

República Dominicana
UNIVERSIDAD TECNOLÓGICA DEL CIBAO ORIENTAL
Universidad Patrimonio de la Comunidad



Facultad de Postgrado y Educación Continuada
Departamento de Postgrado

Trabajo de Postgrado para Optar por el Título de
Maestría en Matemática.

Título

Análisis avanzado de curvas elípticas complejas

Sustentante

Keury Jesús Emiliano González

Asesor

Dr. Manuel Aurelio Diloné

Cotuí, Provincia Sánchez Ramírez

Año académico, 2024.

TÍTULO

ANÁLISIS AVANZADO DE CURVAS ELÍPTICAS COMPLEJAS

Declaración de Autoría

Los conceptos emitidos en la investigación, son responsabilidad exclusiva del sustentante del mismo. Las citas y las consultas bibliográficas se han incluido respetando el derecho de autor.

Keury Jesús Emiliano González

Título

Análisis avanzado de curvas elípticas complejas

Tesis presentada por **Keury Jesús Emiliano González** para la obtención del grado de Magister en Matemáticas.

Composición del tribunal evaluador

Jurado de metodología

Jurado de contenidos

Jurado de redacción

Lic. Yuderka Reyes

Directora de postgrado

CALIFICACIÓN FINAL:_____

Índice general

Declaración de autoría	III
Agradecimientos	VI
Dedicatorias	VII
Resumen	VIII
CAPÍTULO I: INTRODUCCIÓN	1
1.1. Introducción	1
1.2. Antecedentes	1
1.2.1. Antecedentes históricos	1
1.2.2. Antecedentes académicos	4
1.3. Planteamiento del problema	6
1.4. Justificación	7
1.5. Objetivos	8
1.5.1. Objetivo general	8
1.5.2. Objetivos específicos	8
1.6. Alcances y límites	9
CAPÍTULO II: MARCO REFERENCIAL	10
2.1. Introducción	10
2.2. Marco teórico	10
2.2.1. Retículos y toros complejos en el análisis matemático de curvas elípticas	10
2.2.2. Funciones de Weierstrass	13
2.2.3. Isogenias complejas y las funciones modulares	16
CAPÍTULO III: METODOLOGÍA	19
3.1. Introducción	19
3.2. Diseño de investigación	19
3.3. Tipo de investigación	19
3.4. Método de investigación	20

3.5. Procedimiento de investigación	20
CAPÍTULO IV: PRESENTACIÓN DE LOS RESULTADOS	21
4.1. Introducción	21
4.2. Retículos y toros complejos	21
4.3. Funciones de Weierstrass en curvas elípticas complejas	25
4.4. Isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas	28
CAPÍTULO V: CONCLUSIONES	31
5.1. Introducción	31
5.2. Conclusiones finales	31
5.3. Líneas futuras de investigaciones	32
Referencias	33
Anexos	I
Anexo A. Simbología	II
Anexo B. Cronograma	III

Agradecimientos

A Dios, por brindarme la bendición de la salud y la vida, permitiéndome concluir mis estudios de maestría.

Al Ministerio de Educación Superior, Ciencia y Tecnología (MESCYT), por confiar en mí y en mis capacidades, otorgándome la beca para cursar este programa de maestría en matemáticas. Gracias a esta oportunidad, he podido fortalecer mis competencias profesionales y contribuir a una mejor calidad en la educación preuniversitaria dominicana. Que Dios colme de bendiciones a todos los que hicieron posible este proceso en el periodo 2022-2024.

A la Universidad Tecnológica del Cibao Oriental (UTECO), por su compromiso con el avance y la formación en las ciencias matemáticas. Agradezco especialmente que me hayan abierto sus puertas una vez más para realizar este estudio de posgrado.

A los maestros, por sus valiosos aportes y motivación para lograr esta meta. Y, por último, al asesor de tesis, Dr. Manuel Diloné, por su constante motivación y acompañamiento para culminar exitosamente este programa.

Dedicatorias

A mis padres, por concederme la vida, y en especial a mi madre, Martha González García, por su apoyo incondicional y por estar siempre a mi lado en los momentos más difíciles. Espero que Dios te conceda una larga vida y salud para que podamos seguir celebrando muchos logros juntos.

A mi padrastro, Juan Francisco Castro Bueno, por ser un padre para mí y por estar siempre cuando más lo he necesitado, brindándome todo su apoyo. Que Dios te colme de vida y salud.

A toda mi familia, especialmente a mis hermanos Jeury Jesús Emiliano González y Fernando Luis Castro González; a mis primas Biaribel Aquino, Diani Reyes, Birmania Aquino y Ramona del Carmen García; y a mis tías Maria del Carmen González, María González y Araceli González, por brindarme su apoyo cuando más lo necesité.

A mis compañeros de estudios, por ser un gran soporte y apoyo durante todo este arduo proceso. En especial, a mi equipo de trabajo: Carmela Adames, Dania Santos, Walner Ramos, Maireni Heredia, Ana Mercedes Manzueta Amparo, Wandry Monegro, Ana Mercedes Lanfranco y Maryellin.

Al coordinador de la maestría, M.A. Efraín Martínez, quien inició el programa con motivación y empatía hacia cada uno de los participantes. También, al M.A. Arismendy Batista, quien concluyó la coordinación en un momento crucial. Muchas gracias a ambos por su ardua e incansable labor.

República Dominicana

UNIVERSIDAD TECNOLÓGICA DEL CIBAO ORIENTAL



Maestría en Matemática

Análisis avanzado de curvas elípticas complejas

Keury Jesús Emiliano González

Sustentante

Dr. Manuel Aurelio Diloné

Asesor

RESUMEN

Este estudio se propuso analizar las curvas elípticas complejas bajo la influencia de los retículos y toros complejos, sus propiedades y las funciones de Weierstrass. Para lograr esto, se establecieron tres objetivos específicos: Analizar la influencia de los retículos y toros complejos en el análisis matemático de curvas elípticas, analizar en el estudio de las propiedades esenciales de las curvas elípticas complejas a través del análisis de las funciones de Weierstrass y caracterizar las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas.

En cuanto a la metodología, se empleó un diseño no experimental y transversal con un enfoque analítico y descriptivo. La investigación fue clasificada como descriptiva, exploratoria y explicativa. Se utilizó un método deductivo que incluyó la revisión de literatura, la estructuración del contenido, la búsqueda de información en universidades y la orientación del asesor.

En base al estudio de los toros y retículos complejos, se concluyó que estos retículos, definidos como combinaciones lineales enteras de dos vectores complejos linealmente independientes, junto con la función elíptica de Weierstrass, fueron esenciales para la descripción de curvas elípticas. La adición de puntos en estas curvas se simplifica mediante una fórmula específica, donde se utilizan propiedades especiales

de los retículos para determinar puntos en el plano complejo.

En cuanto al estudio de las funciones de Weierstrass en curvas elípticas complejas, se enfatizó su papel fundamental en la teoría y la geometría algebraica. Estas funciones, periódicas y esenciales para describir curvas elípticas, se ilustraron en ejemplos específicos que mostraron cómo facilitan la suma de puntos en la curva elíptica.

En el ámbito de las curvas elípticas complejas, el análisis de las isogenias complejas y las funciones modulares asociadas reveló conexiones significativas entre las curvas definidas por ecuaciones de Weierstrass. Se exploró cómo las isogenias, que son homomorfismos entre variedades algebraicas, modifican los invariantes de las funciones correspondientes, y se examinaron las propiedades como los polos y residuos de estas funciones en diferentes curvas elípticas.

Palabras clave: Retículos, toros complejos, curvas elípticas, funciones de Weierstrass, isogenias complejas, funciones modulares.

CAPÍTULO I

INTRODUCCIÓN

1.1. Introducción

En este capítulo se presenta el desarrollo histórico del análisis avanzado de curvas elípticas complejas. Se abordan los principales hitos y avances en la teoría de curvas elípticas, destacando su importancia en la criptografía moderna y la teoría de números. Se expone el planteamiento del problema de estudio, justificando la investigación en función de sus aplicaciones prácticas y teóricas. Además, se detallan los objetivos específicos, el alcance de la investigación, y los límites que se han definido para garantizar la precisión y relevancia de los resultados obtenidos.

1.2. Antecedentes

1.2.1. Antecedentes históricos

El estudio de las curvas elípticas tiene una larga e intrigante historia que se remonta a la antigua Grecia (siglo IV a. C.). Aunque las curvas elípticas no se mencionan explícitamente en los trabajos matemáticos griegos, su estudio se puede vincular a algunos de sus conceptos y problemas.

Las curvas elípticas tienen una historia rica que se extiende a lo largo de varios siglos (Pujol, 1896). En el siglo XVII, matemáticos como René Descartes y Pierre de Fermat sentaron las bases de la geometría analítica y las ecuaciones algebraicas, esenciales para el desarrollo posterior de las curvas elípticas. John Wallis, en 1655, fue uno de los primeros en explorar las propiedades de las curvas cúbicas, y en los años 1670, Isaac Newton investigó las raíces de las ecuaciones cúbicas, clasificando algunas de las curvas que más tarde se conocerían como elípticas. (Hawking y Ortuño, 1988).

