ESF Exploratory workshop on

Arithmetic, Geometry and Coding Theory

CIRM
12-24 May 2003, Marseilles, France

Convened by

Yves AUBRY, Gilles LACHAUD, Michael TSFASMAN
IML - CNRS
Marseille-Luminy, FRANCE

Scientific Report

Executive summary

The relation of Arithmetic to Information Theory is one of the most fruitful among the new interfaces in contemporary mathematics.

Arithmetic includes Number Theory as well as Algebraic Geometry from an arithmetic viewpoint, and especially Geometry over Finite Fields, in particular the study of solutions of a system of algebraic equations in several variables with coefficients in a finite field.

This ESF meeting gathered two events : an instructional spring school, followed by a research workshop. Both of them were concerned with two interrelated major topics.

The first one belongs to fundamental mathematics, and involves two topics : on one hand, Number Theory (especially, class numbers, zeta functions and divisors of algebraic number fields) and, on the other hand, Algebraic Geometry over finite fields.

These two topics are unified under the theory of global fields and the synergy between them acts like a seesaw : for instance, any statement in the theory of algebraic curves over finite fields, that is of the theory of function fields in one variable, has its counterpart in the theory of algebraic number fields, and conversely.

Of course, the Riemann Hypothesis, which is the heart of the theory, is proved in the function field case. This is equivalent to the Weil bound for the number of points of a curve over a finite field. The meeting offered the opportunity to get more information on the maximal number of points of a curve of given genus over a field with q elements. The Weil bound has been extended to varieties of higher dimensions (Deligne theorem) and can be improved in many specific cases. Hermitian varieties are maximal and caps on these varieties have remarkable combinatorial features

The Riemann Hypothesis remain a conjecture in the number field case. But the function field case provides a fruitful source of speculations for the number field case. This has been apparent during the meeting, for instance with the description of the Picard-Arakelov group of Number fields. On the other hand, most of the results on the zeta function of number fields can be stated (and sometimes proved) in the general framework of the Selberg class

The second topic is relevant to applied mathematics and is related to Error Correcting Codes and Mathematical Cryptography.

Among the new technologies in Computer Science, more and more sophisticated mathematical tools have been recently introduced in Information Theory, specifically in security protocols for data transmissions. This is especially true in the following areas :

- Cryptography,
- Error correcting and error-detecting codes in data transmissions in Galois fields and Galois rings ;
- Generation of random sequences, feedback shift registers.

The discovery of algebraic geometry codes in the eighties created a link between the algebraic theory of curves and the combinatorial theory of linear codes, showing that families of codes could go beyond the Varshamov-Gilbert bound. The design of codes lies on families, or towers, of algebraic curves with many points. The explicit construction of optimal towers of curves was one of the main features of the meeting. This leads to an explicit construction of optimal linear error-correcting codes, &c. In the same way, euclidean lattices, the subject of geometry of numbers, leads to the construction of sphere packings and spherical codes, which are widely used in these applications.

Scientific Content of the events

Instructional lectures : Algebraic Geometry and Information Theory (A.G.I.T.)

1. Algebraic curves over finite fields (Arnaldo Garcia)

The core of applications of algebraic geometry to Information Theory lies on properties of varieties over finite fields, and the number of points of non singular varieties is the most significant invariant.

The number of points of curves obeys to a family of explicit constraints known as « explicit formulas ». Any infinite family of curves must satisfy the Dinrfeld-Vladut bound ; those reaching this bound are called optimal. During the meeting, a comprehensive account of construction of such families has been described : they are the so-called “optimal towers” and are related to modular towers.

2. Mathematical Background of Public Key Cryptography (Gerhard Frey)

One of the most efficient tools in Public Key Cryptography are discrete logarithms. The mathematical task is to construct groups of large prime order in which it is easy to add but very difficult to compute the discrete logarithm.

One can use ideal class groups of rings of integers in global fields for this purpose. leads to the arithmetic of hyperelliptic curves and their Jacobian varieties over finite fields for which we shall establish explicit addition formulas.

The rich structure of these objects and especially the Galois action will imply both possibilities of attacks and of constructions relying on point counting by the use of l-adic and p-adic representations on spaces of differentials.

The main topics were :

- Public Key Cryptography, Discrete Logarithms
- Computational Aspects of Picard Groups
- Duality of Abelian Varieties and Discrete Logarithms

- Point Counting by cohomology methods
- Class fields and Class Groups of global fields, extensions of the Brauer-Siegel Theorem, estimates on zeta and L-functions
- Number of points of curves and varieties over finite fields
- asymptotic estimates, explicit formulas
- Algebraic-geometric codes, constructed from curves and varieties over finite fields, quantum codes
- Properties of the Discrete Logarithm in Abelian Varieties, one-way functions, bent functions.

