Mathematisch Instituut, Universiteit Leiden

Annual Report 2011

Contents

Managing Board and Address 2

Research

Cluster 1. Number Theory, Algebra and Geometry

Programme 1.1 Number Theory and Algebra 3

Programme 1.2 Arithmetic Geometry 6

Cluster 2. Analysis and Stochastics

Programme 2.1 Analysis and Dynamical Systems 8

Programme 2.2 Probability Theory 13

Programme 2.3 Mathematical and Applied Statistics 16

Project Mathematics, Computer Science and Society 18

Kloosterman Professor 19

International and National Programmes 20

Master Theses 23

ALGANT Master Theses 25

Ph.D. Theses 26

Publications 27

Mathematical Institute Reports 33

Workshops, Seminars a.o. 35

Invited Lectures 38

Memberships of Editorial Boards 45

Honors 47

Foreign Visitors 48

Research Staff 50

Support Staff 54

Student Assistants 55

Organization 57

Mathematisch Instituut, Universiteit Leiden

Annual Report 2011

Managing Board
Prof.dr. P. Stevenhagen, scientific director
Prof.dr. S.J. Edixhoven, director of education (till September 15)
Dr. B. de Smit, director of education (from September 15)
Dr. M. Lübke, managing director

Address
Mathematisch Instituut, Universiteit Leiden
Snellius
Niels Bohrweg 1
2333 CA Leiden
The Netherlands
Phone : +31 71 527 7111
Fax : +31 71 527 7101
URL : www.math.leidenuniv.nl

Cluster 1. Number Theory, Algebra and Geometry

Research Programme 1.1: Number Theory and Algebra
Programme leader: H.W. Lenstra

Description of the project

The main focus of the research programme is number theory. Number theory studies the properties of integers, with a historically strong emphasis on the study of diophantine equations, that is, systems of equations that are to be solved in integers. The methods of number theory are taken from several other branches of mathematics. Traditionally, these include algebra and analysis, and in recent times algebraic geometry has become increasingly important. Another recent development is the discovery that number theory has significant implications in more applied areas, such as cryptography, theoretical computer science, the theory of dynamical systems, and numerical mathematics. This discovery led to the rise of algorithmic and computational number theory, which occupies itself with the design, analysis, and efficient implementation of arithmetical algorithms. The overall result has been a unification rather than a diversification of number theory. For example, the applications in cryptography depend heavily on algebraic geometry, and algebraic number theory, which used to stand on itself, is now pervading virtually all of number theory. Themes of the programme reflect the research areas mentioned. They include finding points on algebraic curves, applications of group theory and algebraic number theory, the theory of finite fields, diophantine approximation, words and sequences, discrete tomography, primality tests and factorization methods, and the development of efficient computer algorithms.

The algebra portion of the programme is strongly oriented towards the applications of algebra in number theory and arithmetic geometry and towards algorithmic aspects. Themes include Galois theory and various aspects of group theory and ring theory.

The research programme also includes cryptology and the history of mathematics. Main themes in cryptology are the applications of number theory and algebra to the design of cryptographic schemes, and foundational issues are considered as well. In the history of mathematics, the emphasis is on the edition and translation of early Islamic mathematical and astronomical texts.

Research results in 2011

Cascudo, Cramer and Xing have introduced the novel algebraic notion of “codex" as an abstraction that captures all known types arithmetic secret sharing schemes as well as the notion of bilinear algorithms for multiplication in finite fields as special cases. Algebraically, a codex is a dedicated yet natural type of presentation of a given finite-dimensional algebra (over a field). They have also initiated work on upper- and lower-bounds on the parameters of codices.

Cascudo, Cramer and Xing have also completed their work on torsion limits for algebraic functions fields over finite fields, which gives rise to significant improvements in the area of asymptotically good arithmetic secret sharing schemes.

In other work, addition, Cascudo, Cramer and Xing improved the best known bounds for the asymptotic complexity of multiplication in finite extensions of a given finite field, if the field is small (e.g. the binary field).

