Butlletí de la Societat Catalana de Matemàtiques
Vol. 33, núm. 2, 2018. Pàg. 173–174

English summaries

Carles Barril, Sílvia Cuadrado and Jordi Ripoll

Mathematical models in population dynamics

Population dynamics studies the evolution of size and composition of populations. In this article we present a compilation of the main mathematical models describing the dynamics of biological populations. We start with a historical introduction to the subject showing different problems in ecology, demography and epidemiology, as well as the tools and mathematical techniques used. Then we describe a new formulation in terms of delay equations that establishes a thorough general framework for the mathematical modeling of population dynamics.

Keywords: mathematical biology, structured populations, delay equations, partial differential equations.

MSC2010 Subject Classification: 92D25, 35Q92, 47N20.

Agustí Reventós

Gaspard Monge

This article seeks to pay tribute, 200 years after his death, to Monge's work in the field of differential geometry of curves and surfaces. After a brief reminder of his biography, we focus on his work on evolutes of curves in space and especially on the origin of the lines of curvature, in an article dedicated to transport of land. The Feuille XV of his famous *Feuilles d'analyse* is analyzed in detail and a brief comment is made on the rest of his works in differential geometry. We attach a note, by Josep Lluís Solé, about one of Monge's friends and his biographer: François Arago.

Keywords: Monge, curves, surfaces, evolutes, lines of curvature.

MSC2010 Subject Classification: 53A04, 53A05, 01A50.

Narcís Sayols and Sebastià Xambó

Error-correcting codes and post-quantum cryptography

The forty-year old McEliece public-key crypto-system is revisited with the help of recently developed resources: an improved Peterson-Gorenstein-Zierler decoder for alternant error-correcting codes; a symbolic computation system and a package of functional utilities for the computations involved in defining, coding and decoding error-correcting codes, fully programmed in Python; and a web page with free-access to the materials generated by the project. The main interest of the McEliece system stems from it being a serious candidate for a post-quantum cryptography standard.

Keywords: post-quantum cryptography, alternant codes, symbolic computation, free software.

MSC2010 Subject Classification: 11T71, 68-04, 68W30, 94A60.