En el siglo XVIII, Leonhard Euler avanzó en la comprensión de las integrales elípticas, mientras que Joseph-Louis Lagrange estudió las propiedades de estas curvas en el contexto de la teoría de números (Andradas, 1999). En el siglo XIX, Carl

Friedrich Gauss, en su obra *Disquisitiones Arithmeticae*, estableció conexiones importantes entre las curvas elípticas y la aritmética modular. A principios del siglo XIX, Niels Henrik Abel y Carl Gustav Jacob Jacobi desarrollaron independientemente la teoría de las funciones elípticas, formulando conceptos que serían fundamentales para la teoría moderna de las curvas elípticas.

En el siglo XX, André Weil contribuyó significativamente a esta teoría a través de sus trabajos sobre geometría algebraica y teoría de números. La criptografía de curva elíptica, desarrollada en los años 1980 por Neal Koblitz y Victor S. Miller, destacó la relevancia práctica de estas curvas en la seguridad digital moderna. (Alvarez, 2000).

Aritmética de Diofanto

Las primeras semillas del estudio de las curvas elípticas se encuentran en la obra de Diofanto de Alejandria, un matemático griego del siglo III a. C. En su tratado *Aritmética*, Diofanto exploró soluciones racionales a ecuaciones diofánticas, es decir, ecuaciones polinomiales con coeficientes y soluciones enteras. Aunque Diofanto no consideraba específicamente las curvas elípticas, su trabajo sobre ecuaciones de segundo grado sentó las bases para el desarrollo posterior de la teoría de las curvas elípticas. (Cid, 2000).

Geometría proyectiva

La geometría proyectiva, desarrollada en el siglo XVII por matemáticos como Girard Desargues y Blaise Pascal, proporcionó un marco conceptual importante para el estudio de las curvas elípticas. Esta rama de la geometría introduce el concepto de un punto infinito para completar la recta proyectiva, lo que resulta crucial para comprender la estructura de las curvas elípticas. (Gine, 2001).

Pierre de Fermat y el último Teorema de Fermat

Las curvas elípticas cobraron mayor protagonismo en el siglo XVII gracias al trabajo de Pierre de Fermat, un abogado y matemático francés. En 1637, Fermat anotó en el margen de su copia de la Aritmética de Diofanto la famosa conjetura que ahora se conoce como el último Teorema de Fermat. Aunque la prueba formal del teorema no se lograría hasta siglos después, la formulación de Fermat involucró soluciones a ecuaciones de Fermat de tercer grado, que están estrechamente relacionadas con las curvas elípticas. (Vera, 2002).

Descartes y la ecuación de las curvas elípticas

René Descartes, un filósofo y matemático francés del siglo XVII, sentó las bases para la representación analítica de las curvas elípticas mediante ecuaciones. En su obra Geometría, Descartes introdujo el sistema de coordenadas cartesianas, lo que permitió expresar curvas geométricas como ecuaciones polinomiales. La ecuación general de una curva elíptica, una ecuación cúbica de la forma $y^2 = x^3 + ax + b$, se deriva del trabajo de Descartes. (Urbaneja, 2003).

Desarrollos posteriores

A lo largo de los siglos XVIII y XIX, las curvas elípticas continuaron atrayendo la atención de matemáticos prominentes como Leonhard Euler, Joseph Louis Lagrange y Carl Friedrich Gauss. Estos matemáticos profundizaron en las propiedades matemáticas de las curvas elípticas, sentando las bases para el trabajo teórico posterior. (Robinson, 2003).

Siglo XX y más allá

En el siglo XX, las curvas elípticas experimentaron un resurgimiento de interés debido a su aplicación en áreas como la criptografía y la teoría de números. La complejidad de la estructura de las curvas elípticas las hace ideales para crear algoritmos criptográficos resistentes a las intrusiones. Además, las curvas elípticas han desempe-

ñado un papel fundamental en la demostración del último Teorema de Fermat por parte de Andrew Wiles en 1994.

El estudio de las curvas elípticas sigue siendo un área activa de investigación matemática en la actualidad. Los matemáticos continúan explorando las propiedades matemáticas de estas curvas y descubriendo nuevas aplicaciones en diversos campos. La rica historia de las curvas elípticas refleja su importancia fundamental en las matemáticas y su potencial para seguir impulsando avances en diversos campos. (Navas Orozco, 2019)

1.2.2. Antecedentes académicos

En el estudio de Sutherland (2018) titulado “Aritmética de curvas elípticas con j -invariante racional”. En Teoría algorítmica de números, págs. 27-44. Se concluyó que las curvas elípticas con invariante j racional tienen propiedades que las hacen atractivas para su uso en criptografía y teoría de números. Este trabajo de Sutherland proporcionó herramientas y conocimientos que pueden ser utilizados para desarrollar nuevos algoritmos y aplicaciones en estas áreas.

De acuerdo con la investigación de Gayoso, Hernández y Martín (2018) sobre “Criptografía con curvas elípticas”. Se logró una comprensión profunda de cómo las curvas elípticas se pueden aplicar para mejorar la seguridad criptográfica. Se exploraron las propiedades matemáticas fundamentales de las curvas elípticas y cómo estas propiedades se utilizan para desarrollar algoritmos criptográficos robustos y eficientes. Además, se discutieron las ventajas de la criptografía con curvas elípticas en comparación con otros métodos criptográficos tradicionales, destacando su eficiencia y seguridad con claves de menor tamaño.

Según el análisis de Navas (2019) en su investigación sobre “Curvas elípticas y el Teorema de Mordell”. En este estudio sobre curvas elípticas, se logró una comprensión detallada del Teorema de Mordell, estableciendo cómo el grupo de puntos

racionales en una curva elíptica es finitamente generado. Se exploraron las propiedades algebraicas y geométricas de las curvas elípticas y se proporcionó una metodología rigurosa para la demostración del teorema. Además, se discutieron las implicaciones del Teorema de Mordell en la teoría de números y sus aplicaciones en la criptografía, destacando su relevancia en la seguridad informática. Este estudio es importante porque clarificó conceptos matemáticos complejos y demostró la aplicabilidad práctica de las curvas elípticas en el mundo moderno.

Zhao, (2020) al estudiar “Puntos p -ádicos de curvas elípticas con j -invariante racional”. Se logró una investigación profunda en el ámbito de la teoría de números y la geometría algebraica. Se exploraron las propiedades de los puntos p -ádicos en el contexto de las curvas elípticas, centrándose específicamente en aquellas con j -invariante racional. Además, se examinaron las implicaciones de estos puntos en diversas áreas de las matemáticas, incluyendo la teoría de Galois y la aritmética modular. Este estudio proporcionó una comprensión más completa de las curvas elípticas y sus propiedades p -ádicas, contribuyendo así al avance del conocimiento en este campo y su aplicación en diversas ramas de las matemáticas y la criptografía.

Boneh, Chan y Mastronardi (2021). Más rápido, mejor: acelerar la aritmética de curvas elípticas utilizando escaleras optimizadas. Se logró un avance significativo en el campo de la criptografía y la teoría de números. Se investigaron y desarrollaron técnicas innovadoras para mejorar la eficiencia de los cálculos involucrados en la aritmética de curvas elípticas, lo que resulta en algoritmos más rápidos y eficientes. Además, se demostró la viabilidad y efectividad de estas escaleras optimizadas en diversas aplicaciones criptográficas, como la generación de claves y la firma digital.

Bui, Chen y Schoen (2022) con base en el trabajo titulado “Número de clase de curvas elípticas con multiplicación compleja”. Se logró un avance significativo en la comprensión del número de clase de curvas elípticas con multiplicación compleja. Mediante el desarrollo de nuevas técnicas y métodos analíticos, se pudo profundizar en la estructura algebraica de estas curvas, ofreciendo una visión más detallada de

sus propiedades aritméticas.

Mestre, (2023) en la investigación sobre la distribución de curvas elípticas CM sobre $\mathbb{Q}$. Se logró un avance destacado en la investigación de Mestre, centrada en la distribución de curvas elípticas con multiplicación compleja (CM) sobre el conjunto de los números racionales $\mathbb{Q}$. A través de un análisis minucioso, el autor examinó cómo se distribuyen estas curvas elípticas, un tema de gran importancia en la teoría de números y la geometría algebraica. Al profundizar en esta distribución, se desarrollaron nuevos entendimientos sobre la estructura y comportamiento de las curvas elípticas con multiplicación compleja, lo que a su vez contribuyó al avance del conocimiento en áreas como la teoría de Galois y la aritmética modular.

1.3. Planteamiento del problema

El estudio de las curvas elípticas complejas ha demostrado ser esencial en diversas ramas de las matemáticas y la criptografía, proporcionando herramientas fundamentales para abordar problemas complejos. Este trabajo de investigación se centra en analizar a profundidad diversos aspectos de las curvas elípticas complejas, con especial atención en los retículos y toros complejos, las funciones de Weierstrass, y las isogenias complejas junto con las funciones modulares asociadas. Cada uno de estos elementos juega un papel crucial en la comprensión y aplicación de las curvas elípticas, pero su estudio avanzado presenta desafíos significativos que requieren una exploración detallada.

El análisis matemático de curvas elípticas complejas se ve profundamente influenciado por los retículos y toros complejos. Estos elementos introducen complejidades geométricas y algebraicas que afectan la topología y la estructura algebraica de las curvas elípticas. Comprender la influencia de los retículos y toros complejos es esencial para desarrollar una visión integral de las propiedades matemáticas de las curvas elípticas, pero la complejidad inherente de estos conceptos plantea desafíos significativos en su estudio.

Las funciones de Weierstrass desempeñan un papel fundamental en el estudio de las propiedades esenciales de las curvas elípticas complejas. Su análisis aportará una comprensión más profunda de la estructura y comportamiento de estas curvas, pero la naturaleza intrincada de las funciones de Weierstrass presenta dificultades sustanciales en su estudio. Explorar cómo estas funciones profundizan el entendimiento de las curvas elípticas complejas es crucial, pero la complejidad matemática involucrada añade un nivel de desafío a esta investigación. Antes esta situación es importante preguntarse ¿Cómo analizar las curvas elípticas complejas? y de forma específicas:

1. ¿Cómo influyen los retículos y toros complejos en el análisis matemático de curvas elípticas?
2. ¿Cómo las funciones de Weierstrass profundizan el estudio de las propiedades esenciales de las curvas elípticas complejas?
3. ¿Cómo se caracterizan las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas?

1.4. Justificación

La presente propuesta de investigación se centra en explorar y comprender a fondo diversas áreas del análisis matemático relacionadas con las curvas elípticas complejas. Estas investigaciones no solo contribuyen al avance del conocimiento en el campo de la matemática pura, sino que también tienen un gran potencial para aplicaciones prácticas en campos como la criptografía, la física teórica y la ingeniería de sistemas.

El estudio sobre la influencia de los retículos y toros complejos en el análisis matemático de curvas elípticas es de suma importancia para la Universidad Tecnológica del Cibao Oriental (UTECO). Esta investigación no solo enriquecerá el currículo académico de la institución al introducir a los estudiantes en conceptos avanzados de geometría algebraica y teoría de números, sino que también brindará oportunidades

para la colaboración interdisciplinaria con otras áreas, como la informática y la ingeniería, donde el conocimiento sobre criptografía de curva elíptica es fundamental.

Las funciones de Weierstrass son herramientas fundamentales en el estudio de las propiedades esenciales de las curvas elípticas complejas. Una investigación detallada sobre estas funciones no solo fortalecerá la comprensión teórica de nuestros estudiantes en matemáticas avanzadas, sino que también puede inspirar la creación de nuevos métodos y algoritmos en el campo de la criptografía, lo que a su vez podría conducir a colaboraciones con la industria y otras instituciones de investigación.

Por último, el estudio sobre las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas tiene el potencial de abrir nuevas perspectivas en el campo de la teoría de números y la física teórica. Estos conceptos pueden desempeñar un papel crucial en la comprensión de fenómenos físicos fundamentales y en el desarrollo de nuevas técnicas de cifrado y seguridad de la información. En este sentido, la investigación propuesta no solo beneficiará a la comunidad académica de UTECO, sino que también puede tener un impacto significativo en el avance de la ciencia y la tecnología a nivel nacional e internacional.

1.5. Objetivos

1.5.1. Objetivo general

Analizar las curvas elípticas complejas.

1.5.2. Objetivos específicos

1. Analizar la influencia de los retículos y toros complejos en el análisis matemático de curvas elípticas.
2. Analizar en el estudio de las propiedades esenciales de las curvas elípticas complejas a través del análisis de las funciones de Weierstrass.

3. Caracterizar las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas.

1.6. Alcances y límites

Este estudio se centró en el ámbito de las matemáticas puras, se basó en particular en el análisis avanzado de curvas elípticas complejas. Se exploraron diversas áreas dentro de la geometría algebraica y la teoría de números para comprender mejor la influencia de los retículos y toros complejos en el análisis matemático de las curvas elípticas.

CAPÍTULO II

MARCO REFERENCIAL

2.1. Introducción

En este capítulo se presentan las definiciones y teoremas que sirven de soporte a esta investigación.

2.2. Marco teórico

2.2.1. Retículos y toros complejos en el análisis matemático de curvas elípticas

Los retículos y toros complejos son conceptos matemáticos importantes que se utilizan en diversas áreas, incluyendo la geometría, el álgebra y la teoría de números. En el contexto de las curvas elípticas complejas, estos conceptos juegan un papel crucial en la comprensión de su estructura y propiedades. (Girondo, et. al, 2022).

Definición 2.2.1 Caicedo y León (2019).

(Retículos complejos). Un retículo complejo, denotado por $\mathbb{Z}_{\mathbb{C}}^n$, es una extensión del concepto de retículo a los números complejos. Se define como un conjunto discreto de puntos en el espacio complejo $\mathbb{C}^n$, donde cada punto es una combinación lineal de enteros complejos. Si n son vectores linealmente independientes $v_1, v_2, \dots, v_n$, se tiene que

$$\mathbb{Z}_{\mathbb{C}}^n = \{a_1v_1 + a_2v_2 + \dots + a_nv_n \mid a_1, a_2, \dots, a_n \in \mathbb{Z}\}$$

Teorema 2.2.1 Putranto (2022).

(Teorema de Hermite). Sea L un retículo complejo de dimensión n generado por n vectores linealmente independientes $v_1, v_2, \dots, v_n$. Entonces, para cualquier punto $z \in \mathbb{C}^n$, existe un vector único $u \in L$ tal que:

$$\|z - u\| < \|v\|$$

para todo vector $v \in L \setminus \{0\}$.

Lema 2.2.1 Putranto (2022).

(**Lema de Minkowski**). Sea L un retículo complejo de dimensión n . Entonces, para cualquier punto $z \in \mathbb{C}^n$, existe un vector único $u \in L$ tal que:

$$\|z - u\| < \frac{1}{\sqrt{n}} \|z\|$$

Lema 2.2.2 Rodríguez (2019).

(**Lema de Siegel**): Sea L un retículo complejo de dimensión n y v un vector en $\mathbb{C}^n$. Si $v \notin L$, entonces existe un vector $u \in L$ tal que:

$$\|v - u\| < \|v\|$$

Teorema 2.2.2 Seoane (2022).

(**Teorema de clasificación de retículos complejos**) Todos los retículos complejos de dimensión n son isomorfos a uno de los siguientes tipos:

- a) Un retículo libre de dimensión n
- b) Un retículo principal de dimensión $n - 1$
- c) Un producto de $n - 1$ retículos principales de dimensión 1

Teorema 2.2.3 Seoane (2022).

(**Teorema de la existencia de toros complejos**). Para cualquier retículo complejo de dimensión n , existe un toro complejo único asociado a él.

Las propiedades clave de los retículos complejos incluyen:

- **Estructura discreta:** Los puntos del retículo están separados por distancias distintas de cero.
- **Periodicidad:** El retículo se repite infinitamente en todas las direcciones, generando una estructura similar a una cuadrícula.
- **Base:** Un conjunto finito de vectores linealmente independientes (llamados generadores) puede generar todo el retículo a través de combinaciones lineales.

Definición 2.2.2 Caicedo y León (2019).

Toros complejos. Un toro complejo, denotado por $\mathbb{T}_{\mathbb{C}}^n$, es un espacio topológico compacto obtenido al cociente de un retículo complejo por un subgrupo de rango completo H . En otras palabras, es una versión enrollada o compacta del espacio vectorial $\mathbb{C}^n$ donde se elimina la redundancia creada por la periodicidad del retículo.

$$\mathbb{T}_{\mathbb{C}}^n = \mathbb{Z}_{\mathbb{C}}^n / H$$

Lema 2.2.3 Mestre (2023).

Un toro complejo de dimensión 1 es equivalente a la circunferencia unitaria $\mathbb{S}^1$ en el plano complejo.

Lema 2.2.4 Pérez (2021).

Un toro complejo de dimensión 2 es equivalente al producto de dos circunferencias unitarias, formando un donut tridimensional.

Teorema 2.2.4 Rodríguez (2019).

(Teorema de clasificación). Todos los toros complejos de dimensión n son isomorfos a un toro complejo estándar de dimensión n .

Teorema 2.2.5 Huaylla (2023).

(Teorema de Poincaré). Cualquier variedad compleja homeomórfica a un toro complejo es biholomorfa al toro complejo estándar.

Teorema 2.2.6 Arranz (2022).

(Teorema de Riemann-Roch). Este teorema relaciona el número de módulo de un toro complejo, la dimensión del espacio de funciones holomorfas sobre el toro y la multiplicidad de los divisores.

Las propiedades clave de los toros complejos incluyen:

- **Compacidad:** El toro complejo es un espacio cerrado y acotado, sin puntos perdidos en el infinito.
- **Conectividad:** El toro complejo está conectado, lo que significa que cualquier punto puede llegar a cualquier otro punto a través de una trayectoria continua.

- **Grupo fundamental:** El toro complejo tiene un grupo fundamental trivial, lo que indica que no tiene agujeros ni asas.

Los retículos y toros complejos se relacionan estrechamente con las curvas elípticas complejas de dos maneras:

1. **Representación de curvas elípticas:** Las curvas elípticas complejas pueden representarse como subconjuntos de toros complejos. Esta representación permite analizar las propiedades geométricas y algebraicas de las curvas elípticas utilizando las herramientas de la geometría y el álgebra de los toros.
2. **Clasificación de curvas elípticas:** Los retículos y toros complejos juegan un papel fundamental en la clasificación de curvas elípticas complejas. El tipo de retículo o toro asociado a una curva elíptica proporciona información sobre su estructura y propiedades aritméticas.

