pecials per realitzar a l'estand que la UPC tenia en el Saló Estudia. A més, la Facultat va acollir els dies 12 i 13 d'abril el Fòrum de les Escoles que organitza la UPC per acostar les escoles i facultats als estudiants de secundària.

El 4t Premi Poincaré, que la FME atorga al millor treball de recerca de secundària en matemàtiques i/o estadística, va ser per a «Nombres primers: anàlisi de la complexitat» d'Oriol Lozano d'Aula Escola Europea. El lliurament del premi, juntament amb l'atorgament d'altres premis i mencions, va tenir lloc el dia 15 de maig amb l'assistència del vicerector de recerca de la UPC, Xavier Gil.

Durant molts dijous al matí dels mesos de març i abril, hem tingut a la Facultat grups d'estudiants de batxillerat realitzant activitats a l'entorn de l'estadística.

Els estudiants de la FME organitzen moltes activitats, però segurament entre les que tenen més projecció cal esmentar la representació a càrrec del grup de teatre, els dies 7 i 8 de març, i el concert que es va celebrar el 9 de maig amb la participació de la coral de la FME.

Per contactar amb el món laboral, el dia 25 de maig es va celebrar el 6è Fòrum de la FME amb molt bona assistència.

Algunes de les conferències d'aquest segon quadrimestre han estat: «La música de los números primos», de Marcus de Sautoy el dia 27 de març, o «¿Se puede oir la forma de una red?», de Joachim von Below, ja el mes de maig. Finalment, el dia 20 de juny es va celebrar la cloenda del curs Euler amb la conferència «Euler: idees seminals en combinatòria», a càrrec del professor Josep M. Brunat. En l'acte de cloenda van intervenir la vicerectora de planificació i programació d'infraestructures de la UPC, Teresa Rovira, i el cònsol de Suïssa a Barcelona.

La Facultat de Matemàtiques i Estadística dedicarà el curs 2007–2008 a Bernhard Riemann. Trobareu la informació al nostre web http://www-fme.upc.es.

Margarida Mitjana
Vicedegana de relacions FME

Activitats amb ajut de la SCM

EUROCRYPT 2007

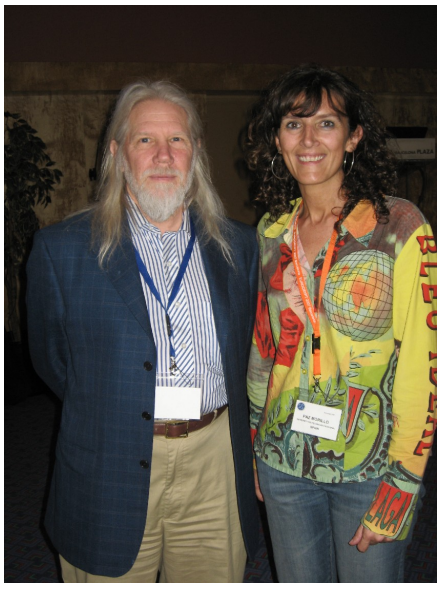
Barcelona, del 20 al 23 de maig de 2007

Del 20 al 23 de maig es va celebrar a Barcelona el congrés «Advances in Cryptology-Eurocrypt 2007, International Conference on the Theory and Application of Cryptologic Techniques». Aquest congrés va ser organitzat pel Grup de Matemàtica Aplicada a la Criptografia del Departament de Matemàtica Aplicada IV de la UPC i per en Javier López del Departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga. Eurocrypt 2007 és la vint-i-sisena edició d'aquest congrés internacional que se celebra des de l'any 1982 i que constitueix el màxim fòrum de trobada i intercanvi d'idees entre els principals investigadors internacionals, d'empreses privades i institucions públiques, que treballen o tenen interès en les àrees de criptologia i seguretat, tant en l'àmbit teòric com en el de les seves aplicacions, implementació i utilització.

Els articles presentats en aquest congrés han de ser articles originals sobre qualsevol dels aspectes tècnics de la criptologia i la seguretat de la informació. Aquest congrés és fortament competitiu, cosa que queda patent per la xifra de trenta-tres articles escollits d'entre els cent setanta-tres presentats pels millors investigadors i centres d'investigació de tot el món. Aquesta qualitat tan alta en els treballs escollits fa que sigui una cita d'obligada assistència per a la comunitat criptogràfica internacional i que concentri els millors científics de l'àrea, procedents fonamentalment de matemàtiques, d'informàtica i d'enginyeria de telecomunicació. El procés de selecció dels articles va ser anònim, es va assignar cada article a almenys tres dels vint-i-quatre membres del comitè de programa i assistits per cent trenta-dos *referees* externs. Tot aquest delicat treball va ser coordinat pel

cap del comitè de programa, en Moni Naor del Weizmann Institute of Science d'Israel. Cal destacar que només hi ha un article acceptat d'un grup d'investigació de tot el sud d'Europa, el del Grup de Matemàtica Aplicada a la Criptografia de la UPC. Els articles seleccionats van ser publicats per l'editorial Springer-Verlag en el volum 4515 de la seva prestigiosa sèrie Lecture Notes in Computer Science.

