Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Cuerpos Finitos

Modalidad:	**Posgrado**	X
	Educación permanente	X

Profesor de la asignatura [1]:
Dr. Claudio Qureshi, Profesor Adjunto del IMERL, UdelaR.
(título, nombre, grado o cargo, instituto o institución)

Profesor Responsable Local [1]: Claudio Qureshi
(título, nombre, grado, instituto)

Otros docentes de la Facultad: No.
(título, nombre, grado, instituto)

Docentes fuera de Facultad: No.
(título, nombre, cargo, institución, país)

[1] Agregar CV si el curso se dicta por primera vez.
(Si el profesor de la asignatura no es docente de la Facultad se deberá designar un responsable local)
Disponible en https://exportcvuy.anii.org.uy/pdf/?f74f87e7c80959c0c238996a4f7abd3e

[Si es curso de posgrado]
Programa(s) de posgrado: Maestría en Ingeniería Matemática

Instituto o unidad: IMERL, FING, UDELAR

Departamento o área: Matemática

Horas Presenciales: 115 horas
(se deberán discriminar las horas en el ítem Metodología de enseñanza)

Nº de Créditos: 12
[Exclusivamente para curso de posgrado]
(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem Metodología de enseñanza)

Público objetivo: Estudiantes que estén cursando la maestría en matemática o en ingeniería matemática. Estudiantes avanzados de la licenciatura en matemática o ingeniería en computación.

Cupos: No.
(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Asimismo, se adjuntará en nota aparte los fundamentos de los cupos propuestos. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción, hasta completar el cupo asignado)

Objetivos: Introducir al estudiante en el área de Cuerpos Finitos y sus aplicaciones, especialmente las referentes a criptografía y telecomunicaciones.

Conocimientos previos exigidos: Álgebra lineal y nociones básicas de aritmética y teoría de grupos (con los cursos de álgebra lineal y matemática discreta 2 de la Fing sería suficiente).

Conocimientos previos recomendados: Nociones básicas de las estructuras algebraicas básicas como espacio vectoriales, grupos, anillos y módulos (estos últimos serán cubiertos rápidamente en las primeras clases).

Metodología de enseñanza:
(comprende una descripción de la metodología de enseñanza y de las horas dedicadas por el estudiante a la asignatura, distribuidas en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

Descripción de la metodología:
Tendremos dos clases teóricas semanales de 2 horas cada una y además una clase práctico y/o de consulta semanal de 2 horas. El estudiante además debe realizar los ejercicios prácticos fundamental para una mejor comprensión de la disciplina.

Detalle de horas:

- Horas de clase (teórico): 76 horas (4 horas semanales)
- Horas de clase (práctico) o consulta: 38 horas (2 horas semanales)
- Horas de clase (laboratorio):
- Horas de consulta:
- Horas de evaluación: 1 hora
    - Subtotal de horas presenciales: 115
- Horas de estudio: 19 (1 hora semanal)
- Horas de resolución de ejercicios/prácticos: 38 (2 horas semanales)
- Horas proyecto final/monografía: 8 (preparación de examen oral)
    - Total de horas de dedicación del estudiante: 180=115+65

Forma de evaluación:
Entrega de ejercicios y examen oral final.

Temario:

Breve repaso de nociones algebraicas (especialmente las referentes a extensiones de cuerpo y teoría de Galois).

Estructura de los cuerpos finitos (propiedades de la traza y la norma, teorema de la base normal, raices de la unidad y polinomios ciclotómicos, teorema de Wadderburn).

Polinomios sobre cuerpos finitos (número de polinomios irreducibles, polinomios primitivos, órdenes de polinomios y propiedades, fórmula de inversión de Mobius, construcción de polinomios irreducibles, polinomios linealizados, algunos resultados sobre binomios y trinomios).

Sumas exponenciales (caracteres, sumas de Gauss, teorema de Davenport-Hasse, teorema de Stickelberger, la ley de reciprocidad cuadrática, sumas de Jacobi, la

relación de Davenport-Hasse, suma de caracteres con argumentos polinomiales, teorema de Weil, sumas de Kloosterman, sumas de Jacobsthal).

Polinomios de permutación, LFSR y otras aplicaciones de cuerpos finitos.

Seguiremos principalmente los capítulos 1,2,3 y 5 del libro [RN]. Para la parte de polinomios de permutación, LFSR y otras aplicaciones estudiaremos tópicos específicos dentro de los capítulos 7 al 9 del libro [RN].

Bibliografía:

[RN] Lidl, Rudolf, and Harald Niederreiter. *Finite fields*. Vol. 20. Cambridge university press, 1997.
[MP] Gary Mullen and Daniel Panario. *Handbook of finite fields*. CRC Press, 2013.
[GG] Golomb, Solomon W., and Guang Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.

Datos del curso

Fecha de inicio y finalización: 15/03/2022 al 23/07/2022

Horario y Salón: A definir.

Arancel: No corresponde
[Si la modalidad no corresponde indique “no corresponde”. Si el curso contempla otorgar becas, indíquelo]

Arancel para estudiantes inscriptos en la modalidad posgrado:
Arancel para estudiantes inscriptos en la modalidad educación permanente: