Criptografía Basada en Grupos Cíclicos, un Análisis desde la Transposición Didáctica

Sistematización Práctica Pedagógica

Fabian Camilo Martínez Silva

Directora: Mg. Yeny Leonor Rosero Rosero

Universidad del Cauca

Facultad de Ciencias Naturales Exactas y de la Educación

Licenciatura en Matemáticas

Popayán 2022

Agradecimientos

A Dios por darme fortaleza en todo tiempo

A mis padres por ser el pilar de mis aspiraciones académicas y por su incondicional apoyo

A mis hermanos por ser parte de mi vida y fuente de descanso e inspiración

A mis amigos del barrio por brindarme su apoyo y amistad

A mis profesoras y profesores por darla toda en cada clase

A todas aquellas personas que aportaron un grano de arena para hacer este sueño una realidad

A todos ustedes gracias.

“De hecho, la teoría de grupos logró precisamente eso: una unidad e indivisibilidad de los patrones subyacentes a una amplia gama de disciplinas aparentemente no relacionadas".

Mario Livio, La ecuación que no se pudo resolver

Resumen

En el marco de la presente sistematización se pretende realizar un análisis desde la Transposición Didáctica en torno al concepto de grupo cíclico, en el contexto de la criptografía asimétrica. Para ello se adelantan reflexiones y estudios acerca del saber didáctico que orienta el trabajo del docente, al igual que de los elementos que direccionan las propuestas formuladas en los libros de texto de Álgebra Abstracta que circulan en el medio respecto al concepto de grupo cíclico. Como parte del trabajo realizado, y en el marco de los análisis propios de la transposición didáctica, se ha adelantado un análisis de las etapas del proceso de transposición, desde el saber sabio (las diferentes formalizaciones del grupo cíclico su proceso de constitución como objeto matemático) hasta el saber seleccionado para ser enseñado (las diferentes formas de presentación de grupo cíclico en el contexto de la criptografía asimétrica).

En las instituciones académicas coexisten, al lado de enfoques aplicados a la criptografía asimétrica, propuestas que recuperan diferentes sentidos del concepto de grupo cíclico, lo cual muchas veces no es del todo consciente en las prácticas pedagógicas de los maestros. Con tales reflexiones se espera producir una propuesta de actividades de aula que integre los elementos didácticos obtenidos a partir de la reflexión de la transposición didáctica del concepto de grupo cíclico en el contexto de la criptografía asimétrica. Con los resultados obtenidos se espera mostrar la forma como el conocimiento relativo a los grupos cíclicos se modifica a través de diferentes instancias y momentos hasta que es efectivamente incorporado en los contextos académicos. Dichos análisis permiten redimensionar el sentido de las prácticas pedagógicas de los maestros, el sentido de la actividad matemática de los estudiantes y por ende de los procesos de aprendizaje de los mismos respecto al grupo cíclico.

Taba de Contenido

Índice de Imágenes

Índice de Tablas

Introducción

Los estudios en psicología cognitiva han permitido el avance y la ampliación de las perspectivas didácticas en torno a la conceptualización del grupo cíclico realizada por Dubinsky (2000). Dichos avances hacen necesario revisar y replantear, tanto los ambientes escolares que se han generado para la enseñanza y el aprendizaje de dicho concepto como el enfoque adoptado en la formación de docentes, para favorecer la comprensión de los fenómenos y los problemas asociados a la construcción y desarrollo del pensamiento matemático. En este sentido, surgen diferentes preguntas a la hora de enfrentar estos estudios: ¿Cuál es el papel y la función de los procesos de comunicación en la formación de saberes matemáticos, en particular el concepto de grupo cíclico?, ¿Cómo integrar las diferentes aplicaciones, como la criptografía asimétrica, como parte relevante del proceso de construcción de significado del grupo cíclico?, ¿Cuáles concepciones sobre grupo cíclico están orientando las prácticas pedagógicas y las propuestas de los libros de texto que circulan en el medio? ¿Cuáles son las conceptualizaciones que se logran formar los estudiantes, luego de haber sido escolarizados durante los cursos de álgebra abstracta, respecto del grupo cíclico?

En respuesta a dichas demandas, el presente documento contiene un análisis desde la transposición didáctica del concepto de grupo cíclico, en el contexto de la criptografía asimétrica. Dicho ejercicio se remite en primera instancia a las reflexiones de orden histórico-epistemológico y cognitivo para, con base en ello, indagar las nociones y los conceptos que están presentes en las prácticas pedagógicas y en los procesos desarrollados por los estudiantes al respecto del concepto en cuestión. A la luz de tales elementos, se caracterizaron y se contrastaron diferentes formas de aproximación ontológica y epistemológica del concepto de grupo cíclico, con los referentes curriculares dados desde el Ministerio de Educación Nacional, con las propuestas pedagógicas de

los textos escolares y con la gestión que el maestro hace de la actividad matemática del estudiante respecto al grupo cíclico.

Para abordar este conjunto de interrogantes en el marco de la teoría de la transposición didáctica se llevaron a cabo diferentes análisis de nociones y conceptos que están presentes en la gestión que desarrolla el docente en el aula de clase, en contraste con diferentes formas de aproximación ontológica y epistemológica del concepto de grupo cíclico. Lo anterior se cristalizó en la elaboración de un análisis a nivel histórico-epistemológico de tal forma que se obtuviera una visión sobre los condicionantes epistemológicos claves en el desarrollo histórico del concepto de grupo cíclico en el contexto de la criptografía asimétrica.

Un segundo análisis a nivel de los libros de texto que permite evidenciar los elementos rectores que están consultando los docentes para la formulación de sus actividades de clase. Un tercer análisis en la perspectiva didáctica que ofrezca elementos de reflexión como enfoques aplicados a la criptografía asimétrica relativos al trabajo de aula y en función de los procesos cognitivos que desarrolla el estudiante para la construcción del concepto de grupo cíclico. Un cuarto análisis se enfoca a la caracterización de las prácticas pedagógicas que emplean los docentes en la gestión de la actividad matemática en el aula.

El reconocimiento, la caracterización y la valoración de las relaciones que se pudieron establecer entre tales elementos del sistema didáctico, permitieron reconocer referentes didácticos básicos para orientar el quehacer docente y permear los diseños curriculares, de tal forma que se privilegien el diseño de situaciones a partir de variables centrales en relación con los diferentes procesos de construcción del grupo cíclico.

Así por ejemplo, desde las prácticas educativas y en particular desde las actividades propuestas en los libros de textos universitarios, se aprecia cómo se aborda la construcción del concepto de grupo cíclico de manera superficial y se centra la atención en la enseñanza de las definiciones, teoremas y demostraciones. Es decir, se dejan de lado los contextos de significación del grupo cíclico y se abordan los procesos demostrativos formales sin dar espacio para el fortalecimiento de los procesos investigativos e interdisciplinares que el estudio de tal objeto permite en áreas como la criptografía asimétrica. Esto implica para muchos estudiantes encontrarse con un entorno que les obliga a realizar pruebas rigurosas y dificulta establecer relaciones con problemas de la vida cotidiana. Por lo anterior, incluir aplicaciones mediadas por tecnologías en el estudio del objeto de grupo cíclico podría contribuir a la motivación en el aula de clase.

Planteamiento del problema

Los procesos de enseñanza del Álgebra Abstracta, en particular en la formación de estudiantes de los programas de Matemáticas y Licenciatura en Matemáticas de la Universidad del Cauca, están enfocados en el desarrollo de contenidos referidos al estudio de estructuras algebraicas. En los respectivos cursos se estudian explícitamente y de manera abstracta todas las propiedades de objetos matemáticos como grupo, anillo y campo. Además, según la descripción del curso Teoría de Grupos ofertado por el Departamento de Matemáticas, el estudiante tiene la oportunidad de ejercitarse y capacitarse en los procesos de razonamiento y argumentación formal, donde la intuición geométrica y física no es tan útil como en otras áreas de las matemáticas.

A pesar del esfuerzo a nivel mundial de muchos investigadores por vincular herramientas tecnológicas en los cursos de álgebra abstracta, el desarrollo de estos en la Universidad del Cauca no ha considerado, de manera explícita, el uso de tales herramientas, pues metodológicamente su

proceso de enseñanza se hace mediante una exposición lógico deductiva -definición, teorema, demostración-.

Una herramienta tecnológica que se puede usar en estos cursos es Sage (sagemath.org) un sistema de software de código abierto y gratuito para matemáticas avanzadas que contribuye al estudio del álgebra abstracta mediante la unificación, bajo un solo entorno, lenguaje y jerarquía de objetos, de toda una colección de software matemático proporcionando una interfaz Python a software libre especializado en distintos campos entre los que se destacan Álgebra, Teoría de grafos, Teoría de grupos y Teoría de números. Respecto al tratamiento de objetos algebraicos, específicamente del objeto Grupo, existen estudios realizados por Dubinsky y colaboradores y notas de clase de cursos de álgebra abstracta que involucran en cada sección ejercicios en Sage. Como por ejemplo Judson, T. W., & Beezer, R. A. (2017)- Álgebra Abstracta Teoría y Aplicaciones.

En tal sentido, y teniendo en cuenta el uso del álgebra abstracta en desarrollos tecnológicos como la criptografía asimétrica sobre curvas elípticas (Bernstein, 2006) y los cifrados extremo a extremo (Ayerra, 2018), se hace necesaria la implementación de herramientas tecnológicas en su enseñanza y la migración del conocimiento hacia un entorno interdisciplinar que contribuya al mejoramiento de las prácticas pedagógicas.

Por lo anterior se propone una articulación entre el concepto de grupo cíclico y la criptografía asimétrica mediada por el software Sagemath a través de la descripción y la caracterización de las etapas que configuran un proceso de transposición didáctica del objeto matemático referido pues el estudio de la aritmética modular asociada a la noción de grupo cíclico es esencial en la construcción de códigos, claves de dominio público y, en general, en disciplinas como la Criptografía y Seguridad Informática, siendo así muy relevantes sus aplicaciones.

Artigue (2015) afirma: “Siempre se han considerado las tecnologías informáticas como una manera de mejorar las prácticas de enseñanza y aprendizaje en matemática, haciéndolas más constructivas y experimentales” (p.17). En esta misma línea, Harel & Sowder (2007) afirman: “queda patente la necesidad del uso de las nuevas tecnologías, especialmente en educación”, estos autores se cuestionan sobre “el papel del álgebra simbólica en la reconceptualización de las matemáticas en general, en vista del auge de las tecnologías electrónicas en educación, especialmente en sistemas informáticos de álgebra (…)”, (p.824).

Respecto de las "nuevas" tecnologías, Balacheff (1993) define el término de transposición informática y subraya que “el desarrollo de las tecnologías informáticas, su introducción en la escuela y lugares de formación, se acompaña de fenómenos nuevos del mismo orden que los de la transposición didáctica” (p.364).

> Con el desarrollo de la informática en las últimas décadas, las aplicaciones que involucran álgebra abstracta y matemáticas discretas se han vuelto cada vez más importantes, y muchos estudiantes de ciencias, ingeniería e informática están eligiendo ahora una especialización en matemáticas. Aunque la teoría todavía ocupa un papel central en la asignatura de álgebra abstracta y ningún estudiante debería pasar por un curso de este tipo sin una buena noción de lo que es una demostración, la importancia de aplicaciones como la teoría de la codificación y la criptografía ha crecido significativamente (Judson & Beezer, 2017)

Como afirman Cesaratto & Fuentes (2015) desde su experiencia, en los cursos de los profesorados de matemática se suele enseñar matemática como una disciplina descontextualizada y sin vínculos con otras ciencias. Y consideran que las razones principales de tal relegación suelen ser “la falta de tiempo” para tratar los contenidos de la materia, las dificultades que presupone

introducir conceptos de otras disciplinas de forma tal que los mismos sean significativos para los estudiantes y que el tratamiento de los mismos deje aprendizajes matemáticos relevantes.

En la asignatura Teoría de Grupos se tratan algunos temas básicos de teoría de números, algebra de polinomios y se fundan las bases teóricas para el estudio de la Teoría de Anillos y la Teoría de Campos. Dichos temas son fundamentales en el estudio y generación de nuevos criptosistemas[1]. Por ejemplo, el protocolo criptográfico diseñado en 1978 por R. Rivest, S. Shamir y L. Adleman y popularmente conocido como RSA. Una de las aplicaciones típicas de la teoría de números a la informática puesto que el proceso de "encriptamiento" de textos utiliza propiedades de la aritmética modular. Además, la garantía que ofrece para la transmisión "segura" de datos por medios digitales radica en la consabida dificultad computacional para factorizar números enteros grandes.

En resumen, se encuentra, por un lado, alto nivel de abstracción en una temática básica para el estudiante, el uso de la tecnología y su influencia en la enseñanza y aprendizaje en el estudio de grupo cíclico. Bajo estas consideraciones, surge la pregunta de investigación.

Pregunta de investigación

¿Cómo realizar un proceso de transposición didáctica del concepto de grupo cíclico, en el contexto de la criptografía asimétrica[2]?

[1] **Criptosistemas**: Un criptosistema es un término general que se refiere a un conjunto de primitivas criptográficas utilizadas para proporcionar servicios de seguridad de la información. La mayoría de las veces el término se utiliza junto con las primitivas que proporcionan confidencialidad, es decir, el cifrado. (Menezes et al., 1996)

[2] **Criptografía asimétrica:** Un sistema criptográfico asimétrico es un sistema que implica dos transformaciones relacionadas -una definida por una clave pública (la transformación pública) y otra definida por una clave privada (la transformación privada)- con la propiedad de que es computacionalmente inviable determinar la transformación privada a partir de la transformación pública (Menezes et al., 1996)

Objetivos

Objetivo general

- ✓ Desarrollar las etapas del proceso de transposición didáctica del concepto de grupo cíclico, en el contexto de la criptografía asimétrica.

Objetivos específicos

- ✓ Describir y caracterizar las etapas del proceso de Transposición didáctica del concepto de grupo cíclico, en el contexto de la criptografía asimétrica.
- ✓ Diseñar una unidad de introducción a la aritmética modular para aplicar a un grupo de estudiantes del semillero de investigación SEC.
- ✓ Generar una propuesta para abordar el protocolo criptográfico ElGamal como una actividad introductoria a la criptografía basada en grupos cíclicos.

Antecedentes

El estudio de las estructuras algebraicas desde Galois hasta la actualidad no solo ha enriquecido al campo de las matemáticas sino también al ámbito tecnológico. Muchas son las aplicaciones que se pueden encontrar en la literatura científica. La noción de grupo es quizá la base para emprender el estudio de dichas estructuras y comprender algunas de las aplicaciones a la tecnología. No obstante, para ciertas aplicaciones y objetos matemáticos es necesario definir algunos conceptos y teorías claves en el tema de estudio entre los cuales se encuentran La Transposición Didáctica, Ciberseguridad y Criptografía

Como antecedentes en el marco de la transposición didáctica se van a citar dos estudios, uno de los cuales se presenta como tesis de maestría, y el otro como un reporte de investigación. Ambos elaboran y reportan modelos didácticos que caracterizan las adaptaciones, las modificaciones, las

reconstrucciones y el tipo de actividad asociada a cierto conocimiento matemático, para luego analizar el tipo de restricciones didácticas que influyen en el proceso de aprendizaje de dicho saber.

El primer estudio titulado *La Transposición Didáctica del Álgebra en las Ingenierías. El Caso de los Sistemas de Ecuaciones Lineales*, elaborado por Silvia Elena Ibarra Olmos (Ibarra, 2008), caracteriza el proceso de transformación del conocimiento referido a las ecuaciones lineales en un plan de estudios de ingeniería desde que ha sido diseñado en el currículo de la carrera hasta que es enseñado en las aulas de clase. El segundo estudio titulado *Un ejercicio de transposición didáctica en torno al concepto de número natural en el preescolar y el primer grado de educación básica*, elaborado por Norma Lorena Vásquez Lasprilla (Vásquez, 2010), analiza y explica los procesos de transposición didáctica en torno al concepto de número natural en el contexto de la enseñanza preescolar y el primer grado de educación básica en Colombia.

En los planteamientos de la tesis de Ibarra se evidencian los diferentes factores que influyen en el proceso de transposición didáctica de las ecuaciones lineales en el marco de un programa de ingeniería a partir del estudio de la constitución de significados personales/institucionales[3]. Dicha tesis asume el análisis del proceso transpositivo a nivel micro, es decir, se estudian los procesos de transformación que tiene el conocimiento matemático al interior de una institución. Para ello examina el significado personal/institucional, el significado pretendido y el significado referencial sobre las ecuaciones lineales a la luz de los sistemas de prácticas matemáticas institucionalizadas. Éstos últimos se estudian como conjunto de acciones y expresiones encaminadas a la solución de una situación puntual. Las relaciones que se establezcan entre cada uno de estos sistemas de

[3] Como lo señala Ibarra (2008), "Entenderemos por significado personal/significado institucional de un objeto matemático al sistema de prácticas operativas y discursivas que hace una persona o una institución para resolver un campo de problemas" (p. 5). Vale la pena aclarar que nociones como significados personales e institucionales, sistemas de prácticas, significado pretendido y referencial son tomadas desde la teoría onto semiótica desarrollada por el profesor Juan D. Godino y sus colaboradores.

prácticas son los que, en mayor proporción, van a determinar cada una de las transformaciones que sufre el conocimiento relativo a las ecuaciones lineales en el programa de ingeniería. Así pues, desde la perspectiva de la transposición didáctica la tesis muestra que:

1. Un análisis transpositivo del saber matemático en el marco de una institución (nivel micro), involucra la reflexión en torno a los diferentes significados construidos: a nivel referencial (alude a la significación institucional que se va a asumir del conocimiento matemático), a nivel de diseño (el significado diseñado y que se espera alcanzar luego de un proceso de enseñanza del conocimiento matemático), y a nivel personal (el significado propio que tiene el docente del conocimiento matemático, el cual permea su acción).
2. Se requiere un estudio sistemático de los sistemas de prácticas, tanto institucionales como personales, para explicar y reconstruir el conocimiento matemático en el marco institucional.
3. Es necesario establecer redes de objetos que conciernen y dan sentido al conocimiento matemático objeto de estudio en función de los requerimientos y responsabilidades sociales de las instituciones donde se estudió dicho objeto, y a partir de las diferentes formas de constitución del mismo a través de la historia.

Por su parte, el segundo estudio elaborado por Norma Vásquez refiere que la enseñanza del número natural en los contextos escolares está pasando por una crisis que se manifiesta, de un lado, por estar fundamentada en la transposición de los fundamentos de la teoría piagetiana sin un análisis crítico de las implicaciones de tal transición, y de otro, de una organización curricular fundamentada en la teoría de conjuntos, que busca la rápida memorización de reglas y algoritmos,

y más complejo aun, que no reconoce de manera consciente y sistemática otras formas ontológicas en los procesos de constitución del número natural.

Adicional a lo anterior, estas propuestas curriculares no se muestran coherentes con los lineamientos curriculares del área de matemáticas. Se requiere entonces en la escuela, un trabajo de corte didáctico encaminado a la construcción del concepto de número de manera significativa y coherente con los marcos institucionales y sociales, epistemológicos y ontológicos. Ello implica indagar sobre los elementos y contextos que permiten dinamizar diferentes significados de número. De igual forma se debe centrar la mirada en las situaciones que generan necesidades de comunicación de cantidades y en el conteo como estrategia fundamental para el desarrollo de las comprensiones numéricas.

Como se observa, los dos estudios referidos toman como base los elementos de la transposición didáctica para construir un proceso que dé cuenta de las transformaciones y reorganizaciones a que tiene lugar el saber matemático en un marco institucional dado. En estos estudios se reporta la complejidad y los aportes que brindan los análisis transpositivos para orientar los procesos de construcción de currículos, de replanteamiento de prácticas escolares y de construcción de significados en torno al saber matemático objeto de estudio.

Justificación

Desde mi experiencia, como estudiante de Licenciatura en Matemáticas de la Universidad del Cauca, cuando cursé las materias relacionadas con álgebra abstracta hasta llegar a teoría de campos, noté gran interés por parte de los profesores por explicar el entramado teórico de cada objeto matemático visto en clase. Sin embargo, a medida que avanzaba en estos cursos percibí que, a pesar de saber recitar la definición de grupo, anillo, campo, campo finito, y de comprender algunos

teoremas fundamentales de estos cursos no le encontraba ningún sentido ni relación con otras áreas del conocimiento. La mayoría de las clases eran totalmente dedicadas al desarrollo de las temáticas mediante una exposición lógico deductiva. No obstante, cuando empecé a asistir al semillero de investigación en ciberseguridad me di cuenta que los profesores que hacían investigación y publicaban artículos con temas afines a los del semillero, realmente usaban muchas de las herramientas mencionadas en los cursos.

Mi participación en este semillero permitió conocer la relación del algoritmo de cifrado RSA y la exponenciación modular con la teoría de números y el concepto de grupo. La Seguridad Informática, el criptoanálisis y su relación profunda con la teoría de anillos y la teoría de campos. Por ello decidí realizar la etapa de intervención en el semillero de investigación SEC, porque estoy convencido que la investigación le da significado a nuestro quehacer académico.

Según Vélez & Dávila (1984) la investigación y la docencia deben conformar una unidad de acción para el investigador, ya que es ésta la mejor manera de aportar al estudiante contenidos que eleven el nivel académico, esta unidad permite al profesor reflexionar sobre sus inquietudes intelectuales y científicas en la medida que investiga y traspasa parte de esas inquietudes y conocimientos a un auditorio preparado. De esta manera logra acercar al estudiante realmente a la realidad nacional, con conocimientos extraídos de esa realidad y superando el nivel mediocre y pragmatista que es tan característico de la cátedra colombiana.

Sobre la población del Semillero SEC

El semillero de investigación SEC (Security, Encryption & Cybersecurity) de la Universidad del Cauca se encuentra adscrito al grupo de investigación matemática discreta y aplicaciones (MATDIS) cuyas principales líneas de investigación son: Criptografía, Seguridad de la

Información, Informática Forense, Teoría de números y Álgebra. Los estudiantes inscritos al semillero, en promedio quince, hacen parte de los programas: Licenciatura en Matemáticas, Matemáticas e Ingeniería de Sistemas y la mayoría se encuentran cursando sexto semestre de sus respectivos programas académicos.

Marco Teórico.

El estudio de las estructuras algebraicas desde Galois hasta la actualidad no solo ha enriquecido al campo de las matemáticas, sino también al ámbito tecnológico. Muchas son las aplicaciones que se pueden encontrar en la literatura científica. La noción de grupo es quizá la base para emprender el estudio de dichas estructuras y llegar a comprender algunas de las aplicaciones a la tecnología. No obstante, para comprender ciertas aplicaciones y objetos matemáticos es necesario definir algunos conceptos y teorías claves en el tema de estudio entre los cuales se encuentran la Transposición Didáctica, Ciberseguridad y Criptografía

La Transposición Didáctica [4]

Las ideas fundamentales de Chevallard (1998) en la teoría sobre la transposición didáctica, a partir de las cuales se llevó a cabo el análisis de la transformación que sufre un conocimiento desde el nivel de objeto matemático hasta el nivel de objeto de enseñanza son la base para dar respuesta a la pregunta de investigación plateada. Para evidenciar esta transformación se analizó el tema de la aritmética modular asociada a la noción de grupo cíclico, necesario para comprender la criptografía asimétrica basada en grupos cíclicos, el cual es un tema de interés en la criptografía moderna.

[4] Las ideas que se presentan a continuación son una síntesis de los desarrollos teóricos hechos por Chevallard al respecto de la transposición didáctica (Chevallard, 1998)

La transposición didáctica es un tema que introduce Chevallard en el año 1978 y posteriormente lo retoma con el libro denominado "La transposition didactique" en 1980. Dicho trabajo ha generado un marco de discusión y de investigación a nivel internacional. Según Carvajal y Vásquez (2012) se puede observar la transformación que sufre la información desde su origen hasta la comunicación de la misma a la sociedad. Un efecto similar ocurre en el proceso que sufre un saber desde sus orígenes hasta el momento en el cual es parte de un sistema didáctico, entendiendo por sistema didáctico la tripleta docente, estudiante y saber.

