PROGRAMA DE ALGEBRA APLICADA

Nombre	**Algebra Aplicada**	
Carrera	Ingeniería Matemática	
Código	22176	
Créditos SCT-Chile	***6 Sct***	*Tbjo. Directo: 6 hrs. pedag. – Tbjo. Autónomo: 6 hrs. cronolog. (semanal)*
Nivel	8vo Semestre	
Requisitos	Algebra Abstracta	
Categoría	*Obligatorio*	
Área de conocimiento según OCDE	*Ciencias Naturales*	

Descripción

Contribución al Perfil de Egreso

La asignatura de Algebra Aplicada tributa a los siguientes desempeños integrales del perfil de egreso de Ingeniería Matemática:

1. Desarrollar constructos matemáticos teóricos y prácticos para estudiar problemas que surgen del ámbito académico o profesional, utilizando herramientas matemáticas avanzadas y el pensamiento abstracto y/o estructurado.
4. Interpretar los resultados obtenidos de la resolución de problemas, analizando la información desde una perspectiva cualitativa y cuantitativa para la toma decisiones en función de los distintos contextos de aplicación, con responsabilidad y ética en el quehacer profesional.

Resultado de aprendizaje general

Al finalizar el curso, el estudiante será capaz de entender y aplicar los conceptos fundamentales del Algebra Aplicada como complejidad de operaciones aritméticas, aritmética modular, criptografía pre-cuántica. También el estudiante conocerá en forma introductoria las curvas elípticas y aplicará transformada de Fourier discreta (DFT) y rápida (FFT). Finalmente podra conocer en forma general conceptos de criptografia post-cuántica.

Resultados de aprendizaje específicos	**Unidades temáticas**
• Reconocer la complejidad de las operaciones aritméticas básicas en anillos comunes como los enteros y anillos de polinomios con coeficientes en un cuerpo. • Conocer el funcionamiento del algoritmo Euclidiano extendido en un dominio Euclidiano. • Entender la relación entre el algoritmo Euclidiano extendido y la construcción de cuerpos finitos con su aritmética básica.	**1) Complejidad de las operaciones aritméticas** • Sumas, restas y multiplicaciones. • El algoritmo Euclidiano extendido y el inverso modular. • Aplicación: Construir efectivamente cuerpos finitos.

	• Conocer las principales técnicas asociadas a la aritmética modular (cambiar de un anillo a un cuerpo, utilización de módulos compuestos para distribuir el trabajo, utilización de potencias de primos y liftings) • Entender la relación entre la interpolación de polinomios y la versión computacional del Teorema Chino de los Restos, y su aplicación en la aritmética modular. • Aplicar la aritmética modular en algunos ejemplos prácticos como el cálculo de determinantes de matrices grandes y el cálculo del polinomio característico de una matriz	**2) La aritmética modular y algunas aplicaciones** • Técnicas de aritmética modular. • Evaluación e interpolación de polinomios. • El Teorema Chino de los Restos. • Determinantes y polinomios característicos de matrices vía aritmética modular.
	• Conocer la aplicación de grupos en comunicaciones seguras a través del problema del logaritmo discreto. • Entender las propiedades básicas del problema del logaritmo discreto y su relación con los isomorfismos de grupos. • Reconocer a través de algunos ejemplos prácticos que el problema del logaritmo discreto no tiene la misma dificultad computacional en todos los grupos finitos.	**3) Criptografía pre-cuántica: algunos casos de logaritmos discretos** • Descripción del intercambio de llaves de Diffie y Hellman (basado en el logaritmo discreto) • Logaritmos discretos en cuerpos finitos. • Logaritmos discretos en grupos de matrices: el efecto de la diagonalización y de la forma de Jordan.
	• Definir el grupo de una curva elíptica. • Conocer la estructura de grupo de una curva elíptica y su aplicación para logaritmos discretos en curvas definidas sobre un cuerpo finito. • Entender algunas aplicaciones computacionales de las curvas elípticas como el test de primalidad de Goldwasser y Killian y el algoritmo de factorización de Lenstra (ambos para números enteros).	**4) Introducción a las curvas elípticas** • El grupo de una curva elíptica. • Curvas elípticas y logaritmos discretos. • Tests de primalidad y factorización de enteros con curvas elípticas.
	• Entender el funcionamiento de la transformada discreta de Fourier y conocer algunas de sus aplicaciones. • Entender la transformada rápida de Fourier (o transformada de teoría de números) y su aplicación para la multiplicación rápida de polinomios.	**5) La transformada discreta de Fourier (DFT) y la transformada rápida de Fourier (FFT)** • Raíces primitivas de la unidad, matrices de Vandermonde y definición de la DFT. • Algunas aplicaciones de la DFT. • La FFT y la multiplicación rápida.

	• Entender de forma general el problema del aprendizaje con errores en anillos de polinomios (RLWE). • Entender con se utiliza el problema RLWE para obtener la transmisión segura de un secreto (encapsulación de llaves). • Conocer la conexión entre la transformada rápida de Fourier y los parametros utilizados en el criptosistema Kyber.	**6) Criptografía post-cuántica: criptosistemas basados en reticulados** • Introducción al problema RLWE (Aprendizaje con errores en anillos) • Utilización del problema RLWE para la criptografía • El protocolo Kyber y la utilización de la FFT
	Metodologías de enseñanza y de aprendizaje Clases expositivas. En el tiempo de **trabajo autónomo** el/la estudiante deberá realizar tareas para reforzar el aprendizaje de la clase	
	Procedimientos de evaluación Se requerirá un mínimo de dos pruebas cuyo promedio debe valer al menos el 50% de la nota final del curso. El resto de las evaluaciones pueden consistir de exposiciones, tareas, etc.	
	Bibliografía básica • von zur Gathen, J.; Gerhard, J. (2013) *Modern Computer Algebra, Third edition*. Cambridge University Press, Cambridge. • Hankerson, D.R.; Menezes, A.; Vanstone, S.A. (2004) *Guide to Elliptic Curve Cryptography*. Springer, New York. • Goldwasser, S.; Kilian, J. (1999) *Primality testing using elliptic curves*, Journal of the ACM, 46 (4), 450-472. • Lenstra, H.W. (1987) *Factoring integers with elliptic curves*. Annals of Mathematics, 126 (3), 649-673. • Schwabe, P.; Avanzi, R.; Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Seiler, G.; Stehle, D.; Ding, J. (2020) CRISTALS-Kyber, NIST Post-Quantum Cryptography Competition, Third round candidates. https://pq-crystals.org/kyber/resources.shtml.	