3. Sphere packings in Euclidean and Hamming spaces (Gregory Kabatianski):

The contents were :

- Sphere packings in general metric spaces
- Minkovski-Hlawka-Varshamov-Gilbert bound
- Spherical codes and error-correcting codes : a unified approach to upper bounds. Examples of optimal or near optimal packings
- Constructions of lattice packing of spheres via error-correcting codes.

4. Elliptic curves over finite fields and algorithms (René Schoof):

Assuming some basic properties of algebraic curves, the theory of elliptic curves over finite fields will be discussed. This includes in particular, the distribution of elliptic curves with respect to their number of points and a description of the various endomorphism rings that may occur Several algorithms involving elliptic curves over finite fields will be studied.

- Number theory, algebraic numbers, global fields, class numbers, regulators, class field towers.
- Algebraic varieties over finite fields, modular varieties, curves and their Jacobians, Frobenius distributions.
- Zeta-functions of global fields, analytic methods and bounds, asymptotic theory.
- Picard-Arakelov theory

In the well known analogy between the theory of function fields of curves over finite fields and the arithmetic of algebraic number fields, the number theoretical analogue of a divisor on a curve is an Arakelov divisor. More precisely, we attach to every Arakelov divisor D its effectivity, a real number between 0 and 1. This notion naturally leads to another quantity associated to D. This is a positive real number which is the arithmetic analogue of the dimension of the vector space of sections of the line bundle associated to a divisor D on an algebraic curve. It can be interpreted as the logarithm of a value of a theta function.

ESF meeting :

Arithmetic, Geometry and Coding Theory (AGCT)

Main features

Special Conference

A conference has been delivered by Jean-Pierre Serre, Abel Prize 2003, on "codes, spinors, and the essential dimension".

General

- Characterization of finite solvable groups

Geometry of Numbers

- Euclidean minima
- New constructions of spherical designs

Number of points of curves and varieties over finite fields

- Number of points of toric varieties
- Weil bound for singular curves
- Superellipitic jacobians
- Chevalley-Warning theorems
- Caps on hermitian varieties
- Characterization of certain maximal curves

Towers of algebraic curves over finite fields

- Towers of function fields over finite fields, non Galois towers over GF(q), where q is a square or a cube
- Modularity of optimal towers

Zeta functions of number fields

- Distinct zeroes in the Selberg class of zeta functions
- Estimates of the class number of CM-fields and residues of zeta functions
- Zeta function as an integral of The Picard-Arakelov group of a number field and the Riemann Hypothesis

Coding theory and cryptography

- Distribution of codes
- Complexity of multiplication in finite fields
- Non linearity of boolean functions
- Error-correcting capability of codes
- Non-binary quantum codes from algebraic curves.
- Codes over p-adic rings
- Codes over the Galois ring GF(8).

ESF Instructional lectures
Algebraic Geometry and Information Theory
Programme

Lundi 12 mai

9h30 - 10h30 **René Schoof** : Elliptic curves over finite fields and algorithms .

11h00 - 12h00 **Gerhard Frey** :Mathematical Background of Public Key Cryptography.

14h30 - 15h30 **René Schoof** : Elliptic curves over finite fields and algorithms .

16h30 - 17h30 **Arnaldo Garcia** : On Curves and Function Fields over finite fields.

Mardi 13 mai

9h30 - 10h30 **René Schoof** : Elliptic curves over finite fields and algorithms .

11h00 - 12h00 **Gerhard Frey** :Mathematical Background of Public Key Cryptography.

14h30 - 15h30 **René Schoof** : Elliptic curves over finite fields and algorithms .

16h30 - 17h30 **Arnaldo Garcia** : On Curves and Function Fields over finite fields.

Mercredi 14 Mai

9h30 - 10h30 **René Schoof** : Elliptic curves over finite fields and algorithms .

11h00 - 12h00 **Arnaldo Garcia** : On Curves and Function Fields over finite fields.

Jeudi 15 Mai

9h30 - 10h30 **Gregory Kabatianski** : Sphere packings in Euclidean and Hamming spaces.

11h00 - 12h00 **Gerhard Frey** :Mathematical Background of Public Key Cryptography.

14h30 - 15h30 **Gregory Kabatianski** : Sphere packings in Euclidean and Hamming spaces.

16h30 - 17h30 **Arnaldo Garcia** : On Curves and Function Fields over finite fields.

Vendredi 16 Mai

9h30 - 10h30 **Gregory Kabatianski** : Sphere packings in Euclidean and Hamming spaces.

11h00 - 12h00 **Gerhard Frey** :Mathematical Background of Public Key Cryptography.

14h00 - 15h00 **Gregory Kabatianski** : Sphere packings in Euclidean and Hamming spaces.