Chevallard describe esta situación a través de su teoría sobre la transposición didáctica, definida como la transformación o cambios que sufre el saber científico para poder ser enseñado. En procura de indicar cuáles son los saberes matemáticos que están presentes, los ha categorizado en nociones matemáticas que, por lo general, son construidas o definidas y objeto de estudio por matemáticos, por ejemplo, la noción de grupo

La transposición de conocimientos científicos a conocimientos escolares es un complejo proceso de movimiento de saberes de una comunidad hacia otra. Ciertos teóricos suponen que debido a que los conocimientos científicos se han construido socialmente en ámbitos no escolares, su introducción al sistema de enseñanza obliga a una serie de modificaciones que afectan su funcionamiento.

Según Cajas, F (2001) el hecho de que la transposición de saberes científicos a saberes escolares ya se ha llevado a cabo de una manera un tanto espontánea significa que casi nunca se estudian sus implicaciones a largo plazo. Este proceso de incorporación de saberes científicos a saberes escolares plantea una serie de problemas teóricos y prácticos fundamentales. Pero más importante que estas implicaciones en las ideologías de los académicos, es que no se ha discutido cómo algunos conocimientos científicos (p.e., el álgebra abstracta) pueden ser útiles en la vida diaria de

quienes los aprenden. Aquí hay dos puntos importantes, uno es la planificación del conocimiento científico como saber escolar y otro el impacto social que un determinado conocimiento científico pueda tener en la vida cotidiana de los individuos. Ambos tienen diferentes historias y propósitos pero están de alguna manera relacionados.

La investigación didáctica junto al trabajo desarrollado por psicólogos cognitivos interesados en la adquisición de conceptos científicos, muestra que los estudiantes no aprenden conceptos aislados sino, más bien, grupos de conceptos interconectados (Chi, 1992, Vosniadou, 1991).

El sistema didáctico no es un modelo estático, sino que en él se recrean dinámicas y relaciones tanto con el entorno físico y cultural de los participantes, como con las concepciones, creencias y fundamentos epistemológicos que orientan las formas de actuar de cada uno de ellos. El análisis de dichos entornos a la luz de relaciones ternarias, en función de un saber matemático, brinda referentes para orientar tanto los procesos de enseñanza como los de aprendizaje. Dicha dinámica de intercambio e interdependencia se puede representar a través de un esquema como el de la imagen 1. (Vásquez, 2010).

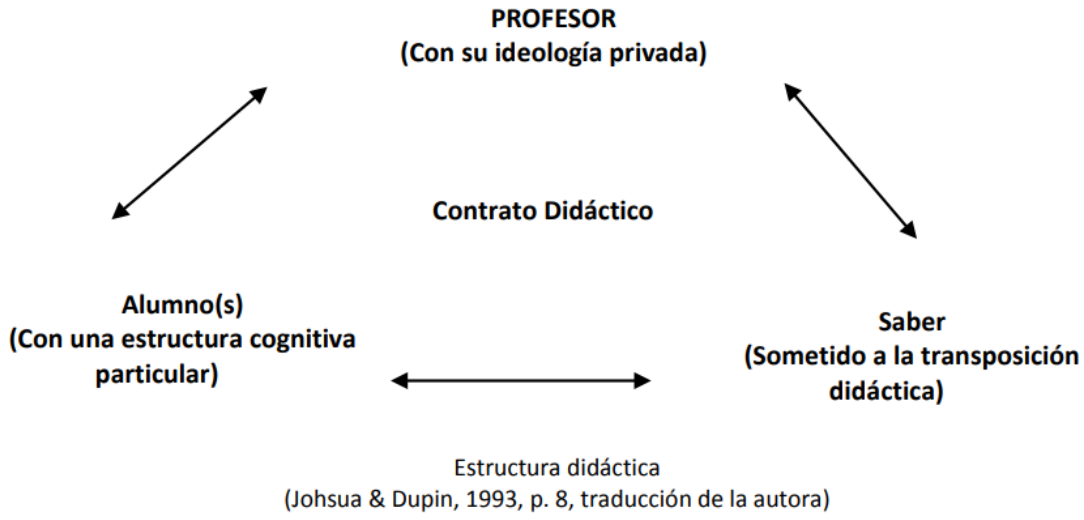


Imagen 1 Estructura didáctica tomado de Johsua & Dupin, 1993

El saber matemático surge en condiciones históricas particulares, se instaura como respuesta a problemáticas específicas y se enmarca en unos elementos epistemológicos particulares. Tal conjunto de factores no puede ser integrado a la estructura didáctica, por ello el saber matemático sufre transformaciones para ser incorporado en los esquemas escolares. De ahí que sea indispensable elegir cuáles de estos saberes son preponderantes en la cultura circundante y qué de ellos es pertinente enseñar y aprender. Este proceso de selección, reconstrucción y adaptación de los saberes matemáticos para ser enseñados en los contextos escolares se denomina *transposición didáctica.*

> En este proceso de análisis se identifican aquellos elementos invariantes propios y que caracterizan el objeto matemático que se quiere abordar, y son justamente esos elementos quienes se convierten en objeto de enseñanza. De ahí que no haya lugar para comparar o decir que "los saberes a enseñar son reducciones o simplificaciones de los saberes científicos". Por el contrario, son los saberes científicos quienes, junto con su historia, evolución y epistemología, dan validez y justifican la escogencia de un determinado saber para ser enseñado. (Vásquez, 2010)

Describir y caracterizar las etapas del proceso de transposición didáctica del concepto de grupo cíclico en el contexto de la criptografía asimétrica fue uno de los objetos centrales. La selección de saberes para ser enseñados requiere la elaboración de análisis epistemológicos, históricos y culturales en torno a los conceptos escogidos dado que cada saber adquiere una connotación diferente y su validez se certifica dentro de su respectiva comunidad científica. Según Chevallard (1998) para el caso de los saberes a enseñar es la *noosfera*[5] la que se encarga de regular de manera

[5] La noosfera es el grupo de personas que se encargan de tomar decisiones globales acerca de los saberes que van a ser enseñados en una determinada comunidad, y el proceso que deben seguir para ser inscritos en el contexto escolar.

general las relaciones entre la estructura didáctica y el medio social en el cual se enmarca la institución donde se lleva a cabo el proceso de transposición

La difusión del saber compartido al interior de una comunidad científica requiere un nivel de despersonalización, descontextualización, de a-temporalización, se necesita dejar de lado las incertidumbres y posibles hipótesis iniciales, los procesos de ensayo y error y separar la persona del saber (el saber que en principio fue personal, pasa a ser social). Sólo se comunica a la comunidad científica un saber claro y riguroso, despersonalizado, formal y objetivo. Este proceso que enmarca la instauración de un saber como saber científico al interior de una comunidad se denomina transposición didáctica en sentido amplio. En contraste, la transposición en sentido estricto se entiende como el proceso de transformación desde el momento en que se instaura un saber científico hasta que es seleccionado para ser enseñado.

En el proceso de transposición didáctica, ya sea en sentido amplio o estricto, se pueden identificar unas características especiales e inherentes, tales como: la especificidad de los saberes, la puesta en textos del saber, la desintetización de los modelos científicos, los tiempos didácticos y tiempos de aprendizaje y las nociones explícitas e implícitas. Cada uno de estos elementos participa activa y determinantemente en dicho proceso. Una revisión de cada una de estas características ayudará a clarificar el concepto mismo de transposición didáctica.

Especificidad de las construcciones didácticas.

Según Chevallard (1998) los objetos de saber que se constituyen en material de enseñanza se denominan nociones matemáticas, estas nociones son construidas a través de definiciones o por medio de la caracterización e identificación de sus propiedades. De igual forma se reconocen a

Está conformada principalmente por gubernamentales, miembros de grupos de investigación, delegados de los padres de familia e instancias representantes de diferentes organizaciones políticas.

partir de sus ocasiones de uso. Durante el proceso de construcción de las nociones matemáticas se presentan y se utilizan otro tipo de nociones las cuales sirven como herramientas y no se constituyen en objetos de aprendizaje. Dichas nociones se denominan paramatemáticas y se utilizan como objetos auxiliares, necesarios para la enseñanza y el aprendizaje de las nociones matemáticas pero que son manejadas por los estudiantes y por el maestro inconscientemente puesto que se asume que ellas ya han sido adquiridas previamente. Dichas nociones son: conjunto, número primo y el conjunto de los números enteros. Se tiene entonces que en el proceso de enseñanza y de aprendizaje se hace uso de diferentes tipos de saberes algunos enseñables, otros enseñados y otros no enseñables. Esta interacción de saberes hace parte de la dinámica de transmisión burocrática de la noosfera y del saber en contextos escolares

Según Chevallard (1998) para incorporar y transmitir los saberes en los contextos escolares es necesaria la división de la teoría en campos específicos de saber, lo cual genera formas particulares y especializadas de aprender y de relacionarse con dicho saber. Para ello, éste es presentado de una manera analítica con un discurso detallado se entrega el saber por fragmentos, sucesiones de capítulos o lecciones, se trata de restablecer unas nuevas relaciones y secuencias, de tal forma que el saber tenga sentido en el contexto donde está inmerso, pero sin perder su estructura general. Se trata de crear un modelo en el contexto didáctico. Este proceso se denomina desincretización del saber.

Una vez se delimitan y se perfilan los campos de saber también se separa el saber de las personas o grupos que lo produjeron, esto es, se despersonaliza el saber, se aísla y se borra todo rastro o relación con aquellas personas que intervinieron en su formalización como objeto de conocimiento. De esta manera el saber se muestra objetivo y universal expresado a través de representaciones

propias para lograr una comunicación dentro de la comunidad ya que se requiere dar un sentido claro y lógico al saber a ser enseñado.

La puesta en textos del saber

La delimitación de los saberes que se van a enseñar requiere que la comunidad que va a participar del proceso de transposición conozca de manera explícita y escrita las nociones matemáticas con las cuales se va a trabajar. Según Vásquez (2010) se requiere de un proceso de textualización del saber que involucra de manera implícita las nociones paramatemáticas que van a ser prerrequisitos o herramienta auxiliares, las concepciones de lo que significa "saber" entre las personas que se asumen el proceso de estudio y la epistemología que orienta el aprendizaje. De manera inherente la puesta en texto del saber determina un camino progresivo del conocimiento dado que el texto se organiza y se estructura a través de una lógica particular la cual sirve como referencia para la medición del aprendizaje.

Para lograr que los saberes textualizados sean integrados como objeto de enseñanza es necesario que se introduzcan como algo novedoso que genere inquietudes y retos para quien aprende. A la vez debe encajar con la estructura de los saberes antiguos para que logre un engranaje inicial o punto de partida para la generación de nuevos aprendizajes. Así la introducción del objeto de enseñanza en la estructura didáctica produce una tensión entre lo nuevo y lo antiguo. Dicha tensión se supera cuando se dan los aprendizajes pues el nuevo saber que fue insertado en la estructura se articula a los saberes precedentes, se "automatiza", se vuelve cotidiano en función de su uso hasta que se desgasta y envejece, en este punto se inicia nuevamente el proceso.

En contraste el tiempo del que aprende es diferente y varía de acuerdo con las condiciones de cada individuo. En el proceso de aprendizaje los conocimientos se reorganizan, se

redescontextualizan y se incorporan a una estructura cognitiva existente, de ahí que este tiempo no pueda ser preestablecido y sólo el estudiante determina cuándo se ha apropiado de un concepto.

Criptografía

La Criptografía es una rama de las matemáticas que al orientarse al mundo de los mensajes digitales proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. El problema de la confidencialidad se vincula comúnmente con técnicas denominadas de "encripción" y la autenticidad con técnicas denominadas de "firma digital", aunque la solución de ambos, en realidad se reduce a la aplicación de procedimientos criptográficos de encripción y desencripción.6.

Según Menezes et al (1996) la Criptografía se divide en dos grandes ramas la Criptografía de clave privada o simétrica y la Criptografía de clave pública o asimétrica. La primera se refiere al conjunto de métodos que permiten una comunicación segura entre las partes siempre que con anterioridad se intercambie la clave correspondiente que se denomina clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar. La Criptografía de clave pública o asimétrica también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la Criptografía asimétrica ocurrió como resultado de la búsqueda de un modo más práctico de intercambiar las llaves simétricas.

Un criptosistema es un término general que se refiere a un conjunto de primitivas criptográficas utilizadas para proporcionar servicios de seguridad de la información. La mayoría de las veces el

[6] Mendvil I. El ABC de los documentos electrónicos seguros. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m163a.htm

término se utiliza junto con las primitivas que proporcionan confidencialidad, es decir, el cifrado. (Menezes et al., 1996).

Aritmética modular

En una división usualmente interesa el cociente, pero en este caso va a interesar el **residuo**. En el conjunto de residuos formado al dividir los números enteros entre un número natural se puede construir una aritmética llamada aritmética modular donde el módulo será este número natural. Este tipo de aritmética pertenece a una rama de las matemáticas de mucha utilidad en Criptografía, ya que permite realizar grandes cálculos manteniendo siempre una representación numérica compacta definida puesto que solo maneja un conjunto finito de números enteros.

La aritmética modular se fundamenta bajo una relación de congruencia entre los números enteros denotada como $a\ mod\ n$. Una relación de congruencia entre enteros es compatible con las operaciones en el anillo de enteros: suma, resta, y multiplicación, para un determinado módulo n, la relación de congruencia se define de la siguiente manera:

Sea $n \in \mathbb{N}$ fijo, sea $M = \{nk : k \in \mathbb{Z}\}$, donde M es el conjunto de múltiplos de n. Se define la relación $\equiv (mod\ n)$, donde: $a, b \in \mathbb{Z}$. Así:

$$a \equiv b\ (mod\ n) \leftrightarrow a - b \in M$$

Esta definición dice que a es congruente con b módulo n sí y sólo si la diferencia entre ambos números es múltiplo de n, o en otras palabras que cuando se divide a a y b entre n esto nos dará el mismo residuo.

Se puede probar que la relación de congruencia definida anteriormente cumple con las siguientes propiedades: reflexividad, simetría y transitividad, lo que la convierte en una relación de equivalencia, induciendo así una partición[7] del conjunto de los números enteros.

Método

Dada la complejidad del análisis del proceso de transposición didáctica del conocimiento matemático y su carácter de fenómeno humano, esta sistematización se enmarca en el *paradigma cualitativo*[8], parte del análisis de problemas de ciberseguridad que se han solucionado usando herramientas de álgebra abstracta como el concepto de grupo cíclico. Se seleccionaron los objetos matemáticos de estudio necesarios para la intervención y algunas estrategias de enseñanza de los mismos con el fin de tener elementos suficientes para el diseño de las fases de la intervención: Identificar las etapas del proceso de transposición didáctica y aplicarlas al concepto de grupo cíclico en el contexto de la criptografía asimétrica. Además, como el proceso de transposición didáctica obedece a las condiciones y necesidades particulares de grupos sociales e instituciones un proyecto de corte cualitativo permite identificar, estudiar y relacionar los diferentes elementos y factores que intervienen y determinan dicho proceso adaptativo.

El proceso de transposición didáctica responde a unas necesidades contextuales particulares y alude a dinámicas humanas que requieren ser descritas e interpretadas: la escogencia, la transformación, la adaptación y la comunicación del concepto de grupo cíclico en el contexto de la

[7] Una **partición** de un conjunto está formada por los subconjuntos que deben cumplir que: la unión de todos los subconjuntos sea igual al conjunto dado, todos los subconjuntos sean disjuntos entre sí, y que ningún subconjunto sea vacío

[8] "La investigación cualitativa es multimetódica, involucra una interpretación, un enfoque naturalístico de su interpretar la materia. Esto significa que la investigación cualitativa estudia cosas en su escenario natural, intenta dar sentido a, o fenómeno en términos del significado que la gente da de ellas. La investigación cualitativa involucra el estudio la recolección y el uso de una variedad de materiales empíricos –estudio de caso, experiencias personales, introspecciones, historias de vida, entrevistas, observaciones, interacciones, y textos- que describen rutinas y momentos problemáticos y significados en la vida de los individuos." (Creswell, 1998, p. 15, citando a Denzin & Linconl (1994)

criptografía asimétrica. Con el análisis interpretativo de las relaciones, las dinámicas y los significados que se construyen durante el proceso de transposición en torno al concepto de grupo cíclico se formulan explicaciones y justificaciones acerca de la naturaleza, el sentido y la funcionalidad que se le otorga a este concepto en el contexto académico. En este sentido, se trata de caracterizar cada uno de los momentos en los que se lleva a cabo la transposición: la constitución del saber matemático como conocimiento científico, la determinación del saber matemático a enseñar, la contextualización del saber matemático enseñado y el saber matemático aprendido por los estudiantes.

No obstante, este análisis, se centra solo en dos momentos de la transposición didáctica: la determinación del saber matemático a enseñar y la contextualización del saber matemático enseñado, en tanto que los demás momentos requerirían de estudios de tipo longitudinal que exceden los tiempos y posibilidades de los alcances de este proyecto de pregrado.

Así, cada etapa donde se produce el proceso de transposición didáctica (Imagen 1) donde cada uno de los momentos descritos se constituye en un caso que va a servir de referente para dimensionar el proceso adaptativo global que se lleva a cabo desde el saber matemático formal hasta la incorporación de dicho saber en los contextos educativos. Es decir, la constitución del saber matemático formalizado, el proceso de determinación del saber matemático a enseñar y la contextualización del saber matemático enseñado son asumidos como casos que aportan para la comprensión de la transposición didáctica del concepto de grupo cíclico en el contexto de la criptografía asimétrica.

Como parte del desarrollo de los momentos o fases descritas se realizó una conferencia en la que se desarrollaron temáticas relacionadas con el concepto de grupo cíclico en el contexto de la

criptografía asimétrica se indagó a los participantes mediante un formulario de Google, previamente elaborado, sobre el desarrollo de las mismas y posibles aportes a las fases presentadas.

Recolección de la Información

Em el proceso de recolección de información se asumió que "la recolección de datos es visualizada como una serie de actividades interrelacionadas orientadas a reunir buena información para responder las preguntas de investigación emergentes." (Creswell, 1998, p. 61). En este sentido se propuso un esquema de relaciones que se dan entre las actividades durante el proceso de recolección de la información. Tal dinámica permitió regresar periódicamente sobre los datos con el fin de revisar el proceso global. El esquema denominado círculo de recolección de datos (Imagen 2) ilustra dichas relaciones.

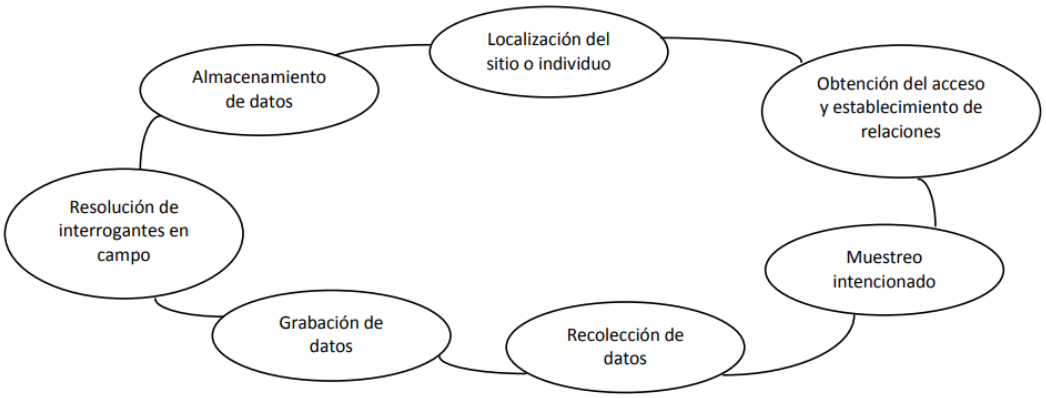


Ilustración 2
Ciclo de recolección de la información en la investigación cualitativa.
(Creswell, 1998, p. 110)

Imagen 2 Ciclo de recolección de información en la investigacion cualitativa tomado de Creswel, 1998

Siguiendo el círculo de recolección de datos y aludiendo al tipo de estudio que se está realizando se plantean dos etapas para analizar el proceso de transposición didáctica: en sentido amplio y en sentido estricto. El sentido amplio abarca los análisis globales al respecto del establecimiento del saber matemático en las instituciones productoras de saber y la selección del saber matemático a

enseñar por parte de la noosfera. El sentido estricto se refiere al estudio de los procesos de enseñanza del concepto de grupo cíclico en el contexto de la criptografía asimétrica. Acorde con esta estructura, se determinan las siguientes etapas:

• Etapa 1: *Determinación del concepto de grupo cíclico que va a ser enseñado*. La determinación del concepto de grupo cíclico que se está privilegiando en el sistema educativo colombiano (como representante de la noosfera) permite evidenciar las adaptaciones que se le hacen a dicho concepto. Esto orienta los procesos de enseñanza, las concepciones que tienen los docentes, la formulación de libros de texto y en últimas define el currículo y el tipo de prácticas (tanto de estudiantes como de docentes) que se van a asumir como válidas en el contexto escolar

• Etapa 2: *El concepto de grupo cíclico, en el contexto de la criptografía asimétrica, a enseñar*. La especificación del proceso de enseñanza del concepto de grupo cíclico en el contexto de la criptografía asimétrica permite perfilar las concepciones que tienen los docentes que participan en el proceso de enseñanza y a la vez establecer el tipo de prácticas que se privilegian al interior de la institución. Esta información se instaura como base para señalar la funcionalidad que se le otorga al grupo cíclico en el marco tecnológico.

Teniendo en cuenta la complejidad y el contexto donde se llevó a cabo el proceso de transposición didáctica se utilizaron las siguientes técnicas de recolección de información: (1) *el análisis textual de diferentes tipos de textos*: La producción escrita de los estudiantes, las grabaciones de las sesiones del semillero, libros de texto y artículos relacionados con teoría de grupos y criptografía, encuestas realizadas a los estudiantes. (2) *la observación participante* de la actividad matemática de los estudiantes, (3) *notas reflexivas* en relación con la información obtenida.

Se estableció para cada caso el tipo de técnica de recolección de información y las fuentes documentales que se emplearon. Así, para:

• Etapa 1: *Determinación del concepto de grupo cíclico que va a ser enseñado*

Se utiliza el análisis textual para reconocer y examinar el proceso de selección y adaptación que ha tenido el concepto de grupo cíclico en el currículo colombiano. Las fuentes documentales que se usan en este caso son: los reportes de investigación y las teorías cognitivas desarrolladas sobre el proceso de construcción y aprendizaje del grupo cíclico y los libros de texto universitarios sobre álgebra abstracta recomendados por profesores del Departamento de Matemáticas de la Universidad del Cauca.

• Etapa 2: *El concepto de grupo cíclico en el contexto de la criptografía asimétrica, a enseñar*

Se emplea el análisis documental que permite identificar las propuestas de trabajo de aula y el tipo de actividad que se plantea al interior de la criptografía asimétrica y dimensionar el efecto de los mismos en el proceso de aprendizaje del concepto de grupo cíclico en el contexto de la criptografía asimétrica. Las fuentes documentales que se usan en este caso son: conferencia y encuesta dirigida a los asistentes al semillero y análisis de algoritmos criptográficos asimétricos basados en grupos cíclicos.

Categorías de análisis

De acuerdo con los planteamientos anteriores el proceso de análisis de la información acerca de la transposición didáctica del concepto de grupo cíclico en el contexto de la criptografía asimétrica se abordó a través del estudio de los datos obtenidos en cada etapa (ver localización de las etapas en la sección recolección de información). Se inició con la organización de datos mediante la creación de archivos. Se procede luego a la lectura reflexiva de dicha información para identificar

categorías básicas de análisis, tales categorías son nominadas en función de las nociones y procesos que abarcan teniendo en cuenta los objetivos específicos formulados. Como punto de partida (categorías a priori) se asumen las categorías de análisis: naturaleza de grupo cíclico, estructura matemática que se establece en torno al grupo cíclico y la criptografía asimétrica que refiere el proceso de transposición didáctica.

Un segundo paso alude a la confrontación de las categorías formuladas con las distintas fuentes (triangulación de datos) y la identificación de estructuras entre los datos. De esta forma se puede caracterizar el proceso de transposición del grupo cíclico en cada etapa. Finalmente se plantea un análisis de las interrelaciones entre las categorías y las estructuras obtenidas en cada caso para obtener un panorama completo y complejo del fenómeno de transposición del grupo cíclico en el contexto de la criptografía asimétrica, es decir, mediante el contraste de la información obtenida en cada uno de las etapas del proceso de transposición didáctica.

