul style="list-style-type: none">• Película o video• Lista de cotejo para evaluar el desarrollo del proyecto, a manera de cronograma, para apoyar en el seguimiento del mismo.
Tiempos de realización.	

Secuencia didáctica (Sesión 1)

	Presentación del problema a resolver Se requiere ilustrar al alumno una aplicación de las funciones con radicales, en este caso será con el uso de una curva elíptica usada como mecanismo de autenticación por firma digital como el que usa la secretaria de hacienda y crédito público para hacer sus declaraciones anuales, las criptomonedas como bitcoin y el SIAE usado por los profesores para registrar las calificaciones de los estudiantes
	Inicio de la Sesión (20 min) El profesor inicia con una pregunta detonadora cuestionando a los alumnos cuales son las aplicaciones de las funciones polinomiales en la vida real, para posteriormente indicarles que las curvas elípticas se utilizan en campos de la computación como la criptografía.
	Desarrollo de la sesión (80 min) Con sus conocimientos previos, el alumno compondrá que una curva elíptica es un conjunto de puntos regidos por una operación. $y^2 = x^3 + ax + b$ (forma general de una curva elíptica)

Secuencia didáctica (Sesión 1)



$$P(x_1, y_1)$$

$$Q(x_2, y_2)$$

$$R(x_3, y_3)$$

En el caso de la curva elíptica es una suma, pero no una suma aritmética sino una suma como la ilustrada en la imagen.

El alumno intentará, y con la guía del profesor, obtener las fórmulas para calcular la suma de dos puntos de una curva elíptica partiendo del siguiente sistema de ecuaciones:

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

$$y = mx + p$$

Y obtener las siguientes fórmulas:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - x_2 - x_1$$

$$y_3 = \lambda(x_3 - x_1) - y_1$$

Una vez entendido y obtenido este conocimiento se procede a entender las congruencias obtenidas con un entero primo módulo una curva elíptica $y^2 \equiv x^3 + ax + b \pmod{p}$. Con el siguiente ejemplo:

$$y^2 \equiv x^3 + 2x + 2 \pmod{17}$$



Secuencia didáctica (Sesión 1)

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
y ²	0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225	256	289	324	361
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x ³	0	1	8	27	64	125	216	343	512	729	1000	1331	1728	2197	2744	3375	4096	4913	5832	6859
2x + 2	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
x ³ 2x + 2	2	10	26	50	82	122	170	226	290	362	442	530	626	730	842	962	1090	1226	1370	1522

x	y
5	1
3	1
6	3
16	4
16	13
0	11
0	6
6	14
3	16
13	7
7	11
7	6
9	1
5	16
10	11

Se comprobarán los resultados explicados por el profesor con el notebook incluido en los anexos de la estrategia



Cierre de la sesión (20 min)

Los alumnos realizarán en equipo un resumen con los conocimientos adquiridos en esta sesión para entregarla posteriormente.



Evaluación

Resumen



Evaluación

Actividad a evaluar

Puntaje



Secuencia didáctica (Sesión 1)

El resumen cuenta con los temas de introducción	2
El resumen cuenta con los temas de desarrollo	2
Los cálculos vienen explícitos en el trabajo	3
El trabajo cuenta con ejemplos claros y conclusiones	3
Total	



Referencias

[Los múltiples usos prácticos de los polinomios - Matemáticas y sus fronteras \(madrimasd.org\)](http://madrimasd.org)

Secuencia didáctica (Sesión 2)



Presentación del problema a resolver

Se requiere ilustrar al alumno una aplicación de las funciones con radicales, en este caso será con el uso de una curva elíptica usada como mecanismo de autenticación por firma digital como el que usa la secretaria de hacienda y crédito público para hacer sus declaraciones anuales, las criptomonedas como bitcoin y el SIAE usado por los profesores para registrar las calificaciones de los estudiantes

Inicio de la Sesión (10 min)

Secuencia didáctica (Sesión 2)



Con los conocimientos adquiridos en la sesión pasada resolverá con guía del profesor un ejemplo de cifrado con curva elíptica propuesto por el profesor. Antes de iniciar el desarrollo los alumnos deben externalizar todas sus dudas al profesor.

