FORMULARIO
Curso de Posgrado

1. Título: Cuerpos Finitos
Abreviatura de título: Cuerpos Finitos

2.Profesor:
Claudio Qureshi

3. Responsable **: Claudio Qureshi**

4. Marque la disciplina más cercana al curso:
- Álgebra y Fundamentos (X)
- Análisis
- Probabilidad y Estadística
- Sistemas Dinámicos y Geometría

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

6. Horas de clase teóricas: 76 horas (4 horas semanales)

7. Horas de clase prácticas/consulta: 38 horas (2 horas semanales)

8. Otros horarios: No.

9. Total de horas presenciales (suma de los tres puntos anteriores):
114 horas (6 horas semanales)

10. Método de aprobación:
Entrega de ejercicios y examen oral final

11. Conocimientos previos recomendados:
Nociones básicas de grupos, anillos y módulos. Álgebra lineal.

12. Programa del Curso:

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].

13. Bibliografía:

Referencia principal:

[RN] Lidl, Rudolf, and Harald Niederreiter. *Finite fields*. Vol. 20. Cambridge university press, 1997.

Referencias secundarias:

[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.