La gestació de l'organització del congrés va començar abans de l'estiu de l'any 2004. Durant gairebé un any vam estar preparant la candidatura amb la inestimable ajuda del Barcelona Convention Bureau. El maig de 2005 a la ciutat d'Aarhus (Dinamarca) es va escollir la nostra entre tres candidatures presentades. Des d'aquesta data fins al maig de 2007 hem estat treballant en l'organització del congrés Mónica Breitman, Paz Morillo, Jorge Villar, Javier López, Germán Sáez (els dos darrers com a general *co-chairs*) i la resta de membres del Grup de Matemàtica Aplicada a la Criptografia de la UPC, especialment els nostres doctorands i exdoctorands. Cal remarcar també el treball de la Mònica Garizuain, administradora del Departament de Matemàtica Aplicada IV de la UPC.



Whitfield Diffie i Paz Morillo

El pressupost total del congrés ha estat d'uns cent vuitanta mil euros sense incloure en aquesta quantitat l'allotjament dels assistents ni l'excursió oficial del congrés. Es van obtenir ajuts dels centres oficials i empreses següents: Ministerio de Educación y Ciencia, AGAUR de la Generalitat de Catalunya, Centro Criptológico Nacional (Centro Nacional de Inteligencia), CatCert, Applus, Safelayer, UPC, CRM i Departament de Matemàtica Aplicada IV de la UPC. També vam comptar amb la col·laboració de la Secció Espanyola de l'IEEE, de la Revista SIC i de l'Ajuntament de Barcelona. Estem molt agraïts a la Societat Catalana de Matemàtiques de l'IEC que va becar uns estudiants per assistir al congrés. Així mateix, la Real Sociedad Española de Matemáticas va becar també l'assistència d'estudiants. A part dels regals típics que es fan en els congressos (en el nostre cas: bossa, llibreta i bolígraf amb inscripció, tassa de ceràmica amb el nom del congrés i un escalfador de tasses USB), una sèrie d'empreses catalanes van regalar productes per fer un lot que va sorprendre gratament a tots els assistents. Les empreses que van donar els productes van ser Galetes Birba, licor de crema catalana Melody Original, carquinyolis Vicens i cerveses Damm. A més també vam afegir a aquest lot un regal solidari d'Intermón-Oxfam.

Els resultats científics del congrés han estat molt satisfactoris, principalment per la qualitat dels articles presentats i per les sessions convidades. El nombre total d'assistents que ens vam congregar a l'Hotel Catalonia Plaza, seu del congrés, va ser de tres-cents vuitanta, entre investigadors d'universitats, d'empreses del món de les telecomunicacions (operadors i subministradors de serveis de telecomunicacions, empreses d'equipaments i serveis, empreses específiques de productes criptogràfics), de laboratoris d'I+D, d'organismes oficials i dels que són dependents de ministeris de defensa de diversos països. El ressò en els mitjans de comunicació també va ser destacable: reportatge a l'informatiu *Hola Barcelona* de BTV del 21 de maig, reportatge al *Telenotícies migdia* de TV3 del 24 de maig, entrevistes a COM Ràdio i Ràdio Barcelona (SER) el 23 de maig, a Ràdio 4 (RNE) el 25 de maig i el 31 de maig, notícia a *Catalunya Informació* el 24 de maig, article a *El Periódico* de Catalunya del 4 de juny, també articles als diaris *Diario de Córdoba*, *La Opinión* de Màlaga, *El Sur*, i repercussió a catorze pàgines web (principalment les versions digitals de diaris i revistes, entre d'altres la versió digital de *La Vanguardia*). La importància i la qualitat del congrés va ser entesa també pel conseller d'Innovació, Universitats i Empreses de

la Generalitat de Catalunya, Josep Huguet, i per la comissionada d'universitats, Blanca Palmada, que van donar la benvinguda i van oferir un còctel en el Palau de Pedralbes. La importància del congrés també va fer que se celebressin altres reunions relacionades: «Conference on Cryptology and Digital Content Security» (CDCSEC) i el «Workshop on Mathematics of Cryptology (Recent Trends in Secure Computation)», tots dos organitzats pel CRM; «ECRYPT Hash Workshop 2007» organitzat per la xarxa ECRYPT; «International Conference on Information Theoretic Security» (ICITS), organitzat per la Universitat de Màlaga i la Universitat Rey Juan Carlos.

Paz Morillo i Germán Sáez
UPC

NEEDS 2007 School and Workshop

Ametlla de Mar, del 15 al 24 de juny de 2007

L'Ametlla de Mar va acollir del 15 al 24 de juny la 17a edició del congrés «Nonlinear Evolution Equations and Dynamical Systems (NEEDS)» amb la participació de més de centsetanta investigadors en matemàtiques i física de més de trenta països. Els congressos NEEDS tenen una llarga tradició dins de l'àrea de la física matemàtica i, en especial, de l'estudi de sistemes integrables en sistemes dinàmics. A part de les qüestions estrictament científiques, els congressos s'han distingit en les seves edicions per la seva contribució al diàleg entre els dos blocs durant la guerra freda i, de fet, el congrés comptà amb la presència d'un dels seus impulsors, Francesco Calogero, que rebé el Premi Nobel de la Pau en nom de l'organització Pugwash Conferences on Science and World Affairs. Com a novetat d'aquesta edició, el congrés ha estat precedit d'una escola.