Cramer, Damgaard and Pastro have introduced a novel way to prove, in zero knowledge, multiplicative relations among committed secrets, using the asymptotically good arithmetic secret sharing schemes of Chen/Cramer (2006).

Cramer, Damgaard, Kiltz and Zottarel initiated work on the difficulty of Diffie-Hellman problems under extensions of the field of definition.

Evertse, together with A. Bérczes and K. Győry, finished a paper on multiply monogenic orders. Most of this research was carried out in 2010.
Together with K. Győry Evertse finished a paper on effective results for unit equations over finitely generated domains. This concerns equations ax+by=c where the coefficients a,b,c belong to an integral domain A which is finitely generated over Z and the unknowns x, are taken from the unit group A* of A. They proved in a well defined sense that if the domain A is "effectively given", then the solutions x,y of this equation can be effectively determined in principle. Further, they obtained a quantitative result, giving an explicit upper bound for the "sizes" of x,y.
Presently, Evertse is working together with A. Bérczes and K. Győry on generalizations of the above result to other types of Diophantine equations, such as Thue equations, and hyper- and super elliptic equations. This is ongoing research.
Finally, together with K. Győry Evertse is writing a book on unit equations and discriminant equations. This is ongoing work.

B. van Dalen, L. Hajdu and R. Tijdeman studied discrete tomography in two dimensions and published their results in arxiv 1104.5589.
L. Hajdu, N. Saradha and R. Tijdeman investigated a conjecture of Pomerance and established it under the Riemann Hypothesis: arxiv 1107.5191.
R. Tijdeman solved a problem of M. Spijker with applications in the theory of multi-step methods. Later he extended the paper in collaboration with F. Beukers. See arxiv 1107.5495.
L. Hajdu and R. Tijdeman dealt with a problem of M. Nathanson and some related results in arxiv 1201.3991.

H.W. Lenstra worked on the following projects:

With Y. Kilic on super solvable groups
With M. Lopuhaä on topological fields
With A. Javanpeykar on Brauer groups
With R. Eggermont on Witt-vectors and the theorem of Brauer-Nesbitt
With H. Matthijsse on Archimedes
With M. Kosters on commutative algebra and curves over finite fields
With B. Jansen on Mersenne prime numbers and class field theory
With A. Lbekkouri on wild extensions of local fields
With G. Dalla Torre on the unit residue group
With B.M. Hoang on algebras and the theorem of Skolem-Noether
With D. Duong Hoang on group theory
With J. Bouw on the norm residue symbol
With J. Daems on the history of the crystallographic groups
With A. Gioia on the theory of Tate-Bhargava-Galois

R. van Luijk has been working with C. Salgado on the density of rational points on Del Pezzo surfaces. He has also been working with D. Testa and B. Poonen on the computability of Picard numbers and with M. Bright and D. Testa on a book about Brauer-Manin obstructions.

B. de Smit continued joint work with T. Chinburg (Philadelphia) and F. Bleher (Iowa City) on the inverse problem for deformation rings of linear representations, extending the results already obtained.
In October 2011 ALGANT PhD student K. Dorobisz started his PhD project in this topic.

A. Siviero obtained results with B. de Smit on statistical behaviour of abelian extensions of number fields, and in particular on the interplay between the local structure (following methods of M. Wood) and the Galois module class of the ring of integers (following L. McCulloh, A. Agboola). These results will be part of the ALGANT PhD thesis of A. Siviero in 2013, which will be supervised by B. de Smit and B. Erez (Bordeaux).

Following up on questions of G. Cornelissen (Utrecht), B. de Smit obtained finer results on the degree to which a number field can be characterized by its abelian L-functions.

The collaborative computational project ABC@Home (abcathome.com) continued to run in 2011 under supervision of B. de Smit. It was improved further, and the data collected from many thousands of computers have been published.

Stevenhagen finished a paper with Lenstra and Moree (MPIM Bonn) on the use of character sums in the evaluation of Artin primitive root densities.
With E. Howe (CCR San Diego) he worked on genus-2 curves and abelian surfaces over finite fields.
With A. Angelakis, he studied absolute abelian Galois groups of imaginary quadratic fields.
J. Brau worked on algorithmic aspects of Galois representations attached to elliptic curves over the rational numbers.