15h15 - 16h30 **Arnaldo Garcia** : On Curves and Function Fields over finite fields

ESF Instructional lectures
Participants

Miriam ABDON, PUC-Rio
R. Prof. Ortiz Monteiro 152/503 Laranjeiras, 22245-10 Rio de Janeiro, BRESIL
miriam@mat.puc-rio.br

Ekaterina AMERIK, Univ. Paris 11
Laboratoire des Maths Batiment 425 Orsay, 91405 Paris, FRANCE
Ekaterina.Amerik@math.u-psud.fr

Ramamonjy ANDRIAMIFIDISOA, Univ. d'Antananarivo
Département de Mathématiques et Informatique, Faculté des Sciences, BP 906, 101 Antananarivo, MADAGASCAR
rmw278@yahoo.fr

Nicolas ARNAUD, IML et ENS-Lyon
Univ. de la Méditerranée, 163 Avenue de Luminy - Case 907, 13288 Marseille Cedex 9, FRANCE
niarnaud@yahoo.fr

Jeremy ARNOLD, Univ. de la Méditerranée
IML, Cite universitaire de Luminy, 171 avenue de luminy, 13288 Marseille Cedex 9, FRANCE
arnold@iml.univ-mrs.fr

Yves AUBRY, Univ. de la Méditerranée
IML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9, FRANCE
aubry@iml.univ-mrs.fr

Alain BARICHARD, Univ. de la Méditerranée
IML, 163 Avenue de Luminy - Case 907, 13288 Marseille Cedex 9, FRANCE
barichar@iml.univ-mrs.fr

Alexis BONNECAZE, IAAI Marseille
12 Avenue du Général Leclerc, 13003 Marseille, FRANCE
alexis.bonnecaze@iaai.fr

Julien BRINGER, Univ Toulon
UTV GRIM BP 132, 83957 La Garde Cedex, FRANCE
bringer@univ-tln.fr

Iftikhar BURHANUDDIN, Univ. of South. California
Computer Science Department 941 W. 37th Place, CA 90007 Los
Angeles, U.S.A.
burhanud@usc.edu

Yves DRIENCOURT, Univ. de la Méditerranée
Département de Mathématiques - Case 901, 13288 Marseille Cedex 9,
FRANCE
Y.Driencourt@wanadoo.fr

Gerhard FREY, Univ. Duisburg-Essen
Institut fuer Experimentelle Mathematik, 45326 Essen, GERMANY
frey@exp-math.uni-essen.de

Arnaldo GARCIA, IMPA
Estrada Dona Castorina,110, 22460320 Rio de Janeiro, BRESIL
garcia@impa.br

Alexander GEWIRTZ, Univ. Grenoble I
Institut Fourier UFR de Math. UMR 5582 BP 74, 38402 Saint Martin
d'Heres Cedex, FRANCE
Alexander.Gewirtz@ujf-grenoble.fr

Sudhir GHORPADE, Indian Institute of Technology
Department of Mathematics, Bombay Powai, 400076 Mumbai, INDIA
srg@math.iitb.ac.in

Valérie GILLOT, Univ. de Toulon
BP 132, 83957 La Garde, FRANCE
gillot@univ-tln.fr

Sergey GORCHINSKIY, Independent Univ. of Moscou
11, Bolshoy Vlasievskiy, 121002 Moscow, RUSSIA
gorchins@mccme.ru

Nicolas GOUILLON, Univ. de la Méditerranée
IML, 163 av de luminy case 907, 13288 Marseille, FRANCE
gouillon@iml.univ-mrs.fr

Iman ISLIM, Univ. de la Méditerranée
IML, 163 av de luminy case 907, 13288 Marseille Cedex 9, FRANCE
imane.islim@voila.fr

Gilles LACHAUD, Univ. de la Méditerranée
IML, 163 av de luminy case 907, 13288 Marseille Cedex 9, FRANCE
lachaud@iml.univ-mrs.fr

Fabien LAGUILLAUMIE, Univ. Caen
LMNO Campus 2, B.P. 5186, 14032 Caen Cedex, FRANCE
laguillaumie@math.unicaen.fr

Tanja LANGE, Ruhr-University of Bochum
Informationsecurity and Cryptology, NA 5/74 Universitaetsstr. 150 ,
44780 Bochum, GERMANY
lange@itsc.ruhr-uni-bochum.de

Philippe LANGEVIN, Univ. de Toulon
GRIM, Avenue de l'Université, 83957 La Garde, FRANCE
langevin@univ-tln.fr

Stephane LOUBOUTIN, Univ. de la Méditerranée
IML, 163 avenue de Luminy Case 907, 13288 Marseille, FRANCE
loubouti@iml.univ-mrs.fr

Olga MASNYK HANSEN, Univ. of Odense
Dept. of Math. & Comp. Science, Campusvej 55, 5230 Odense M, DENMARK
masnyk@get2net.dk

