Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016. Pàg. 91–93

English summaries

Vladimir Koltchinskii, Richard Nickl, Sara van de Geer and Jon A. Wellner

The mathematical work of Evarist Giné

In this article we give an overview of Evarist Giné's contributions to the modern probability theory and mathematical statistics in an infinite-dimensional setting. The sections correspond to the areas in which he had the most relevant participation: probability in Banach spaces, empirical processes, the bootstrap, U-statistics and U-processes, and mathematical statistics. Emphasis is put on the profound impact his work has had on the present probability theory, mathematical statistics and more recently machine learning. It also contains a short biography and a list of his publications. It has been written on the occasion of his death.

Keywords: probability in Banach spaces, central limit theorem, empirical processes, bootstrap, U-statistics, density estimation.

MSC2010 Subject Classification: 60B12, 60G15, 60E15, 62F40, 62G07.

Elitza Maneva

The mathematics behind cryptocurrencies

In the context of a presentation on the basics of cryptocurrencies like Bitcoin, we introduce three topics central to modern cryptography: digital signatures, hash functions and zero-knowledge proofs. The mathematical problems that arise here can be used as examples by teachers and professors to encourage the study of modular arithmetic, probability theory, graph theory and computational complexity.

Keywords: cryptography, cryptocurrencies, RSA, elliptic curves, hash, probability, graphs, computational complexity, modular arithmetic.

MSC2010 Subject Classification: 68-02, 68Q15, 68Q17, 68Q05.

M. Rosa Massa-Esteve

New results and procedures in the mathematics of the 17th century: maxima's calculations in Pietro Mengoli (1626/1627–1686)

The publication in 1591 of *In artem analyticen isagoge* by François Viète (1540–1603) constituted an important step forward in the development of a symbolic language. As Viète's work came to prominence at the beginning of the 17th century, other authors, like Pietro Mengoli (1626/1627–1686), also began to consider the benefit of algebraic procedures for solving all kind of problems. Mengoli followed the algebraic research of Viète in order to construct geometry of species, *Geometriae Speciosae Elementa* (1659), which allowed him to use algebra in geometry in complementary ways to solve quadrature problems. Mengoli, like Viète, considered his algebra as a technique in which symbols are used to represent not just numbers but also values of any abstract magnitudes. He dealt with species, forms, triangular tables, quasi ratios and logarithmic ratios. However, the most innovative aspect of his work was his use of letters to directly study geometric figures via their algebraic expressions. In this article, I analyze the algebraic construction of these geometric figures, the use of triangular tables and the singular proof developed by Mengoli for finding the maxima of these geometric figures before the development of Newton's and Leibniz's calculus. This analysis illustrates Mengoli's mathematical ideas on the specific role of symbolic language as a means of expression and as an analytic tool.

Keywords: geometric figures, triangular tables, Pietro Mengoli, mathematics of the 17th century, maxima, logarithms, algebraic expression.

MSC2010 Subject Classification: 01A45, 3303, 2603.

Günter M. Ziegler

Cannons at Sparrows

The story told here starts with an innocuous little geometry problem, posed in a September 2006 blog entry by R. Nandakumar, an engineer from Calcutta, India: This little problem is a «sparrow», tantalizing, not as easy as one could perhaps expect, and Recreational Mathematics: of no practical use.

I will sketch, however, how this little problem connects to very serious mathematics: For the modelling of this problem we employ insights from a key area of Applied Mathematics, the Theory of Optimal Transportation. This will set up the stage for application of a major tool from Very Pure Mathematics, known as Equivariant Obstruction Theory. This is a «cannon», and we'll have some fun firing it at the sparrow.

On the way to a solution, combinatorial properties of a very classical geometric object, the permutahedron, turn out to be essential. These will, at the end of the story, lead us back to India, with some time travel that takes us one hundred years into the past: For the last step in our (partial) solution of the sparrows problem we need a simple property of the numbers in Pascal's triangle, which was first observed by Balak Ram, in Madras 1909.

But even if the existence problem is solved, the little geometry problem is not: If the solution exists, how do you find one? This problem will be left to you. Instead, I will comment on the strained relationship between cannons and sparrows, and to this avail quote a poem by Hans Magnus Enzensberger.

Keywords: partitions of a polygon, configuration spaces, obstruction theory, binomial coefficients, pure and applied mathematics.

MSC2010 Subject Classification: 00A08, 52A38, 55P91, 55R80.