Research Programme 1.2: Arithmetic Geometry
Programme leader: S.J. Edixhoven

Description of the project

Geometers study geometric properties of sets of solutions of systems of equations. According to the possible kinds of equations (continuous, differentiable, analytic, polynomial), and of the structures that one studies, one distinguishes kinds of geometry (topology, differential topology and differential geometry, analytic geometry, algebraic geometry, arithmetic geometry).

In algebraic geometry the equations are given by polynomials. Classically, the coefficients and solutions were complex numbers. Number theorists consider integer or rational coefficients and solutions. The goal of arithmetic geometry is to understand the relations between algebraic geometry and number theory.

Three important notions in arithmetic geometry are “algebraic variety” (abstraction of system of polynomial equations), “zeta function” and “cohomology”. Zeta functions associated to algebraic varieties are generating functions defined using the numbers of solutions in finite fields. Cohomology associates vector spaces equipped with certain structures to algebraic varieties. One important aim of arithmetic geometry is to understand the relations between the values of zeta functions at integers and properties of the set of rational solutions. Cohomology plays an important role here. Cohomology also provides representations of Galois groups, which is essential for Langlands's program (relations between such representations and “automorphic” representations of matrix groups). The most striking results obtained in this field are the proof of Weil's conjectures (Dwork, Grothendieck, Deligne), Faltings's proof of Mordell's conjecture, Fontaine's theory (comparison between certain cohomologies), Wiles's proof of Fermat's Last Theorem, and Lafforgue's and Ngo's results on Langlands's conjectures.

Apart from its numerous applications within mathematics, algebraic geometry over finite fields provides error correcting codes and crypto systems, both used in everyday life.

Research results in 2011

Edixhoven has made a counterexample to a relative Manin-Mumford conjecture for semi-abelian schemes by D. Bertrand (Paris) more explicit. He has found a new proof of Gauss's theorem on sums of three squares of integers that uses simple properties of group schemes over the integers.

He supervised the master thesis in which Jinbi Jin has shown that multiplication on elliptic curves by an integer n can be described by three polynomials.

Another master student, M. Derickx, has made significant progress on the question of primes that occur as order of a point on an elliptic curve over a number field of degree at most d, for d is 5, 6, or 7, and on the question of determining the gonality of some modular curves.

De Jong has found precise asymptotic formulae for Arakelov invariants related to Gross-Schoen cycles. He has obtained results on special values of canonical Green's functions on hyper-elliptic Riemann surfaces. Using the concept of Bloch pairing he has extended a result of S. Zhang on the height of Gross-Schoen cycles. In particular this led to a differential-geometric criterion for the vanishing of the height.

Together with J. Draisma he has explored a numerical approach to the SICPOVMs problem using theta functions on elliptic curves.

Together with Y. Achnine he has proved that for MDS Goppa codes, for sizes of the field of definition larger than some linear function in the dimension of the code, the length is bounded as predicted by the main conjecture on MDS codes.

Taelman has continued his research on the subtle arithmetic invariants that are reflected in special values of L-functions associated with Drinfeld modules and related objects. Most importantly, he has obtained the first case of a function field Herbrand-Ribet theorem (to appear in Inventiones Mathematicae).
Together with Bruno Anglès from Caen he has obtained a counter-example to the function field case of the Kummer-Vandiver conjecture.
Ongoing work with Bruno Anglès focuses on generalizing these results into a Main Conjecture for Drinfeld modules.

