Universidad Nacional de Córdoba
FACULTAD DE MATEMATICA ASTRONOMÍA Y FÍSICA

Expte. 03-05-00814

RESOLUCION HCD N° 29/2005

VISTO

Las propuestas presentadas por los señores docentes Dr. Juan Pablo ROSSETTI y Roberto Jorge MIATELLO, por las cuales solicitan que las materias "Retículos en Espacios Euclídeos" e "Introducción a Códigos y Criptografía" sean incorporadas a la nómina de materias optativas del Plan de Estudios de la Licenciatura en Ciencias de Computación, aprobado por Res. H. Consejo Superior N° 470/01; y

CONSIDERANDO

Que estas propuestas han sido discutidas en la Comisión Asesora de Computación y cuentan con el aval de la misma;

Que los objetivos, programas y cargas horarias de las mismas corresponden a materias optativas del Plan de Estudios de la Licenciatura en Ciencias de la Computación;

Que hay alumnos interesados en cursarlas como optativas de dicha Licenciatura;

Que mediante Resolución HCS n° 122/02 se ha delegado en este Cuerpo la facultad de modificar la nómina de materias optativas del Plan de Estudios de la Licenciatura en Ciencias de la Computación;

Que se hace necesario incorporarlas a la nómina de materias optativas, aprobada por Res. H. Consejo Directivo N° 207/02;

POR ELLO

EL HONORABLE CONSEJO DIRECTIVO DE LA FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA
R E S U E L V E :

ARTÍCULO 1°: Modificar la nómina de materias optativas del Plan de Estudios de la Licenciatura en Ciencias de la Computación, incorporando a la misma las materias **"Retículos en espacios Euclídeos"** e **"Introducción a Códigos y Criptografía"** cuyos programas, correlativas y cargas horarias están detalados en el Anexo que forma parte de la presente Resolución.

ARTÍCULO 2°: Con ajuste a lo determinado en el artículo 2° de la Res. HCS n° 122/02, remítase a la Secretaría de Asuntos Académicos de la Universidad, la nómina de materias de que se trata, para su conocimiento y evaluación.

ARTÍCULO 3°: Comuníquese y archívese.

DADA EN LA SALA DE SESIONES DEL HONORABLE CONSEJO DIRECTIVO DE LA FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA, A VEINTIÚN DIAS DEL MES DE MARZO DE DOS MIL CINCO.

mjm.

Dr MIGUEL A. RE
Secretario General Fa.M.A.F

Dr. GIORGIO M. CARANTI
Decano de Fa.M.A.F

Expte. 03-05-00814

ANEXO A RES. HCD N° 29/2005

MATERIA OPTATIVA	CORRELATIVAS			CARGA HORARIA
	PARA CURSAR		PARA RENDIR	
	REGULARIZADA	APROBADA	APROBADA	
Retículos en Espacios Euclídeos	Algebra; Análisis Matemático II	Matemática Discreta I; Análisis Matemático I	Algebra; Análisis Matemático II	120
Introducción a Códigos y Criptografía	Algebra	Matemática Discreta I	Algebra	90

MATERIA

RETICULOS EN ESPACIOS EUCLIDEOS

Introducción. Un *retículo* (o *lattice*) en R^n es el conjunto de combinaciones lineales enteras de n vectores linealmente independientes de R^n. Con la operación de suma de vectores, un lattice es también un grupo abeliano.

Entre los problemas más importantes relacionados con lattices están: empaquetamiento de esferas (*packing problem*); cubrimiento con esferas (*covering problem*); número de contacto (*kissing number*); retículos cuantizadores (*lattice quantizer problem*); todos con muchísimas aplicaciones.

Si bien en el curso se verán los lattices más bien desde un punto de vista geométrico, en la actualidad, muchos de estos problemas son abordados con algoritmos y métodos computacionales. Por ejemplo, la reciente solución al famoso problema de empaquetamiento de esferas en dimensión 3 ---*Conjetura de Kepler*--- involucra una gran cantidad de algoritmos y cuentas hechas con la computadora (las cuales llevarán años para su completa verificación).

Objetivos. Se pretende dar un panorama general de los lattices en R^n y de los problemas más importantes relacionados con ellos, y que los alumnos adquieran herramientas como para entender y, con un poco de audacia, atacar algunos de estos problemas.

PROGRAMA

Contenidos Mínimos

1. Motivación. Planteo de los problemas más importantes relacionados con lattices, mencionados en la Introducción: problemas de empaquetamientos; de cubrimientos, de kissing numbers y de cuantizadores.

