

El jurat del premi, integrat pels professors

Núria Vila (Presidenta, UB), Maria Alberich (UPC), Xavier Bardina (UAB), Sílvia Cuadrado (UAB) i Jordi Marzo (UB),

ha decidit atorgar el Premi al treball de grau:

Self-similar profiles in Analysis of Fluids. A 1D model and the compressible Euler equations,

presentat pel senyor **Gonzalo Cao Labora** i dirigit pels professors Javier Gómez-Serrano (Princeton U.) i Juan Carlos Felipe Navarro (UPC).

Així mateix, el jurat ha decidit atorgar la menció ex aequo als treballs de grau:

Criptografia basada en isogènies,

presentat pel senyor **Enric Florit Zacarías** i dirigit pels professors Xavier Guitart (UB), Santiago Seguí (UB) i Ramsès Fernández (UB)

i

Mesures de Zygmund,

presentat per la senyora **Laia Weisz Font** i dirigit pel professor Juan J. Donaire Benito (UAB).

El senyor Gonzalo Cao realitza al seu treball dues contribucions noves a la dinàmica de fluids. La primera part del treball consisteix en una demostració amb tècniques diferents a la ja existent, de l'existència de singularitats per al model d'Okamoto-Sakajo-Wunchs per a valors petits de la constant al terme de convexió. A la segona part del treball realitza una nova demostració de l'existència de perfils autosimilars per a les equacions d'Euler isentròpiques compressibles que inclou rangs més amplis de la constant adiabàtica. El jurat ha valorat molt positivament la dificultat dels continguts així com la maduresa mostrada a la redacció del treball en tractar temes profunds i molt actuals com queda reflectit a l'extensa bibliografia.

El treball del senyor Enric Florit està dedicat a l'estudi del protocol SIDH/SIKE, basat en el problema de trobar isogènies entre dues corbes el·líptiques, un dels candidats al procés d'estandardització de criptografia postquàntica de l'institut NIST. El treball realitza un estudi acurat de les eines que necessita sobre corbes el·líptiques i isogènies. Així mateix presenta els principis de la criptografia en l'intercanvi de claus tipus Diffie-hellman basat en isogènies entre corbes el·líptiques supersingulars sobre cossos finits. Estudia la tria de paràmetres i les optimitzacions necessàries per fer eficient el càlcul d'isogènies. L'autor implementa una sèrie de rutines en Sage per tal de definir el protocol, testejar-lo i analitzar-ne la seguretat, estudiant dos dels atacs proposats. El jurat ha valorat molt positivament la tasca realitzada tan teòrica com pràctica en un tema molt actual amb possibles continuacions que s'expliciten al final de la memòria.

El treball de la senyora Laia Weisz és un molt bon treball formatiu i de recerca on l'autora ha fet desenvolupaments propis rellevants en la solució d'un problema obert no trivial. L'objectiu d'aquest treball és l'estudi de les mesures de Zygmund, més concretament, la descripció dels conjunts que poden ser suport d'aquest tipus de mesures que és un problema obert. En una primera part es demostren, introduint algunes millores, dos dels resultats més importants en l'estudi de les mesures de Zygmund: el teorema de Kaufman i el teorema de Makarov. En la segona part, més de recerca, l'autora introdueix el concepte de capacitat Zygmund. Al treball es conjectura que la positivitat d'aquesta capacitat caracteritza el fet de suportar mesures de Zygmund. L'autora demostra una implicació d'aquesta conjectura, desenvolupa alguns exemples interessants que la recolzen i descriu un intent de demostració de l'altra implicació que no aconsegueix completar, tot i que la prova amb algunes restriccions. El treball acaba amb una interessant descripció de futures línies de recerca.

A part dels treballs guardonats, el jurat del premi vol fer constar la qualitat remarcable de tots els treballs presentats al concurs, tant pel que fa al contingut, com a la presentació de resultats i redacció.