Para dar repuesta al **primer objetivo específico:** desarrollar las etapas del proceso de transposición didáctica del concepto de grupo cíclico en el contexto de la criptografía asimétrica, se formula la categoría **análisis de textos** referente a los libros de texto sobre algebra abstracta seleccionados**.**

En este sentido para analizar el saber matemático que en torno al concepto de grupo cíclico en contexto de la criptografía asimétrica se plantea en los libros de texto se toman como referentes tres aspectos. El primero identificó cómo se ha ejemplificado el concepto de grupo cíclico multiplicativo[9] dado que en la generación de criptosistemas asimétricos se requiere de la operación multiplicativa. Este estudio proporciona entre otros una base acerca de la naturaleza que se le ha

[9] Grupo cíclico, definido bajo la multiplicación

asignado al grupo cíclico y el tipo de fuentes de donde se obtiene el conocimiento válido en cada institución. Así, a través de estas distinciones se puede dimensionar el estatus otorgado al grupo cíclico multiplicativo en cada libro de texto seleccionado.

El segundo aspecto a considerar está relacionado con el uso de software para el desarrollo de ejercicios sobre grupo cíclico multiplicativo. Dado que en el diseño del currículo confluyen diversos intereses y concepciones tanto del objeto matemático como de aspectos relativos a la pedagogía y didáctica de las matemáticas, así como la implementación de tecnologías mediadoras del proceso de enseñanza que determina la actividad matemática que se espera el estudiante desarrolle y en últimas se delimitan los sentidos y la funcionalidad de los conceptos matemáticos estudiados, por ello es pertinente incluir en las categorías de análisis de los libros de textos factores asociados al uso de herramientas tecnológicas.

El tercer aspecto identifica en los libros de texto seleccionados las diferentes aplicaciones del grupo cíclico en la criptografía asimétrica, pues la relación entre un concepto matemático y sus aplicaciones se constituye en referente para la práctica pedagógica del docente y la asunción de una u otra perspectiva cognitiva para la enseñanza del concepto de grupo cíclico en el contexto de la criptografía asimétrica potencia y desencadena en los estudiantes ciertos sentidos, habilidades, relaciones y conceptualizaciones. Por ello, es conveniente involucrar algunas aplicaciones en la categoría de análisis de los libros de texto.

Una Mirada a los Libros de Texto de Álgebra Abstracta

En el proceso de transposición didáctica se requiere la selección de los contenidos y de los objetos matemáticos que van a ser enseñados en un contexto educativo: grupo cíclico en el contexto de la criptografía asimétrica. La delimitación de dichos saberes responde a las perspectivas y concepciones de quien realiza este trabajo “la noosfera”. El proceso de selección del saber está

orientado por las concepciones de aprendizaje que tenga la noosfera y por las metas y el tipo de formación que se quiera ofrecer a una comunidad. Como producto de esta mezcla de intereses y metas se obtiene el saber matemático que va a circular en los contextos educativos.

Como parte del proceso de textualización[10] del saber que se ha seleccionado para que circule en los contextos escolares se encuentran las propuestas de trabajo que se formulan en los libros de texto. Estos instrumentos recogen gran parte de los elementos teóricos y didácticos que deben ser tenido en cuenta por los docentes e instituciones para la enseñanza del saber matemático en el aula. De ahí que los libros de textos se conviertan en otro referente para analizar el proceso de transposición didáctica que ha tenido el concepto de grupo cíclico en el contexto de la criptografía asimétrica.

Además, dado que los libros de texto son un instrumento empleado por los docentes para el diseño de actividades de aula el estudio de las propuestas que traen los libros permite configurar elementos sobre el modelo de enseñanza que se emplea y por ende prever los posibles aprendizajes en torno al grupo cíclico en el contexto de la criptografía asimétrica. Como lo propone Gómez (1999) "En efecto, los libros de texto, además de un reflejo del estado de la ciencia, son una muestra indicativa de las concepciones dominantes en los distintos momentos de la historia acerca de qué contenidos deben ser enseñados, cuáles deben ser enfatizados, cuál es la forma de organizarlos, con qué enfoques conceptuales y con qué metodología".

En este sentido el presente apartado se orienta hacia la caracterización de las propuestas que traen algunos de los libros de texto de álgebra abstracta que han circulado y han servido de referente para el trabajo educativo en torno al concepto de grupos cíclico a lo largo del siglo XX y XXI en

[10] Textualizar es escribir textos con sentido, que reconozcan el contexto social en que se inscriben, que se adecuen a la intención comunicativa, a los destinatarios y al género elegido. García (2011)

Colombia. Los criterios de selección de los libros de texto se establecieron con base en: una encuesta[11] realizada a los profesores del Departamento de Matemáticas de la Universidad del Cauca que han orientado el curso de Teoría de Grupos durante los últimos siete años y la recurrencia de aparición en los planes de estudio de la asignatura Teoría de Grupos de once universidades colombianas que ofertan pregrados en matemáticas, obteniendo los siguientes resultados y codificaciones:

Codificación

Tabla 1. Codificación Docentes

Codificación
D1
D2
D3
D4
D5
D6
D7

Tabla 2. Codificación Planes de estudio Teoría de Grupos

Planes de estudio Teoría de Grupos	Codificación
Universidad de los Andes	U1
Universidad de Antioquia	U2
Universidad del Atlántico	U3

[11] Formulario: https://forms.gle/ZutrNLuP2wS8LneY9

Universidad Pedagógica y Tecnológica de Colombia	U4
Universidad del Cauca	U5
Universidad de Córdoba	U6
Universidad Distrital "Francisco José De Caldas"	U7
Universidad Nacional Bogotá	U8
Universidad Nacional Medellín	U9
Universidad Industrial de Santander	U10
Universidad del Valle	U11

Tabla 3. Codificación libros de texto seleccionados

Bibliografía / Textos Guía	Codificación
T Judson Abstract Algebra: theory and applications	L1
D. Dummit, R. Foote.Abstract Algebra	L2
Herstein, I.N. Álgebra Abstracta.	L3
Fraleigh, John B. Algebra Abstracta, 2nd edition.	L4
Gallian, Joseph A.Contemporary abstracta algebra	L5
T. W.HUNGERFORD.Abstract algebra	L6
Dubreil, P. (1975). Teoría de grupos	L7
J. Dorronsoro y E. Hernández: Números, grupos y anillos	L8
Lang, S. Algebra, Addison- Wesley,	L9
Neumann, P. Stoy G., Thompson E., Groups and Geometry	L10
Dean, R. (1967). Elements of Abstract Algebra	L11
McCoy N. (1972). Fundamentals of Abstract Algebra.	L12

Suárez, Marco F. "Elementos de álgebra"	L13
Ruiz, Roberto. De los enteros a los dominios	L14

Resultados

Los libros de texto con mayor recurrencia o empleados como texto guía de la asignatura teoría de grupos según las encuestas realizadas y los contenidos programáticos consultados se evidencian en la imagen 3. En particular los libros empleados como texto guía que privilegian el estudio del concepto de grupo cíclico en el contexto de la criptografía asimétrica se analizan con base en las diferentes fichas técnicas, los tipos de ejemplos, los tipos de ejercicios y el tipo de software utilizado en cada libro.

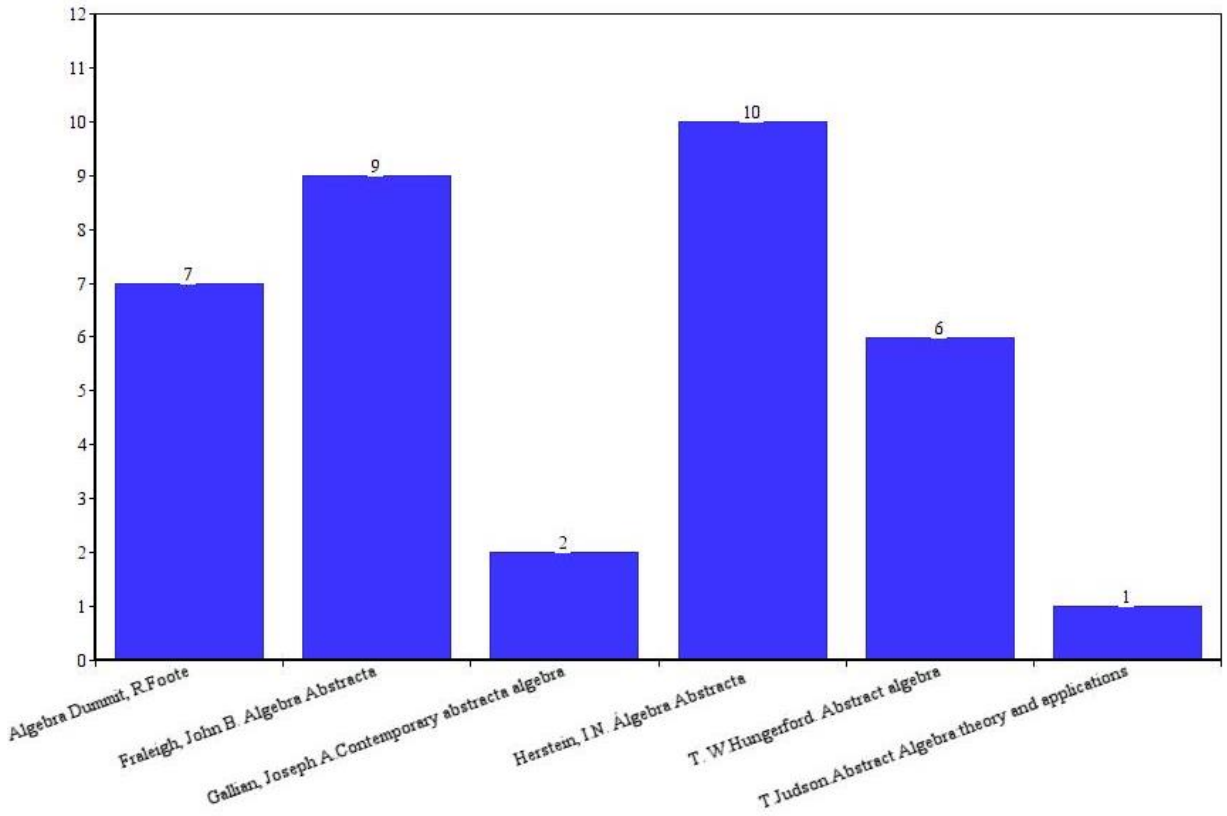


Imagen 3. recurrencia de aparición en los planes de estudio de la asignatura Teoría de Grupos

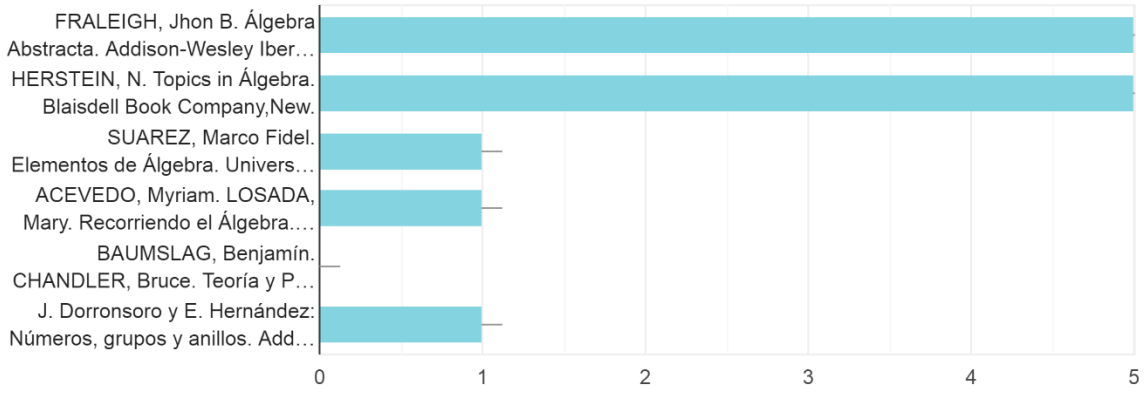


Imagen 4. Resultados encuesta realizada a los profesores del Departamento de Matemáticas

El primer libro seleccionado fue Álgebra abstracta de Fraleígh (1988) allí el capítulo seis está dedicado al estudio de grupos cíclicos. El propósito de esta sección es clasificar todos los grupos cíclicos y todos los subgrupos de los grupos cíclicos. En general dicho capitulo se organizan así: se presenta un compendio de las definiciones teoremas, lemas, demostraciones, ejemplos y ejercicios. La mayoría de los ejemplos que se ilustran tienen como base grupos cíclicos aditivos. No se hace referencia a aplicaciones a la criptografía ni se sugiere la implementación de software que facilite el estudio del concepto de grupo cíclico.

Si G es un grupo y $a \in G$, entonces

$$H = \{a^n \mid n \in \mathbf{Z}\}$$

es un subgrupo de G (Teorema 3.2). Este grupo es el **subgrupo cíclico de G generado por a**. Además, dado un grupo G y un elemento $a \in G$, si

$$G = \{a^n \mid n \in \mathbf{Z}\},$$

entonces a es un **generador de G** y el grupo $G = \langle a \rangle$ es **cíclico**.

El propósito de esta sección es clasificar todos los grupos cíclicos y todos los subgrupos de los grupos cíclicos.

Imagen 5. Definición de grupo cíclico, libro de Fraleigh (1987)

Ejemplo 6.1 Podrá parecer extraño que $\mathbf{Z}$ y $3\mathbf{Z}$, ambos grupos cíclicos infinitos bajo la suma, sean estructuralmente idénticos a pesar de que $3\mathbf{Z} < \mathbf{Z}$. Podría decirse que $1 \in \mathbf{Z}$ pero $1 \notin 3\mathbf{Z}$, así que ¿cómo pueden ser estrueturalmente iguales? Los nombres no importan, y si al 1 lo nombramos 3, al 2 lo nombramos 6 y en general al n lo nombramos $3n$, habremos convertido $\mathbf{Z}$ en $3\mathbf{Z}$ como grupo aditivo. ■

Imagen 6. Ejemplo de grupo cíclico, libro de Fraleigh (1987)

Ejercicios

6.1 Encuéntrese el número de generadores de los grupos cíclicos de órdenes 6, 8, 12 y 60.

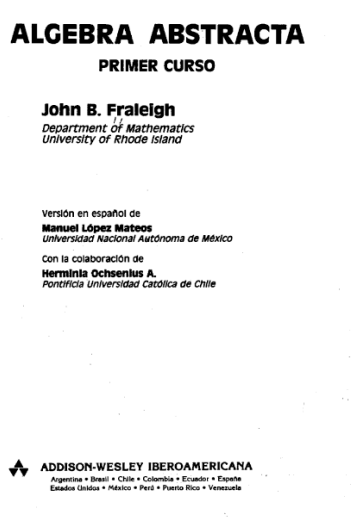
6.2 Muéstrese que un grupo que tenga sólo un número finito de subgrupos debe ser un grupo finito.

6.3 Encuéntrese el número de elementos en cada uno de los grupos cíclicos indicados.

a) El subgrupo cíclico de $\mathbf{Z}_{30}$ generado por el 25.
b) El subgrupo cíclico de $\mathbf{Z}_{42}$ generado por 30.
c) El subgrupo cíclico $\langle i \rangle$ del grupo $\mathbf{C}^*$ de números complejos distintos de cero, bajo la multiplicación.
d) El subgrupo cíclico del grupo $\mathbf{C}^*$ de la parte c) generado por $(1 + i)/\sqrt{2}$.
e) El subgrupo cíclico del grupo $\mathbf{C}^*$ de la parte c) generado por $1 + i$.

Imagen 7. Ejercicios de grupos cíclicos, libro de Fraleigh (1987)

Tabla 4. Ficha general libro de Fraleigh (1987)

FICHA GENERAL DEL LIBRO DE TEXTO		
TÍTULO	Álgebra abstracta primer curso	
DIRIGIDO A	Estudiantes, Docentes	
AUTOR	John B. Fraleígh	
PERFIL AUTOR	Profesor emérito Departamento de Matemáticas University of Rhode Island	
IMPRENTA	Addison- Wesley Publishing Company	
CIUDAD	Massachusetts, USA	
AÑO	1988	

Ver Libro	https://apuntespme.cl/material/AlgAbs/textos/algabs.pdf

El segundo libro seleccionado fue Álgebra abstracta de Herstein (1986), el capítulo dos está dedicado al estudio del objeto grupo. A diferencia de otros libros de texto en este libro no se dedica un capítulo al estudio exclusivo del concepto de grupo cíclico. Si embargo el autor hace una nota aclaratoria sobre la definición de grupo:

> En realidad, en la historia de esta materia transcurrió bastante tiempo para reconocer que estas cuatro propiedades, desempeñaban el papel clave. Nosotros tenemos la ventaja de poder realizar una mirada retrospectiva a la historia y con ello elegir las propiedades no sólo para estudiar A (S), (conjunto de todas las aplicaciones inyectivas de S en S), sino también como las pautas principales para realizar abstracción a un contexto mucho más amplio. (pág 40).

La mayoría de los ejemplos que se ilustran tienen como base grupos cíclicos aditivos. No se hace referencia a aplicaciones a la criptografía ni se sugiere la implementación de software que facilite el estudio del concepto de grupo cíclico.

Se dice que un grupo G es *cíclico* si existe un $a \in G$ tal que todo $x \in G$ es una potencia de a, esto es, $x = a^j$ para cierto j. En este caso a se llama un *generador* de G.

Imagen 8. Definición de grupo cíclico, libro de Herstein, I.N (1988)

3. $U_9 = \{[1], [2], [4], [5], [7], [8]\}$. Obsérvese que $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [8]$, $[2]^4 = [16] = [7]$, $[2]^5 = [32] = [5]$; además $[2]^6 = [2][2]^5 = [2][5] = [10] = [1]$. Así que las potencias de [2] proporcionan todos los elementos de U_9. Por consiguiente U_9 es un grupo *cíclico* de orden 6. ¿Qué otros elementos de U_9 lo generan?

Imagen 9. Ejemplo de grupo cíclico, libro de Herstein, I.N (1988)

13. Hallar los órdenes de todos los elementos de U_{18}. ¿Es cíclico U_{18}?

14. Hallar los órdenes de todos los elementos de U_{20}. ¿Es cíclico U_{20}?

15. Si p es primo, demuéstrese que las únicas soluciones de $x^2 \equiv 1(p)$ son $x \equiv 1(p)$ o bien $x \equiv -1(p)$.

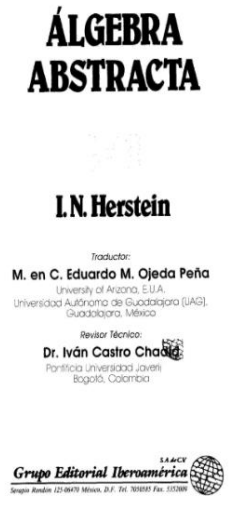
16. Si G es un grupo abeliano finito y $a_1, \ldots, a_n$ son todos sus elementos, demuéstrese que $x = a_1 a_2 \cdots a_n$ debe satisfacer $x^2 = e$.

Imagen 10. Ejercicios grupo cíclico, libro de Herstein, I.N (1988)

Tabla 5. Ficha general libro de Herstein, I.N (1988)(Herstein, 1986)

FICHA GENERAL DEL LIBRO DE TEXTO

TÍTULO	Álgebra Abstracta
DIRIGIDO A	Estudiantes, Docentes
AUTOR	Israel Nathan Herstein
PERFIL AUTOR	Matemático, nombrado profesor en la Universidad de Chicago en 1951. Trabajó en una variedad de áreas del álgebra, incluida la teoría de anillos, con más de 100 trabajos de investigación y más de una docena de libros.
IMPRENTA	Macmillan Publishing Company,
CIUDAD	Estados Unidos de América
AÑO	1986



Ver Libro	https://vereniciafunez94hotmail.iles.wordpress.com/2014/08/algebra-abstracta-herstein.pdf

En el tercer libro seleccionado Álgebra Abstracta de Dummit & Foote (1986) la sección 2.3 está dedicada al estudio de grupos cíclicos. El propósito de esta sección es clasificar todos los grupos cíclicos y todos los subgrupos de los grupos cíclicos. En general dicho capitulo se organizan así: se presenta un compendio de las definiciones teoremas, lemas, demostraciones, ejemplos y ejercicios. La mayoría de los ejemplos que se ilustran tienen como base grupos cíclicos multiplicativos. No se hace referencia a aplicaciones a la criptografía ni se sugiere la implementación de software que facilite el estudio del concepto de grupo cíclico.

Definition. A group H is *cyclic* if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

Imagen 11. Definición de grupo cíclico, libro de Dummit, R. Foote. (2004)

Example

Proposition 6 tells precisely which residue classes mod n generate $\mathbb{Z}/n\mathbb{Z}$: namely, $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $(a, n) = 1$. For instance, $\bar{1}, \bar{5}, \bar{7}$ and $\overline{11}$ are the generators of $\mathbb{Z}/12\mathbb{Z}$ and $\varphi(12) = 4$.

Imagen 12. Ejemplo de grupo cíclico, libro de Dummit, R. Foote. (2004)

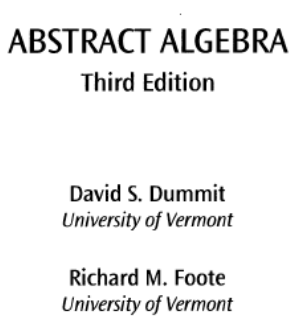
EXERCISES

1. Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.
2. If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.
3. Find all generators for $\mathbb{Z}/48\mathbb{Z}$.
4. Find all generators for $\mathbb{Z}/202\mathbb{Z}$.
5. Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.
6. In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \bar{a} \rangle$ for every $\bar{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Imagen 13. Ejercicios grupo cíclico, libro de Dummit, R. Foote. (2004

Tabla 6. Ficha general libro de Dummit, R. Foote. (2004)

FICHA GENERAL DEL LIBRO DE TEXTO

TÍTULO	Álgebra Abstracta	
DIRIGIDO A	Estudiantes, Docentes	
AUTOR	D. Dummit, R. Foote	
PERFIL AUTOR	David S. Dummit y Richard Foote son profesores eméritos del Departamento de Matemáticas y Estadística de la Universidad de Vermont. Áreas de especialización y/o investigación: Álgebra y Teoría de Números. Teoría de grupos y aplicaciones, teoría algebraica de números, respectivamente	
IMPRENTA	Phoenix Color Corporation.	John Wiley & Sons, Inc.
CIUDAD	Estados Unidos de América	
AÑO	1986	
Ver Libro	https://pdfroom.com/books/abstract-algebra-3rd edition/7jgkR9GEdMV	

En el cuarto libro seleccionado Contemporary Abstract Algebra de Gallian (2010) la sección 2.4 está dedicada al estudio de grupos cíclicos. El propósito de esta sección es clasificar todos los grupos cíclicos y todos los subgrupos de los grupos cíclicos. En general dicha sección se organiza así: se presenta un compendio de las definiciones teoremas, lemas, demostraciones, ejemplos y ejercicios. La mayoría de los ejemplos que se ilustran tienen como base grupos cíclicos multiplicativos. Se hace referencia a aplicaciones a la criptografía sugiriendo la implementación de software que facilite el estudio del concepto de grupo cíclico. En particular se hace uso del sistema algebraico computacional[12] GAP (Grupos, Algoritmos y Programación) especialmente orientado a teoría de grupos.

Recall from Chapter 3 that a group G is called *cyclic* if there is an element a in G such that $G = \{a^n \mid n \in Z\}$. Such an element a is called a *generator* of G. In view of the notation introduced in the preceding chapter, we may indicate that G is a cyclic group generated by a by writing $G = \langle a \rangle$.