Expte. 03-05-00814

ANEXO A RES. HCD N° 29/2005

2. Lattices. Generalidades. Ejemplos en dimensiones bajas. Celdas de Dirichlet-Voronoi. Celda de Voronoi de un lattice. Triangulación de Delone. Vectores de Voronoi. Bases, superbases y superbases obtusas. Matriz, determinante y discriminante de un lattice. Parametrizaciones. Forma y algoritmo de Minkowski y de Korkine-Zolotareff. Vonormas y conormas de lattices. Conormas en dimensiones bajas. Algoritmos de reducción. Clases de Bravais. Simetría de algunas fórmulas usando conormas.

Formas cuadráticas definidas positivas. Relación con lattices. Funciones theta. Algunos teoremas básicos de la teoría de lattices (suma directa, cancelación).

3. Algunos lattices importantes. Lattices enteros. Dual de un lattice. Lattices unimodulares. Lattices de Raíces. El método de pegado de Kneser. El lattice cúbico Z^n. Los lattices *An* y An^*. Los lattices *Dn*, Dn^+ y Dn^*. Los lattices *E6*, *E7* y *E8*. El lattice de Leech.

4. Relación entre lattices y códigos. Códigos. Códigos binarios y lineales. De códigos a lattices y de lattices a códigos. Códigos autoduales y lattices unimodulares pares. El problema de los sombreros rojos y azules. Códigos de Hamming. El lattice *E8*.

5. Isospectralidad de lattices. Fórmula de Poisson. Ejemplo de Milnor (y Witt) en dimensión 16, de Kneser en dimensión 12. Ejemplos de Conway-Sloane en dimensión 6 y 5. Ejemplos de Schiemann y de Conway-Sloane en dimensión 4. Dimensión 3: Teorema de Schiemann con métodos computacionales.

6. Soluciones a algunos problemas. Mejor lattice packing y lattice covering en dimensiones muy bajas.

Algunos temas posibles para agregar:

7. Poliedros. Sólidos platónicos y arquimedianos. Sólidos que llenan el espacio, parallelohedra. Embaldozamientos del plano (*tilings*).

8. Platycosms. Descripción, parametrización y estudio de las variedades planas en dimensión 3, o *platycosms*. Isospectralidad de platycosms.

9. Lattices laminados. Mejores empaquetamientos con lattices conocidos hasta el momento.

10. Lattice quantizers. Solución al problema del óptimo lattice quantizer en dimensión 3 por Barnes y Sloane.

Bibliografia.

[CS] *Sphere Packings, Lattices and Groups*, por J. H. Conway y N. J. A. Sloane. Springer-Verlag, New York, 1999 (3rd Edition).

[E] *Lattices and Codes* (A course partially based on Lectures by F. Hirzebruch), por W. Ebeling. Vieweg, 1994.

[C] *The sensual (quadratic) form*, por J. H. Conway. The Carus Math. Monographs, nro. 26, 1997.

[O] *Introduction to Quadratic Forms*, por O. T. O'Meara. Springer-Verlag, 1973.

Universidad Nacional de Córdoba
FACULTAD DE MATEMATICA ASTRONOMÍA Y FÍSICA

Expte. 03-05-00814

ANEXO A RES. HCD N° 29/2005

MATERIA

INTRODUCCIÓN A CÓDIGOS Y CRIPTOGRAFÍA

PROGRAMA

1.1 Códigos autocorrectores, generalidades. Códigos lineales. Matriz de chequeo de paridad.

1.2 Códigos perfectos. Cotas. Código de Hamming, Golay, extendido, Reed-Müller. Decodificación rápida.

1.3 Cuerpos finitos, morfismos, polinomios minimales, polinomios irreducibles.

1.4 Códigos cíclicos, duales. Codificación y decodificación. Códigos BCH, de Reed-Solomon, decodificación. Algoritmo de Berlekamp-Massey. Decodificación de códigos de Reed-Müller y de códigos de convolución. Aplicación a "compact discs."

1.5 Criptografía. Orígenes históricos. Factorización. Primalidad.

1.6 Congruencias. Función phi de Euler. Logaritmos discretos.

1.7 Criptosistemas de clave pública. Autentificación.

1.8 Tests de primalidad.

1.9 Algoritmos de Factoreo. Cribas.

1.10 Residuos Cuadráticos. Reciprocidad. Aplicaciones a códigos y criptografía.

Bibliografía:

1. D. Hoffman et al, *Coding Theory. The Essentials*, Marcel Dekker.
2. S. Roman, *Information theory and Coding,* Springer Verlag.
3. R. Mollin, *An introduction to cryptography,* Chapman-Hall Inc.
4. W. Ebeling, *Lattices and codes,* Vieweg Verlag.
5. Hill R., *A first course on coding theory.* Clarendon Press, Oxford.

Dr. MIGUEL A. PE
Secretario

Dr. GIORGIO M. CARANTI
Decano