Jahresber Dtsch Math-Ver (2012) 114:57–58
DOI 10.1365/s13291-012-0043-1

PREFACE

Preface Issue 2-2012

Hans-Christoph Grunau

Distinguishing between pure and applied mathematics has, in my opinion, never been particularly helpful. The current issue of the "Jahresbericht der DMV", focussing on topics from Algebra, shows once more that such a distinction, if possible at all, would be most difficult.

"Elliptic curves are beautiful mathematical objects that again and again appear in the most surprising places" is the first sentence of the survey article on "The Magic of Elliptic Curves and Public-Key Cryptography" by Florian Heß, Manfred Lochter, Andreas Stein, and Sandra Stein. Public-key cryptography is based on "one-way functions", of which the inverse is hard to compute. The discrete logarithm problem for the abelian group of points of an elliptic curve over a finite field appears to be in general computationally hard to solve and provides an efficient example of such a one-way function. For this reason elliptic curves have become ubiquitous in modern public-key cryptography. Since one of the authors, Manfred Lochter, is working for the German Federal Office for Information Security and so very much involved in the development of cryptographic standards, explicit technical solutions and their security, the article also gives in some detail real world applications.

"Mathematicians love to count things." This is the first phrase of Michael Vaughan-Lee's survey article on "Graham Higman's PORC conjecture". It is the number of groups of order p^n which has to be counted here, and it is known that this number can be estimated and is approximately $p^{\frac{2}{27}n^3}$. Higman's PORC conjecture states that for fixed n, these numbers do not only enjoy polynomial bounds but that it should be possible to calculate them by means of a finite set of polynomials in p. "PORC" stands for **P**olynomial **O**n **R**esidue **C**lasses. It is known since 2005 that the

H.-Ch. Grunau (✉)
Institut für Analysis und Numerik, Fakultät für Mathematik, Otto-von-Guericke-Universität,
Postfach 4120, 39016 Magdeburg, Deutschland
e-mail: hans-christoph.grunau@ovgu.de

conjecture holds true for $n \leq 7$. In a very comprehensible way, Michael Vaughan-Lee gives an introduction to this topic, provides some historical background, and sketches Higman's proof of a special case of the PORC conjecture. In the second part of this survey article, however, the author summarises a recent work by Marcus du Sautoy and himself on properties of a specific family of groups, which does not yet disprove the PORC conjecture, but which does obstruct the envisaged strategy of proof, and so gives some evidence that the conjecture might indeed be false.

As usual we try to present book reviews focussing on subjects different from those of the survey articles. For the current issue this means that one finds a review of a "synopsis" of numerical methods for nonlinear elliptic differential equations as well as of a book on ergodic theory and its applications in number theory.