Imagen 14. Definición de grupo cíclico, libro de Gallian, Joseph A (2010)

■ **EXAMPLE 1** The set of integers Z under ordinary addition is cyclic. Both 1 and -1 are generators. (Recall that, when the operation is addition, 1^n is interpreted as

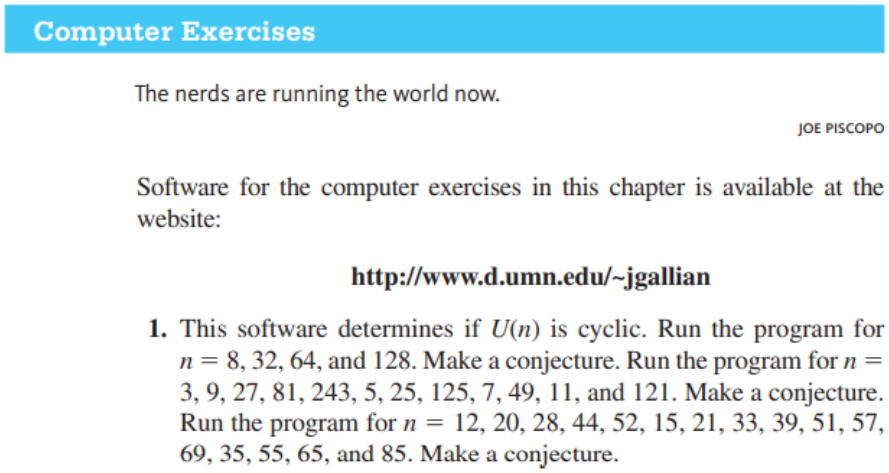
$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}}$$

when n is positive and as

$$\underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ terms}}$$

Imagen 15. Ejemplo grupo cíclico, libro de Gallian, Joseph A (2010)

[12] Un **sistema algebraico computacional** o **sistema de álgebra computacional** (**CAS**, del inglés *computer algebra system*) es un programa de ordenador o calculadora avanzada que facilita el cálculo simbólico. La principal diferencia entre un CAS y una calculadora tradicional es la habilidad del primero para trabajar con ecuaciones y fórmulas simbólicamente, en lugar de numéricamente.



Computer Exercises

The nerds are running the world now.

JOE PISCOPO

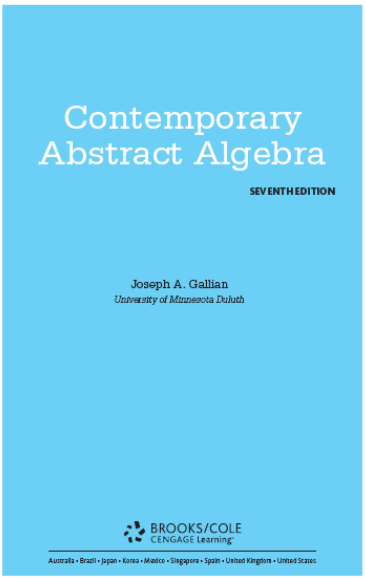
Software for the computer exercises in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

1. This software determines if $U(n)$ is cyclic. Run the program for $n = 8, 32, 64$, and 128. Make a conjecture. Run the program for $n = 3, 9, 27, 81, 243, 5, 25, 125, 7, 49, 11$, and 121. Make a conjecture. Run the program for $n = 12, 20, 28, 44, 52, 15, 21, 33, 39, 51, 57, 69, 35, 55, 65$, and 85. Make a conjecture.

Imagen 16. Ejercicio grupo cíclico, libro de Gallian, Joseph A (2010)

Tabla 7. Ficha general libro de Gallian, Joseph A (2010)

FICHA GENERAL DEL LIBRO DE TEXTO		
TÍTULO	Contemporary Abstract Algebra	
DIRIGIDO A	Estudiantes, Docentes	
AUTOR	Gallian, Joseph A	
PERFIL AUTOR	Matemático estadounidense Profesor del Teaching en el Departamento de Matemáticas y Estadística de la Universidad de Minnesota Duluth.	
IMPRENTA	Brooks/Cole Publishing Company	
CIUDAD	Estados Unidos de América	
AÑO	2010	
Ver Libro	https://ict.iitk.ac.in/wp-content/uploads/CS203-Mathematics-for-Computer-Science-III-Gallian.pdf	

En el quinto libro seleccionado Hungerford (2012) la sección 7.2 está dedicada al estudio del objeto grupo. A diferencia de otros libros de texto, en este libro no se dedica un capítulo al estudio

exclusivo del concepto de grupo cíclico. En general dicha sección se organiza así: se presenta un compendio de las definiciones teoremas, lemas, demostraciones, ejemplos y ejercicios. La mayoría de los ejemplos que se ilustran tienen como base grupos cíclicos multiplicativos. No se sugiere la implementación de software que facilite el estudio del concepto de grupo cíclico. No obstante, en el capítulo 13 se presenta una introducción a la Criptografía asimétrica en particular se ilustra el funcimiento del protocolo criptográfico RSA.

Cyclic Groups

An important type of subgroup can be constructed as follows. If G is a group and $a \in G$, let $\langle a \rangle$ denote the set of all powers of a:

$$\langle a \rangle = \{ \ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \} = \{ a^n \mid n \in \mathbb{Z} \}.$$

Imagen 17. Definición de grupo cíclico, libro de Hungerford (2012)

EXAMPLE 11

The multiplicative group of units in the ring $\mathbb{Z}_{15}$ is $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ by Theorem 2.10. In order to determine the cyclic subgroup generated by 7, we compute

$$7^1 = 7 \qquad 7^2 = 4 \qquad 7^3 = 13 \qquad 7^4 = 1 = 7^0.$$

Therefore, the element 7 has order 4 in U_{15}. We claim that the cyclic subgroup $\langle 7 \rangle$ consists of $\{7^0, 7^1, 7^2, 7^3\} = \{1, 7, 4, 13\}$. [*Proof:* By definition, every ele-

Imagen 18. Ejemplo de grupo cíclico, libro de Hungerford (2012)

■ Exercises

A. 1. List all the cyclic subgroups of

(a) U_{15} (b) U_{30}

2. (a) List all the cyclic subgroups of D_4.

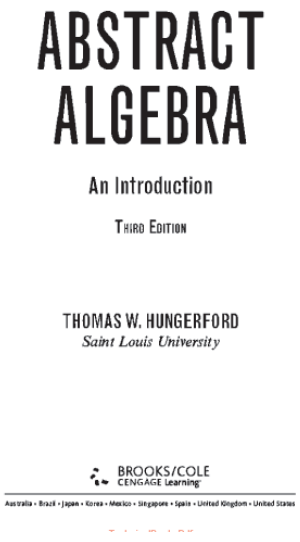
(b) List at least one subgroup of D_4 that is not cyclic.

3. List the elements of the subgroup $\langle a \rangle$, of S_7, where

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 6 & 5 & 1 & 4 \end{pmatrix}.$$

Imagen 19. Ejercicios grupo cíclico, libro de Hungerford (2012)

Tabla 8. Ficha general libro de Hungerford (2012)

FICHA GENERAL DEL LIBRO DE TEXTO		
TÍTULO	Abstract Algebra: An Introduction	
DIRIGIDO A	Estudiantes, Docentes	
AUTOR	Thomas W. Hungerford	
PERFIL AUTOR	Matemático estadounidense que trabajó en álgebra y educación matemática. Es autor o coautor de varios libros de texto ampliamente utilizados y ampliamente citados que cubren matemáticas de escuela secundaria a nivel de posgrado	
IMPRENTA	Brooks/Cole Publishing Company	
CIUDAD	Estados Unidos de América	
AÑO	2012	
Ver Libro	https://engineeringbookspdf.com/download/?file=4065&format=pdf	

En el sexto libro seleccionado Algebra Abstracta Teoría y Aplicaciones de Judson (2017) el capítulo 4 está dedicado al estudio del objeto grupo cíclico. En este capítulo se estudian las propiedades de grupos cíclicos y subgrupos cíclicos los cuales juegan un papel clave en la clasificación de los grupos abelianos. En general dicho capitulo se organiza así: se presenta un compendio de las definiciones teoremas, lemas, demostraciones, ejemplos y ejercicios. La mayoría de los ejemplos que se ilustran tienen como base grupos cíclicos multiplicativos. Se sugiere la implementación de software que facilite el estudio del concepto de grupo cíclico. En particular se hace uso del sistema algebraico computacional SageMath. Además, en el capítulo 7 se presenta una introducción a la criptografía asimétrica en particular se ilustra el fruncimiento del protocolo criptográfico RSA.

Para $a \in G$, llamamos a $\langle a \rangle$ el ***subgrupo cíclico*** generado por a. Si G contiene algún elemento a tal que $G = \langle a \rangle$, entonces G es un ***grupo cíclico***. En ese caso a es un ***generador*** de G. Si a es un elemento de un grupo G,

Imagen 20. Definición de grupo cíclico, libro de Thomas W. Judson (2017)

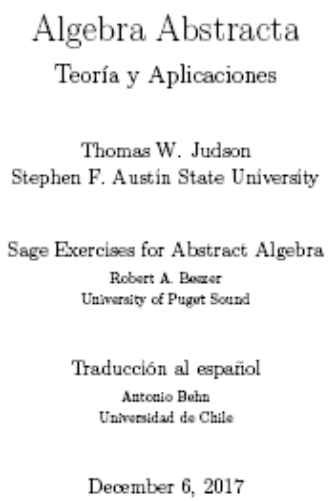
Ejemplo 4.5. Note que un grupo cíclico puede tener más que un generador. Tanto 1 como 5 generan $\mathbb{Z}_6$; por lo tanto, $\mathbb{Z}_6$ es un grupo cíclico. No todo elemento en un grupo cíclico es un generador del grupo. El orden de $2 \in \mathbb{Z}_6$ es 3. El subgrupo cíclico generado por 2 es $\langle 2 \rangle = \{0, 2, 4\}$.

Imagen 21. Ejemplo de grupo cíclico, libro de Thomas W. Judson (2017)

1. Ejecute el comando `R = Integers(40)` para crear el conjunto `[0,1,2,...,39]` Éste es un grupo con la operación de suma mód 40, que ignoraremos. En cambio estamos interesados en el subconjunto de los elementos que tienen inverso respecto a la *multiplicación* mód 40. Determine el tamaño de este subgrupo ejecutando el comando `R.unit_group_order()`, y obtenga una lista de estos elementos con `R.list_of_elements_of_multiplicative_group()`.

Imagen 22. Ejercicio grupo cíclico, libro de Thomas W. Judson (2017)

Tabla 9. Ficha general libro de Thomas W. Judson (2017)

FICHA GENERAL DEL LIBRO DE TEXTO		
TÍTULO	Algebra Abstracta Teoría y Aplicaciones	
DIRIGIDO A	Estudiantes, Docentes	
AUTOR	Thomas W. Judson Robert A. Beezer	
PERFIL AUTOR	Profesor Departamento de Matemáticas y Estadística de Stephen F. Austin State University. Mathematics And Computer Science. Profesor Departamento de Matemáticas University of Puget Sound.	
IMPRENTA	Brooks/Cole Publishing Company	
CIUDAD	Estados Unidos de América	
AÑO	2017	
Ver Libro	http://abstract.ups.edu/	

La ejemplificación del concepto de grupo cíclico multiplicativo, el tipo de ejercicios, la implementación de software, las aplicaciones a la criptografía asimétrica presentadas en los libros

de texto seleccionados, los aspectos contemplados y obtenidos como resultado de estos tres análisis se convierten en la base para la formulación de las categorías de estudio de los libros de texto. La imagen 23 muestra el esquema general de las categorías formuladas.

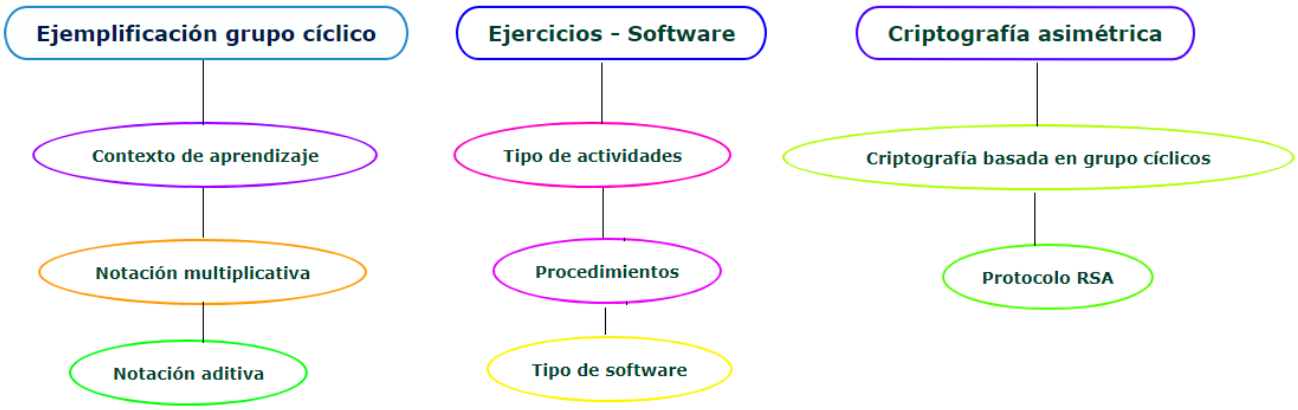


Imagen 23. Esquema general de las categorías formuladas.

La categoría designada como *ejemplificación de grupo cíclico* integra las perspectivas dadas desde los análisis curriculares y proporciona una base acerca de la naturaleza que se le ha asignado al grupo cíclico y se puede dimensionar el estatus otorgado al grupo cíclico multiplicativo en cada libro de texto seleccionado. Aquí se agrupan las categorías que aluden a los ambientes, los procesos y las actividades que se emplean para la enseñanza del grupo cíclico en contextos educativos. La categoría consta de tres subcategorías: Contexto de aprendizaje, notación multiplicativa y notación aditiva

La categoría designada como *ejercicios – software* recoge los elementos básicos referentes a la pedagogía y didáctica de las matemáticas en torno al grupo cíclico en el contexto de la criptografía asimétrica, así como la implementación de tecnologías mediadoras del proceso de enseñanza. La categoría consta de tres subcategorías: tipo de actividades, procedimientos y tipo de software.

La categoría designada como *criptografía asimétrica* recoge los elementos básicos referentes a la relación entre un concepto matemático y sus aplicaciones y se constituye en referente para la práctica pedagógica del docente. La categoría consta de dos subcategorías: criptografía basada en grupos cíclicos y protocolo RSA.

Contexto de aprendizaje

Dado que cada libro de texto se formula en un período de tiempo, el esquema que se adopta en su diseño integra diversos intereses, entre ellos, las perspectivas cognitivas del aprendizaje. En este sentido, la categoría contexto de aprendizaje sistematiza los enfoques cognitivos y didácticas generales, que orientan las propuestas de trabajo de los libros de texto en torno al concepto de grupo cíclico. Esta categoría se estructura a través de dos subcategorías: ejemplos de enunciado abstracto y ejemplos concretos o numéricos.

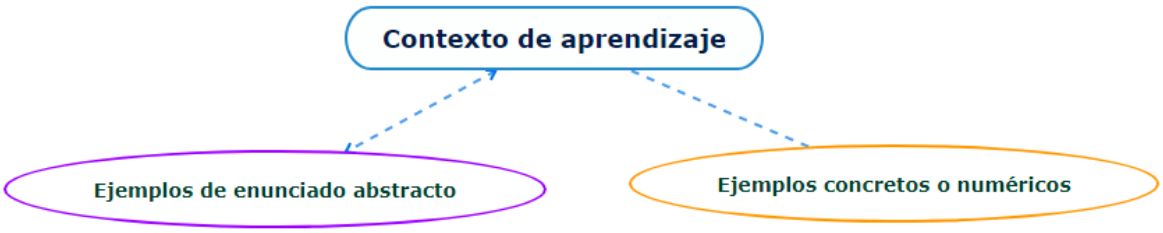


Imagen 24. Subcategorías contexto de aprendizaje

Ejemplos de enunciado abstracto: esta subcategoría agrupa los contextos que proponen como herramientas de enseñanza actividades de solución de ejercicios de enunciados relacionados con definiciones o teoremas sobre grupos cíclicos. Los ejercicios de enunciado abstracto se asumen como enunciados escritos donde se hace uso de destrezas o técnicas que requieren de abstracción o generalización de propiedades vistas en curso anteriores al de teoría de grupos.

Ejemplos concretos o numéricos:

Esta agrupa los contextos que proponen como herramientas de enseñanza actividades de solución de ejercicios de enunciados relacionados con operaciones, generadores u orden de elementos del grupo cíclico, donde se hace "…uso de destrezas o técnicas sobre aprendidas (es decir, convertidas en rutinas automatizadas como consecuencia de una práctica continuada)" (Pozo, 1994, p. 18). Así, en esta subcategoría se inscriben todos aquellos contextos de enseñanza donde se propone un paquete de definiciones con sus correspondientes ejemplos seguidos de un gran número de formulaciones concretas (denominados en los libros de texto como problemas o ejercicios) donde el trabajo del estudiante se encamina a repetir técnicas que han sido explicadas previamente para dar solución a situaciones ya conocidas.

Notación multiplicativa

Esta subcategoría agrupa los contextos que proponen como ejemplos grupos cíclicos multiplicativos. Dichos ejemplos constituyen los elementos más relevantes para el análisis propuesto pues como se evidencia en las secciones siguientes los grupos cíclicos multiplicativos proporcionan herramientas para la construcción de criptosistemas asimétricos.

Se define un grupo multiplicativo de enteros módulo n como un conjunto finito de enteros positivos menores que n siendo números coprimos respecto a n. [13]

Notación aditiva

La notación aditiva designa el hecho de notar una operación de grupo o más generalmente una ley de composición de una estructura algebraica. Esta es la notación habitual para un grupo

[13] Weisstein, Eric W. «Modulo Multiplication Group». mathworld.wolfram.com (en inglés). Consultado el 20 de marzo de 2022.

abeliano. Aunque la mayoría de los ejemplos referidos en los libros de texto seleccionados proponen ejemplos con grupos cíclicos bajo la notación aditiva. Vale aclarar que para efectos de la ilustración del funcionamiento de criptosistemas asimétricos expuestos se privilegia la estructura de grupo cíclico bajo la multiplicación. Una de las razones por la que se elige la notación multiplicativa tiene que ver con la definición de logaritmo discreto, la cual es esencial para la generación de criptosistemas asimétricos y cuya definición depende de un grupo cíclico multiplicativo.

Resultados obtenidos con respecto a la ejemplificación de grupo cíclico

Al respecto de los enfoques didácticos generales que orientan las propuestas de trabajo de los libros de texto seleccionados en torno al concepto de grupo cíclico en el contexto de la criptografía asimétrica se obtuvo que respecto al *contexto de aprendizaje*: ejemplos de enunciado abstracto y ejemplos concretos o numérico, el segundo fue el enfoque más empleado para orientar el proceso de enseñanza del grupo cíclico a lo largo de los períodos analizados como se evidencia en los resultados obtenidos al respecto del contexto de aprendizaje imagen 25.

Respecto a la *notación aditiva* se identifica que si bien esta ha estado presente en varias épocas ha sido menos frecuente su empleo en los últimos años, períodos donde aparecen otros tipos de contextos de enseñanza en las propuestas de los libros de texto. Se puede argumentar que ha estado presente en las propuestas de trabajo de los libros de texto a lo largo de las épocas y que fue el contexto más empleado em el libro Contemporary Abstract Algebra de Gallian (2010) donde el trabajo con el grupo cíclico bajo la adición se circunscribe a la representación de cantidades y al desarrollo de habilidades de cálculo usuales en el conjunto de los números enteros.

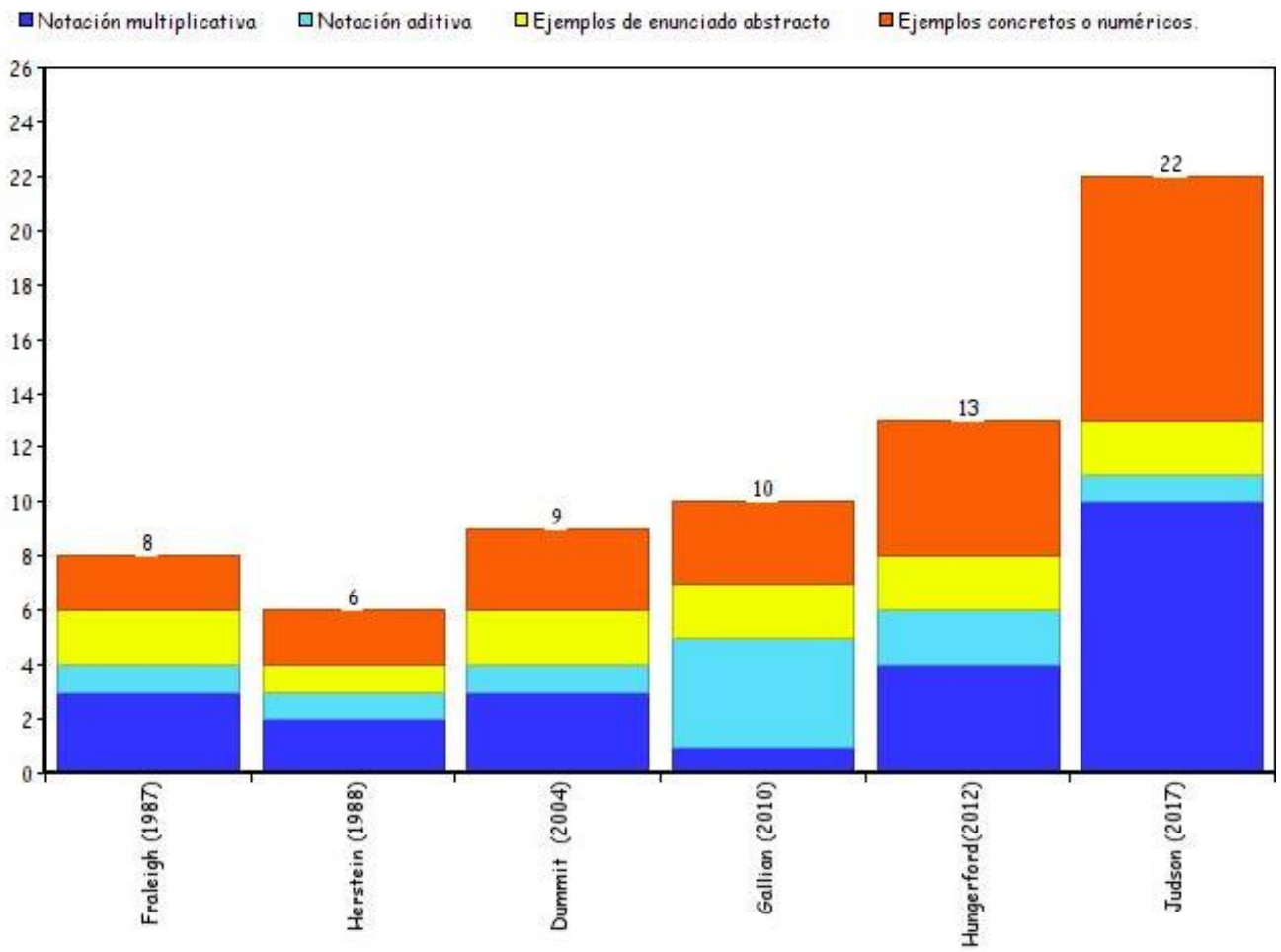


Imagen 25. Resultados categoría ejemplificación de grupo cíclico

Respecto a la *notación multiplicativa* se identifica que si bien esta ha estado presente en varias épocas ha sido frecuente su empleo en los últimos años, períodos donde aparecen otros tipos de contextos de enseñanza relacionados con los protocolos criptográficos asimétricos en las propuestas de los libros de texto. Se puede argumentar que ha estado presente en las propuestas de trabajo de los libros de texto a lo largo de las épocas y que fue el contexto más empleado en los libros Algebra Abstracta Teoría y Aplicaciones de Judson (2017) y Abstract Algebra An Introduction de Hungerford (2012) donde el trabajo con el grupo cíclico multiplicativo se

circunscribe con la ilustración de diversas aplicaciones criptográficas las cuales serán expuestas en las secciones siguientes.

Tipo de actividades

Las propuestas de actividades que se formulan en los libros de texto para abordar el concepto de grupo cíclico se enmarcan en ciertas posturas cognitivas, didáctica y epistemológica. Tales supuestos teóricos se operacionalizan a través de las formas de comunicación y los tipos de actividades planteados, los cuales integran elementos representativos de cada teoría. En este sentido la categoría tipo de actividades reúne los diferentes tipos de actividades que plantean los libros de texto para enseñar y dar sentido al concepto de grupo cíclico en el contexto de la criptografía asimétrica como se evidencia en la imagen 26.