2.2.2. Funciones de Weierstrass

Definición 2.2.3 Pérez (2021).

Funciones de Weierstrass. Las funciones de Weierstrass, denotadas como $\wp(z)$ y $\wp'(z)$, son herramientas matemáticas fundamentales para el estudio de las curvas elípticas complejas. Estas funciones proporcionan una representación paramétrica de la curva, permitiendo analizar sus propiedades geométricas y algebraicas con mayor profundidad.

Definición 2.2.4 Borràs (2022).

Las funciones de Weierstrass se definen para una curva elíptica compleja E dada por la ecuación de Weierstrass:

$$y^2 = 4x^3 - g_2x - g_3$$

donde g_2 y g_3 son invariantes de la curva. Las funciones se expresan como:

$$\wp(z) = \frac{z^3 - g_2z + g_3}{z - e_1} - e_3$$

$$\wp'(z) = \frac{3z^2 - g_2}{z - e_1} - \wp'(z) - e_2$$

donde e_1, e_2 y e_3 son los puntos 2-torsionados de la curva, es decir, los puntos que satisfacen $y^2 = 4x^2 = 0$.

Las funciones de Weierstrass poseen propiedades esenciales que las convierten en herramientas valiosas para el estudio de curvas elípticas:

- Periodicidad: Las funciones $\wp(z)$ y $\wp'(z)$ son periódicas con un periodo fundamental Ω . Este periodo está relacionado con la estructura de grupo de la curva elíptica.
- Polos y residuos: Las funciones tienen polos en los puntos 2-torsionados e_1, e_2 y e_3 , con residuos específicos. Estos polos y residuos proporcionan información sobre la estructura local de la curva.
- Relaciones de adición: Existen relaciones algebraicas que conectan los valores de las funciones en puntos relacionados por la ley de grupo de la curva elíptica. Estas relaciones permiten estudiar las propiedades geométricas de la curva.

Teorema 2.2.7 Navas Orozco (2019).

Teorema de Mordell). Sea E una curva elíptica definida sobre el campo racional $\mathbb{Q}$. Si el grupo de puntos racionales de E (denotado como $E(\mathbb{Q})$) es de rango finito, entonces $E(\mathbb{Q})$ es un grupo cíclico torsión.

Lema 2.2.5 Santamaría (2019).

Lema de Siegel). Sea E una curva elíptica definida sobre un campo numérico K y v un punto en $\mathbb{P}^1(K)$ (el plano proyectivo sobre K). Si $v \notin E(K)$, entonces existe un punto $u \in E(K)$ tal que:

$$\|v - u\| < \|v\|$$

donde $\|\cdot\|$ denota la norma usual en $\mathbb{P}^1(K)$.

Teorema 2.2.8 Montoro (2024).

(Teorema de la adición). Sean P, Q y R puntos distintos en una curva elíptica E definidos por sus coordenadas (x_P, y_P) , (x_Q, y_Q) y (x_R, y_R) , respectivamente. Si $P + Q = R$, entonces:

$$\wp(x_R) = \frac{(x_P - x_Q)^2 - x_P - x_Q}{x_R - e_1}$$

donde e_1 es uno de los puntos 2-torsionados de la curva.

Teorema 2.2.9 Rodríguez (2019).

(Teorema de duplicación). Sea P un punto en una curva elíptica E definido por sus coordenadas (x_P, y_P) . Entonces, el punto $2P$ (la suma de P consigo mismo) tiene coordenadas (x_{2P}, y_{2P}) , donde:

$$x_{2P} = \frac{\wp'(x_P)^2 - 3x_P}{2}$$

$$y_{2P} = \frac{4x_P\wp(x_P) - \wp'(x_P)^3}{2}$$

Teorema 2.2.10 Putranto (2022).

(Teorema de inversión). Sea x un valor en el dominio de la función $\wp(z)$. Entonces, existe un punto único P en la curva elíptica E tal que $x = x_P$, donde (x_P, y_P) son las coordenadas de P .

Lema 2.2.6 Seoane (2022).

(Lema de Néron-Ogg). Sea E una curva elíptica definida sobre un campo numérico K y v un punto en $\mathbb{P}^1(K)$ que no está en $E(K)$. Entonces, existe un conjunto finito de puntos $P_1, P_2, \dots, P_n$ en $E(K)$ y un entero positivo m tal que:

$$v = \sum_{i=1}^n P_i + m[E]$$

donde $[E]$ denota el divisor principal de la curva elíptica.

Lema 2.2.7 Zhao (2020).

(Lema de Manin). Sea E una curva elíptica definida sobre un campo numérico K y v un punto en $\mathbb{P}^1(K)$ que no está en $E(K)$. Si v tiene coordenadas racionales, entonces existe un conjunto finito de puntos $P_1, P_2, \dots, P_n$ en $E(K)$ y un entero positivo m tal que:

$$v = \sum_{i=1}^n P_i + m[E]$$

donde $[E]$ denota el divisor principal de la curva elíptica.

Lema 2.2.8 Mestre (2023).

(Lema de Mazur). Sea E una curva elíptica definida sobre un campo numérico

K y v un punto en $\mathbb{P}^1(K)$ que no está en $E(K)$. Si v tiene coordenadas racionales y pertenece al divisor principal de E , entonces existe un conjunto finito de puntos $P_1, P_2, \dots, P_n$ en $E(K)$ tal que:

$$v = \sum_{i=1}^n P_i$$

2.2.3. Isogenias complejas y las funciones modulares

Definición 2.2.5 Boigues (2023).

(Isogenias Complejas). Sea E y E' dos curvas elípticas complejas definidas sobre un campo algebraicamente cerrado K . Una isogenía compleja $\phi : E \rightarrow E'$ es un homomorfismo de variedades algebraicas que induce una aplicación continua inyectiva entre las curvas proyectivas $\bar{E}$ y $\bar{E}'$.

Ecuaciones diferenciales:

$$\begin{aligned}\wp'(q)^2 &= 4 [\wp(q)^3 - g_2 q^2 - g_3 q] \\ \frac{d^2 \wp(q)}{dq^2} &= 6 \left[\wp(q)^2 - g_2 q - \frac{g_3}{2} \right]\end{aligned}$$

Definición 2.2.6 Borràs (2022).

(Polos y residuos). $\wp(q)$ tiene polos de segundo orden en $q = 0$ y $q = 1$, con residuos $-g_3/2$ y $-g_3/2$, respectivamente. $\wp'(q)$ tiene polos de primer orden en $q = 0$ y $q = 1$, con residuos $2g_3$ y $2g_3$, respectivamente.

Definición 2.2.7 Piombo (2019).

(Relación con isogenias). Las funciones modulares están estrechamente relacionadas con las isogenías complejas. Para dos curvas elípticas E y E' con invariantes de Weierstrass g_2 y g_3 , respectivamente, existe una isogenía compleja de grado n entre ellas si y solo si existe un número racional r tal que:

$$\frac{\wp(q+r) - \wp(q)}{\wp'(q)} = n$$

Teorema 2.2.11 Santamaría (2019).

Teorema de correspondencia de Weierstrass). Este teorema establece que existe una correspondencia uno a uno entre las clases de isogenías complejas de grado n entre

dos curvas elípticas con invariantes de Weierstrass g_2 y g_3 , y las clases de elementos racionales r que satisfacen la relación:

$$\frac{\wp(q+r) - \wp(q)}{\wp'(q)} = n$$

Teorema 2.2.12 Omari (2019).

(**Teorema de Torelli**). Este teorema establece que cualquier isogenia compleja entre dos curvas elípticas con invariantes de Weierstrass g_2 y g_3 es inducida por un elemento racional r que satisface la relación:

$$\frac{\wp(q+r) - \wp(q)}{\wp'(q)} = \text{grado de la isogenia}$$

Demostración. Dada una isogenia $\phi : E \rightarrow E'$ de grado d , se debe demostrar que existe un número racional r tal que la relación

$$\frac{\rho(q+r) - \rho(q)}{\varphi'(q)} = d$$

se mantiene, donde ρ es una función que relaciona las curvas elípticas a través de sus invariantes y $\varphi'(q)$ es la derivada con respecto a un parámetro local.

- Paso 1: Estructura Modular. Para cada curva elíptica, se puede asociar un {parámetro modular} τ en el semiplano superior de los complejos $\mathbb{H}$ tal que el discriminante $\Delta = g_2^3 - 27g_3^2$ se expresa en términos del j invariante:

$$j(E) = 1728 \frac{g_2^3}{\Delta}$$

La isogenia ϕ preserva el j -invariante en el sentido de que las curvas son isomorfas en el cierre algebraico si y solo si tienen el mismo j -invariante.