Sylvain MAUGEAIS, Univ. Bordeaux 1
Laboratoire A2X, 351 Cours de la liberation, 33405 Bordeaux, FRANCE
maugeais@math.u-bordeaux.fr

Jean Francis MICHON, Univ. de Rouen
Dépt Informatique Place Emile Blondel, 76821 Mont St Aignan, FRANCE
jean-francis.michon@univ-rouen.fr

M.A. MOHAMED SAADBOUH, Univ. de la Méditerranée
IML, Cité Universitaire de Luminy, Stdio EF 42, 13288 Marseille cedex 9, FRANCE
saadbouh@iml.univ-mrs.fr

Christophe NEGRE, Univ Montpellier 2
Place eugene Bataillon, 34 000 Montpellier, FRANCE
negre@lirmm.fr

Dmitry NOGIN, Inst. Info. Transm. Probl.
19 Bol. Karetnyi, 101447 Moscow, RUSSIE
nogin@iitp.ru

Maria PETKOVA, Humboldt Univ.
Institut für Mathematik Rudower Chaussee 25, 12489 Berlin, GERMANY
mpetkova@mathematik.hu-berlin.de

Patrice RABIZZONI, Univ. de Toulon
BP 132, 83975 La Garde, FRANCE
rabizzon@univ-tln.fr

Christophe RITZENTHALER, Univ. Paris VII
Projet "Théorie des nombres" Institut de Mathématiques Case 247 4, place Jussieu, 75252 Paris, FRANCE
ritzenth@math.jussieu.fr

François RODIER, Univ. de la Méditerranée
IML, 163 Av. de Luminy - Case 907, 13288 Marseille Cedex 9, FRANCE
rodier@iml.univ-mrs.fr

Robert ROLLAND, Univ. de la Méditerranée
IML, 163 av de luminy case 907, 13288 Marseille Cedex 9, FRANCE
rolland@iml.univ-mrs.fr

Marat ROVINSKY , IML
Luminy case 907, 13288 marseille, FRANCE
marat@mccme.ru

Serguei RYBAKOV, Independent Univ. of Moscou
Bolshoi Vlasevsky, 11, 121002 Moscow, RUSSIA
rybakov@mccme.ru

Redha SAMET, Univ. de la Méditerranée
IML, upr 9016 - 163 av de luminy-case 907., 13009 Marseille, FRANCE
samet@iml.univ-mrs.fr

Alexander SAMOKHIN, Univ. Paris 13
Dépt. de Math., 99 Av.J-B.Clement, 93430 Villetaneuse, FRANCE
sasha@math.univ-paris13.fr

Rene SCHOOF, Univ. di Roma 2
Dipartimento di matematica, 00133 Rome, ITALY
schoof@mat.uniroma2.it

Maxim SKRIGANOV, Russian Acad. of Sc.
Steklov Mathematical Institute, Fontanka 27, 191011 St.Petersburg, RUSSIA
skrig@pdmi.ras.ru

Kotyada SRINIVAS, Madras - India
MSC, C.I.T. Campus, Taramani, 600 113 Chennai, INDIA
srini@imsc.res.in

Michael TSFASMAN, Univ. de la Méditerranée
IML, 163 Avenue de Luminy, Case 907, 13288 Marseille, FRANCE
tsfasman@iml.univ-mrs.fr

Stephane VINATIER, EPFL Lausanne
CSAG, 1015 Lausanne, SUISSE
stephane.vinatier@epfl.ch

Marie VIRAT, Univ. Nice Sophia Antipolis
Laboratoire J A Dieudonné, Parc Valrose, 06108 Nice, FRANCE
virat@math.unice.fr

Serge VLADUTS, Univ. de la Méditerranée
IML, 163, Avenue de Luminy - Case 907, 13008 Marseille Cedex 9, FRANCE
vladut@iml.univ-mrs.fr

Rania WAZIR, University of Turin
Via Carlo Alberto, 10, 10123 Turin, ITALY
wazir@dm.unito.it

Christian WITTMANN, UniBw München
Fakultät für Informatik, Inst. für Theoretische Informatik und Math.,
85577 Neubiberg, GERMANY
wittmann@informatik.unibw-muenchen.de

Siman YANG, National Univ. of Singapore
Department of Mathematics, 2, Science Drive 2, 117543 Singapore,
SINGAPORE
scip0242@nus.edu.sg

Alexei ZYKIN, Independent Univ. of Moscou
Bolshoi Vlasevsky, 11, 121002 Moscow, RUSSIA
zykin@comtv.ru

ESF meeting
Arithmetic, Geometry and Coding Theory (AGCT)

Lundi 19 Mai

Séance du matin Président S. Vladut

10h00 - 10h50 **M. Tsfasman** : 49 and beyond.