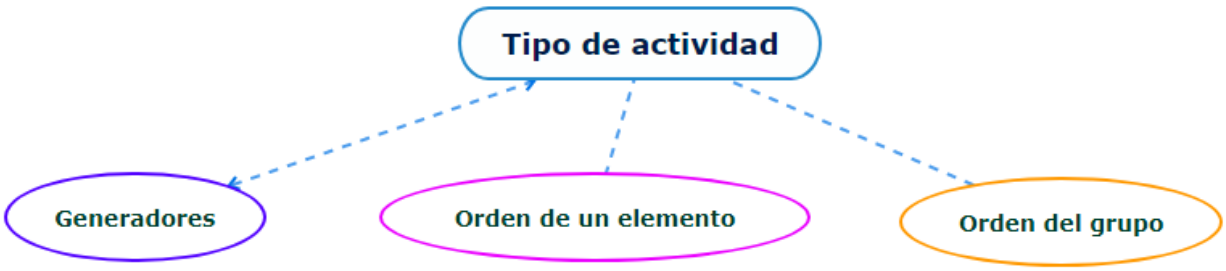


Imagen 26. Subcategorías tipo de actividad

Esta categoría se estructura a partir de tres subcategorías fundamentales para la criptografía asimétrica: generadores, orden de un elemento y orden del grupo.

Generadores: en esta subcategoría se recogen las actividades donde se requiere identificar, comparar y relacionar elementos de un grupo cíclico con elementos que cumplan con la definición

de ser generador, puesto que los generadores juegan un papel importante en la construcción de protocolos criptográficos basados en grupos cíclicos.

Dado un grupo G y un elemento $a \in G$, si

$$G = \{a^n \mid n \in Z\}$$

entonces a es un generador de G y el grupo $G = < a >$ es cíclico.

Orden de un elemento: en esta subcategoría se recogen las actividades donde se requiere identificar, comparar y relacionar el orden de elementos de un grupo cíclico: El orden de un elemento a de un grupo G es el entero positivo m más pequeño tal que:

$$a^m = e$$

donde e denota el elemento identidad también llamado neutro del grupo y a^m denota el producto de m veces a. Si no existe tal m se dice que a tiene un orden infinito.

Orden del grupo: en esta subcategoría se recogen las actividades donde se requiere identificar, comparar y relacionar el orden de un grupo cíclico: el orden de un grupo es su cardinalidad, es decir, el número de elementos que tiene.

En las propuestas de trabajo de los libros de texto seleccionados se observa una clara tendencia a emplear actividades donde se requiere identificar, comparar y relacionar generadores de grupo y orden de elementos. Dichas actividades se presentan en los libros: Contemporary Abstract Algebra de Gallian (2010) y Algebra Abstracta Teoría y Aplicaciones de Judson (2017) donde el currículo se enmarca en la propuesta de la matemática moderna reconociendo los avances y conexiones de la teoría de grupos con la criptografía lo cual se evidencia en la implementación de ejercicios que

implementan protocolos como RSA en cada sección dedicada al estudio del concepto de grupo cíclico.

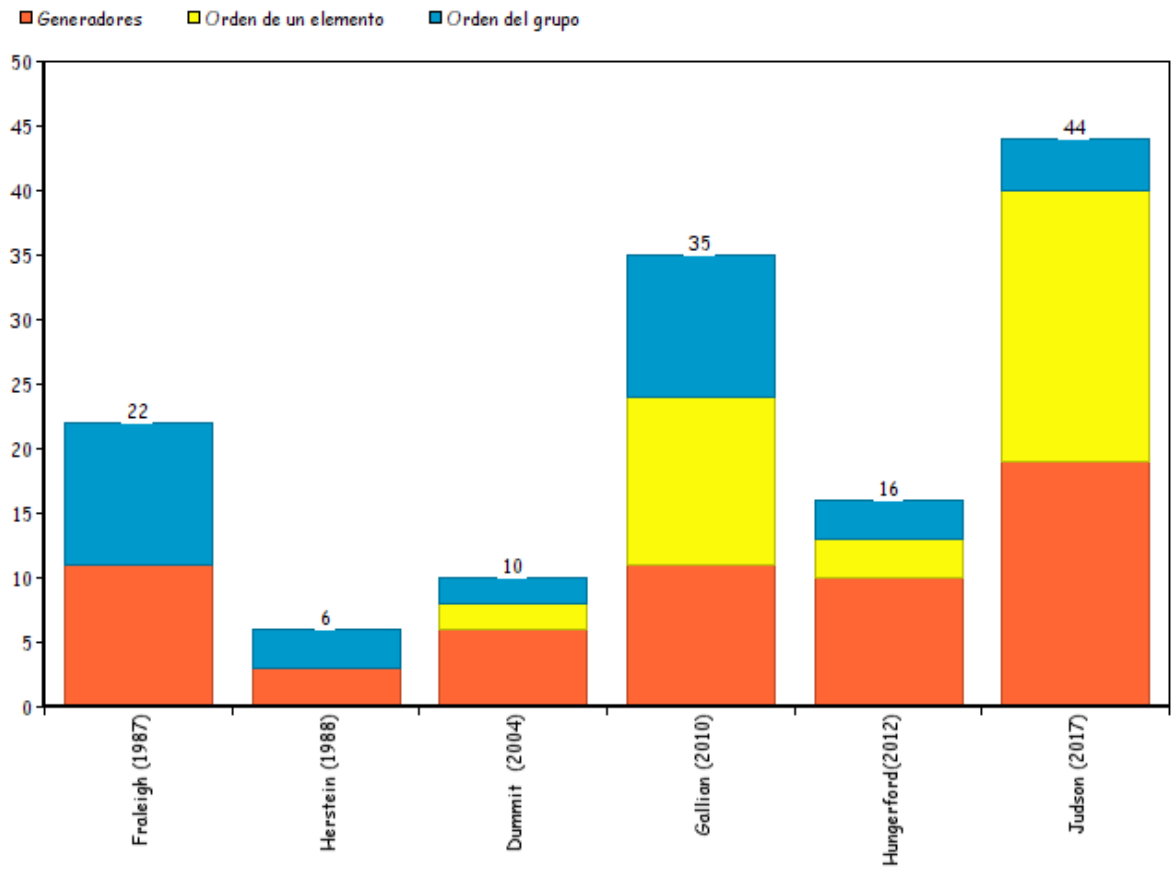


Imagen 27. Resultados categoría tipo de actividad

En contraste se observa que las propuestas de trabajo de los libros de texto Algebra Abstracta de Fraleígh (1988) y An Introduction de Hungerford (2012) no incorporan explícitamente ejercicios relacionados con generadores de grupo y orden de elementos como actividad básica para la construcción de criptosistemas asimétricos basado en grupos cíclicos multiplicativos. En particular en estos libros los generadores y orden del grupo fueron las actividades más empleadas para la enseñanza del grupo cíclico.

Es de resaltar la proporción que ocupan las actividades de identificación de los generadores y orden de elementos en las propuestas de trabajo de los libros de texto Contemporary Abstract Algebra de Gallian (2010) y Algebra Abstracta Teoría y Aplicaciones de Judson (2017) evidenciada en la imagen 27. Esta tendencia puede explicarse en función de la incorporación de herramientas informáticas y la ilustración de aplicaciones a la criptógrafa asimétrica que se ilustran en secciones de dichos libros, los cuales cumplen con institucionalizar el saber matemático que circula en la actualidad en otras disciplinas aplicadas y el grupo cíclico hace parte de ello.

Procedimientos- software

Una vez que el concepto de grupo cíclico en el contexto de la criptografía asimétrica es adaptado e incorporado al tejido educativo se determina por parte de la noosfera la perspectiva epistémica que va a dar sentido a dicho concepto. Se determinan procedimientos que van a ser asumidos como válidos para expresar mediante la implementación de software algebraico especializado y relacionar propiedades de grupo cíclico con la generación de criptosistemas asimétricos. Los procedimientos aluden a una serie de pasos definidos previamente que se ejecutan de la misma manera y que conducen a un resultado. De acuerdo con lo anterior esta categoría recoge los procedimientos que proponen los libros de texto seleccionados en función de dos subcategorías: para calcular el orden de un elemento, para calcular el orden de un grupo.

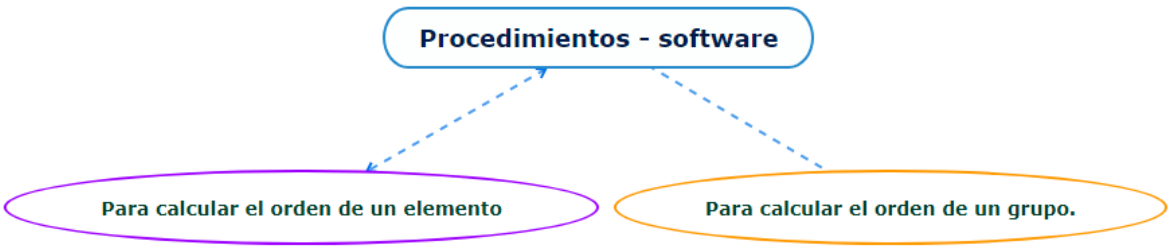


Imagen 28. Subcategorías procedimientos- software

En el análisis de los libros de texto al respecto de los procedimientos válidos para expresar y relacionar propiedades de grupo cíclico con la generación de criptosistemas asimétricos se obtuvo que es poco frecuente encontrar enunciados y representaciones que indiquen el uso de software algebraico para hallar el orden de un elemento o el orden de un grupo. Esta tendencia se identifica solo en los libros texto Contemporary Abstract Algebra de Gallian (2010) y Algebra Abstracta Teoría y Aplicaciones de Judson (2017). Dicho énfasis se puede explicar a la luz de los referentes dados por los lineamientos curriculares y de la perspectiva integradora sobre el aprendizaje del concepto de grupo cíclico en las diferentes épocas. Así pues, respecto a los años de publicación se puede notar un incremento en la implementación de recursos tecnológicos en contexto con las aplicaciones criptográficas de cada época.

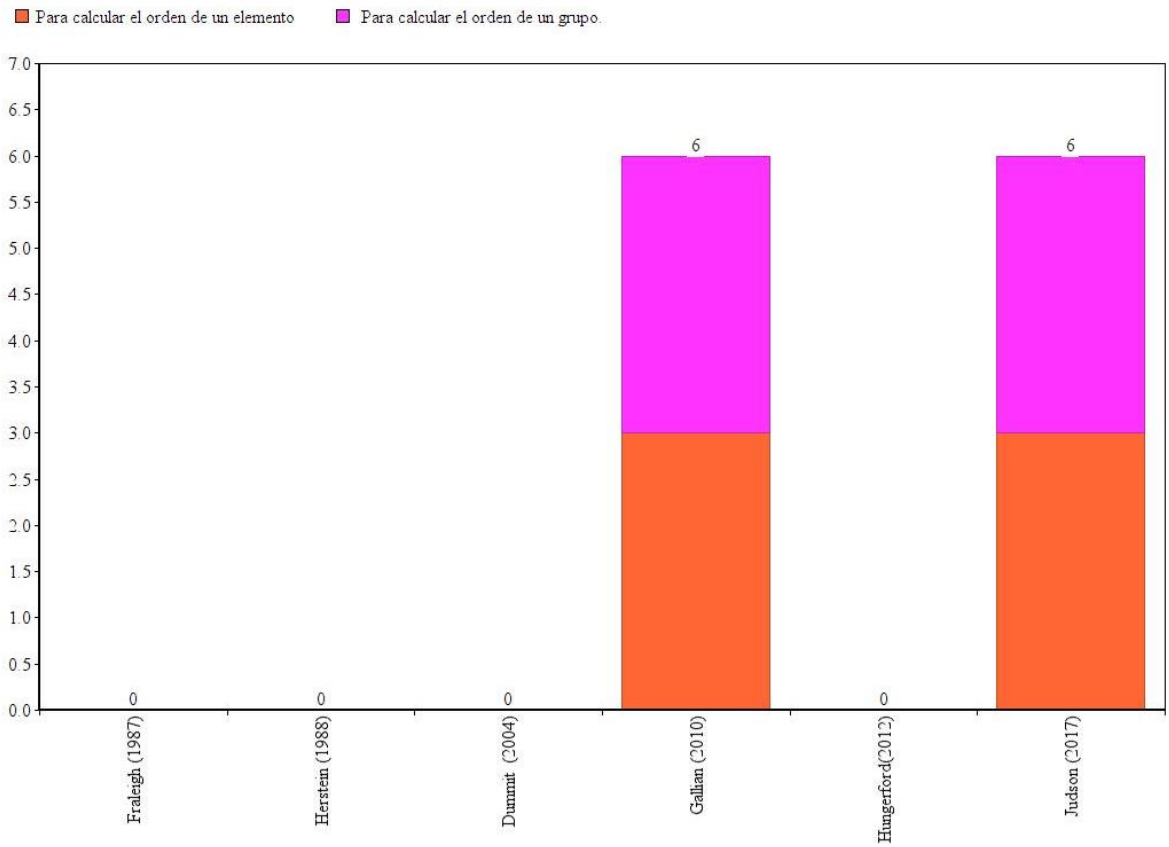


Imagen 29. Resultados categoría procedimientos- software

Tipo de software

Esta categoría hace referencia al tipo de software empleado en los libros de texto seleccionados que vinculan aplicaciones a la criptografía asimétrica y promueven el uso de herramientas tecnológicas que incorporan sistema algebraico computacional CAS, (del inglés Computer Algebra System). Este programa de ordenador o calculadora avanzada facilita el cálculo simbólico. La principal diferencia entre un CAS y una calculadora tradicional es la habilidad del primero para trabajar con ecuaciones y fórmulas simbólicamente en lugar de numéricamente[14]. A continuación, se lista la funcionalidad de los CAS de carácter general usados en los libros seleccionados haciendo especial énfasis en el software SageMath.

Ecuaciones diferenciales	Relaciones de recurrencia	Teoría de grafos	Teoría de números	Álgebra de Boole	Tensores	Probabilidad	Teoría de control	Teoría de códigos	Teoría de grupos	Sistema
✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✗ No	✓ Sí	✓ Sí	SageMath
✓ Sí	✗ No	✗ No	✗ No	✗ No	✗ No	✗ No	✗ No	✗ No	✗ No	MATLAB
✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✗ No	✓ Sí	Mathematica
✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✗ No	✓ Sí	Maple
✗ No	✗ No	✓ Sí	✓ Sí	✗ No	✗ No			✓ Sí	✓ Sí	Magma

Imagen 30. Funcionalidad de los CAS, tomado de base de datos swMATH

El libro Algebra Abstracta Teoría y Aplicaciones de Judson (2017) hace uso del CAS SageMath como herramienta fundamental para el tratamiento del concepto de grupo cíclico, los cuales aparecen en diferentes formas en Sage. A continuación, se ilustra una guía a las diferentes formas de construir y estudiar un grupo cíclico en Sage. Las imágenes 31 y 32 fueron tomadas del libro mencionado.

[14] Richard J. Fateman. "Essays in algebraic simplification". Technical report MIT-LCS-TR-095, 1972. (Of historical interest in showing the direction of research in computer algebra

Grupos Cíclicos de Orden Infinito en SageMath

Los enteros Z se construyen con el comando ZZ, para construir un grupo cíclico infinito como 3Z simplemente se debe usar 3*ZZ, con unconjunto infinito no es mucho lo que se pueda hacer. Se puede determinar si un entero está en el conjunto o no, también es posible recuperar el generador con el comando .gen ()

```
G = 3*ZZ
-12 in G
```

```
True
```

```
37 in G
```

```
False
```

```
G.gen()
```

```
3
```

Imagen 31 Grupos Cíclicos de Orden Infinito en SageMath

Grupos Multiplicativos Abstractos

En Sage se puede crear un grupo cíclico abstracto. En la sintaxis que sigue a es un nombre para el generador y 14 es el orden del elemento con la notación multiplicativa, así es que multiplicar los elementos y los productos repetidos pueden ser escritos como potencias. Se pueden formar subgrupos con el comando .subgroup(). Una ventaja de esta implementación es la posibilidad de crear todos los posibles subgrupos. Como ejemplo ilustrativo se creará la lista de subgrupos extrayendo uno en particular (el tercero) obteniendo su orden.

```
G.<a> = AbelianGroup([14])
G.order()
```

```
14
```

```
G.list()
```

```
(1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^10, a^11,
    a^12, a^13)
```

```
a.order()
```

```
14
```

```
H = G.subgroup([a^2])
H.order()
```

```
7
```

```
K = G.subgroup([a^12])
K.order()
```

```
7
```

```
allsg = G.subgroups(); allsg
```

```
[Multiplicative Abelian subgroup isomorphic to C2 x C7
    generated by {a},
 Multiplicative Abelian subgroup isomorphic to C7 generated
     by {a^2},
 Multiplicative Abelian subgroup isomorphic to C2 generated
     by {a^7},
 Trivial Abelian subgroup]
```

```
sub = allsg[2]
sub.order()
```

```
2
```

Imagen 32. Grupos Multiplicativos Abstractos en SageMath

Por otro lado el libro Contemporary Abstract Algebra de Gallian (2010) propone un manual de laboratorio en línea escrito en colaboración con Julianne Rainbolt, con ejercicios diseñados para ser realizados con ayuda del software GAP (acrónimo de Groups, Algorithms and Programming,

en español, Grupos, Algoritmos y Programación), el cual es un sistema algebraico computacional (CAS) especialmente orientado a teoría de grupos. En la página de inicio se puede encontrar el software para explorar las propiedades de grupos y anillos específicos. Los ejercicios están diseñados para ayudar a formular y probar conjeturas. Las siguientes imágenes fueron tomadas del libro mencionado.

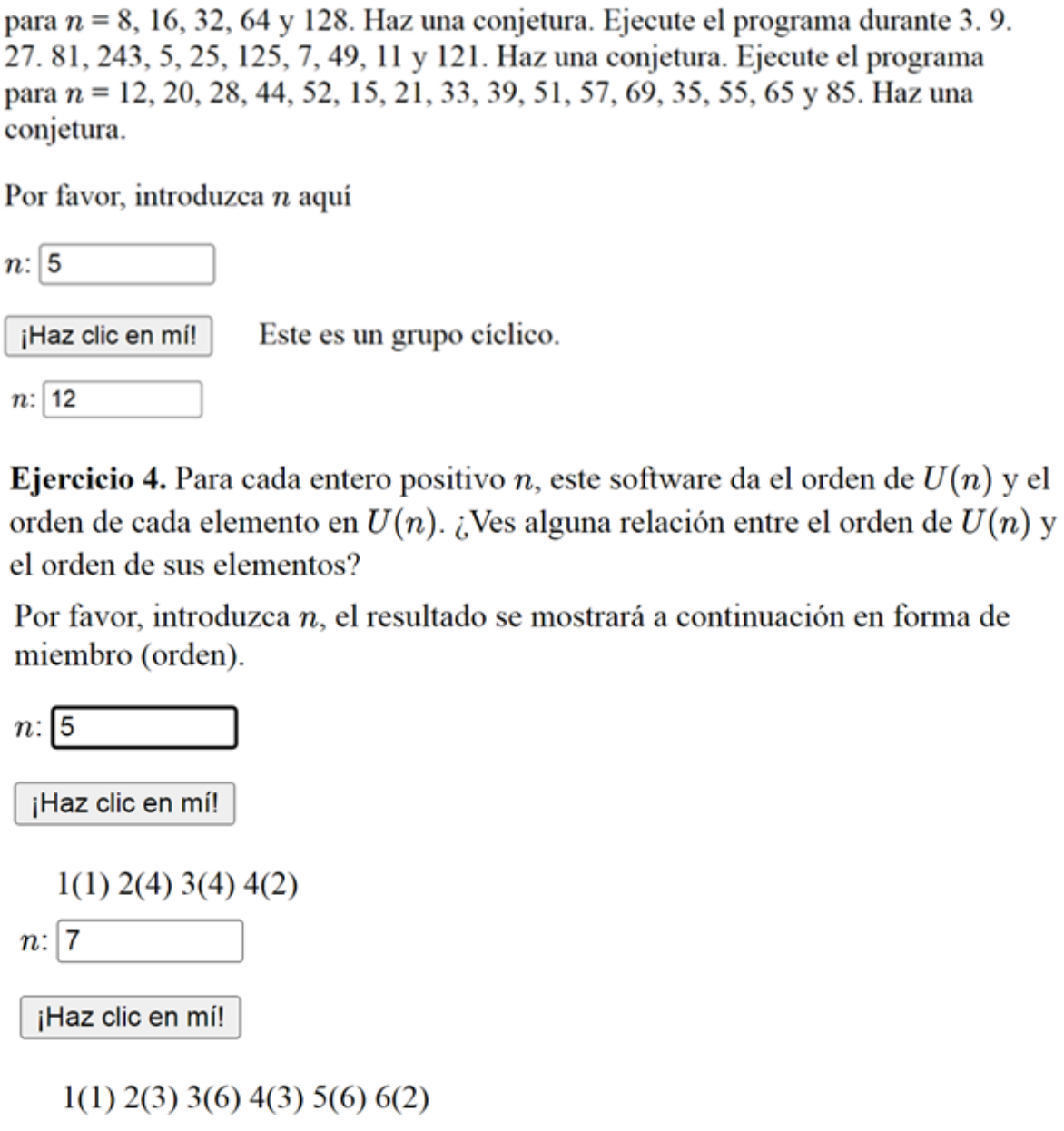


Imagen 33. Eejercicios de computadora libro Contemporary Abstract Algebra de Gallian (2010)

En los tipos de software empelados en los libros de texto seleccionados para expresar y relacionar propiedades de grupo cíclico con la generación de criptosistemas asimétricos se obtuvo que en los libros: Contemporary Abstract Algebra de Gallian (2010) y Algebra Abstracta Teoría y Aplicaciones de Judson (2017) es frecuente encontrar implementaciones de software algebraico para hallar generadores, orden de un elemento, orden de un grupo y listar elementos de un grupo cíclico. Dicho énfasis se puede explicar a la luz de los referentes dados por los lineamientos curriculares y de la perspectiva integradora sobre el aprendizaje del concepto de grupo cíclico en las diferentes épocas. Así pues, respecto a los años de publicación se puede notar un incremento en la implementación de recursos tecnológicos en contexto con las aplicaciones criptográficas de cada época.

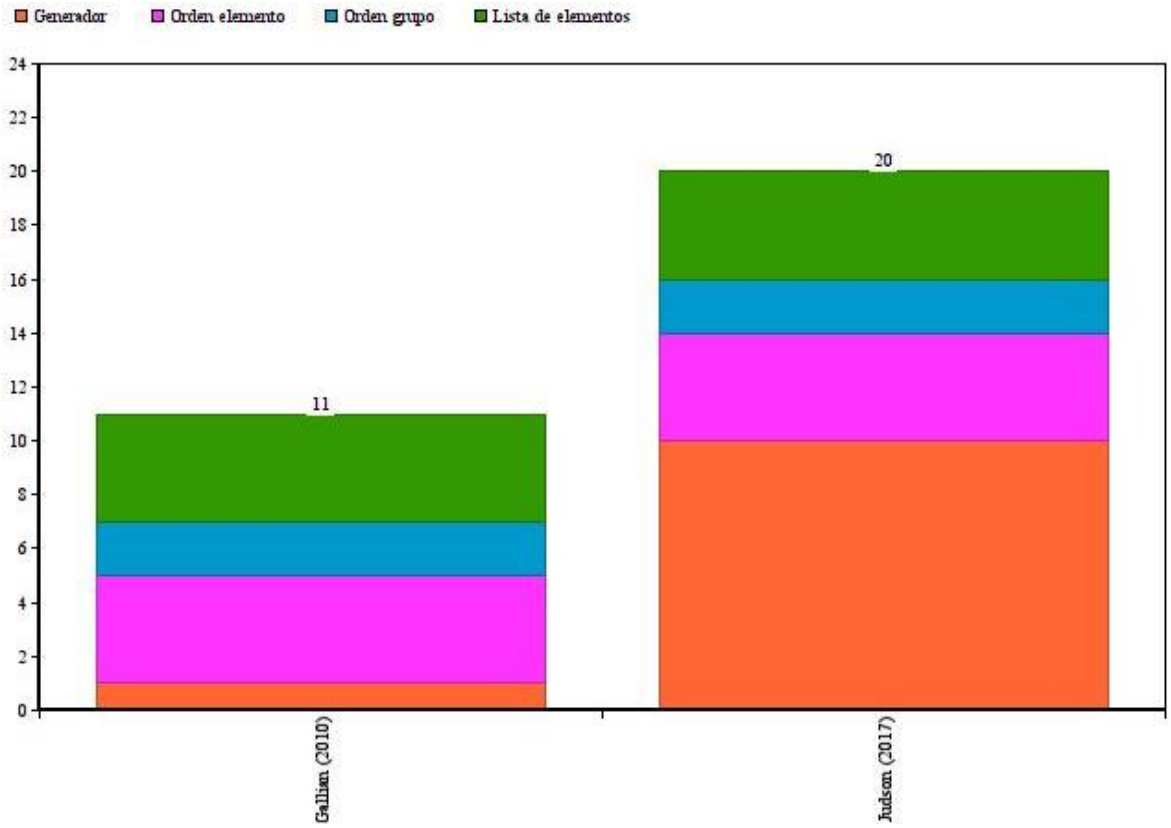


Imagen 34.Resultados categoría tipo de software

C***riptografía basada en grupos cíclicos.***

Esta categoría recoge los elementos básicos referentes a la relación entre un concepto matemático y sus aplicaciones y se constituye en referente para la práctica pedagógica del docente. Se identifica en los libros de texto seleccionados las diferentes aplicaciones del grupo cíclico en la criptografía asimétrica. Como lo describe Franchi (2012) la criptografía es un tema que ha fascinado y ocupado a la humanidad desde la época de los egipcios. La transmisión segura de la información ha encontrado una gran variedad de aplicaciones en las áreas política, militar y económica. La criptografía asimétrica (o de clave pública) es una tecnología que se ocupa de la comunicación sobre redes abiertas transformándose en la piedra fundamental de todos los negocios que se basen en transacciones electrónicas.