Cluster 2. Analysis and Stochastics

Research Programme 2.1: Analysis and Dynamical Systems
Programme leader: A. Doelman

Description of the project
This program focuses on asymptotic operator-theoretical methods to analyze problems arising from concrete classes of integral, differential and difference equations. Both linear and non-linear equations are studied, and the problems may have a finite-dimensional or infinite-dimensional character. Typical for this program is a strong interaction with dynamical systems, functional analysis, numerical analysis, partial differential equations, probability theory and complex function theory.
There is a special focus on the analysis of infinite dimensional dynamical systems and applications. Determining the long-term behavior of dynamical systems can be a time consuming and difficult task. It is often essential to combine perturbation and numerical methods with methods from dynamical systems theory. Rather than considering the equations for fixed values of the physical parameters, we often study solutions as a function of the physical parameters. Specific examples that are investigated include singularly perturbed equations, dynamical systems with time delays in the feedback loop, differential equations modeled on a lattice, and various model systems that govern processes in earth sciences, life sciences and engineering.
The current research interests of the group include: Algebras associated with dynamical systems, pattern formation, differential-difference equations of mixed type, localized structures in reaction-diffusion equations, invariant measures for stochastic delay equations, Ginzburg-Landau equations, etc.

Algebras associated with dynamical systems
When a group G acts on a Banach algebra A there are several algebras of crossed product type naturally associated with these data. It is the aim of this project to understand the relationship between the associated algebra and the initial dynamical system. Well rooted in C*-theory is the case where A is the algebra of continuous functions on a compact Hausdorff space X and the group G is the integers, in which case one wants to understand the structure of the associated algebra in terms of the dynamical system on X, but the even more naturally associated involutive Banach algebra of crossed product type (an L^1-algebra with twisted convolution) is also under investigation.
Another main line of research consists of constructing the appropriate Banach algebra crossed product for a given set of covariant representations of a Banach algebra dynamical system. This is a natural generalization of C*-crossed products and is analogously expected to be the main tool when studying group representations in Banach spaces and induction procedures in these spaces.

Positive representations
There is an abundance of examples, within and outside mathematics, of groups acting as positive operators in Riesz spaces and Banach lattices. Quite in contrast to the analogous case of unitary representations, such positive representations have not yet been investigated systematically. It is the aim of this project to initiate this theory. Current focuses are on finite and compact groups, and on the construction of a Banach lattice algebra of crossed product type analogous to the group C*-algebra in the unitary case. For the latter, there is a close connection with the previous project.

Pattern Formation
Pattern formation, or: the dynamics of spatial structures described by high dimensional dynamical systems (mostly partial differential equations) is a central theme within the research of Doelman. His research builds on two foundations: fundamental analysis of “simple” patterns such as localized or spatially periodic patterns and applied analysis of explicit models that generate patterns. Of course there is a strong interaction between these two aspect of Doelman's research. Topics within the former aspect include Evans function methods, the dynamics of modulated waves, the interactions between localized structures.
The applications range from phytoplankton dynamics and internal (oceanic) waves to Josephson junctions and fuel cells. The models often have a reaction-diffusion structure, but can also be of sine-Gordon, nonlinear Schrodinger or Cahn-Hilliard type

Singularity formation in natural systems.
Singularities arise when nonlinear effects dominate the dispersive ones, up to the formation of the singularity. Singularity formation, also called blowup, has received a considerable amount of attention in problems ranging from nonlinear optics, plasma physics and combustion to hydrodynamics,and from stellar dynamics to chemotaxis in bacteria. In work of Rottschäfer, the formation of singularities is studied in projects that are motivated by these concrete applications. The equations that are used to model the applications can be divided into two classes: amplitude equations, such as the Korteweg-de Vries equation, and systems of reaction-diffusion equations. In the study of blowup solutions for these equations, combination of numerical, asymptotical and geometrical methods is used.
This research is part of the VIDI project of Rottschäfer.