11h20 - 11h50 **M. Perret** : A Chevalley-Warning theorem on toric varieties.

12h00 - 12h30 **Y. Aubry** : Zeta functions and bounds ``à la Weil".

Séance de l'après-midi Président R. Schoof

16h00 - 16h50 **G. Lachaud** : Integration on the Picard-Arakelov group and the Riemann Hypothesis.

17h20 - 17h50 **K. Srinivas** : Distinct zeroes in the Selberg class.

18h00 - 18h30 **S. Louboutin** : Explicit bounds on residues of zeta functions and applications.

18h40 - 19h10 **F. Hajir** : Galois *p*-groups unramified at *p* (after N. Boston).

Mardi 20 Mai

Séance du matin - Président T. Hoeholdt

9h30 - 10h20 **M. Skriganov** : The Rosenbloom-Tsfasman metric and related topics in codes, discrepancy and harmonic analysis.

10h50 - 11h20 **G. van der Geer** :

11h30 - 12h00 **A. Barg** : Estimating the distance distribution of codes.

Séance de l'après-midi Président B. Kunyavski

16h00 - 16h50 **E. Bayer** : Minima euclidiens.

Pause

17h20 - 17h50 **C. Bachoc** : A new construction of spherical designs.

18h00 - 18h30 **E. Howe** : Improved upper bounds for the number of points on curves over finite fields.

18h40 - 19h10 **S. Ballet et R. Rolland** : Tensor rank of the multiplication in finite fields.

Mercredi 21 Mai

Séance du matin - Morning session Président W.-C. Winnie Li

9h30 - 9h45 **M. Gyllenberg** : (European Science Foundation), Information about funding possibilities from the ESF.

9h45 - 10h30 **H. Stichtenoth** : Towers of function fields over finite fields.

10h45 - 11h30 **P.H.T. Beelen** : Graphs and towers of function fields

11h45 - 12h30 **A. Garcia** : On certain non-Galois towers over $\mathbf{F}_{q2}$ and $\mathbf{F}_{q3}$.

Jeudi 22 Mai

Séance du matin - Président E. Bayer

9h30 - 10h20 **W.-C. Winnie Li** : Modularity of optimal towers.

10h50 - 11h20 **. Zarhin** : Homomorphisms of superelliptic jacobians.

11h50 - 12h20 **K. Thas** : Number of points of a hypersurface (by combinatorial methods).

Séance de l'après-midi Président J. Hirschfeld

16h00 - 16h50 **B. Kunyavski** : Application of arithmetic geometry to characterization of finite solvable groups.

17h00 - 18h00 **J.-P. Serre** : Codes, Spineurs et ``dimension essentielle".

18h30 Réception en l'honneur de J.-P. Serre

Vendredi 23 Mai

Séance du matin Président S. Ghorpade

9h30 - 10h00 **O. Moreno** : Chevalley-Warning-Ax-Katz type results and applications.

10h10 - 10h40 **J. Hirschfeld** : Caps on hermitian varieties.

11h10 - 11h40 **I. Duursma** :*p*-adic codes.

11h50 - 12h20 **F. Rodier** : Nonlinearity of boolean functions.

Séance de l'après-midi Président G. Kabatiansky

14h00 - 14h30 **T. Helleseth** : Error-correcting capability of codes.

14h40 - 15h10 **J. Walker** : Non-binary quantum codes from algebraic curves.

15h20 - 15h50 **O. Geil** : On the performance of Hyp $q(s,m)$ and Herm $q(s,m)$.

16h10 - 16h30 **P. Solé** : Codes over **Z**/8 **Z**.

16h35 - 16h50 **M. Abdon** : A characterization of certain maximal curves.

16 h 55 - 17 h 10 **M. Bras-Amoros** : Acute numerical semigroups and the order bound on the minimum distance.

ESF meeting
Arithmetic, Geometry and Coding Theory
Participants

Miriam ABDON, PUC-Rio
R. Prof. Ortiz Monteiro 152/503 Laranjeiras, 22245-10 Rio de Janeiro, BRESIL
miriam@mat.puc-rio.br

Ramamonjy ANDRIAMIFIDISOA, Univ. d'Antananarivo
Département de Mathématiques et Informatique, Faculté des Sciences, BP 906, 101 Antananarivo, MADAGASCAR
rmw278@yahoo.fr

Nicolas ARNAUD, IML et ENS-LYON
Univ. de la Méditerranée, 163 Avenue de Luminy - Case 907, 132888 Marseille Cedex 9, FRANCE
niarnaud@yahoo.fr

Yves AUBRY, Univ. de la Méditerranée
IML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9, FRANCE
aubry@iml.univ-mrs.fr

Christine BACHOC, Univ. Bordeaux I
Laboratoire A2X - 351 cours de la liberation, 33450 Talence, FRANCE
bachoc@math.u-bordeaux.fr