Las aplicaciones que se formulan en los libros: Algebra Abstracta Teoría y Aplicaciones de Judson (2017) , Abstract Algebra: An Introduction de Hungerford (2012) y Contemporary Abstract Algebra de Gallian (2010) para abordar el concepto de grupo cíclico en el contexto de la criptografía asimétrica, se enmarcan en nociones matemáticas y herramientas, tales como: aritmética modular congruencia modular, campo finito, extensión de campo, criptografía asimétrica, uso de software, ejercicios y el protocolo criptográfico RSA. En la imagen 35 se evidencia la frecuencia de aparición de dichos tópicos en los libros seleccionados. La frecuencia con la que aparecen dichas nociones y herramientas en los libros seleccionados permiten inferir que en la formulación de la criptógrafa de clave publica es esencial la estructura algebraica de grupo y en particular para algunos criptosistemas de intercambio de claves es necesaria la estructura de grupo cíclico.

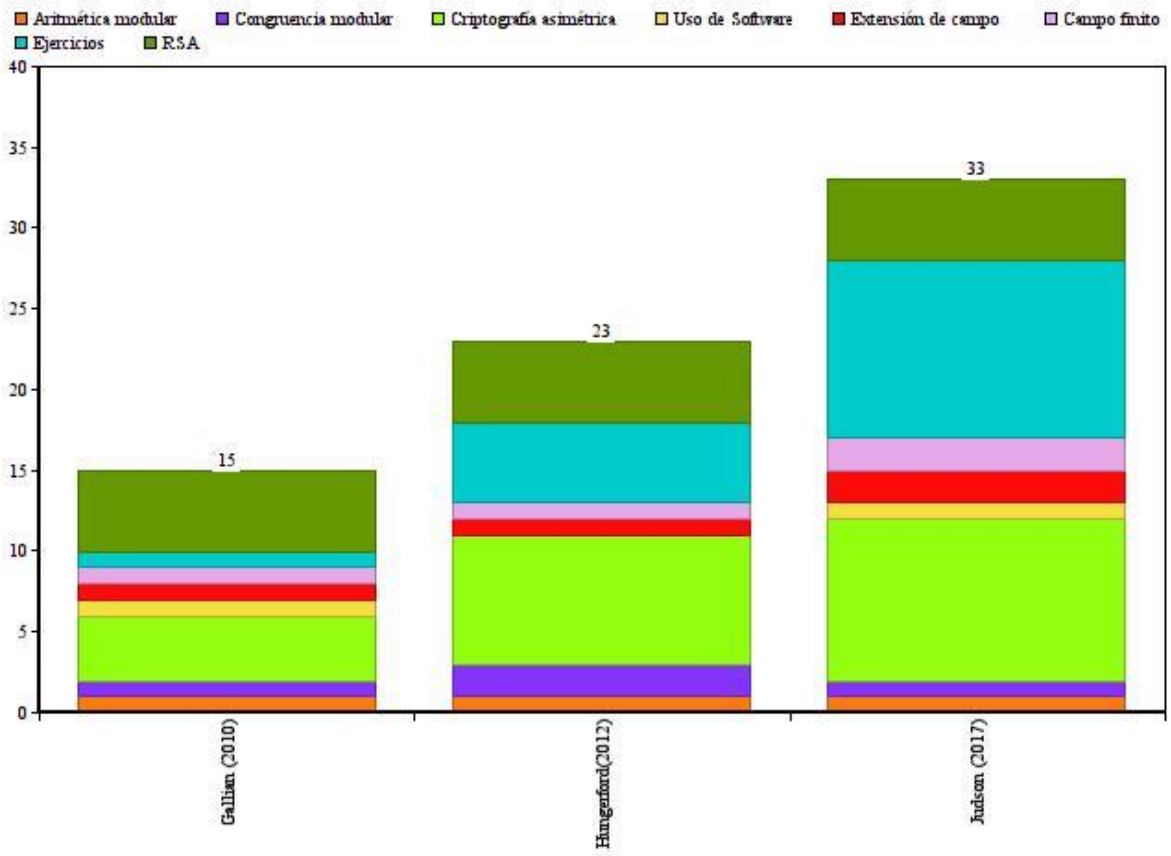


Imagen 35. Resultados categoría criptografía basada en grupos cíclicos.

Al analizar los libros de texto seleccionados en torno al concepto de grupo cíclico en el contexto de la criptografía asimétrica se observa que éstas incorporan diversos referentes matemáticos y didácticos para diseñar las actividades. En cuanto a los referentes didácticos se tiene que la ejemplificación del concepto de grupo cíclico multiplicativo es un referente frecuente en el diseño de las propuestas de trabajo de los libros de texto. Tal perspectiva promueve el acercamiento por parte del estudiante a la comprensión de criptosistemas asimétricos a partir de relaciones entre generadores y el orden de los elementos de un grupo cíclico. El concepto de grupo cíclico se asume como una construcción lógica dentro de un contexto aplicado. En este sentido los libros de texto formulan actividades de clasificación, seriación y correspondencias uno a uno para tratar de acercar

al estudiante al tipo de operaciones lógicas que les permitirían construir un grupo cíclico multiplicativo.

Por otro lado, al analizar los referentes pedagógicos y didácticos que orientan las propuestas de trabajo de los libros: Álgebra Abstracta de Dummit & Foote (1986), Álgebra Abstracta Herstein (1986) y Álgebra abstracta de Fraleígh (1988) en lo relativo al uso de software para el desarrollo de ejercicios sobre grupos cíclicos se observa una baja tendencia para asumir los procedimientos válidos para expresar y relacionar propiedades de grupo cíclico con la generación de criptosistemas asimétricos. Es poco frecuente encontrar enunciados y representaciones que indiquen el uso de software algebraico para hallar el orden de un elemento o el orden de un grupo. Dicho énfasis se puede explicar a la luz de los referentes dados por los lineamientos curriculares y de la perspectiva integradora sobre el aprendizaje del concepto de grupo cíclico de la época en que fueron escritos dichos libros.

Otro de los referentes respecto a las diferentes aplicaciones del grupo cíclico que también se identifican en los libros de texto es la criptografía asimétrica. Dicho enfoque corresponde a un enfoque moderno donde el grupo cíclico expresa la posibilidad de conectar las prácticas pedagógicas del docente con los sentidos, habilidades, relaciones y conceptualizaciones necesarias en el proceso de enseñanza del objeto matemático en función de las relaciones cuantitativas que se establezcan con otras disciplinas como la computación. La perspectiva de cuantificación resulta ser un contexto bastante natural para que los estudiantes inicien el estudio del grupo cíclico. Pese a ello la cuantificación no se limita a las aplicaciones inmediatas sino que abre la puerta a nuevas conjeturas y la vulnerabilidad de los criptosistemas asimétricos estimula la creación de nuevos objetos y teorías matemáticas que permitan brindar seguridad y confidencialidad a la información.

Frente a la caracterización de los referentes epistemológicos y cognitivos que orientan las propuestas de trabajo de los libros de texto en lo relativo al concepto de grupo cíclico en el contexto de la criptografía asimétrica se concluye que el proceso de transposición didáctica sí determina los elementos que van a circular en el contexto educativo en cuanto a saber matemático y en lo relativo a aspectos cognitivos, por lo que es pertinente que el docente reconozca los sentidos que cada libro de texto privilegia y en función de ello complemente sus propuestas de trabajo de aula de tal forma que integre actividades que potencien y desencadenen en los estudiantes mayores habilidades, relaciones y sentidos del concepto de grupo cíclico.

Unidad de introducción a la aritmética modular

Para dar repuesta al **segundo objetivo específico:** Diseñar una unidad de introducción a la aritmética modular para aplicar a un grupo de estudiantes del semillero de investigación SEC se formulan actividades referentes al tipo de conceptos y definiciones básicas para emprender el estudio del grupo cíclico en el contexto de la criptografía asimétrica

Introducción

Como se mencionó en la sección anterior la transposición didáctica se enfoca en el proceso de selección, reconstrucción y adaptación de los saberes matemáticos para ser enseñados en los contextos educativos. Este proceso se lleva a cabo en diferentes niveles: (1) en las instituciones productoras de saber, (2) en la "noosfera", (3) en el aula y (4) en la comunidad de estudio. En los capítulos precedentes se ha analizado cómo se lleva a cabo el proceso de transposición didáctica en torno al concepto de grupo cíclico en el contexto de la criptografía asimétrica, en los niveles (1) y (2).

En el presente apartado se pretende estudiar algunos aspectos acerca de cómo se desarrolla el proceso de transposición didáctica en el nivel (3). Una vez que la "noosfera" designa qué saberes

matemáticos van a ser enseñados el proceso de transformación y adaptación continúa. Los programas y referentes curriculares junto con los libros de textos se convierten en los mecanismos básicos de distribución del saber matemático en los contextos educativos. Así cada institución y su correspondiente cuerpo de docentes incorpora en los esquemas institucionales el saber matemático que se va a enseñar.

A este nivel el proceso de transposición didáctica se extiende y el docente quien es el directamente responsable de orientar los procesos de enseñanza organiza sus propuestas de trabajo de aula en función de los requerimientos institucionales sin dejar de lado sus concepciones, sus experiencias personales y sus conocimientos matemáticos, pedagógicos y didácticos. Estos aspectos determinan el discurso y las prácticas de enseñanza que el docente emplea en su trabajo de aula. En ese sentido se propone una unidad de introducción a la aritmética modular la cual pretende conectar a los estudiantes con los conceptos y definiciones básicas para emprender el estudio del grupo cíclico implementado en el contexto de la criptografía asimétrica.

Método

Se parte del análisis de problemas de ciberseguridad que se han solucionado usando herramientas de álgebra abstracta como el concepto de grupo cíclico. Se seleccionaron los objetos matemáticos de estudio necesarios para la intervención y algunas estrategias de enseñanza de los mismos con el fin de tener elementos suficientes para el diseño de las fases de la intervención. Los objetos matemáticos seleccionados para la intervención corresponden a nociones intuitivas y definiciones formales referentes a la aritmética modular, congruencia modular, grupo, grupo cíclico y logaritmo discreto los cuales se presentan en conexión con la criptografía asimétrica. Algunas estrategias de enseñanza de estos objetos se enmarcan en el uso de imágenes, esquemas y gráficos que permiten visualizar la estructura matemática de fondo en cada uno de estos objetos.

Criptografía

La unidad de introducción a la aritmética modular inicia con una breve explicación del significado de la palabra criptografía proveniente del griego kryptos: "ocultar" y grafos: "escribir", es decir, "escritura oculta" Santamaría (2013). Entendiéndose esta como el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Además, se hace una distinción entre criptografía simétrica y criptografía asimétrica. Si tanto el emisor como el receptor usan la misma clave el sistema se denomina simétrico de clave única, de clave secreta o cifrado convencional. En cambio, si el emisor y el receptor usan cada uno claves diferentes el sistema se denomina asimétrico, de dos claves o cifrado de clave pública.

Aritmética modular[15]

Cuando dividimos dos números enteros tenemos una ecuación que se ve como lo siguiente:

$$\frac{A}{B} = \text{ Q residuo R}$$

Donde A es el dividendo, B es el divisor, Q es el cociente y *R* es el residuo. A veces solo estamos interesados en cuál es el valor del **residuo** cuando dividimos A entre B, ara estos casos hay un operador llamado el operador módulo abreviado como mod y en lenguajes de programación y calculadoras modulares es representado con el símbolo %

[15] Las ideas presentadas en esta sección fueron tomadas del artículo ¿Qué es la aritmética modular? https://es.khanacademy.org/computing/computer-science/cryptography/modarithmetic

Al usar los mismos A, B, Q y R tendríamos: $A \bmod B = R$, donde a B se le conoce como el **módulo**.

Por ejemplo:

$$\frac{13}{5} = 2 \text{ residuo } 3$$

O equivalentemente

$$13 \bmod 5 = 3$$

Es importante observar el comportamiento del residuo cuando incrementamos números de uno en uno y luego los dividimos entre 3.

$\frac{0}{3}$ = 0 residuo **0**

$\frac{1}{3}$ = 0 residuo **1**

$\frac{2}{3}$ = 0 residuo **2**

$\frac{3}{3}$ = 1 residuo **0**

$\frac{4}{3}$ = 1 residuo **1**

$\frac{5}{3}$ = 1 residuo **2**

$\frac{6}{3}$ = 2 residuo **0**

$\frac{7}{3}$ = 2 residuo **1**

Los residuos comienzan en 0 y se incrementan en 1 cada vez hasta que el número alcanza uno menos que el número entre el que estamos dividiendo. Después de eso, la secuencia **se repite**. Este comportamiento induce conjeturas del tipo: si dividimos los números pares entre dos siempre se va a obtener residuo **0** y si dividimos los impares siempre vamos a obtener residuo **1**. Este tipo de análisis es importante pues más adelante se podrá explicar la conexión entre el código binario

conformado por { **0, 1**} y la aritmética modular. Para avanzar con la explicación de este tópico es menester introducir el concepto de congruencia modular.

Congruencia modular

$$A \equiv B \ (\mathbf{mod}\ C)$$

Esto se lee como: *A* es congruente con B módulo C se puede discutir el significado de la congruencia modular al realizar un experimento con el operador regular de módulo. Imaginando que se está calculando **mod 5** para todos los enteros, es decir, se está dividiendo cada número entero entre el número 5 y tomando como resultado el residuo que deja dicha división. Por ejemplo:

$\frac{0}{5}$ = 0 residuo **0**

$\frac{1}{5}$ = 0 residuo **1**

$\frac{2}{5}$ = 0 residuo **2**

$\frac{3}{5}$ = 0 residuo **3**

$\frac{4}{5}$ = 0 residuo **4**

$\frac{5}{5}$ = 1 residuo **0**

$\frac{6}{5}$ = 1 residuo **1**

$\frac{7}{5}$ = 1 residuo **2**

Supongamos que etiquetamos cinco rebanadas con 0, 1, 2, 3, 4. Luego para cada uno de los números enteros lo ponemos en una rebanada que coincida con el valor del entero mod 5. En la imagen 33 se muestran algunos enteros que se encuentran en cada una de las rebanadas.

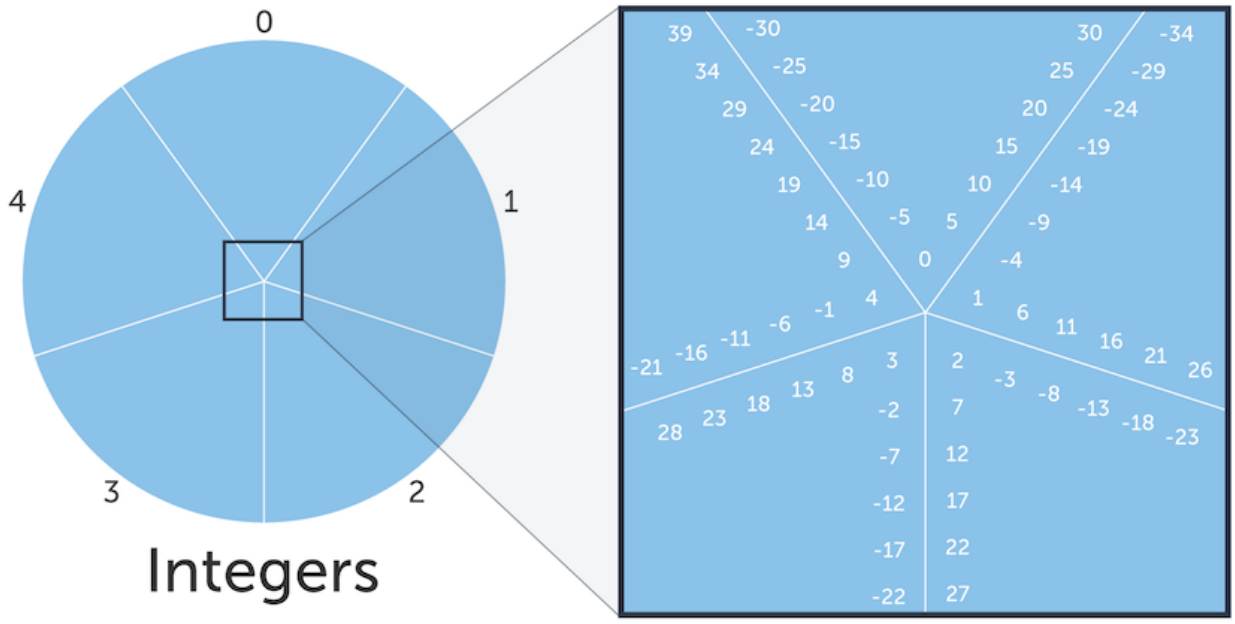


Imagen 36. Esquema gráfico mod 5 para los enteros

Fuente: khanacademy.org

Una manera común de expresar que dos valores están en la misma rebanada es decir que están en la misma **clase de equivalencia, l**a manera en que expresamos esto matemáticamente para un módulo C es:

$$A \equiv B \ (\textbf{mod}\ C)$$

Al examinar más de cerca la expresión:

- ✓ $\equiv$ es el símbolo de congruencia, lo que significa que los valores A y B están en la misma clase de equivalencia.
- ✓ (**mod** C) nos dice qué operación le aplicamos a A y a B.
- ✓ Cuando tenemos ambo, a " $\equiv$ " lo llamamos congruencia módulo C.

Por ejemplo $26 \equiv 11 \ (\text{mod } 5)$

$26 \pmod 5 = 1$, así que 26 está en la clase de equivalencia de 1

$11 \pmod 5 = 1$, así que 11 está en la clase de equivalencia de 1

Se puede generalizar la congruencia módulo al realizar el mismo experimento pensado al usar un entero positivo C etiquetando C rebanadas con 0, 1, 2, …, C - 2, C – 1. Luego se ubica cada uno de los números enteros en una rebanada que coincidiera con el valor del entero (**mod** C), la imagen 34 muestra algunos valores representativos que se encontrarían en cada una de las rebanadas.

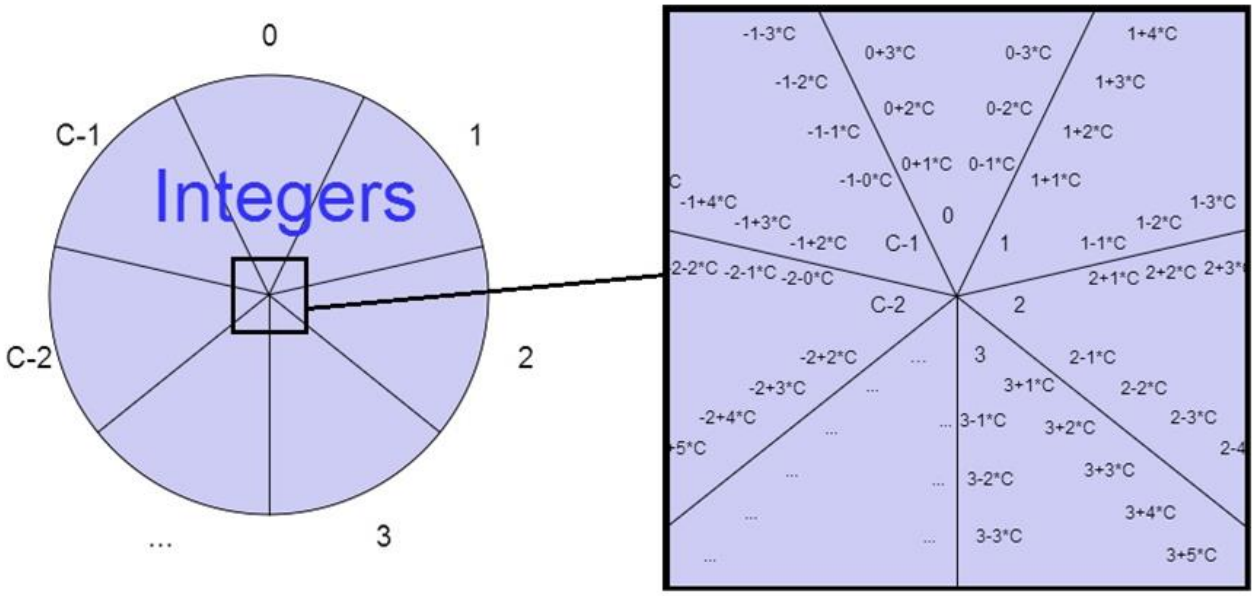


Imagen 37. Partición de los enteros en C clases de equivalencia diferentes.

Fuente: khanacademy.org

A partir de este experimento surge una observación clave: los valores en cada una de las rebanadas son iguales a la etiqueta $\boldsymbol{E}$ en la rebanada, más o menos un múltiplo de C, es decir:

Números en una rebanada: $\boldsymbol{E} \pm \boldsymbol{kC}, \boldsymbol{k} \in \mathbb{Z}$

Esto significa que la diferencia entre cualesquiera dos valores en una rebanada es un múltiplo de C.

Proposiciones equivalentes

Antes de continuar es importante recordar que las siguientes proposiciones son equivalentes

- ✓ $\mathrm{A} \equiv \mathrm{B} \pmod{\mathrm{C}}$
- ✓ $\mathrm{A} \pmod{\mathrm{C}} = \mathrm{B} \pmod{\mathrm{C}}$
- ✓ $C|(\mathrm{A} - \mathrm{B})$, (El símbolo | significa divide o es un factor de)
- ✓ $\mathrm{A} = \mathrm{B} + \mathrm{K} \cdot \mathrm{C}),\ K \in \mathbb{Z}$

Esto permite expresar la misma idea de diferentes formas. Ahora se estudia una propiedad de relevancia la cual indica que la congruencia modular $\equiv$ es una relación de equivalencia. Una relación de equivalencia define cómo se puede cortar un pastel (cómo hacer una partición de nuestro conjunto de valores) en rebanadas (clases de equivalencia).

En general las relaciones de equivalencia deben tener estas propiedades:

- El pastel: una colección de todos los **valores que nos interesan**.
- Una rebanada de pastel: una **clase de equivalencia**.
- Cómo cortamos el pastel en rebanadas: **relación de equivalencia**.

Específicamente, para nuestro ejemplo anterior:

- El pastel: la colección de **todos los enteros**.
- Una rebanada del pastel etiquetada con B*:* una clase de equivalencia en donde todos los valores son $\pmod{\mathrm{C}} = \mathrm{B}$

- ¿Cómo cortamos el pastel en rebanada?: al usar la relación de **congruencia módulo C,**

  $\equiv \ (\mathrm{mod}\ \mathrm{C}\ )$

Es por esto que la *congruencia módulo C es una relación de equivalencia* y genera una partición de los enteros en **C clases de equivalencia diferentes**. Saber que la congruencia módulo C es una relación de equivalencia permite conocer algunas propiedades que deben tener las **relaciones de equivalencia**:

- Son **reflexivas**: A está relacionada con A.
- Son **simétricas**: si A está relacionada con B, entonces B está relacionada con A.
- Son **transitivas**: si A está relacionada con B y B está relacionada con C, entonces A está relacionada con C.