Applications to Life Sciences
This research project concerns the modeling, analysis and simulation of long-term behaviour of discrete and continuous dynamical systems that occur in Life Sciences, in particular in chemotaxis of unicellular organisms, cell signaling and plant (secondary) metabolism. From a mathematical modeling perspective, these three biological topics result in the analysis and simulation of measure-valued structured population models with “internal” dynamics for individuals described by systems of nonlinear ordinary differential equations. That is, a prototypical example of a system of mixed type.
The mathematical research focuses on: (1) the long-term behaviour of systems of measure-valued evolutionary equations of mixed type using a functional analytic (semi-group) approach; (2) application of the fundamental results of part (1) to experimental systems, in particular the gradient detection system in Dictyostelium chemotaxis, auxine transport in Arabidopsis and secondary metabolite production in cell suspension cultures of Catharanthus roseus (among others in collaboration with the groups of, respectively, prof.dr. T. Schmidt, prof.dr. B. van Duijn and prof.dr. R. Verpoorte); and (3) data oriented system's analysis: e.g. system properties, like attractors, are numerically approximated based on experimental data, and parameter estimation.

Applications to Earth Sciences
Development of a computational method for the control of dike heights (research carried out at both the Mathematical Institute and CWI).
The Dutch government institute Deltares (the former Rijkswaterstaat) continuously inspects the degree of protection against flooding of large parts of the Netherlands, offered by primary dikes and by the dunes.
Following the 1953 floodings, van Dantzig (Mathematisch Centrum, the current CWI) developed a mathematical model with which the optimal height of a dike can be computed. The model also allows to compute when and how much, optimally, a dike has to be increased.

The model concerns a control problem in which a minimum is found in the cost for dike increase plus the expected cost due to flooding. The model has been elaborated in software which is being used on a routine basis for many years already. However, the model no longer satisfies tomorrow's safety requirements. It is unsuited for quickly incorporating new insights, e.g., new flooding chances (following from more accurate predictions of climate change) and new rates of economical growth (or shrinkage); the model lacks dynamics. Further, it does not consider uncertainty in the underlying climatological and economical models; it also lacks stochastics. Both shortcomings are remedied in the current research project.

Environmental Sciences
Two research projects within the group are in the field of environmental sciences and appear at the overlap between earth and life sciences. The first one is a collaboration between Doelman, de Swart (IMAU, Utrecht), Zagaris (UT) and their mutual PhD student Zijlstra (CWI). In the project the dynamics of phytoplankton is studied. Central topic of investigation is the formation and subsequent bifurcations of “deep chlorophyll maxima”. In another project, Doelman studies the dynamics of vegetation patterns and their crucial role in the process of desertification. This is a joint project with Rademacher (CWI), Rietkerk (Environmental Sciences, Utrecht) and van der Stelt (PhD student, CWI/UvA).

Applications to Energy Engineering
Development of a computational tool for the simulation of wind-farm aerodynamics (research carried out at both the Mathematical Institute, CWI and the Energy Research Center of the Netherlands).
The Dutch government plans that a significant portion of the Dutch future energy need is to be produced by wind farms at the North Sea. A wind farm is a large set of wind turbines positioned in some matrix form. Various research questions still exist with respect to wind farms; economical, ecological and technological. A major technological question is how to position and design the separate wind turbines, such that the energy production of the wind farm as a whole is maximal.
Investigation, with analytical and computational tools, of instabilities in tokamak plasmas, in which fusion of deuterium and tritium nuclei occurs. This research is done in cooperation with the FOM Institute for Plasma Physics, and is directed towards the ITER tokamak, which is currently under construction in Cadarache, France. The specific instabilities that are investigated are so-called edge localized modes, instabilities at the outer edge of the tokamak plasma, that show similarity with solar flares.

Lattice structure in partially ordered vector spaces
In most partially ordered vector spaces there is some natural lattice structure present, such as, for instance, disjointness of supports of functions. Such lattice structure is not captured by the rich theory of vector lattices, nor by the traditional theory of partially ordered vector spaces. It is the aim of the project to develop a theory on lattice structure in partially ordered vector spaces similar to the theory for vector lattices. A key technique is the use of the Riesz completion or, more generally, order dense embeddings in larger vector lattices. It is systematically investigated which intrinsically defined notions correspond to those of larger vector lattices and which properties can be established similar to the vector lattice case.