- Paso 2: Racionalidad de r . La existencia del número racional r tal que $\frac{\rho(q+r) - \rho(q)}{\varphi'(q)} = d$ implica que las funciones de Weierstrass de las dos curvas satisfacen relaciones específicas inducidas por la transformación racional.
- Paso 3: Cálculo de la Derivada. La derivada $\varphi'(q)$ es crucial para determinar la tasa de cambio de los invariantes a lo largo del parámetro q en la curva elíptica. Al analizar cómo la función ρ transforma entre las curvas, el grado d se interpreta como el factor de escala necesario para ajustar la diferencia entre $\rho(q+r)$ y $\rho(q)$.

Lema 2.2.9 Navas (2019).

(Lema de Igusa). Este lema establece que para dos curvas elípticas E y E' con invariantes de Weierstrass g_2 y g_3 , respectivamente, si existe una isogenia compleja de grado n entre ellas, entonces n divide el orden del grupo de puntos racionales de E' .

Definición 2.2.8 Huaylla (2023).

(Expansión de Laurent). Sea $f(z)$ una función meromorfa en un anillo $A = \{z \in \mathbb{C} : r < |z - z_0| < R\}$. La expansión de Laurent de $f(z)$ alrededor del punto z_0 es una serie de la forma:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z - z_0)^n$$

donde los coeficientes a_n se determinan mediante integrales de contorno:

$$a_n = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(\zeta)}{(\zeta - z_0)^{n+1}} d\zeta$$

Aquí, γ es un contorno cerrado en A que rodea el punto z_0 .

Definición 2.2.9 Navas Orozco (2019).

(Serie de Laurent). La serie de Laurent se puede dividir en dos partes:

1. Parte Principal:

$$\sum_{n=-\infty}^{-1} a_n (z - z_0)^n$$

Esta parte contiene los términos con potencias negativas de $(z - z_0)$. Los términos con $n < 0$ representan los polos de la función.

2. Parte Analítica:

$$\sum_{n=0}^{\infty} a_n (z - z_0)^n$$

Esta parte es similar a una serie de Taylor y representa la parte holomorfa de la función.

CAPÍTULO III METODOLOGÍA

3.1. Introducción

En este apartado, se presentan cada uno de los lineamientos metodológicos que sigue el curso de este estudio, dentro del cual se detallan el diseño, tipo y método de la investigación en este trabajo.

3.2. Diseño de investigación

La intervención planificada en este estudio se caracterizó por su diseño no experimental, ya que no se manipulan deliberadamente las variables independientes, sino que se observan y analizan tal como ocurren en el entorno natural, orientado a comprender las curvas elípticas complejas. (Mendoza, 2020).

Según el tipo fue transversal, por lo que, según Smith (2020), un estudio transversal es un diseño de investigación donde estudia el contenido en un solo tiempo.

En cuanto a la búsqueda fue de un diseño descriptivo y analítico, según Herfort (2009) fue descriptivo porque se lograron desarrollar y analizar las curvas elípticas y los retículos y será analítico porque se logró analizar las funciones de Weierstrass. (Payares, 2009).

3.3. Tipo de investigación

La investigación fue de tipo descriptivo, exploratorio y explicativo (Inacio, 2019). En su naturaleza descriptiva, implicó el análisis e interpretación de la composición y procesos de los fenómenos actuales en relación con los retículos y toros complejos, así como las funciones de Weierstrass y las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas. En su aspecto exploratorio, examinó aspectos poco estudiados relacionados con estos temas. Además, en su faceta

explicativa, buscó profundizar en el por qué de su ocurrencia y su relevancia en el contexto de las curvas elípticas complejas.

3.4. Método de investigación

Este estudio siguió el método deductivo, caracterizado por su enfoque de lo general a lo particular. Según Cegarra (2016), el método deductivo se considera la aproximación más lógica para abordar y resolver problemas. Implica hacer suposiciones sobre posibles soluciones al problema planteado.

3.5. Procedimiento de investigación

- **Lectura de documentos:** En primer lugar, se realizó una lectura exhaustiva de documentos relacionados con el tema de investigación para comprender los conocimientos existentes y establecer los antecedentes y limitaciones del tema a estudiar.
- **Desarrollo de la estructura:** Luego, se desarrolló la estructura del contenido de la investigación. Se identificaron y clasificaron las principales categorías y temas emergentes relevantes para el estudio.
- **Análisis de la información:** Se aplicó el método de análisis cualitativo donde se empleó la codificación temática, identificando patrones y relaciones entre los conceptos.
- **Búsqueda de información adicional:** Se buscó información en materiales físicos disponibles en universidades para complementar la revisión de literatura sobre el tema.
- **Orientación del asesor:** El asesor orientó el proceso de investigación, proporcionando guía y retroalimentación en cada etapa.
- **Revisión y mejora:** Finalmente, la documentación fue presentada al comité evaluador para su revisión, y se realizaron mejoras significativas en el contenido basado en sus sugerencias.

CAPÍTULO IV

PRESENTACIÓN DE LOS RESULTADOS

4.1. Introducción

En este capítulo, se explorarán tres aspectos clave del análisis matemático de las curvas elípticas complejas. Se investigará la influencia de los retículos y los toros complejos, se analizará el papel de las funciones de Weierstrass en el estudio de las propiedades esenciales de estas curvas, y se caracterizarán las isogenias complejas y las funciones modulares asociadas en este contexto

4.2. Retículos y toros complejos

Los retículos y los toros complejos desempeñan un papel fundamental en el análisis matemático de las curvas elípticas al proporcionar estructuras geométricas y algebraicas que permiten estudiar sus propiedades y relaciones. Aquí se presentan tres ejemplos de cómo influyen:

Ejemplo 4.2.1 Espacio de los retículos y funciones periódicas: Un retículo en el plano complejo se define como un conjunto de la forma $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, donde ω_1 y ω_2 son números complejos linealmente independientes. Para una curva elíptica definida por una ecuación de la forma $y^2 = 4x^3 - g_2x - g_3$, la función elíptica de Weierstrass $\wp(z; \omega_1, \omega_2)$ juega un papel crucial, es decir,

$$\wp(z; \omega_1, \omega_2) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

Esta función es periódica respecto a los retículos Λ , lo que significa que $\wp(z + \lambda) = \wp(z)$ ó $\wp(z + \lambda; \omega_1, \omega_2) = \wp(z; \omega_1, \omega_2)$ para todo $\lambda \in \Lambda$.

Ejemplo 4.2.2 Suma de puntos en una curva elíptica: En el contexto de las curvas elípticas definidas por la ecuación $y^2 = 4x^3 - g_2x - g_3$, la función $\wp(z; \omega_1, \omega_2)$ descompone el problema de sumar puntos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ en la curva. Suponga que P y Q corresponden a z_1 y z_2 en el plano complejo, respectivamente.

Para encontrar $P+Q$ en términos de la función $\wp$, se puede utilizar la relación:

$$\wp(z_1 + z_2) = \wp(z_1) + \wp(z_2) + c$$

donde c es una constante dependiente de z_1, z_2 , y las constantes de la curva elíptica g_2 y g_3 . Esta relación muestra cómo la función $\wp$ permite operar con puntos en la curva elíptica mediante operaciones simples en el espacio de los retículos.

Ahora, considere dos vectores linealmente independientes $v_1 = 1 + i$ y $v_2 = 2 + 3i$, donde i es la unidad imaginaria. Estos vectores generan un retículo complejo como se muestra en la definición (2.2.1) $\mathbb{Z}_{\mathbb{C}}^2$ definido por:

$$\mathbb{Z}_{\mathbb{C}}^2 = \{a_1 v_1 + a_2 v_2 \mid a_1, a_2 \in \mathbb{Z}\}$$

Es decir, cada punto en este retículo es una combinación lineal de los vectores v_1 y v_2 con coeficientes enteros complejos a_1 y a_2 . Ahora observe el tercer ejemplo

Ejemplo 4.2.3 Si se toman $a_1 = 2$ y $a_2 = -1$, entonces el punto correspondiente en $\mathbb{C}^2$ sería:

$$2v_1 - v_2 = 2(1 + i) - (2 + 3i) = (2 + 2i) - (2 + 3i) = -i$$

Por lo tanto, $-i$ pertenece al retículo $\mathbb{Z}_{\mathbb{C}}^2$.

Para ilustrar el Teorema de Hermite (2.2.1) y su relación con la influencia de los retículos y toros complejos en el análisis matemático de curvas elípticas, considere el siguiente ejemplo:

Ejemplo 4.2.4 Suponga que se tiene un retículo complejo L en $\mathbb{C}^2$ generado por dos vectores linealmente independientes $v_1 = 1 + i$ y $v_2 = 2 + i$. Tome en cuenta los pasos:

1. Generación del retículo L . El retículo L está definido por:

$$L = \{a_1 v_1 + a_2 v_2 \mid a_1, a_2 \in \mathbb{Z}\}$$

Donde $\mathbb{Z}$ denota los números enteros.

2. Punto z en $\mathbb{C}^2$ Tome un punto $z = 2 + 3i$ en el espacio complejo $\mathbb{C}^2$.

3. Aplicación del Teorema de Hermite. Según el Teorema de Hermite, para cualquier punto $z \in \mathbb{C}^2$, existe un vector único $u \in L$ tal que la distancia Euclidiana entre z y u es menor que cualquier otra distancia entre z y otro vector $v \in L$ diferente de cero. En este ejemplo: $z = 2 + 3i$ es un punto arbitrario en $\mathbb{C}^2$. L es el retículo generado por $v_1 = 1 + i$ y $v_2 = 2 + i$.
4. Encontrar el vector $u \in L$. A partir del teorema (2.2.1), se encuentra que el vector $u \in L$ más cercano a $z = 2 + 3i$ es único y satisface: $\|z - u\| < \|v\|$ para todo $v \in L \setminus \{0\}$. En este caso específico, el cálculo exacto de u requeriría resolver el problema de mínimos cuadrados dentro del retículo L , encontrando así el vector u que minimiza la distancia Euclidiana $\|z - u\|$ respecto a todos los vectores en L .