Dado que **la congruencia módulo es una relación de equivalencia para (mod C)**. Esto significa:

- ✓ $\mathrm{A} \equiv \mathrm{A}\ (\mathrm{mod}\ \mathrm{C}\ )$, (**propiedad reflexiva**)
- ✓ si $\mathrm{A} \equiv \mathrm{B}\ (\mathrm{mod}\ \mathrm{C}\ )\ entonces\ \mathrm{B} \equiv \mathrm{A}\ (\mathrm{mod}\ \mathrm{C}\ )$, (**propiedad simétrica**)
- ✓ si $\mathrm{A} \equiv \mathrm{B}\ (\mathrm{mod}\ \mathrm{C}\ )\ y\ \mathrm{B} \equiv \mathrm{D}\ (\mathrm{mod}\ \mathrm{C}\ )\ entonces\ \mathrm{A} \equiv \mathrm{D}\ (\mathrm{mod}\ \mathrm{C}\ )$, (**propiedad transitiva**)

A continuación, se ilustra un ejemplo para aplicar estas propiedades a un ejemplo concreto usando $(\mathrm{mod}\ 5\ )$

- ✓ $3 \equiv 3\ (\mathrm{mod}\ 5\ )$, (**propiedad reflexiva**)
- ✓ si $3 \equiv 8\ (\mathrm{mod}\ 5\ )\ entonces\ 8 \equiv 3(\mathrm{mod}\ 5\ )$, (**propiedad simétrica**)
- ✓ si $3 \equiv 8\ (\mathrm{mod}\ 5\ )\ y\ 8 \equiv 18\ (\mathrm{mod}\ 5\ )\ entonces\ 3 \equiv 18\ (\mathrm{mod}\ 5\ )$(**propiedad transitiva**)

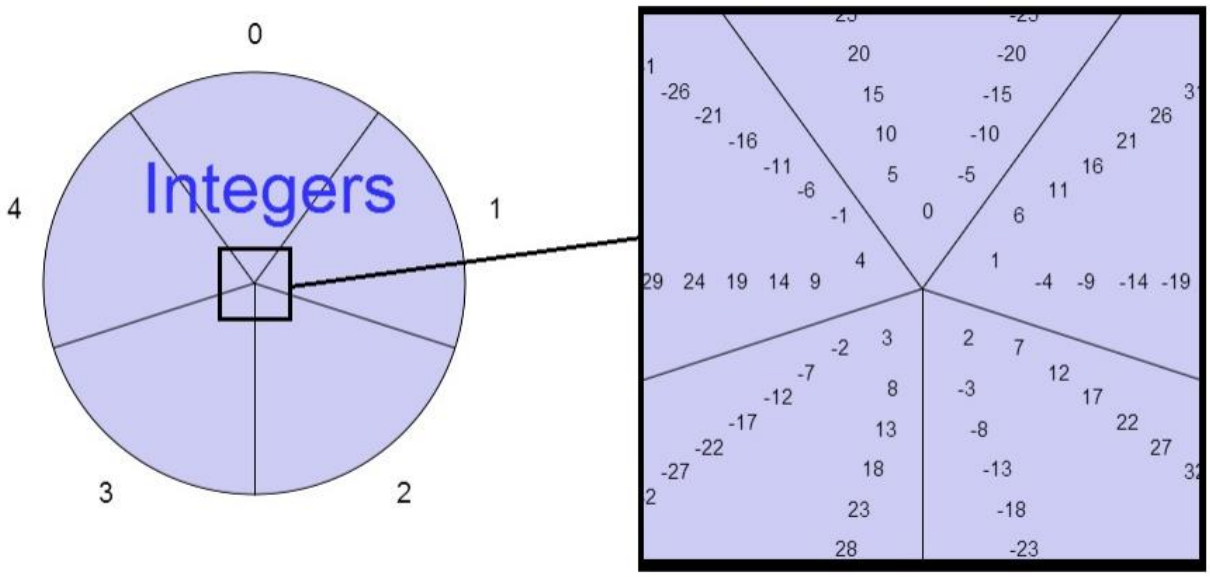


Imagen 38. Partición de los enteros en 5 clases de equivalencia diferentes.

Fuente: khanacademy.org

Las operaciones básicas de la aritmética modular se ilustran a continuación. No obstante, para fines de estudio del concepto de grupo cíclico en el contexto de la criptografía asimétrica se hará énfasis en la exponenciación modular.

Suma y resta modular:

- (A + B) mod C = (A mod C + B mod C) mod C
- (A - B) mod C = (A mod C - B mod C) mod C

Multiplicación modular

- $(A \cdot B)$ mod C = (A mod C · B mod C) mod C

Exponenciación modular

- A^Bmod C = ((A mod C)^B) mod C

A menudo en la formulación de un criptosistema asimétrico se requiere calcular $A^B(\text{mod C})$ para *valores grades de B*. Sin embargo A^B se vuelve muy grande incluso para valores pequeños de B.

Por ejemplo: A = 2, B= 90 y A = 7, B= 256

$2^{\mathbf{90}}$ = 1,237,940,039,290,000,000,000,000,000

$\mathbf{7}^{\mathbf{256}}$=2,213,595,400,050,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,00083,794,038,078,300,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,721,264,246,243,000,000,000,000,000

Estos valores tan grandes causan que las calculadoras y computadoras den un mensaje de error (overflow) incluso aunque no lo hicieran tomaría mucho tiempo encontrar el módulo de estos números tan largos de manera directa. Para reducir el tamaño de los términos involucrados y hacer el cálculo más rápido se descompone el número usando la regla de los exponentes.

$$2^{90}\ mod\ 13 = (2^{50} \cdot 2^{40})\ mod\ 13$$

$$2^{90}\ mod\ 13 = (2^{50}\ mod\ 13 \cdot\ 2^{40}\ mod\ 13)\ mod\ 13$$

$$2^{90}\ mod\ 13 = (\ 4 \cdot 3\ )\ mod\ 13$$

$$2^{90}\ mod\ 13 =\ 12\ mod\ 13$$

$$2^{90}\ mod\ 13\ =\ 12$$

Se debe tener en cuenta que al realizar exponenciación modular en criptografía no es raro utilizar exponentes para B > 1000 bits. El algoritmo de exponenciación modular rápida que se ilustra en la imagen 36 permite realizar dichos cálculos en la mitad del tiempo. La potencia del algoritmo radica en el uso de notación binaria del exponente B. La criptografía moderna usa en sus algoritmos de clave pública operaciones de exponenciación modular $A^B \pmod n$ con números muy grandes para protegerse de ataques por fuerza bruta, es decir, mediante un enfoque de prueba y error. No obstante para permitir realizar las operaciones de cifrado y descifrado en tiempos mínimos se hace uso de las propiedades de la congruencia modular y en particular del algoritmo de exponenciación rápida AER.

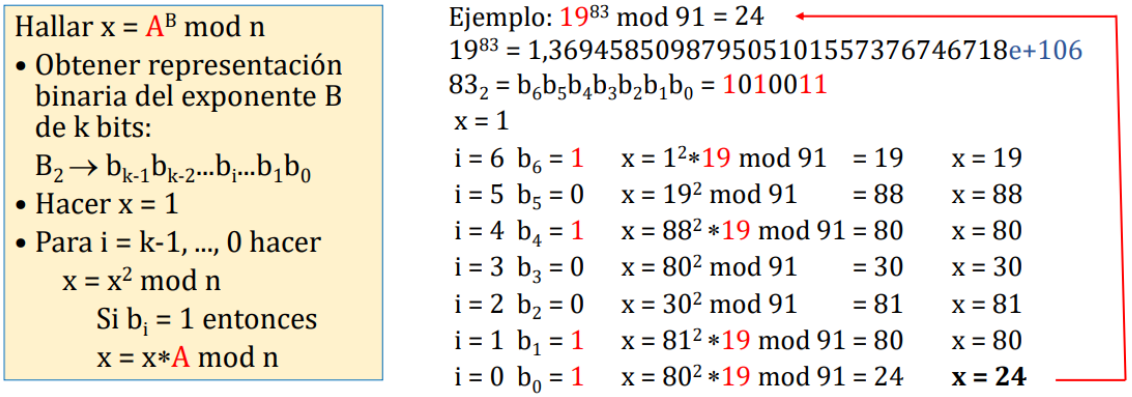


Imagen 39. Ejemplo algoritmo de exponenciación rápida AER

Fuente: criptored.upm.es/crypt4you

En el ejemplo anterior se realizaron 16 operaciones frente a las 164 si se usase reducción por cuadrados. ¿Cuántas operaciones se harán en una firma digital RSA sobre un hash de: $(256 \text{ bits})^{(2.048 \text{ bits})} \bmod (2.048 \text{ bits})$? Con el Algoritmo de exponenciación modular rápida 2.048 cuadrados y 1.000 multiplicaciones. Algunos algoritmos de cifra y firma digital en

criptografía asimétrica que usan operaciones de exponenciación modular con números muy grandes son:

Diffie y Hellman

$X_A = \propto^a \ mod\ p$ (con p un primo, α una raíz primitiva de p y a una clave secreta de A)

$X_B = \propto^b \ mod\ p$ (con p un primo, α una raíz primitiva de p y b una clave secreta de B)

RSA

$X = K^{eR} mod\ n_R$ (con $n_R = p_R \cdot q_R$, E_R clave pública, R = Receptor)

$X = h(M)^{dE} mod\ n_E$ (con $n_E = p_E \cdot q_E$, d_E clave privada, E = Emisor)

Elgamal

Clave privada = x

Clave pública = α^x mod p (con p un primo y α una raíz primitiva de p)

Grupo cíclico

Las definiciones de grupo y grupo cíclico con sus respectivos ejemplos presentadas durante la intervención se seleccionaron con base en el análisis hecho a los libros de texto estudiados. Siguiendo los resultados y análisis obtenidos en la categoría **análisis textual** en esta sección se privilegia la noción de grupo cíclico multiplicativo.

Grupo

Un grupo es un conjunto G junto con una operación $*$ que satisface las siguientes propiedades:

- ✓ Es **cerrado** bajo la operación $*$: si a, b ∈ G entonces a $*$ b ∈ G

- ✓ La operación $*$ es **asociativa**: si a, b, c ∈ G entonces (a$*$ b) $*$c =a$*$ (b$*$ c)
- ✓ Existe un elemento **identidad** denotado por *i:* si a ∈ G entonces a $*$ $i = i *$ a=a
- ✓ Todo elemento tiene un **inverso:** si a ∈ G entonces existe b ∈ G: a $*$ b = b$*$ a= i

Por su parte un **grupo cíclico** es aquel que puede ser generado por un solo elemento, es decir, existe un elemento g del grupo G (llamado "generador" de G) tal que todo elemento de G puede ser expresado como una potencia de g, G es cíclico con generador g si:

$$G = \{g^n \mid n \in Z\}$$

En general los generadores de Zn el conjunto de las clases de equivalencia son los enteros que son primos relativos con n, es decir, $mcd\ (n, j) = 1$. El número de tales generadores se designa por $\varphi(n)$ donde φ designa la función φ de Euler. Si p es primo el único grupo con p elementos (salvo isomorfismos) es Zp. Además si n es primo tendrá, $n - 1$ elementos ya que $\varphi(n) = n - 1$

$(\mathbb{Z}_5^*, \cdot_5)$

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$\{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 3\}$$
$$\{3^0, 3^1, 3^2, 3^3\} = \{1, 3, 4, 2\}$$
$$\{4^0, 4^1, 4^2, \ldots, 4^i, \ldots\} = \{1, 4\}$$

Imagen 40.Ejemplo grupo cíclico $(\mathbb{Z}_5^*, \cdot)$

$(\mathbb{Z}_5^*,\cdot)$ es el grupo cíclico multiplicativo formado por los elementos $\{1,2,3,4\}$ con elemento generador $\{1\}$. Con ayuda de la tabla de multiplicación módulo cinco se puden comprobar que el conjunto satisface las propiedades de grupo.

Definido el grupo cíclco multiplicativo se puede incompoprar al contexto de la criptografía asimetrica a traves del problema del logaritmo discreto cuya definicion requiere de dicha estructura algebraica y es de gran importamcia para la construción de protocolos criptográficos asimétricos.

Logaritmo discreto

Sea (G , ·) un grupo cíclico., finito de orden n (con n elementos), es decir:

$$G=\left\{ i = g^0, g^1, g^2, \dots, g^{n-1} \right\}, \text{ para cierto elemento } g \text{ de } G.$$

Dado $h \in G$ existe un $k \in \mathbb{Z}$ tal que $h=g^k$,el valor de k es el logaritmo discreto de h en base g. formalmente se define el logaritmo discreto así:

$$log_g : G \rightarrow \mathbb{Z}/n\mathbb{Z}$$

Como la funcion que asigna valores de la siguiente forma:

$$log_g(x) = k \quad tal\ que \quad x \equiv g^k$$

Según Santamaría (2013) no se conocen algoritmos clásicos para la computación del logaritmo discreto. Un algoritmo es elevar b a sucesivas potencias k hasta encontrar la deseada g. Este algoritmo requiere una complejidad temporal lineal respecto del tamaño del grupo G y por lo tanto exponencial respecto del número de dígitos en el tamaño del grupo. Algunos de los algoritmos funcionan para cualquier grupo mientras otros sólo pueden ser utilizados para ciertos grupos

concretos. Existe un algoritmo cuántico eficiente debido a Peter Shor este algoritmo abre la puerta a la criptogarfia postcuántica y en efecto requiere de un computador cuántico.[16]

Al mismo tiempo el problema inverso la exponenciación modular no es difícil ya que puede ser computada eficientemente usando exponenciación binaria (AER). Esta ***asimetría*** es análoga a la que ocurre entre la factorización de enteros y la multiplicación de enteros. Ambas ***asimetría***s han sido explotadas en la construcción de sistemas criptográficos.

Opciones populares para el grupo ciclico en la criptografía asimetrica usando logaritmos discretos son aquellos para los que no existen buenos algoritmos entre los que se encuentran los grupos cíclicos $\mathbb{Z}_p^*$ (e.g. Cifrado ElGamal, Diffie-Hellman y el algoritmo de firma digital) y subgrupos cíclicos de curvas elípticas sobre campos finitos los cuales introducen la criptografía de curva elíptica.

Encuesta a los asistentes a la conferencia.

Para la recolección de información sobre el tipo de conceptos y definiciones básicas para emprender el estudio del concepto de grupo cíclico en el contexto de la criptografía asimétrica se elaboró un paquete de preguntas organizadas a través de una encuesta la cual integra preguntas de respuesta abierta y cerrada. La encuesta pretende identificar en los asistentes a la conferencia titulada: "**Introducción a la Criptografía basada en Grupos Cíclicos**" el conocimiento de los participantes sobre la relación entre la teoría de grupos y criptografía asimétrica.

[16] Weisstein, Eric W. «Discrete Logarithm». En Weisstein, Eric W, ed. MathWorld (en inglés). Wolfram Research.

Codificación

Tabla 10. Codificaciones asistentes a la conferencia

Asistente	Programa Académico	Institución
A1	Ingeniería de sistemas	Universidad del Cauca
A2	----	Fundación Universitaria FUP
A3	Ingeniería de Sistemas	Universidad del Cauca
A4	Ingeniería de sistemas	Universidad del Cauca
A5	Licenciatura en matemáticas	Universidad del Cauca
A6	Filosofía	Universidad del Cauca
A7	Licenciatura en Matemáticas	Universidad del Cauca
A8	Matemáticas	Universidad del Cauca
A9	Ingeniería de sistemas	Universidad del Cauca

Estructura del instrumento y respuestas obtenidas

La primera pregunta busca indagar sobre la interdisciplinaridad entre los programas académicos a los que pertenecen los participantes, ya que en el proceso de transposición didáctica es importante determinar la población, sus necesidades e intereses. Esto permite incluir reflexiones en torno a los procesos educativos y de formación a cerca del concepto de grupo cíclico en el contexto de la criptografía asimétrica. Este aspecto además influye en los procesos de articulación y proyección de la educación tradicional con una educación que promueva el desarrollo de la investigación e interdisciplinaridad entre las ciencias involucradas en el proceso de transposición didáctica.

Durante la conferencia se indagó a los participantes mediante un formulario de Google[17] previamente elaborado sobre el desarrollo de la misma y posibles aportes a las fases presentadas. Se tuvo en cuenta las respuestas de los asistentes y las grabaciones de las sesiones del semillero.

Ante la pregunta referida: "Deja un comentario sobre la charla" destacan las siguientes respuestas:

"Excelente trabajo, muy buen acercamiento de los conceptos matemáticos de una manera muy sencilla y lo más importante sin cambiar las nociones fundamentales en el álgebra, con un tema que puede resultar difícil como lo es la teoría de grupos, no en vano hay un solo curso para estudiar la teoría de grupos". Asistente A5

"A modo personal, los temas que se abordaron fueron congruentes a medida que se desarrollaron en su respectivo orden. así, se facilita la referencia del tema, teniendo en cuenta la ingente envergadura que amerita los temas esbozados, que, a la vez, hacen la invitación a ampliar por medio de la investigación.". Asistente A6

Ante la pregunta ¿Conocías la relación entre Teoría de Grupos y Criptografía? destacan las siguientes respuestas de los asistentes A3, A5, A6, respectivamente:

"No, esta charla me dio a conocer sobre estos conceptos".

"Si, pero no he tenido la oportunidad de ahondar y conocer mejor la relación existente"

"Solamente referencias muy breves de investigaciones personales motivadas por la curiosidad"

[17] Formulario: https://forms.gle/aqFfrUTeGafpqs918

La imagen 41 presenta los resultados de la encuesta realizada a los asistentes referentes al programa académico, institución, conocimiento de la relación entre grupos cíclicos y criptografía asimétrica y la percepción de la presentación de los temas abordados en la conferencia.

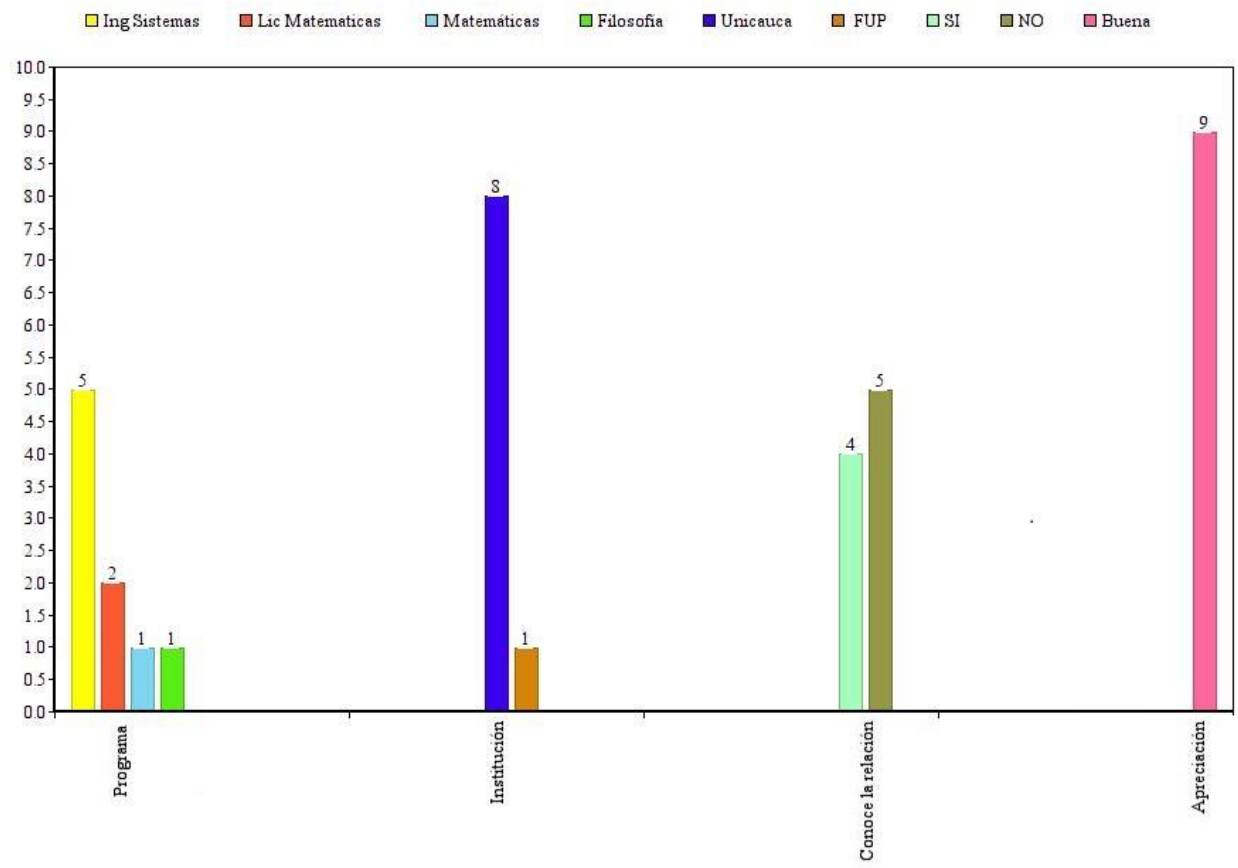


Imagen 41. Resultados encuesta

En la conferencia titulada Introducción a la Criptografía basada en Grupos Cíclicos destacan las siguientes apreciaciones hechas por el tutor del semillero SEC, asistente A9.

"Nos paseaste por una parte introductoria y básica de una manera muy didáctica, para cualquiera que quiera meterse poco a poco al tema de los algoritmos criptográficos esta clase o este tipo de conocimientos básicos es lo que tiene que afrontar para poderlos entender y tú lo hiciste en menos

de dos horas de una forma muy didáctica y muy sencilla, te felicito. Esta grabación me va a servir de material para los chicos de criptografía que a veces me preguntan cosas y a veces el bagaje matemático no lo manejo muy bien, me voy a apoyar muchísimo en esta grabación. A1 te lo tiene que estar agradeciendo porque esto lo necesita él para su trabajo de grado"

A lo que el asistente A1, responde: "bastante explicadito, quedó muy claro la explicación de los grupos, las clases, tenía una duda sobre la congruencia, pero con esta charla la resolví". Vale aclarar que A1 hace parte del semillero de investigación SEC, y se encuentra realizando su trabajo de grado en tópicos que conectan el álgebra abstracta y la criptografía asimétrica.

Durante el desarrollo de esta actividad se expone a los asistentes la relación entre la aritmética modular, los grupos cíclicos y la criptografía asimétrica a partir del establecimiento de correspondencias entre el problema del logaritmo discreto y los grupos cíclicos multiplicativos. A la vez que se establece el interés de los asistentes de diferentes programas académicos por un tema que se extiende más allá del pragmatismo de las aplicaciones haciendo un llamado de atención acerca de la relación entre los desarrollos teóricos de las matemáticas y la seguridad de la información la cual se ve cada vez más amenazada por el crecimiento del mundo digital.

Propuesta para abordar el protocolo criptográfico ElGamal

Para dar cumplimiento al **tercer objetivo específico**: generar una propuesta para abordar el protocolo criptográfico ElGamal como una actividad introductoria a la criptografía basada en grupos cíclicos. Se inicia con una introducción a la criptografía desde una mirada histórica. Seguidamente se describe la definición del Problema del Logaritmo Discreto para que pueda utilizarse en criptografía suele requerirse que el grupo cíclico cumpla algunas condiciones las cuales serán expuestas y ejemplificadas. Además, es necesario definir *el Problema* de Diffie-

Hellman (búsqueda) a partir de esta idea de generación de claves se propone con los mismos parámetros el criptosistema de clave publica ElGamal.

Introducción

El uso de problemas matemáticos difíciles o imposibles de resolver bajo ciertas condiciones con las herramientas de cálculo disponibles hoy en día es algo habitual en Criptografía. Uno de los problemas matemáticos en los que se basan algunos sistemas criptográficos es el tópico de esta sección, el logaritmo discreto. Aunque el logaritmo discreto se ha definido en un grupo multiplicativo y en este trabajo sólo se consideran grupos de este tipo se puede definir de forma general en un grupo. Según Santamaría (2013) es posible definir el logaritmo discreto en grupos aditivos como el conjunto de puntos de una curva elíptica en tal caso se habla de logaritmo discreto elíptico.