Eiichi BANNAI, Kyushu University
Graduate School of Mathematics Hakozaki, 6-10-1, Higashi-ku, 812-8581 Fukuoka, JAPAN
bannai@math.kyushu-u.ac.jp

Alexander BARG, Rutgers University
DIMACS, CoRE Building, Room 428, 08854 Piscataway, NJ, U.S.A.
abarg@ieee.org

Alain BARICHARD, Univ. de la Méditerranée
IML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9,
FRANCE
barichar@iml.univ-mrs.fr

Eva BAYER FLUCKIGER, EPF Lausanne
Departement de Mathématiques, 1015 Lausanne, SUISSE
eva.bayer@epfl.ch

Peter BEELEN, University Essen
Institut für experimentelle Mathematik, Ellernstrasse 29, 45326 Essen,
GERMANY
peter.beelen@uni-essen.de

Régis BLACHE, Univ. Antilles Guyane
Rue Louis Boucard Caraque, 97139 Les Abymes, FRANCE
rblache@univ-ag.fr

Maria BRAS-AMOROS, Univ. Politècnica de Catalunya
c. Pau Gargallo 5, 08028 Barcelona, ESPAGNE
maria.bras@upc.es

Iftikhar BURHANUDDIN, Univ. of South. California
Computer Science Department 941 W. 37th Place, CA 90007 Los
Angeles, U.S.A.
burhanud@usc.edu

Antonio CAMPILLO, Univ.de Valladolid
Facultad de Ciencias Prado de la Magdalena, 47005 Valladolid,
ESPAGNE
campillo@agt.uva.es

Mireille CAR, Univ. Aix-Marseille 3
Mathématiques, Cr. A, Av. Escadrille Normandie-Niemen, 13013 Marseille, FRANCE
mireille.car@vmesa12.u-3mrs.fr

Guy CHASSÉ, Ecole des Mines de Nantes
4, rue Alfred Kastler BP 20722, 44307 Nantes Cedex 3, FRANCE
chasse@emn.fr

Jean-pierre CHERDIEU, univ Antilles-Guyane
Fac des Sciences Campus de fouillole, 97159 Pointe-à-Pitre, FRANCE
jpcherdi@univ-ag.fr

Miguel CONCY, Univ. Paris 6
53, rue du chateau d'eau, 75010 Paris, FRANCE
mconcy@math.jussieu.fr

Yves DRIENCOURT, Univ. de la Méditerranée
Département de Mathématiques - Case 901, 13288 Marseille Cedex 9, FRANCE
Y.Driencourt@wanadoo.fr

Iwan DUURSMA, University of Illinois at U-C
Department of Mathematics 1409 W. Green Street (MC-382), IL 61801 Urbana, U.S.A.
duursma@math.uiuc.edu

Arnaldo GARCIA, IMPA
Estrada Dona Castorina,110, 22460-32 Rio de Janeiro, BRAZIL
garcia@impa.br

Olav GEIL, Aalborg University
Dept. of Mathematics Fr. Bajersvej 7G, 9220 Aalborg, DENMARK
olav@math.auc.dk

Alexander GEWIRTZ, Univ. Grenoble I
Institut FourierUFR de Mathematiques UMR 5582 BP 74, 38402
Saint Martin d'Heres Cedex, FRANCE
Alexander.Gewirtz@ujf-grenoble.fr

Sudhir GHORPADE, IIT Bombay
Indian Institute of Technology Bombay Powai, 400076 Mumbai,
INDIA
srg@math.iitb.ac.in

Valérie GILLOT, Univ. Toulon
GRIM, Avenue de l'Université, BP 132, 83957 Toulon, FRANCE
gillot@univ-tln.fr

Sergey GORCHINSKIY, Independent Univ.of Moscou
11, Bolshoy Vlasievskiy, 121002 Moscow, RUSSIA
gorchins@mccme.ru

Farshid HAJIR, Univ. of Massachusetts
Department of Mathematics, 01003 Amherst MA, U.S.A.
hajir@math.umass.edu

Johan P. HANSEN, Aarhus University
Matematisk Institut, Ny Munkegade, 8000 Aarhus, DENMARK
matjh@imf.au.dk

Tor HELLESETH, University of Bergen
Department of Informatics Hoyteknologisenteret, 5020 Bergen,
NORWAY
Tor.Helleseth@ii.uib.no

James HIRSCHFELD, University of Sussex
School of Mathematical Sciences, BN1 9QH Brighton, UNITED
KINGDOM (THE)
jwph@susx.ac.uk

Tom HOEHOLDT, Technical Univ. of Denmark
Department of Mathematics Bldg.303, DK-2800 Lyngby,
DENMARK
T.Hoeholdt@mat.dtu.dk

