M95'

9

NUEVO MODELO DE PROGRAMA A REGIR A PARTIR

DEL 1ER. CUATRIMESTRE DE 1994

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

UNIVERSIDAD DE BUENOS AIRES

1. DEPARTAMENTO/INSTITUTO DE MATEMATICA
2. CARRERA de: a) Licenciatura en Cs Matemáticas
   Orientación Pura y Aplicada
   b) Doctorado y/o Post-grado en ---
   c) Profesorado en ---
   d) Cursos Técnicos en Meteorología ---
   e) Cursos de Idiomas ---
3. 1er. Cuatrimestre/2do. Cuatrimestre 2do Cuat. Año 1995
4. N* DE CODIGO DE CARRERA 03
5. MATERIA ELEMENTOS DE TEORIA DE NUMEROS
6. N* DE CODIGO ----
7. PUNTAJE PROPUESTO (en caso de tratarse de materias optativas para la Licenciatura o de Doctorado y/o Post-Grado) 3 ptos
8. PLAN DE ESTUDIOS Año 1982
9. CARACTER DE LA MATERIA (Obligatoria u optativa) Optativa
10. DURACION (anual, cuatrimestral, bimestral u otra) Cuatrimestral
11. HORAS DE CLASES SEMANALES

a) Teóricas	3 hs	d) Seminarios	..... hs
b) Problemas	3 hs	e) Teórico-Problemas	..... hs
c) Laboratorio	..... hs	f) Teórico-Práctico	..... hs

g) Totales Horas 6

APROBADO POR RESOLUCION C.D. Nº 178/96

12. CARGA HORARIA TOTAL .....6..

FORMA DE EVALUACION ..... Examen final .....

13. ASIGNATURAS CORRELATIVAS ..... 8 materias cualesquiera de la Lic. .....

.....

14. PROGRAMA ANALITICO (adjuntarlo) Se adjunta

15 BIBLIOGRAFIA (indicar título del libro, autor, editorial y año de publicación; adjuntar luego del programa)

Fecha ..... 2do. Cuatrimestre 1995 .....

Firma Profesor .....

Aclaración de firma. ..... Dr. Eduardo DUBUC.

Firma del Director .....

Sello aclaratorio .....

Nota: Para la validez de la información presentada se solicita que todas las páginas estén inicialadas y firmadas al final por el Sr. Director del Departamento/Instituto/Carrera o Responsable debidamente selladas y fechadas.

Otra: Se recuerda que los objetivos y los contenidos mínimos están incluídos en el Plan de Estudios respectivo y sólo son modificables por Resolución del Consejo Superior de la Universidad de Buenos Aires.

Elementos de Teoría de Números

Síntesis del Programa:

-Grupo modular y el algoritmo de Euclides.
-Fracciones continuas.
-Teorema Chino del Resto.
-Función φ de Euler/Cuerpos Finitos.
-Ley de reciprocidad cuadrática.
-Grupo de clases de extensiones cuadráticas.
-Desarrollo y análisis de diversos tests de primalidad y algoritmos de factorización.
-Demostraciones de complejidad.(de costado se vera su interés en la criptografía, en especial en los sistemas a llave abierta).

Bibliografía:

Harvey Cohn. Advanced Number Theory.
Neal Koblitz. A course in Number Theory and Criptograph
Hans Riesel. Prime Numbers and computer methods for Factorización.

2do Cuatrimestre 1995.

Firma del Profesor:

Aclaración de Firma: Dr. Eduardo DUBUC.