Fundamentos Matemáticos de Códigos y Criptografía (24P)

Profesor: José Noé Gutiérrez H. Cubículo: AT-210
Correo: ngh@xanum.uam.mx
Asesorías: Miércoles y viernes de 13:00 a 14:30 o por correo en cualquier momento.

Temario

1. **Teoría de 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, Maple®, Mahtematica®, Macaulay2®, Máxima. Programación para realizar aritmética sobre diversas estructuras algebraicas.

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 SAGE, 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 las semana 11, respectivamente; mientras que el examen global o de reposición será el miércoles de la semana 12. Estas fechas se refieren al trimestre 24P.

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, 7th Edition, Brooks/Cole, Cengage Learning, 2010.
2. Gutiérrez, J.N. Fundamentos Matemáticos de Códigos y Criptografía. Notas de Clase, 2014.
3. Koblitz, N.I. Algebraic Aspects of Cryptography. Algorithms and Computation in Mathematics, vol. 3, Springer, 1998.
4. Lild, R. and Niederreiter, H., Finite Fields. Addison-Wesley, 1983.
5. MacWilliams, F.J. and Sloane, N.J.A. The Theory of Error-Correcting Codes. North Holland, 1977.
6. McEliece, R.J. Finite Fields for Computer Scientist and Engineers. The Kluwer International Series in Engineering and Computer Sciences, Boston, 1982.
7. Niven, I, Zuckerman, H. Introducción a la Teoría de los Números. Limusa, 1976.
8. Roman, S. Coding and Information Theory. Springer-Verlag (GTM), 1992.
9. Shoup, V.A. Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2008.
10. Stinson, D.R. y Paterson, M.B. Cryptography: Theory and Practice. CRC Press, 4th Edition, 2019.