La Criptografía se definía como el arte de escribir mensajes en clave secreta o de modo enigmático para evitar que su contenido fuese inteligible por un posible intruso en la comunicación. Es decir, el único objetivo de la Criptografía era conseguir la confidencialidad de los mensajes. No obstante, con la publicación del artículo de Shannon (1948), *una teoría matemática de las comunicaciones,* la Criptografía comenzó a ser considerada una ciencia aplicada que requiere conocimientos de otras ciencias como las Matemáticas o la Teoría de la Información.

A finales del siglo XX el desarrollo de la informática e Internet dieron lugar a grandes cambios en Criptografía. Por ejemplo, la gran cantidad de información a disposición de muchos usuarios hace necesario que los datos estén protegidos durante su almacenamiento no sólo durante la transmisión. Es por eso que actualmente la Criptografía tiene otros objetivos aparte de la transmisión secreta de la información. Este tipo de aplicaciones se engloba dentro de lo que se denominan protocolos criptográficos. Según Santamaría (2013), un protocolo criptográfico es un

conjunto bien definido de etapas, implicando a dos o más partes y acordado por ellas, designado para realizar una tarea específica que utiliza como herramienta algún algoritmo criptográfico, ejemplos de estos son:

- ✓ Protocolos de autentificación: hay dos tipos de autentificación: autentificación de mensaje y autentificación de usuario. La primera asegura que el contenido del mensaje no ha sido alterado. La segunda, certifica la identidad del remitente.
- ✓ Protocolos para compartir secretos: la finalidad de este tipo de protocolos es distribuir un cierto secreto entre un conjunto *P* de participantes de manera que ciertos subconjuntos prefijados de *P* puedan, uniendo sus participaciones, recuperar dicho secreto.
- ✓ Pruebas de conocimiento cero: hacen posible que un individuo pueda convencer a otro de que posee cierta información sin revelarle nada sobre el contenido de la misma.
- ✓ Transacciones electrónicas seguras: permiten realizar de manera electrónica segura las operaciones bancarias habituales, firma electrónica de contratos.
- ✓ Votaciones electrónicas: permiten realizar un proceso electoral electrónicamente, garantizando la privacidad de cada votante y la imposibilidad de fraude.

Así pues, la Criptografía ya no sólo se utiliza para preservar la confidencialidad, sino que con ella se buscan también otros objetivos:

- ✓ Autentificación: es la propiedad que permite identificar el generador de la información (y de esta manera evitar posibles suplantaciones de identidad).
- ✓ Integridad: es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- ✓ No repudio: proporciona protección contra la interrupción por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la

comunicación. Esto evita que el emisor niegue el envío de cierta información o que el receptor niegue que la recibió.

En criptografía de clave pública es importante notar que la clave pública se obtiene a partir de la privada (o viceversa). Por tanto, para que realmente el secreto sea tal es necesario que la clave pública venga definida por una función conocida, pero de la que sea computacionalmente imposible deducir la clave privada sin el conocimiento de cierta información suplementaria que sólo posee cada usuario. Este tipo de funciones se denominan funciones trampa y están basadas en la dificultad computacional de ciertos problemas matemáticos. Algunos criptosistemas de clave pública utilizan la exponenciación en un ***grupo cíclico*** **multiplicativo** finito como función trampa y en su criptoanálisis es necesario resolver el problema del logaritmo discreto. El conjunto de técnicas utilizadas por el enemigo para descifrar los mensajes secretos es una ciencia conocida como Criptoanálisis.

Los primeros usos conocidos de Criptografía se remontan a la antigüedad, el primera data del siglo V a. C, durante la guerra entre Atenas y Esparta. El método utilizado es conocido como la ***escítala*** y consistía en escribir el mensaje sobre una cinta enrollada en un rodillo de manera que al desenrollarla las letras quedaban descolocadas y el mensaje sólo podía ser leído en otro rodillo de igual grosor. Asimismo, se sabe que los romanos utilizaban un cifrado consistente en sustituir unas letras por otras según una regla fija conocida como ***Cifrado del César***. Dicha regla era trasladar la letra a cifrar unas posiciones en el alfabeto. También aparecen textos cifrados por sustitución en la Biblia. No obstante, en la actualidad la seguridad de un criptosistema se mide suponiendo que el enemigo conoce completamente los procesos de cifrado y descifrado.

En el siglo XX se produjo un gran desarrollo en Criptografía debido a las guerras mundiales en las cuales era necesario establecer comunicaciones secretas a través del telégrafo y la radio. En la

Primera Guerra Mundial el descifrado del conocido como telegrama ***Zimmermann*** en el que el ministro alemán pretendía convencer a Japón y México de invadir EE.UU. fue clave para que EE.UU. entrase en guerra. Durante la Segunda Guerra Mundial se construyó la máquina ***Colossus***, precursora de los ordenadores modernos, ésta permitió a la oficina criptoanalítica británica capitaneada por ***Alan Turing*** romper la seguridad de la máquina de cifrado alemana ***Enigma***.

Hasta 1976 todos los criptosistemas eran de clave privada, en ese momento Diffie-Hellman establecieron los principios teóricos que debería satisfacer un criptosistema de clave pública estas son las conocidas como condiciones de Diffie-Hellman:

- ✓ El cálculo de las claves pública y privada debe ser computacionalmente sencillo, es decir, dado por un algoritmo de complejidad polinómica.
- ✓ El proceso de cifrado ha de ser computacionalmente sencillo.
- ✓ El proceso de descifrado, conociendo la clave secreta, debe ser computacionalmente sencillo.
- ✓ La obtención de la clave secreta a partir de la pública ha de ser un problema computacionalmente imposible, es decir, dado por un algoritmo de complejidad exponencial
- ✓ La obtención del mensaje original, conociendo el mensaje cifrado y la clave pública, debe ser computacionalmente imposible

Nacieron a partir de entonces nuevos criptosistemas como el RSA o ElGamal. Según Santamaría (2013) el primero basa su seguridad en la dificultad de factorizar un número natural compuesto, el sistema criptográfico ElGamal por su parte utiliza como función trampa la exponenciación modular, cuya función inversa es el logaritmo discreto.

En 1985 el investigador egipcio Taher Elgamal popularmente conocido como el padre de SSL, Secure Socket Layer, propone algoritmos de cifra y firma digital que llevan su nombre. Su seguridad reside en el problema del logaritmo discreto al igual que en el intercambio de clave de Diffie y Hellman. Aunque el algoritmo es muy seguro no logra desbancar a RSA como estándar de cifra. No obstante, una variación de su algoritmo de firma conocido como DSA, Digital Signature Algorithm, se establece como estándar de firma digital por el NIST en 1994. Según Glez (2003) al igual que el problema de factorización de enteros el llamado problema del logaritmo discreto ha jugado un papel fundamental en la construcción de los cimientos de la criptografía de clave pública. Su formulación se presenta a continuación:

Problema del Logaritmo Discreto:

Sea G un grupo, g ∈ G un elemento de orden n. Dado $h \in \langle g \rangle$, encontrar $k \in \{0, \dots, n-1\}$ tal que $h = g^k$

Para que dicho problema pueda utilizarse en criptografía suele requerirse que el grupo G involucrado cumpla al menos dos condiciones:

- La ley de grupo ha de ser fácil de implementar
- No debe conocerse un algoritmo polinomial que resuelva el problema del logaritmo discreto en G.

Además, es importante resaltar que $\beta = \alpha^x \bmod p$ con *x* como variable se resuelve en un tiempo polinomial (P), pero $x = \log_\alpha \beta \bmod p$ tiene una solución polinomial no determinista (NP). Esta asimetría es la encargada de brindar seguridad ante ataques por fuerza bruta, es decir, ataques que pretendan probar una a una cada posible solución

Algunos grupos que reúnen estas condiciones son:

- ✓ El grupo multiplicativo $\mathbb{F}_{p^m}^*$ asociado al campo finito $\mathbb{F}_{p^m}$ de característica prima *p*, *m* cualquier número natural.
- ✓ El grupo de puntos de una curva elíptica sobre un campo finito.
- ✓ El grupo de unidades $\mathbb{z}_n^*$, donde *n* es un entero compuesto.
- ✓ El jacobiano de una curva hiperelíptica definida sobre un campo finito.

Muchos esquemas criptográficos basados en el logaritmo discreto emplean el grupo multiplicativo $\mathbb{F}_p^*$ con *p* primo o bien el grupo asociado a un campo finito de característica dos. Además, la mayor parte de las herramientas criptográficas no se fundamentan exactamente en el problema del logaritmo discreto sino en un problema relacionado con él: el llamado problema de Diffie-Hellman.

Problema de Diffie-Hellman (búsqueda): dados un número entero *n*, un generador *g* del grupo cíclico multiplicativo de orden *n* y dos elementos $\mathrm{g}^a, \mathrm{g}^b,\ a, b \in \{0, \dots, n-1\}$ encontrar el elemento $\mathrm{g}^{a \cdot b}$.

En la literatura a menudo se llama al problema anterior *problema de Diffie-Hellman generalizado* denominando entonces *problema de Diffie-Hellman* al caso particular planteado sobre el grupo multiplicativo $\mathbb{z}_p^*$ con *p* primo. En este se basan el esquema de intercambio de claves Diffie-Hellman y el criptosistema ElGamal[18], dos herramientas clásicas que han sido analizadas en profundidad tanto teóricamente como desde el punto de vista práctico.

Intercambio de claves de Diffie-Hellman:

[18] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithm . IEEE Trans. Info. Theory, 31:469–472, 1985

Sea *p* un número primo *g* un ***generador*** del grupo $\mathbb{z}_p^*$. Los individuos *A* y *B* quieren intercambiar una clave secreta para comunicarse, para ello actúan según los siguientes pasos:

- ✓ *A* elige un entero $a \in \{0, \dots, p-2\}$, y envía a *B* el elemento g^a
- ✓ De modo análogo, *B* elige un entero $b \in \{0, \dots, p-2\}$, y envía a *A* el elemento g^b
- ✓ *A* y *B* computan la clave común $\mathrm{k} = \mathrm{g}^{ba} = \mathrm{g}^{ab}$.

A partir de esta idea de generación de claves se propone con los mismos parámetros el Criptosistema de Clave Pública ElGamal***:***

ElGamal

- ✓ Clave pública: $(p, \mathrm{g}, \ \mathrm{g}^a)$.
- ✓ Clave privada: $a \in \{0, \dots, p-2\}$.

Supongamos que *B* quiere enviar un mensaje $m \in \mathbb{z}_p^*$ a *A*:

- ✓ Cifrado: *B* elige un elemento $b \in \{0, \dots, p-2\}$, y envía a *A* el elemento g^b y $\mathrm{m} \cdot \mathrm{g}^{ab}$
- ✓ Descifrado: *A* recibe un par $(c, d) \in \mathbb{z}_p^* \times \mathbb{z}_p^*$. Usando su clave privada, recupera el mensaje $\mathrm{m} = (c^a)^{-1} \cdot \mathrm{d}$

Todos los productos indicados en las descripciones anteriores se consideran en $\mathbb{Z}_p^*$

Una pregunta que justifica la importancia del uso de grupos cíclicos en el contexto de la criptografía asimétrica es ¿Qué sucede si no se usa un generador α del grupo cíclico multiplicativo? Para el primo p = 2.017 existen 576 (aproximadamente 30%) *generadores* o *raíces primitivas* α, siendo 5 el valor más pequeño. Si se usa como α un valor que no sea una raíz primitiva, por ejemplo, el número 2 el cifrado y descifrado de Elgamal siguen siendo correctos. Solamente sucederá que

para la clave pública existirán más de un valor de clave privada que sea válido. Eso significa una menor seguridad.

A continuación, se ilustra una implementación del protocolo criptográfico ElGamal haciendo uso del software SageMath recomendado en el libro Algebra Abstracta Teoría y Aplicaciones de Judson (2017) y el software para explorar las propiedades de grupos y anillos específicos que proporciona programas interactivos para los ejercicios de computadora en el libro Contemporary Abstract Algebra de Gallian (2010) .[19]

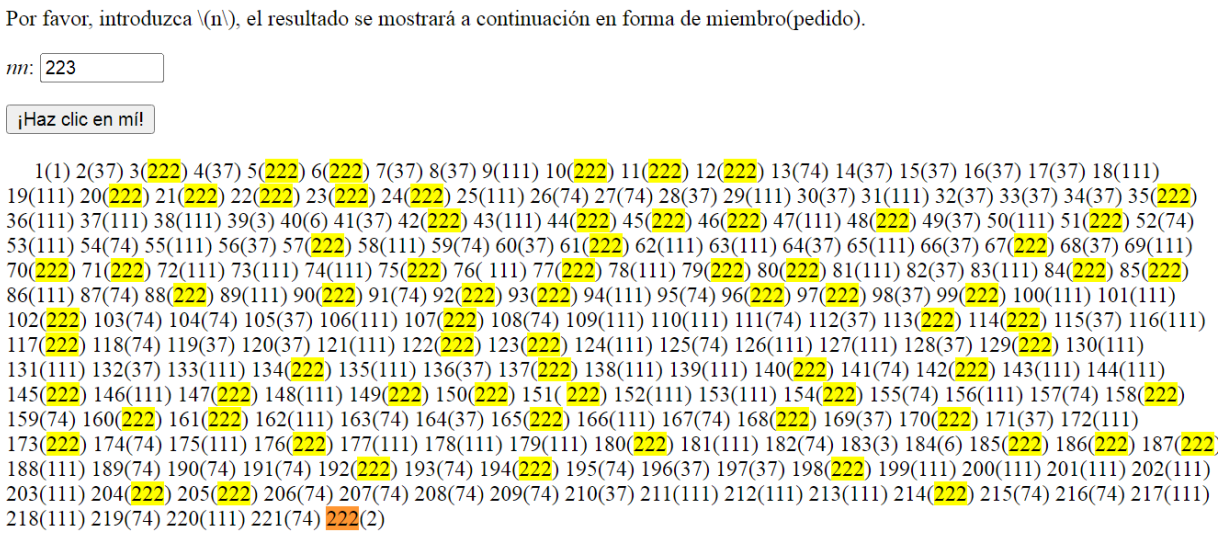


Imagen 42.Generadores del grupo cíclico $\mathbb{z}_{223}^{*}$

Fuente: software libro Gallian. (2010)

De la lista de generadores del grupo cíclico multiplicativo $\mathbb{z}_{223}^{*}$ obtenida con el software desarrollado por Gallian. (2010) se va a seleccionar el generador g = *20*. Con SageMath se implementó el siguiente código, el cual simula el funcionamiento del criptosistema ElGamal.

[19] Software: Software Supplement to Abstract Algebra (umn.edu)

```
# Código Elgamal en SageMath
# Camilo Martínez

# Generación de claves
p = int(input('Ingrese un número primo : '))
d = int(input('Ingrese la clave privada: '))
e1 = int(input('Ingrese un generador del grupo cíclico'))
e2 = mod(e1^(d), p)

# Cifrado
plain = input('Ingrese el texto plano: ')
r = int(input('Ingrese la clave del remitente: '))

encrypyted = ""
decrypted = ""
c1 = mod(e1^r, p)
mul = e2^r

# Cifrar cada carácter en plano y almacenarlo en cifrado
for x in list(plain):
    c2 = mod(mul*ord(x), p)
    encrypyted += chr(c2)

# Descifrado
dec_inv = Integer(c1^d).inverse_mod(p)

# Descifrar cada carácter en cifrado y almacenar en descifrado
for x in list(encrypyted):
    pp = mod(ord(x)*dec_inv, p)
    decrypted += chr(pp)

# Resultado
print('\ntexto plano: '+ (plain))
print('\ntexto Cifrado: '+ (encrypyted))
print('\ntexto Descifrado: '+ (decrypted))
```

Imagen 43. Código que simula el funcionamiento del criptosistema ElGamal

Una vez se ejecuta el programa diseñado se obtiene la siguiente salida.

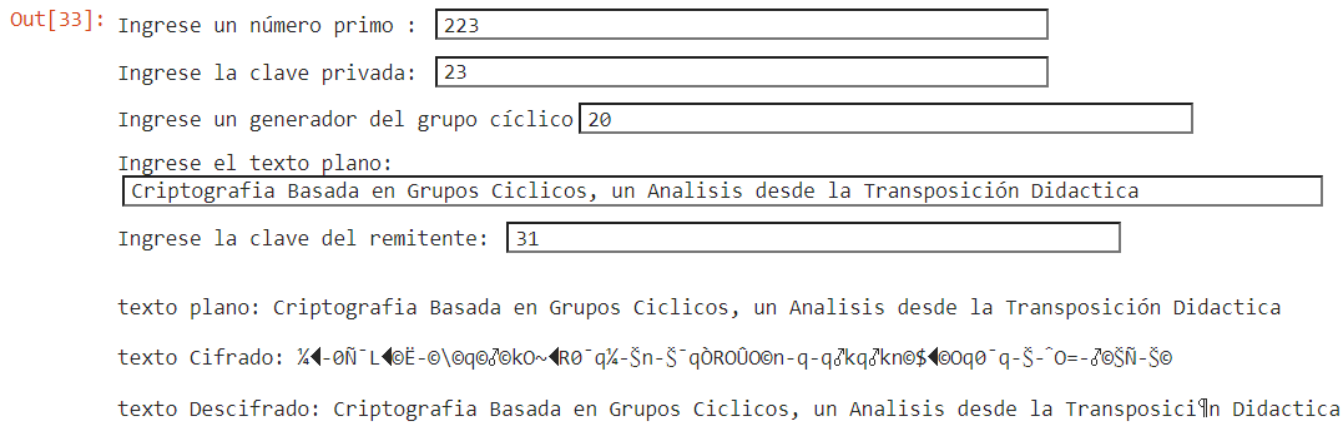


Imagen 44. Salida del algoritmo ElGamal

Conclusiones

El estudio de la problemática relativa al proceso transposición didáctica respecto al concepto de grupo cíclico en el contexto de la criptografía asimétrica es un ejercicio investigativo, que si bien es particular dado que alude a un concepto matemático abordado desde la interdisciplinaridad refleja en gran medida el proceso adaptativo que recorre el saber matemático para lograr ser incorporado en los contextos educativos como tecnológicos. Dicho proceso adaptativo se lleva a cabo en diferentes instancias acorde con por los objetivos planteados y responde a una multiplicidad de factores: las políticas públicas sobre educación, las políticas económicas y de desarrollo del país, los procesos evaluativos del sistema escolar, los intereses privados de las casas editoriales de libros de texto, las necesidades contextuales de las instituciones de educación superior, los saberes didácticos de los docentes, entre otros.

La descripción y caracterización de las etapas del proceso de transposición didáctica en torno al concepto de grupo cíclico permitió identificar las instancias donde se lleva a cabo y los factores que lo determinan. El proceso recorrido en cuanto a los análisis de orden histórico-epistemológico, de orden didáctico y de las propuestas que presentan los libros de texto que se ponen en juego en el proceso de construcción del concepto de grupo cíclico es un mapa de ruta para elaborar futuros estudios en torno a otros conceptos matemáticos, además de brindar elementos para la elaboración de propuestas curriculares muy bien fundamentadas en torno a la enseñanza del concepto de grupo cíclico.

Desde el inicio se tomaron decisiones para acotar la problemática y elegir el concepto matemático objeto de reflexión. En ese sentido el concepto de grupo cíclico en el contexto de la criptografía asimétrica y el ciclo de formación en el semillero de investigación fueron seleccionados dado que no se encontraban registros de trabajos de investigación en educación

matemática que aludieran al proceso de transposición didáctica en este contexto. Se generó un documento de referencia tanto para docentes como investigadores que evidenciara cómo llega el saber matemático al contexto educativo y en esa línea aportar elementos de reflexión didáctica para cualificar el saber didáctico y las prácticas del docente en estos escenarios. Dicho propósito se cumplió pues el presente informe de sistematización sintetiza análisis epistemológicos, didácticos y cognitivos en torno a un concepto central en el desarrollo del pensamiento matemático que se trabaja cotidianamente en las aulas de clases. De ahí que los análisis que aquí se exponen pueden ser atractivos y funcionales para ser consultados por el docente interesado.

El marco teórico de la transposición didáctica y su desarrollo a través de contexto tecnológicos ofrecieron un referente fundamental para determinar qué tipo de análisis se debían elaborar para caracterizar las adaptaciones que ha tenido el concepto de grupo cíclico en el contexto de la criptografía asimétrica. Cada uno de los cuatro saberes que se denotan en el proceso transpositivo (el saber matemático, el saber matemático a enseñar, el saber matemático enseñado y el saber matemático disponible) y las instancias en las que se producen demarcaron hacia dónde enfocar la investigación. El saber matemático se reconstruyó a partir de los estudios histórico – epistemológicos, el saber matemático a enseñar mediante el análisis de los programas y reglamentaciones curriculares y a través de la caracterización de las propuestas de trabajo de los libros de texto. En este ejercicio investigativo queda abierta la línea de trabajo que se pregunte y de cuenta del saber matemático disponible en el aula de clase, lo que los estudiantes aprenden y cómo lo aprenden.

Bibliografía

Alfaro Carvajal, C., & Chavarría Vásquez, J. (2012). La transposición didáctica: un ejemplo en el sistema educativo costarricense. *Uniciencia*, *26*(1), 153–168.

Ayerra, I. (2018). *Criptografía y curvas elípticas. La curva de WhatsApp* [Universidad de Zaragoza Director]. https://zaguan.unizar.es/record/76745/files/TAZ-TFG-2018-3214.pdf

Bernstein, D. J. (2006). Curve25519: nuevos récords de velocidad diffie-Hellman. *Lecture Notes in Computer Science*, *3958*, 207–228. https://doi.org/10.1007/11745853_14

Cesaratto, E., & Fuentes, C. (2015). Criptografía en el profesorado de matemática. *Revista de Educación Matemática*, *30*(1), 3–25.

Chevallard, Y. (1998). *La transposición didáctica: Del saber sabio al saber enseñado*. *16*(1), 45–66. http://ciiepatagones.com.ar/sitio/wp-content/uploads/2014/02/51745084.03-La-Trasposicion-Didactica-Del-Saber-Sabio-al-Saber-Enseñado-Yves-Chevallard-pag.-3-24si.pdf

Dubinsky, E. (2000). De la investigación en la matemática teórica a la investigación en la Matemática Educativa: un viaje personal. *Revista Latinoamericana de Investigación En Matemática Educativa*, *3*(1).

Dummit, D., & Foote, R. (1986). *Álgebra Abstracta*. https://doi.org/10.1007/s11425-010-4066-8

Fraleígh, J. B. (1988). *Algebra Abstracta Primer Curso* (3rd ed.). ADDISON-WESLEY IBEROAMERICANA, S. A. https://apuntespme.cl/material/AlgAbs/textos/algabs.pdf

Franchi, M. R. (2012). *ALGORITMOS DE ENCRIPTACIÓN DE CLAVE ASIMÉTRICA*.

Glez Vasco, I. (2003). *Criptosistemas basados en Teoríua de Grupos*.

Gómez, B. (1999). Tendencias metodológicas en la enseñanza de la proporcionalidad derivadas del análisis de libros antiguos: el caso de los problemas de "compañías." *Revista Latinoamericana de Investigación En Matemática Educativa*, *2*(2–3), 19–29.

Herstein, I. N. (1986). *ÁLGEBRA ABSTRACTA*.

Hungerford, T. (2012). *www.TechnicalBooksPdf.com*.

Ibarra, S. (2008). La Transposición Didáctica del Álgebra en las Ingenierías. El Caso de los Sistemas de Ecuaciones Lineales. *Cic.Ipn.Mx*.

Joseph A. Gallian. (2010). Contemporary Abstract Algebra. In *Contemporary Abstract Algebra*.

Judson, T. W., & Beezer, R. A. (2017). *Algebra Abstracta Teoría y Aplicaciones*. antoniobehn.cl/aata

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. *Handbook of Applied Cryptography*, 15. https://doi.org/10.5860/choice.34-4512

Santamaría, J. (2013). *El logaritmo discreto y sus aplicaciones en Criptografía*. https://repositorio.unican.es/xmlui/bitstream/handle/10902/3101/Jennifer Santamaria Fernandez.pdf?sequence=1

Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*, *27*(4), 623–656. https://doi.org/10.1002/j.1538-7305.1948.tb00917.x

Vásquez, N. (2010). *Un ejercicio de transposición Didáctica en Torno al Concepto de Número Natural en el Preescolar y el Primer Grado de Educación Básica*.