El profesor propone y explica un ejemplo de autenticación con curva elíptica y protocolo de intercambio de claves Diffie-Hellman con la siguiente curva:

$$y^2 \equiv x^3 + 2x + 2 \pmod{17}.$$

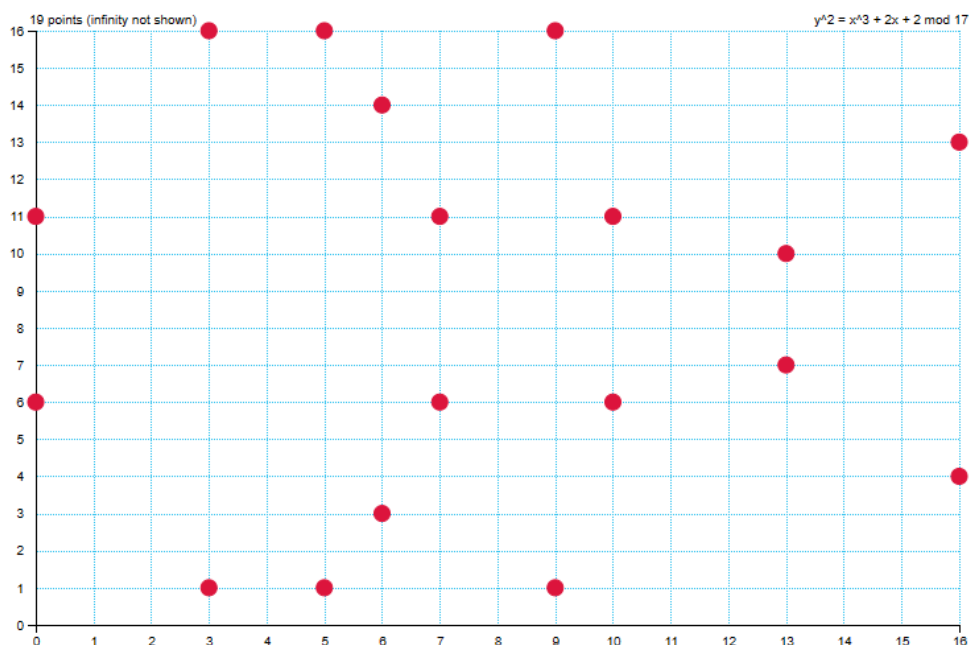


Desarrollo de la sesión (50 min)

Explica conceptos como el punto generador de la curva, orden de la curva y el inverso multiplicativo modular para el desarrollo de este ejemplo.

Con ayuda de un software en línea ([Elliptic Curves over Finite Fields \(grau.de\)](https://grau.de)) se obtienen los puntos obtenidos de la curva propuesta

Draw the elliptic curve $y^2 = x^3 + ax + b \pmod{r}$, where a b r





Secuencia didáctica (Sesión 2)

Point Detail

Point:	(5,1)
Inverse:	(5,16)
Order of subgroup:	19
Generated subgroup:	(5,1) → (6,3) → (10,6) → (3,1) → (9,16) → (16,13) → (0,6) → (13,7) → (7,6) → (7,11) → (13,10) → (0,11) → (16,4) → (9,1) → (3,16) → (10,11) → (6,14) → (5,16) → ∞

Al ser de orden primo cualquier punto puede ser generador, en caso de no ser de orden primo el generador se puede encontrar con la ayuda de este recurso online.

Con ayuda de las siguientes fórmulas y las obtenidas en la sesión anterior el profesor comprueba los resultados arrojados por el software.

$$\lambda = \frac{3x_G^2 + a}{2y_G}$$

$$x_2 = \lambda^2 - 2x_G$$

$$x_2 = \lambda (x_G - x_2) - y_G$$

Nota: Estas fórmulas no se demuestran solo se proponen

Se propone como generador el punto G (5,1) y se calcula el punto $2G = G + G$. El profesor aclara que en el dominio de los números enteros no existen número fraccionarios por lo tanto se debe calcular el inverso multiplicativo modular para expresar las divisiones en el dominio de los números enteros: El profesor explica el procedimiento para calcular el inverso multiplicativo modular usando el algoritmo extendido de Euclides para el M.C.D. y se comprueban los resultados con un software propuesto por el profesor ([Wolfram|Alpha Widgets: "Modular Multiplicative Inverse" - Free Mathematics Widget \(wolframalpha.com\)](#)).



Secuencia didáctica (Sesión 2)

$$s = \frac{3x_G^2 + a}{2y_G}$$

$$s \equiv \frac{3(5^2) + 2}{2(1)} \equiv 77 \cdot 2^{-1} \equiv 9 \cdot 9 \equiv 13 \pmod{17}$$

$$x_{2G} = s^2 - 2x_G$$

$$x_{2G} \equiv 13^2 - 2(5) \equiv 16 - 10 \equiv 6 \pmod{17}$$

$$y_{2G} = s(x_G - x_{2G}) - y_G$$

$$y_{2G} \equiv 13(5 - 6) - 1 \equiv -13 - 1 \equiv -14 \equiv 3 \pmod{17}$$

Obteniendo $2G$ (6,3) corroborando lo obtenido con el software. El alumno calculará el punto $3G = 2G + G$. Se enlistan los puntos obtenidos en esta curva obtenidos por el software y comprobados por los cálculos.