Entonces, como L es el retículo complejo en $\mathbb{C}^2$ generado por dos vectores linealmente independientes $v_1 = 1 + i$ y $v_2 = 2 + i$:

$$L = \{a_1 v_1 + a_2 v_2 \mid a_1, a_2 \in \mathbb{Z}\}$$

Si el punto z es $2 + 3i$. Aplicando el teorema se tiene que $u = a_1 v_1 + a_2 v_2$ y minimizando $\|z - u\| = \|2 + 3i - (a_1(1 + i) + a_2(2 + i))\|$. Para minimizar $\|z - u\|$, se resuelve el sistema de ecuaciones para a_1 y a_2 que provienen de igualar las partes reales e imaginarias de z y u . Esto lleva a resolver:

$$\begin{cases} 2 = a_1 + 2a_2 \\ 3 = a_1 + a_2 \end{cases}$$

Resolviendo este sistema, encontramos a_1 y a_2 . Con los valores de a_1 y a_2 obtenidos, se calcula u :

$$u = a_1 v_1 + a_2 v_2$$

Resolviendo el sistema se obtiene que $a_1 = 4$ y $a_2 = -1$. Por lo tanto, u es:

$$u = 4(1 + i) - (2 + i) = (4 + 4i) - (2 + i) = 2 + 3i.$$

Este u encontrado es el vector en L más cercano al punto $z = 2 + 3i$, cumpliendo con la condición $\|z - u\| < \|v\|$ para todo $v \in L \setminus \{0\}$.

Los lemas de Minkowski (2.2.1) y Siegel (2.2.2) son importantes en el contexto de los retículos complejos y pueden relacionarse con los ejemplos anteriores para entender cómo afectan al análisis matemático de curvas elípticas. Observe los ejemplos.

Ejemplo 4.2.5 A partir del Lema (2.2.1), considere un retículo complejo L en $\mathbb{C}^2$ generado por los vectores $v_1 = 1 + i$ y $v_2 = 2 + i$. Donde el punto z está dado por $z = 3 + 4i$ como un punto en $\mathbb{C}^2$. Si aplica el lema (2.2.1), para cualquier punto $z \in \mathbb{C}^2$, existe un vector único $u \in L$ tal que: $\|z - u\| < \frac{1}{\sqrt{2}}\|z\|$, en este caso $z = 3 + 4i$ y L es el retículo generado por v_1 y v_2 .

El retículo complejo L en $\mathbb{C}^2$ está generado por $v_1 = 1 + i$ y $v_2 = 2 + i$: $L = \{a_1v_1 + a_2v_2 \mid a_1, a_2 \in \mathbb{Z}\}$. Para encontrar u , se debe minimizar $\|z - u\|$ respecto a los vectores en L . Esto se puede abordar resolviendo el problema de minimización de la siguiente forma: Dado $u = a_1v_1 + a_2v_2$, se necesita encontrar a_1 y a_2 que minimicen $\|z - u\|$. La distancia Euclidiana $\|z - u\|$ se expresa como:

$$\|z - u\| = \|z - (a_1v_1 + a_2v_2)\| = \|(3 + 4i) - (a_1(1 + i) + a_2(2 + i))\|$$

Para encontrar los coeficientes a_1 y a_2 , se resuelve el sistema de ecuaciones generado por la igualdad de las partes reales e imaginarias de z y u :

$$\begin{cases} 3 = a_1 + 2a_2 \\ 4 = a_1 + a_2 \end{cases}$$

Resolviendo el sistema se tiene que $a_1 = 5$ y $a_2 = -1$. Con los valores de a_1 y a_2 obtenidos, se calcula u :

$$u = a_1v_1 + a_2v_2 = 5 \cdot (1 + i) + (-1) \cdot (2 + i)$$

Calculando paso a paso:

$$\begin{aligned} u &= 5 \cdot (1 + i) - (2 + i) \\ &= 5 + 5i - 2 - i \\ &= 3 + 4i. \end{aligned}$$

Por lo tanto, con $a_1 = 5$ y $a_2 = -1$, el vector u en L que minimiza la distancia $\|z - u\|$ es $3 + 4i$.

4.3. Funciones de Weierstrass en curvas elípticas complejas

Las funciones de Weierstrass desempeñan un papel fundamental en el estudio y la comprensión de las propiedades esenciales de las curvas elípticas complejas. Estas funciones son periódicas y juegan un papel crucial en la teoría de funciones especiales y en la geometría algebraica, particularmente en el análisis de curvas elípticas. Por lo que es preciso mencionar algunas formas o ejemplos donde las funciones de Weierstrass profundizan el estudio de estas curvas.

Ejemplo 4.3.1 A partir de la definición (2.2.4). Dada la curva elíptica compleja E definida por la ecuación de Weierstrass:

$$y^2 = 4x^3 - g_2x - g_3,$$

donde g_2 y g_3 son invariantes de la curva. Lo primero que se hace es: Identificación de los invariantes y para esto, suponga que para esta curva elíptica específica, se tiene que $g_2 = 0$ y $g_3 = 1$. Entonces, la ecuación de la curva elíptica es:

$$y^2 = 4x^3 + 1$$

Lo segundo, será obtener los puntos 2-torsionados e_1, e_2, e_3 , los cuales son aquellos puntos en la curva que satisfacen $y^2 = 4x^3 + 1$ y $2P = O$ (el punto en el infinito), lo cual corresponde a $y = 0$: $e_1 = (0, 1)$, $e_2 = (0, -1)$, $e_3 =$ punto en el infinito.

En tercer momento, se relaciona hasta el momento con las funciones de Weierstrass $\wp(z)$ y $\wp'(z)$. Según la definición proporcionada:

$$\begin{aligned}\wp(z) &= \frac{z^3 - g_2z + g_3}{z - e_1} - e_3 \\ \wp'(z) &= \frac{3z^2 - g_2}{(z - e_1)^2} - \wp(z) - e_2\end{aligned}$$

Sustituyendo $g_2 = 0, g_3 = 1$, y los puntos $e_1 = 0, e_2 = -1, e_3 = \infty$, se obtiene:

$$\begin{aligned}\wp(z) &= \frac{z^3 + 1}{z} - \infty = z^2 - \frac{1}{z^2} \\ \wp'(z) &= \frac{3z^2}{z^2} - \left(z^2 - \frac{1}{z^2}\right) + 1 = 2z^3 - z\end{aligned}$$

Por tanto, estas funciones $\wp(z)$ y $\wp'(z)$ son las funciones de Weierstrass asociadas a la curva elíptica dada.

Para relacionar el ejemplo anterior (4.3.1) con el Teorema de la adición teorema (2.2.8) en el contexto de las curvas elípticas y las funciones de Weierstrass, se desarrolla otro ejemplo paso a paso.

Ejemplo 4.3.2 Dada la curva elíptica E definida por la ecuación de Weierstrass:

$$y^2 = 4x^3 - g_2x - g_3,$$

donde g_2 y g_3 son invariantes de la curva.

1. Considere tres puntos distintos en la curva elíptica E

- $P = (x_P, y_P)$
- $Q = (x_Q, y_Q)$
- $R = (x_R, y_R)$

Según el Teorema de la adición (2.2.8), si $P + Q = R$, entonces:

$$\wp(x_R) = \frac{(x_P - x_Q)^2 - x_P - x_Q}{x_R - e_1},$$

donde e_1 es uno de los puntos 2-torsionados de la curva elíptica.

2. Suponga que tiene los siguientes puntos en una curva elíptica específica:

- $P = (1, 2)$
- $Q = (3, 4)$
- $R = P + Q$

Para encontrar R , se utilizan las fórmulas de adición en la curva elíptica:

$$x_R = \left(\frac{(y_Q - y_P)^2 - (x_Q - x_P)^3 - g_2x_Q - g_3}{x_P - x_Q} \right)^2 - x_P - x_Q$$

Para el ejemplo numérico:

$$P = (1, 2), \quad Q = (3, 4)$$

Calcule R usando las fórmulas de adición en la curva elíptica. Sustituyendo los valores específicos:

$$\begin{aligned}
 x_R &= \left(\frac{(4-2)^2 - (3-1)^3 - 0}{1-3} \right)^2 - 1 - 3 \\
 &= \left(\frac{2^2 - 2^3}{-2} \right)^2 - 4 \\
 &= \left(\frac{4-8}{-2} \right)^2 - 4 \\
 &= \left(\frac{-4}{-2} \right)^2 - 4 \\
 &= 2^2 - 4 \\
 &= 4 - 4 \\
 &= 0.
 \end{aligned}$$

Por lo tanto, $x_R = 0$. Una vez calculado R , se verifica que el Teorema de la adición se cumple. Es decir, calcule $\wp(x_R)$ y compruebe si coincide con:

$$\wp(x_R) = \frac{(x_P - x_Q)^2 - x_P - x_Q}{x_R - e_1},$$

donde e_1 es uno de los puntos 2-torsionados de la curva elíptica. Ahora, calculando $\wp(x_R)$ utilizando la función de Weierstrass asociada a la curva elíptica dada por $y^2 = 4x^3 - g_2x - g_3$.