El congrés NEEDS 2007 forma part d'una sèrie de conferències internacionals iniciada l'any 1980 i de la qual fou la 17a edició. La temàtica de les conferències NEEDS és a mig camí entre la física i les matemàtiques, sense oblidar la interacció amb la modelització de processos físics, químics i biològics. Juntament amb les tradicionals aplicacions a la física, han aparegut en els darrers temps nous camps d'aplicació en la biologia i en la química en els quals el coneixement adquirit en aquest tipus d'equacions pot ser essencial en treballs interdisciplinars.

Ja des dels inicis, la sèrie de conferències NEEDS va concentrar la seva atenció sobre el camp dels sistemes no lineals, on s'inclouen la majoria de models matemàtics de la naturalesa. Des d'aleshores en aquest camp d'estudi s'han anat configurant dues línies de recerca, la dels sistemes integrables (aquells que en teoria són solubles explícitament i, per tant, hom en pot tenir un coneixement més detallat) i la dels que no ho són, que constitueixen la majoria dels models no lineals i on s'inclouen els sistemes caòtics. Tanmateix aquestes dues línies no són compartiments estancs sinó que molts dels resultats per a sistemes caòtics s'obtenen a partir de considerar pertorbacions de sistemes integrables.

Precisament aquesta voluntat de traspassar les fronteres que sovint s'estableix entre diferents camps de la ciència ha motivat que, en aquesta edició, el congrés anés precedit d'una escola avançada. Els cursos han estat: An introduction to pattern formation per Alastair Rucklidge, de la Universitat de Leeds, Properties of low dimensional systems in the large per Carles Simó, de la Universitat de Barcelona, The transition from regular to irregular motion explained as a travel on Riemann Surfaces per Paolo M. Santini, de la Universitat de Roma, i Synchronization and Networks per Steven H. Strogatz, de la Universitat Cornell. Gairebé un centenar d'investigadors varen assistir a aquesta escola, la qual considerem un dels grans èxits del NEEDS 2007.

Essent fidel a la seva tradició de transversalitat, en aquesta edició s'ha intentat afavorir els intercanvis entre els científics de diferents àrees geogràfiques i crear un entorn adient per a la comunicació entre investigadors en totes les etapes de la seva carrera científica. En aquesta edició es presentaren més d'un centenar de contribucions entre comunicacions i pòsters que s'editaran en un volum d'actes. El congrés dedicà una sessió a la memòria de Martin Kruskal, històric participant del congrés i recentment desaparegut. Finalment, també es realitzà una excursió al delta de l'Ebre.

El congrés i l'escola han estat finançats per diverses agències catalanes i estatals, entre elles el Fons de Promoció d'Activitats de la Societat Catalana de Matematiques, cosa que ha permès la participació de participants joves i de països en vies de desenvolupament, com ha estat sempre en l'esperit de les trobades NEEDS.

Per a més informació, vegeu el web del congrés http://www.needs-conferences.net/2007

Joaquim Puig i Sadurní
Comitè organitzador, UPC

Participants al NEEDS 2007

Activitats de la SCM

Quarta Jornada d'Ensenyament

Aquest curs 2007–2008 inaugurem nous currículums a primària i a l'ESO fruit de la implantació inicial de la LOE. Al mateix temps, les universitats catalanes estan immerses en la planificació dels nous títols de graduats, màsters i doctorats seguint les directrius de l'espai europeu d'educació superior, que es concreten en la LOU.

Entrega de la documentació als participants

Tot aquest procés de renovació curricular torna a plantejar, des de diferents perspectives, responsabilitats i objectius, el problema de decidir quines matemàtiques s'han d'estudiar a les diferents etapes educatives, quina importància se li ha de dedicar en relació en les altres matèries i quin tipus d'innovació aportarà el nou llenguatge de les competències, ja sigui pel que fa a la manera de concebre les matemàtiques i la seva raó de ser, com la manera d'organitzar-ne l'ensenyament i l'aprenentatge.

El dissabte 29 de setembre gairebé dos-cents professors de primària, secundària i universitat van participar a la Quarta Jornada d'Ensenyament organitzada, com en les edicions anteriors, per la SCM i la FEEMCAT, a les quals s'afegeix ara la Societat Balear de Matemàtiques Xeix. L'objectiu de la jornada va ser debatre entorn del problema del currículum de matemàtiques i la manera com s'elaboren els diferents plans d'estudis, des d'infantil fins a la universitat.

Al matí es van celebrar dues taules rodones, la primera centrada en l'elaboració del currículum i la segona en els definidors curriculars que influeixen en el que s'ensenya més enllà dels programes. Hi van participar dos re-