Everett HOWE,
Center for Communications Research, 4320 Westerra Court, 92121
San Diego, CA, U.S.A.
however@alumni.caltech.edu

Iman ISLIM, Univ. de la Méditerranée
IML, 163 av de luminy case 907, 13288 Marseille Cedex 9, FRANCE
imane.islim@voila.fr

Motoko KAWAKITA, BunkyoOchanomizu Univ.
Kaneko Lab., Faculty of Science, 2-1-1 Otsuka, Bunkyo, 112-8610
Tokyo, JAPON
motoko@atom.is.ocha.ac.jp

Boris KUNYAVSKII, Bar-Ilan University
Department of Mathematics and Statistics, 52900 Ramat Gan,
ISRAEL
kunyav@macs.biu.ac.il

Gilles LACHAUD, Univ. de la Méditerranée
IML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9,
FRANCE
lachaud@iml.univ-mrs.fr

Philippe LANGEVIN, Univ. Toulon
GRIM, Avenue de l'Université, BP 132, 83957 La garde, FRANCE
langevin@univ-tln.fr

Michel LAURENT, Univ. de la Méditerranée
ML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9,
FRANCE
laurent@iml.univ-mrs.fr

Dominique LE BRIGAND, Univ. Paris 6
IMJ 175 rue du Chevaleret, 75013 Paris, FRANCE
lebrigan@math.jussieu.fr

Frederic LEHOBEY, Canon Research
Centre France S.A.S., Rue de la Touche Lambert, 35517 Cesson-Sevigne cedex, FRANCE
Frederic.Lehobey@crf.canon.fr

Winnie LI, Penn State University
Department of Math., 16802 University Park, PA, U.S.A.
wli@math.psu.edu

Pierre LIARDET, Univ. de Provence
CMI - 39 Rue F. Joliot-Curie, 13453 Marseille Cedex 13, FRANCE
liardet@cmi.univ-mrs.fr

Stephane LOUBOUTIN, Univ. Aix-Marseille II
IML 163, Avenue de Luminy, Case 90, 13288 Marseille, FRANCE
loubouti@iml.univ-mrs.fr

Christian MAIRE, Univ.Toulouse 2
Departement Math/Info UFR SES, 31058 Toulouse, FRANCE
christian.maire@univ-tlse2.fr

Olga MASNYK HANSEN, Univ. of Odense
Dept. of Math. & Comp. Science, Campusvej 55, 5230 Odense M, DENMARK
masnyk@get2net.dk

M.A. MOHAMED SAADBOUH, Univ. de la Méditerranée
Cité universitaire Luminy, Studio Ef:42, 13288 Marseille Cedex 9, FRANCE
saadbouh@iml.univ-mrs.fr

Oscar MORENO, Universidad de Pueto Rico
Gauss Research Lab PO Box 23334, 00931-33 San Juan, PR, U.S.A.
O_MORENO@UPR1.UPR.CLU.EDU

Dmitrii NOGIN, IITP Moscou
19 Bol. Karetnyi,, 101447 Moscou, RUSSIE
nogin@iitp.ru

Marc PERRET, Univ. Toulouse II
5, Allées A. Machado, 31 058 Toulouse, FRANCE
perret@univ-tlse2.fr

Heinz-Georg QUEBBEMANN, Univ. Oldenburg
Institut fuer Mathematik, D-26111 Oldenburg, GERMANY
quebbemann@mathematik.uni-oldenburg.de

Patrice RABIZZONI, Univ. Toulon
Avenue de l'Université, BP 132, 83975 La Garde, FRANCE
rabizzon@univ-tln.fr

Christophe RITZENTHALER, Univ. Paris VII
Projet "Théorie des nombres" Institut de Mathématiques Case 247 4,
place Jussieu, 75252 Paris, FRANCE
ritzenth@math.jussieu.fr

François RODIER, Univ. de la Méditerranée
IML, 163 Av. de Luminy - Case 907, 13288 Marseille Cedex 9,
FRANCE
rodier@iml.univ-mrs.fr

Robert ROLLAND, Univ. de la Méditerranée
ML, 163 av de luminy case 907, 13288 Marseille Cedex 9, FRANCE
rolland@iml.univ-mrs.fr

Marat ROVINSKY, Univ. de la Méditerranée
IML, 163 Avenue de Luminy - Case 907, 13288 Marseille, FRANCE
marat@mccme.ru

Serguei RYBAKOV, Independent Univ. of Moscou
Bolshoi Vlasevsky 11, 121002 Moscow, RUSSIA
rybakov@mccme.ru

Redha SAMET, Univ. de la Méditerranée
IML, upr 9016 - 163 av de luminy-case 907, 13288 Marseille Cedex
9, FRANCE
samet@iml.univ-mrs.fr

