Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

PROGRAMA DE ESTUDIOS

UNIDAD **IZTAPALAPA**	DIVISION **CIENCIAS BASICAS E INGENIERIA**	1/ 2
NOMBRE DEL PLAN **POSGRADO EN MATEMATICAS**		

CLAVE	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CREDITOS	9
2138024	**ARITMETICA Y CAMPOS FINITOS**	TIPO	**OPT.**
H.TEOR. **4.5**		TRIM.	**I AL IX**
H.PRAC. **0.0**	SERIACION **AUTORIZACION**		

OBJETIVO(S):

Que al final de la UEA el alumno sea capaz de:

1. Dominar los conceptos básicos de Teoría de los Números y Álgebra Conmutativa.
2. Manejar con soltura la aritmética modular y de campos finitos.
3. Utilizar programas de cómputo algebraico en la solución de problemas aritméticos y algebraicos.

CONTENIDO SINTETICO:

1. Teoría de Números. Aritmética modular. Teoremas de Fermat, Euler y Chino del residuo. Residuos Cuadráticos.
2. Números primos. Técnicas básicas de generación de primos y pruebas de primalidad. Pruebas de Miller-Rabin y AKS. Método de Pollard.
3. Álgebra. Grupos, anillos, anillos de polinomios, campos.
4. Campos finitos. Conceptos básicos y ejemplos de campos finitos. Extensión de campos. Construcción de campos finitos. Clases ciclotómicas y polinomios irreducibles. Norma y traza. Bases normales.
5. Álgebra computacional. Uso de programas algebraicos de cómputo como Maple®, Mathematica® o Macaulay® para resolver ejercicios relacionados con los temas vistos.

Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

ADECUACION
PRESENTADA AL COLEGIO ACADEMICO
EN SU ~~SESION~~ NUM. 336

EL SECRETARIO DEL COLEGIO

CLAVE **2138024** **ARITMETICA Y CAMPOS FINITOS**

MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:

El profesor impartirá las lecciones y destinará algunas sesiones a la resolución de ejercicios. El alumno usará algún manipulador algebraico para ilustrar los conceptos vistos y para resolver ejercicios. Se asignarán ejercicios que deberán entregarse resueltos en fechas preestablecidas.

MODALIDADES DE EVALUACION:

Se aplicarán al menos dos evaluaciones periódicas. La ponderación de las evaluaciones y tareas queda a juicio del profesor.

BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

1. Koblitz, N.I., Algebraic Aspects of Cryptography. Algorithms and Computation in Mathematics, vol. 3, Springer, 1998.
2. Koblitz, N.I. A Course in Number Theory and Cryptography (Graduate Texts in Mathematics, No 114), Springer Verlag, 2nd ed., 1994.
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. Menezes et al., Applications of Finite Fields. Kluwer Academic Publishers, 1993.
7. Roman, S. Coding and Information Theory. GTM Springer, 1992.
8. Roman, S., Field Theory. Springer Verlag, 1995.
9. Shoup, V. A computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005.
10. Shparlinski, I., Computational and Algorithmic Problems in Finite Fields. Kluwer Academic Publishers, 1992.
11. Stinson, D. R. Cryptography: Theory and Practice. Chapman & Hall/CRC, 3rd ed., 2006.

Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

ADECUACION
PRESENTADA AL COLEGIO ACADEMICO
EN SU SESION NUM. 336

EL SECRETARIO DEL COLEGIO