PROGRAMA DE ALGEBRA APLICADA[1]

<table>
<tr><td>Nombre</td><td colspan="3">Algebra Aplicada</td></tr>
<tr><td>Carrera</td><td colspan="3">Ingeniería Matemática</td></tr>
<tr><td>Código</td><td colspan="3"></td></tr>
<tr><td>Créditos SCT-Chile</td><td>6 Sct</td><td colspan="2">Tbjo. Directo: 6 hrs. pedag. – Tbjo. Autónomo: 6 hrs. cronolog. (semanal)</td></tr>
<tr><td>Nivel</td><td colspan="3"></td></tr>
<tr><td>Requisitos</td><td colspan="3">Computación II, Álgebra Abstracta</td></tr>
<tr><td>Categoría</td><td colspan="3">Obligatorio</td></tr>
<tr><td>Área de conocimiento según OCDE</td><td colspan="3">Ciencias Naturales</td></tr>
<tr><td rowspan="3">Descripción</td><td colspan="3">Contribución al Perfil de Egreso</td></tr>
<tr><td colspan="3">Resultado de aprendizaje general</td></tr>
<tr><td>Resultados de aprendizaje específicos</td><td colspan="2">Unidades temáticas</td></tr>
<tr><td>● 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.</td><td colspan="2">1) Complejidad de las operaciones aritméticas
● Sumas, restas y multiplicaciones.
● El algoritmo Euclidiano extendido y el inverso modular.
● Aplicación: Construir efectivamente cuerpos finitos.</td></tr>
</table>

[1]

	● 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.

<table>
<tr><td></td><td>

- 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.

</td><td>

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

</td></tr>
<tr><td></td><td colspan="2">Metodologías de enseñanza y de aprendizaje</td></tr>
<tr><td></td><td colspan="2">Procedimientos de evaluación</td></tr>
<tr><td></td><td colspan="2">

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.

</td></tr>
</table>