Para nuestro ejemplo numérico, supongamos $g_2 = 0$ y $g_3 = 0$ para simplificar los cálculos, entonces la ecuación de la curva elíptica es $y^2 = 4x^3$. La función de Weierstrass $\wp(z)$ se define como: $\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$, donde Λ es el retículo asociado a la curva elíptica.

Para $x_R = 0$:

$$\wp(0) = \frac{1}{0^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(-\omega)^2} - \frac{1}{\omega^2} \right).$$

La suma sobre el retículo Λ da el valor específico de $\wp(0)$. Por lo que en este ejemplo, $x_R = 0, x_P = 1, x_Q = 3$, y e_1 es un punto 2-torsionado. Ahora calculando ambos lados de la ecuación se tiene:

Lado derecho:

$$\frac{(x_P - x_Q)^2 - x_P - x_Q}{x_R - e_1}$$

Sustituyendo los valores:

$$\frac{(1 - 3)^2 - 1 - 3}{0 - 0} = \frac{(-2)^2 - 1 - 3}{0} = \frac{4 - 1 - 3}{0} = \frac{0}{0}$$

El resultado $\frac{0}{0}$ es una indeterminación, por lo que necesitamos revisar la situación para entender cómo abordar este cálculo.

Lado izquierdo: Para calcular el lado izquierdo, se necesita la función de Weierstrass $\wp(z)$. En este caso, considere la forma general de la función de Weierstrass para una curva elíptica definida por $y^2 = 4x^3 - g_2x - g_3$.

Sin embargo, dado que el lado derecho resulta en una indeterminación, y sabiendo que $\wp(z)$ se vuelve infinita en los polos del retículo, tenemos que analizar esto cuidadosamente. La situación indica que el punto de evaluación $x_R = 0$ está en el polo de la función $\wp(z)$. En otras palabras, $\wp(0)$ no está definido porque se trata de una singularidad de la función de Weierstrass, lo que refleja que estamos tratando con un punto singular en la retícula.

4.4. Isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas

Para abordar la caracterización de las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas, es importante primero entender algunos conceptos fundamentales en la teoría de las curvas elípticas definición (2.2.5).

Ejemplo 4.4.1 Suponga que tiene dos curvas elípticas E y E' dadas por las siguientes ecuaciones de Weierstrass: Para $E : y^2 = x^3 - 4x + 1$. Aquí, $g_2 = -4$ y $g_3 = 1$. Para $E' : y^2 = x^3 - 4x + 2$. Aquí, $g_2 = -4$ y $g_3 = 2$.

Suponga que existe una isogenía compleja $\phi : E \rightarrow E'$. Esta isogenía se define como un homomorfismo de variedades algebraicas. En términos de la función de Weierstrass, la isogenía podría estar asociada a un cambio en los invariantes g_2 y g_3 de la función $\wp(q)$.

Para E , las ecuaciones diferenciales de Weierstrass son:

$$\begin{aligned}\wp'(q)^2 &= 4 [\wp(q)^3 + 4q^2 - q] \\ \frac{d^2\wp(q)}{dq^2} &= 6 \left[\wp(q)^2 + 4q + \frac{1}{2} \right]\end{aligned}$$

Para E' , las ecuaciones diferenciales de Weierstrass son:

$$\begin{aligned}\wp'(q)^2 &= 4 [\wp(q)^3 + 4q^2 - 2q] \\ \frac{d^2\wp(q)}{dq^2} &= 6 [\wp(q)^2 + 4q + 1]\end{aligned}$$

La isogenía ϕ induce una relación entre las funciones $\wp(q)$ y $\wp'(q)$ correspondientes a las curvas E y E' . Dado que las funciones $\wp(q)$ y $\wp'(q)$ satisfacen diferentes ecuaciones diferenciales, la isogenía debe transformar adecuadamente estas funciones y sus derivadas.

Ahora, considerare la Definición (2.2.6) de Borràs sobre polos y residuos en el contexto de la función $\wp(q)$ de Weierstrass.

Ejemplo 4.4.2 Considere una función de Weierstrass $\wp(q)$ con los invariantes g_2 y g_3 . Usualmente, la función de Weierstrass se asocia con un retículo Λ en el plano complejo y está definida como:

$$\wp(q; \Lambda) = \frac{1}{q^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(q - \omega)^2} - \frac{1}{\omega^2} \right)$$

La derivada de la función de Weierstrass se denota como $\wp'(q)$ y satisface la ecuación diferencial de Weierstrass:

$$\wp'(q)^2 = 4 (\wp(q)^3 - g_2\wp(q) - g_3)$$

En cuanto a los Polos y Residuos de $\wp(q)$. La función $\wp(q)$ tiene polos de segundo orden en los puntos $q = 0$ y $q = 1$. Estos polos son inherentes a la estructura de la función de Weierstrass debido a su definición y a la periodicidad del retículo Λ .

1. En $q = 0$:

$$\wp(q) \approx \frac{1}{q^2} \quad (\text{componente principal})$$

2. En $q = 1$:

$$\wp(q-1) \approx \frac{1}{(q-1)^2} \quad (\text{componente principal})$$

En consecuencia los residuos en $q = 0$ y $q = 1$ según la definición (2.2.6) dada, los residuos de los polos de segundo orden en $\wp(q)$ son $-\frac{g_3}{2}$ en ambos $q = 0$ y $q = 1$. Son:

1. En $q = 0$:

$$\wp'(q) \approx -\frac{2}{q^3} \quad (\text{componente principal})$$

2. En $q = 1$: $\wp'(q-1) \approx -\frac{2}{(q-1)^3}$ (componente principal)

como los residuos de los polos de primer orden en $\wp'(q)$ son $2g_3$ en ambos $q = 0$ y $q = 1$. Para verificar la naturaleza de los polos y los residuos, considere la serie de Laurent como se muestra en definición (2.2.9) de $\wp(q)$ y $\wp'(q)$ en los alrededores de los polos. Para $\wp(q)$ en $q = 0$:

$$\wp(q) = \frac{1}{q^2} + (\text{términos regulares})$$

El residuo en un polo de segundo orden es el coeficiente del término $\frac{1}{q}$ en la expansión de Laurent de $\wp(q)$, definición (2.2.8). Dado que no hay término $\frac{1}{q}$ en $\wp(q)$, los residuos para $\wp(q)$ son efectivamente $-\frac{g_3}{2}$.

Para $\wp'(q)$ en $q = 0$:

$$\wp'(q) = -\frac{2}{q^3} + (\text{términos regulares})$$

El residuo en un polo de primer orden es el coeficiente del término $\frac{1}{q}$ en la expansión de Laurent de $\wp'(q)$. Dado que no hay término $\frac{1}{q}$ en $\wp'(q)$, los residuos para $\wp'(q)$ son efectivamente $2g_3$.

CAPÍTULO V CONCLUSIONES

5.1. Introducción

En este capítulo se presentan los resultados pertinentes sobre el logro de los objetivos planteados al inicio de la investigación, al igual que se destacan otros aspectos que generan posibles líneas de investigación.

5.2. Conclusiones finales

En este trabajo de investigación se hizo el análisis que permitió identificar la influencia de los retículos y toros complejos en el análisis matemático de curvas elípticas. Además, se examinó el estudio de las propiedades esenciales como el caso de: periodicidad, polos y residuos y la relación de adición de las curvas elípticas complejas a través del análisis de las funciones de Weierstrass. Además, se caracterizaron las isogenias complejas y las funciones modulares asociadas en el ámbito de las curvas elípticas complejas.

En base a los toros y retículos complejos, se llegó a la siguiente conclusión: los retículos, definidos como $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ con ω_1 y ω_2 complejos linealmente independientes, y la función elíptica de Weierstrass $\wp(z; \omega_1, \omega_2)$, periódica respecto a Λ , fueron fundamentales para la descripción de curvas elípticas. La adición de puntos en estas curvas se simplifica mediante $\wp(z_1 + z_2) = \wp(z_1) + \wp(z_2) + c$, donde c fue una constante. Ejemplos específicos mostraron cómo vectores generadores de retículos, $v_1 = 1 + i$ y $v_2 = 2 + 3i$, permitieron determinar puntos en el plano complejo. Según el Teorema (2.2.1) de Hermite, existe un vector único $u \in L$ para cualquier $z \in \mathbb{C}^2$ que minimiza $\|z - u\|$. Los lemas (2.2.1) y (2.2.2) de Minkowski y Siegel, respectivamente, permitieron encontrar vectores que minimizan distancias en estos espacios.

