

PREFACE

During five days from 7 to 11 May 2007, the mathematics symposium SAGA devoted to the applications of algebraic geometry, was held in Tahiti in the honor of Gilles Lachaud, Director of the *Institut de Mathématiques de Luminy*, bringing together researchers from about fifteen countries of Europe, Asia, America and Oceania. It made it possible to give a progress report on the current state of knowledge and research in the field of algebraic geometry and its applications to information theory.

The first conference of mathematics ever held in French Polynesia was organized jointly by the *Université de la Polynésie Française (UPF)* and the *Institut de Mathématiques de Luminy (IML)*. It is the result of a partnership developed between the team ATI of Luminy and the young research team GAATI, of the *Université de la Polynésie Française*. Let me thank the members of the team GAATI who by their scientific work, their cohesion and especially their good results, allowed the behaviour of this conference.

Among the fifty-nine participants who accept to come to Tahiti were two academicians, Mr Christophe Soulé of the *Académie des Sciences de Paris*, and Mr Igor Shparlinsky of the *Australian Academy of Science* and many of the best specialists of the domain.

Special thanks are due to all the authors who submitted papers and to the conference participants from all over the world. Among them, there were seven invited speakers : Jean-Marc Couveignes, (*Institut de Mathématiques de Toulouse, Université de Toulouse-Le Mirail, France and CNRS*), Gerhard Frey, (*Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Germany*), Marc Girault, (*France Télécom R&D*), Everett Howe, (*IDA Center for Communication Research, USA*), Gilles Lachaud, (*Institut de Mathématiques de Luminy*), Christophe Soulé (*IHES, Bures-sur-Yvette, France*), and Felipe Voloch, (*University of Texas, Austin, USA*)

The timetable of the week devoted to the conference was distributed over four working days: Monday, Tuesday, Thursday and Friday. Wednesday was free and reserved to the visit of Mooréa. As part of the side events

of the scientific meeting, three conferences for the general public were given by Pierre Bathélemy, (*Institut de Mathématiques de Luminy*), Marc Girault, (*France Télécom R&D*), Robert Rolland, (*Institut de Mathématiques de Luminy*). These three conferences aimed at informing the public on the current use of mathematical results in everyday life (smart cards, encoding, security) and at communicating with local engineers and technicians responsible for networks.

The session was opened by Louise Peltzer, president of the *Université de la Polynésie Française*, in the presence of local ministry officials in charge of research, at the Sheraton hotel of Papeete. Thirty five conferences showed the vitality, dynamism and richness of research in algebraic geometry and related topics. Conferences of two types were held: one-hour conferences suggested by the guests made it possible to present an survey of the current state of knowledge in the various fields touched upon in this symposium, and half-hour talks were reserved for the presentations of recent findings by lecturers. Out of the thirty-five conferences, twenty-seven were submitted and selected for publication in this volume of the Proceedings of SAGA in *Series on Number Theory and its Applications*, published by World Scientific.

The topics announced at the time of the call for papers were related to arithmetic and algebraic geometry over finite fields, combinatorial geometry over finite fields, algorithms over finite fields, error correcting codes, cryptography, boolean functions and sequences.

In this book of proceedings, many very interesting theoretical and applied new results, and surveys are presented. For example, one can find new results on a conjecture of J.-P. Serre, which answer a question setted in a letter from J.-P. Serre also published in this book. New results in the domain of applications of the discrete logarithm problem and elliptic curves to cryptography, including discrete logarithm computation also appear in these proceedings. Other domains are covered as towers of function fields, new designs of classes of boolean cryptographic functions ... Some of the papers are surveys giving an overview of the state of the art in these related domains of research.

The working sessions were a powerful channel for the presentation of research in a field where popularization is not over-abundant, and they strengthened the links between various research centers with an interest in those topics. This symposium could not have been born without the effective support of the french national *Ministère de l'Éducation Nationale*, the

Ministère de l'Éducation, de l'Enseignement Supérieur et de la Recherche de la Polynésie Française, the Fonds français Économique, Social et Culturel pour le Pacifique, the Institut de Mathématiques de Luminy, and the Université de la Polynésie Française.

The participants appreciated the Polynesian welcome which touched them deeply; a significant number of them extended their stay in French Polynesia, visiting the islands and discovering more about this country.

We would like to thank the sponsors, the corporate outfits which trustingly gave us support, namely OSB (*Océanienne de Services Bancaires*), ISS (Isis, Sigma, Spin), MANA (the Polynesian Internet provider). They showed us the interest of Polynesian companies in contacts with the world of research. Information concerning the conference was accessible on the site of the University of French Polynesia <http://www.upf.pf> as well as on that of the Mathematics Institute of Luminy: <http://iml.univ-mrs.fr/ati/saga2007/welcome.html>

Our thanks go to all the personnel of the *Institut de Mathématiques de Luminy*, of the *Université de la Polynésie Française*, the Sheraton Hotel in Tahiti and the various companies which contributed to the smooth running of the conference.

We would like to take this opportunity to thank the Program Committee members and the experts for their help in producing the conferences program. We also wish to thank Jean Chaumine, James Hirshfeld, Robert Rolland for their involvement in the editorial process. Let us thank again all the members of the team GAATI for their deep implication in the organization of this symposium and particularly Jean Chaumine who was the main coordinator.

J.-M. Goursaud