

Fundamentos Matemáticos de Códigos y Criptografía (250)

Profesor: José Noé Gutiérrez H. Cubículo: AT-210

Correo: ngh@xanum.uam.mx

Asesorías: Lunes de 12:30 a 14:00 o por correo en cualquier momento.

Temario

1. **Teoría de los Números** Aritmética modular. Teoremas de Fermat y Euler. Algoritmos. Teorema Chino del Residuo.
2. **Residuos cuadráticos** Definición. Símbolos de Legendre y Jacobi.
3. **Conceptos de Álgebra** Grupos, anillos, campos, anillos de polinomios, extensiones de campos.
4. **Campos Finitos** Conceptos básicos y construcción de campos finitos. Propiedades básicas de campos finitos. Función Traza.
5. **Aplicaciones** Uso de sistemas algebraicos computacionales como SageMath, Python, Mahtematica®. Programación para realizar aritmética sobre diversas estructuras algebraicas. Cifrado de ElGamal. Curvas elípticas.

Evaluación del curso

El 70% de la calificación se asignará al resultado de tres exámenes parciales, o bien al de un global. Las tareas tendrán un valor de 30% de la calificación final. Los ejercicios de las tareas pueden responderse con ayuda de la computadora, por ejemplo utilizando SAGEMath, Mathematica o Maxima.

Con dos exámenes parciales aprobados se tiene derecho a presentar un examen de reposición de un examen parcial.

Los exámenes parciales se aplicarán en los días: **viernes** de la semana **4**, **viernes** de la semana **8** y **miércoles** de la semana **11**, respectivamente; mientras que el examen global o de reposición será el miércoles de la semana **12**. Estas fechas se refieren al trimestre 250.

Escala de calificaciones

Una calificación en el intervalo:

[0, 6) corresponde a **NA**

[6, 7.5) corresponde a **S**

[7.5, 8.8) corresponde a **B**

[8.8, 10] corresponde a **MB**

Bibliografía

1. Gallian, J.A., *Contemporary Abstract Algebra*, 9th Edition, CENGAGE Learning, 2015.
2. Gutiérrez, J.N. *Fundamentos Matemáticos de Códigos y Criptografía*. Notas de Clase, 2014.
3. Lidl, R. and Niederreiter, H., *Finite Fields*. Addison-Wesley, 1983.
4. MacWilliams, F.J. and Sloane, N.J.A. *The Theory of Error-Correcting Codes*. North Holland, 1977.
5. McEliece, R.J. *Finite Fields for Computer Scientist and Engineers*. The Kluwer International Series in Engineering and Computer Sciences, Boston, 1982.
6. Niven, I, Zuckerman, H. *Introducción a la Teoría de los Números*. Limusa, 1976.
7. Roman, S. *Coding and Information Theory*. Springer-Verlag (GTM), 1992.
8. Shoup, V.A. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.
9. Stinson, D. R. y Paterson, M.B. *Cryptography: Theory and Practice*. CRC Press, 4th Edition, 2019.
10. Wan, Z.-X. *Lectures on Finite Fields and Galois Rings*. World Scientific, 2012.