Alexander SAMOKHIN, Univ. Paris 13
99 Av. J.-B.Clement, 93430 Paris, FRANCE
sasha@math.univ-paris13.fr

Jasper SCHOLTEN, Universiteit Leuven
COSIC, Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, BELGIUM
jasper.scholten@esat.kuleuven.ac.be

Rene SCHOOF, Universita di Roma 2
Dipartimento di matematica , 00133 Rome, ITALIE
schoof@mat.uniroma2.it

Jean-Pierre SERRE, Collège de France
6 avenue de Montespan, 75116 Paris, FRANCE
serre@noos.fr

Maxim SKRIGANOV, Russian Acad. of Sc.
Steklov Mathematical Institute, Fontanka 27, 191011 St.Petersburg,
RUSSIA
skrig@pdmi.ras.ru

Patrick SOLE, ESSI - Sophia Antipolis
Laboratoire I3S BP 145 Route des Colles, 06903 Sophia Antipolis, FRANCE
ps@essi.fr

Kotyada SRINIVAS, Madras-India
IMSC, C.I.T. Campus, Taramani, 600 113 Chennai, INDIA
srini@imsc.res.in

Henning STICHTENOTH, Universitaet Essen
Fachbereich 6 Mathematik, 45117 Essen, GERMANY
stichtenoth@uni-essen.de

Alexandre TEMKINE, Lycée Michelet, Vanves
14, Rue Eugene Carriere, 75018 Paris, FRANCE
atemkine@planetis.com

Koen THAS, Ghent University
Department of Pure Mathematics and Computer Algebra Galglaan 2, 9000 Ghent, BELGIUM
kthas@cage.rug.ac.be

Lara THOMAS, Univ. Toulouse II
Equipe GRIMM 7, Allée Antonio Machado, 35058 Toulouse, FRANCE
Lara.Thomas@univ-tlse2.fr

Alev TOPUZOGLU, Sabanci Univ., Istanbul
MDBF Orhanli,, 34956 Tuzla Istanbul, TURKEY
alev@sabanciuniv.edu

Michel TSFASMAN, Univ. de la Méditerranée
IML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9, FRANCE
tsfasman@iml.univ-mrs.fr

Gerard VAN DER GEER, Univ. Amsterdam
Korteweg-de Vries Instituut, Plantage Muidergracht 24, 1018 TV
Amsterdam, NETHERLANDS (THE)
geer@science.uva.nl

Pascal VERON, Univ. Toulon
GRIM, Avenue de l'université, B.P. 13, 83957 La Garde Cedex,
FRANCE
veron@univ-tln.fr

Serge VLADUTS, Univ. de la Méditerranée
IML, 163 avenue de Luminy - Case 907, 13288 Marseille Cedex 9,
FRANCE
vladut@iml.univ-mrs.fr

Judy WALKER, University of Nebraska
Department of Mathematics 810 Oldfather Hall, 68516 Lincoln, NE,
U.S.A.
jwalker@math.unl.edu

Rania WAZIR, University of Turin
Via Carlo Alberto, 10, 10123 Turin, ITALY
wazir@dm.unito.it

James WOLPER, Idaho State University
Department of MathematicsCampus Box 8085, 83209 Pocatello, ID,
U.S.A.
wolpjame@isu.edu

Yuri ZARHIN, Pennsylvania State University
Dept. of Math., 218 McAllister Building, University Park, 16803
University Park, PA, U.S.A.
zarhin@math.psu.edu

Alexei ZYKIN, Independent Univ. of Moscou
Bolshoi Vlasevsky, 11, 121002 Moscow, RUSSIA,
zykin@comtv.ru**Erreur! Signet non défini.**

Statistical information on participants of the Instructional lectures

The total number of participants of the Instructional lectures was equal to 50.

There were 11 differents representated countries : Brazil, France, Madagascar, USA, Germany, India, Russia, Danemark, Italy, Suisse and Singapore.

There were 56% of frenchs, 14% of russians, 8% of germans, 4% of italians, 4% of brazilians, and 2% of all the others countries.

There were 76% of europeans.

There were 20% of women (historically, the Mathematics are not a domain where the place of women is very large, thus twenty percents is a very good number).

The young researchers constituted 60% of the participants.

Statistical information on participants of the ESF meeting

Arithmetic, Geometry and Coding Theory

The total number of participants of the ESF meeting « Arithmetic, Geometry and Coding Theory » was equal to 79.

There were 19 differents representated countries : Brazil, France, Madagascar, Japan, USA, Germany, Antilles, Spain, India, Russia, Norway, United Kingdom, Israel, Belgium, Danemark, Italy, Suisse, Turkey and Netherlands.

There were 43% of frenchs, 13% of americans, 9% of russians...

There were 70% of europeans researchers.

There were 19% of women.

The young researchers constituted 34% of the participants.