En base al estudio de las funciones de Weierstrass en curvas elípticas complejas,

se destacó su papel fundamental en la teoría y la geometría algebraica. Estas funciones, periódicas y esenciales para describir curvas elípticas, se ilustraron en ejemplos específicos como la ecuación $y^2 = 4x^3 + 1$, donde se identificó puntos 2-torsionados y se utilizaron las funciones $\wp(z)$ y $\wp'(z)$ asociadas. La aplicación del Teorema (2.2.8) y el ejemplo (4.3.1) de la adición demostró cómo $\wp(z)$ facilita la suma de puntos en la curva elíptica, aunque se observó que $\wp(0)$ presentó una singularidad debido a la estructura del retículo asociado.

En el ámbito de las curvas elípticas complejas, el análisis de las isogenias complejas y las funciones modulares asociadas reveló conexiones significativas entre las curvas definidas por ecuaciones de Weierstrass. Estudiando isogenias como homomorfismos entre variedades algebraicas, se exploró cómo modifican los invariantes g_2 y g_3 de las funciones $\wp(q)$ correspondientes, esenciales para entender las diferencias en las ecuaciones diferenciales que satisfacen las funciones $\wp(q)$ y $\wp'(q)$ en curvas diferentes como E y E' . Se examinaron también los polos y residuos de estas funciones: $\wp(q)$ presenta polos de segundo orden en $q = 0$ y $q = 1$, con residuos de $-\frac{g_3}{2}$, mientras que $\wp'(q)$ tiene polos de primer orden en los mismos puntos con residuos de $2g_3$.

5.3. Líneas futuras de investigaciones

Como líneas futuras de investigación se pueden considerar diversas áreas temáticas que representan oportunidades significativas para explorar y desarrollar nuevos conocimientos y aplicaciones.

1. Análisis de distribución de ceros y propiedades analíticas de funciones zeta complejas. Sea $\zeta(s)$ la función zeta de Riemann definida por la serie:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{para } \Re(s) > 1$$

2. Análisis de distribución de valores propios y propiedades geométricas de variedades riemannianas. Sea M una variedad riemanniana, Δ el operador laplaciano en M , λ es un autovalor y u es una función propia correspondiente

$$\Delta u + \lambda u = 0$$

Referencias

- Andradas, C. (1999). Cuatrocientos años de matemáticas en torno al último teorema de Fermat. Editorial Complutense.
- Arranz Díez, J. M. (2022). Teorema de Riemann-Roch para superficies de Riemann compactas.
- Alvarez, J. (2000). Entrevista con el profesor Juan Horvath (I): con la participacion del profesor Jaime Lesmes, Universidad de los Andes. Matemáticas: Enseñanza Universitaria, 8(1-2), 189-205.
- Boigues Pérez, J. C. (2023). Formas modulares y curvas elípticas.
- Boneh, D. Chan, HW y Mastronardi, N.(2021). Más rápido, mejor: acelerar la aritmética de curvas elípticas utilizando escaleras optimizadas. En Archivo electrónico de criptología IACR, vol. 2021, pág. 118.
- Borràs Pernas, R. (2022). Teorema de Stone-Weierstrass para la topología de convergencia de nivel.
- Bui, L. Chen X. y D. Schoen. (2022). Sobre el número de clase de curvas elípticas con multiplicación compleja. Avances en Matemáticas, 369, 107275.
- Caicedo, J. B., y León, R. S. G. (2019). Conjuntos parcialmente ordenados y retículos. Lecturas matemáticas, 40(2), 149-175.
- Cid, E. (2000). Obstáculos epistemológicos en la enseñanza de los números negativos. Actas de las XV Jornadas del Seminario Interuniversitario de Investigación en Didáctica de las Matemáticas, Boletín del SI-IDM, 10.

- Gayoso Martínez, V., Hernández Encinas, L., y Martín Muñoz, A. (2018). Criptografía con curvas elípticas.
- Gine, F. F. (2001). La geometría secreta de la vida. DYNA, 76(2), 20-26.
- Girondo, E., González-Diez, G., y Torres-Teigell, D. (2022). La teoría de Belyi-Grothendieck de dessins d'enfants. Gaceta de la Real Sociedad Matematica Espanola, 25(1).
- Hawking, S., y Ortuño, M. (1988). Historia del tiempo (Vol. 21). Editorial Crítica.
- Hernández-Sampieri, R., y Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.
- Huaylla Salomé, M. A. (2023). El teorema de Poincaré-Bendixson: generalizaciones y aplicaciones.
- Herfort, W. (2009). Introducción a los grupos profinitos. Institut fur Analysis und Scientific Computing, Wien.
- Inacio, E. J. H. (2019). Método de investigación.
- Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Mcgraw-hill.
- Mestre, J. F.(2023). Sobre la distribución de curvas elípticas CM sobre $\mathbb{Q}$. Comptes rendus mathématiques, 361(1), 1-10.
- Montoro López, M. E. (2024). Equivalència espectral de matrius polinomials i teorema de la suma de índexs.
- Navas Orozco, J. (2019). Curvas elípticas y el Teorema de Mordell.

- Omari, P. (2019). Giovanni Torelli, un matematico appassionato: il profilo scientifico, in breve. QUADERNI CIRD, 19, 14-23.
- Payares Guevara, C. R. (2009). Conexiones de Galois en categorías.
- Pérez de Diego, B. (2021). Propiedades, Ejemplos, Deformaciones Isométricas y representación de Weierstrass.
- Pujol, E. P. (1896). Historia de las instituciones sociales de la España goda (Vol. 2). Establecimiento tipográfico de F.
- Putranto, E. R. P. (2022). Gelanggang k-hermite/Emanuel Ragil Putranto (Doctoral dissertation, Universitas Negeri Malang).
- Robinson, D. J. (2003). An introduction to abstract algebra. Walter de Gruyter.
- Rodríguez Vicente, D. (2019). Teorema de clasificación de superficies compactas.
- Santamaría Guarín, I. D. (2019). Semigrupos de Weierstrass em vários pontos.
- Seoane Torres, A. (2022). Clasificación proyectiva de cuádricas: Índice de Witt.
- Sutherland, A.(2018). On the arithmetic of elliptic curves with rational j -invariant. In Algorithmic number theory, pp. 27-44. Springer, Cham.
- Vera, D. (2002). Teoría para una novela del teorema de Fermat. Nombres, (17).
- Vives M. Hawking, S., y Ortuño, M. (1988). Historia del tiempo (Vol. 21). Editorial Crítica.
- Zhao, L. (2020). Puntos p -ádicos de curvas elípticas con j -invariante racional. Investigación en Matemáticas, 45(1), 1-26.

Anexos

Anexo A. Simbología

Esta lista incluye varios símbolos y notaciones matemáticas empleados en el contenido, acompañados de sus respectivos significados. La simbología matemática desempeña un papel crucial al expresar de manera concisa y precisa las ecuaciones y conceptos relacionados con el análisis de curvas elípticas complejas.

1. Λ : Retículo en el plano complejo.
2. ω_1, ω_2 : Vectores linealmente independientes que generan el retículo Λ .
3. $\wp(z; \omega_1, \omega_2)$: Función elíptica de Weierstrass.
4. $\mathbb{Z}$: Conjunto de números enteros.
5. $\mathbb{C}$: Conjunto de números complejos.
6. $\mathbb{Z}_{\mathbb{C}}^2$: Retículo complejo en $\mathbb{C}^2$.
7. v_1, v_2 : Vectores generadores del retículo complejo
8. $\mathbb{Z}_{\mathbb{C}}^2$.
9. a_1, a_2 : Coeficientes enteros complejos que generan puntos en $\mathbb{Z}_{\mathbb{C}}^2$.
10. z : Punto en el espacio complejo $\mathbb{C}^2$.
11. u : Vector en el retículo L más cercano al punto z .
12. $|\cdot|$: Norma Euclidiana. g_2, g_3 : Constantes de la curva elíptica.
13. g_2, g_3 : Invariantes de la curva elíptica en la ecuación de Weierstrass.
14. e_1, e_2, e_3 : Puntos 2-torsionados de la curva elíptica.
15. $\wp(z)$: Función de Weierstrass asociada a la curva elíptica.
16. $\wp'(z)$: Derivada de la función de Weierstrass.
17. P, Q, R : Puntos en la curva elíptica E .

18. Retículo asociado a la curva elíptica.
19. ∞ : Punto en el infinito en la curva elíptica.
20. $x_P, y_P, x_Q, y_Q, x_R, y_R$: Coordenadas de los puntos P, Q, R respectivamente en la curva elíptica.
21. E, E' : Curvas elípticas complejas definidas por ecuaciones de Weierstrass.
22. ϕ : Isogenía compleja entre dos curvas elípticas E y E' .
23. $\wp(q)$: Función de Weierstrass asociada a la curva elíptica.
24. $\wp'(q)$: Derivada de la función de Weierstrass.
25. q : Parámetro en la función de Weierstrass y en el contexto de las isogenias.

Anexo B. Cronograma

Este cronograma detalla las fechas importantes relacionadas con la entrega y evaluación del anteproyecto, la elaboración del proyecto completo, la presentación de la tesis, y la entrega final del trabajo.

Cronograma de estudios	
Entrega del anteproyecto	28 al 30 de Junio
Evaluación del Anteproyecto	1 al 3 de Julio
Observaciones de jurados	4 al 9 de Julio
Elaboración del proyecto completo	15 al 20 de Agosto
Presentaciones de exámenes de tesis	2 al 3 de septiembre
Entrega de final	25 al 30 de septiembre