$G = (5, 1)$	$11G = (13, 10)$
$2G = (6, 3)$	$12G = (0, 11)$
$3G = (10, 6)$	$13G = (16, 4)$
$4G = (3, 1)$	$14G = (9, 1)$
$5G = (9, 16)$	$15G = (3, 16)$
$6G = (16, 13)$	$16G = (10, 11)$
$7G = (0, 6)$	$17G = (6, 14)$
$8G = (13, 7)$	$18G = (5, 16)$
$9G = (7, 6)$	$19G = \mathcal{O}$
$10G = (7, 11)$	

El profesor explica cómo se cifra con los puntos obtenidos por la curva elíptica con el siguiente ejemplo:

Secuencia didáctica (Sesión 2)

<p>Bob</p>	<p>Eve</p>	<p>Alice</p>
<p>Bob picks</p> $\beta = 9$ <p>Computes</p> $B = 9G = (7, 6)$ <p>Receives</p> $A = (10, 6)$ <p>Computes</p> $\beta A = 9A = 9(3G) = 27G = 8G = (13, 7)$	$y^2 \equiv x^3 + 2x + 2 \pmod{17}$ $G = (5, 1)$ $n = 19$ $A = (10, 6)$ $B = (7, 6)$	<p>Alice picks</p> $\alpha = 3$ <p>Computes</p> $A = 3G = (10, 6)$ <p>Receives</p> $B = (7, 6)$ <p>Computes</p> $\alpha B = 3B = 3(9G) = 27G = 8G = (13, 7)$



Cierre de la sesión (50 min)

Se solicita a los alumnos hacer equipos de 2 a 5 personas

Con los conocimientos adquiridos y en equipos resuelve el siguiente cuestionario final.

Anexa los conocimientos adquiridos en esta sesión en su trabajo de investigación de la primera sesión, así como el cuestionario final.

Considere la siguiente curva elíptica:

$$y^2 \equiv x^3 + 7 \pmod{17}$$

Con ayuda de sus conocimientos adquiridos y el software recomendado llene la siguiente tabla y conteste las preguntas:

G	10G (1,12)
2G	11G (10,15)
3G (8,14)	12G (5,8)
4G (12,16)	13G (6,6)
5G (6,11)	14G (12,1)
6G	15G (8,3)
7G (10,2)	16G (2,10)



Secuencia didáctica (Sesión 2)

8G (1,5)

17G

9G (3,0)

18G (0)

¿Todos los puntos pueden ser generadores para esta curva elíptica?

¿Por qué?

¿Cuál es el punto generador para esta curva elíptica?

¿Cuál es el orden de la curva?

Compruebe los puntos arrojados (G, 2G, 6G y 17G) por el software [Elliptic Curves over Finite Fields \(graui.de\)](https://graui.de/elliptic-curves-over-finite-fields/) con lo visto en clase (agregue los cálculos)

II. Implemente a mano un cifrado de clave privada Diffie-Hellman con la curva elíptica de este ejercicio.

Comprobar los resultados con el notebook proporcionado por el profesor

Nota: Si necesita calcular el inverso multiplicativo modular vaya a la siguiente página: [Wolfram|Alpha Widgets: "Modular Multiplicative Inverse" - Free Mathematics Widget \(wolframalpha.com\)](https://www.wolframalpha.com/widget/widget.jsp?math=modular+multiplicative+inverse)

Comprobar el mecanismo de autenticación por firma digital con un software proporcionado por el profesor (JULNAM)



Evaluación



Secuencia didáctica (Sesión 2)



Cuestionario



Evaluación

Actividad a evaluar	Puntaje
Contesto correctamente las preguntas justificando sus respuestas	2
Los cálculos vienen explícitos en el trabajo	3
Comprobó los resultados con el software proporcionado por el profesor	3
Comprobar el mecanismo de autenticación por firma digital con un software proporcionado por el profesor (JULNAM)	2
Total	



Referencias

[Elliptic Curves over Finite Fields \(grau.de\)](http://grau.de)

[Elliptic Curve Diffie Hellman - YouTube](#)