Dynamics of stochastic differential equations
If a deterministic dynamical system is perturbed by noise, it is important to know how its dynamic characteristics are changed by the noise. Persistence of stability is of particular interest. It is investigated under what conditions steady states of deterministic differential equations lead to stationary solutions, when the equation is perturbed by stochastic noise. The

research focusses on infinite dimensional equations such as delay equations and partial differential equations, nonlinearities, and noise driven by Levy processes.

Research results in 2011

Kalauch (Dresden), Lemmens (Canterbury) and van Gaans have shown that in finite dimensional partially vector ordered spaces with polyhedral cones the number of bands is bounded by a number only depending on the dimension of the space and that, consequently, the same number bounds the number of bands in any Archimedean finite dimensional partially ordered vector space with order unit. The number of bands can be strictly greater than in the vector lattice case.

Chen, van Gaans and Verduyn Lunel have established new criteria for stability of nonlinear neutral differential equations with variable delays by means of a fixed point technique.

P. Haccou c.s. further developed the "hazard rate" concept in the context of genetic introgression, adding more realistic genetical mechanisms. Furthermore, they developed methods to calculate the hazard rate of introgression for small populations. In addition, they examined the effect of random environmental fluctuations on the hazard rate.
They developed a model for bacterial sporulation, as a basis for examining the form of bet hedging strategies under different environmental conditions. It was found that the delay between the initiation of sporulation and the final time at which spores are completed plays a crucial role.

The stability of self-similar, radially symmetric blowup solutions of the Ginzburg-Landau equation (GL) for all dimensions $2<d<4$ has been studied by A. Doelman, V. Rottschäfer and the Ph.D. student M. van der Schans.
The previous study of stability with respect to radially symmetric perturbations has been extended to analysis of the linear stability with respect to non-radially symmetric perturbations.
The asymptotic construction of the solution and Evans function techniques are used to analyse the discrete spectrum. However, due to the nature of the solutions that were found in the asymptotic analysis, Evans function techniques are not directly applicable.

S.C. Hille continued his collaboration with the Plant BioDynamics Laboratory at the Institute of Biology Leiden (IBL) on mathematical modeling, analysis and simulation of auxin transport in Chara species and Arabidopsis thaliana (a.o. C.J.M. Boot, B. van Duijn,. K.J.M. Libbenga, R. Offringa and L.A. Peletier)

S.C. Hille collaborated with P. Haccou (CML, UL), M. Emmerich (LIACS, UL), L. Sella (UL) and the experimental microbiology group of O. Kuipers (RUG) in the interdisciplinary project "BetNet" within NWO's Computational Life Science programme. The project concerns (a.o.) the mathematical modeling and analysis of stochastic effects in part of the sporulation signaling and regulatory network of Bacillus subtilis. A stochastic simulation and optimisation tool have been developed. The project ended October 2011.

O. van Gaans, S.C. Hille and T.S.O. Alkurdi work on existence, uniqueness and asymptotic stability of invariant measures associated to dynamical systems perturbed by stochastic interventions at discrete time points.

S.C. Hille collaborates with J. Dubbeldam (TUD) on the effects of stochasticity in signal and chemical dynamics on signal detection and transduction for G-protein coupled receptors, using analysis and stochastic simulations.

S.C. Hille started a new collaboration with A. Muntean (TU Eindhoven) on a measure-valued formulation of models for crowd dynamics, including boundary conditions.

M. de Jeu continued his collaboration with J. Tomiyama (Tokyo) and obtained several results on spectral synthesis for the involutive Banach algebra associated with a dynamical system.

M. de Jeu and M. Wortel studied positive representations of compact groups in Banach lattices. Amongst others, a decomposition into order irreducibles was established for Banach sequence spaces that parallels the classical result for unitary representations in Hilbert spaces.

M. de Jeu and M. Messerschmidt continued the earlier investigations of crossed products of Banach algebras already done in the group. They showed that L_1-algebras and Beurling algebras are crossed products and that Johnson's classical result on the relation between G-bimodules and $L_1(G)$-bimodules is a special cases of the general bijection theorem for crossed products of Banach algebras. First steps were made to take this into an ordered context.

Research Programme 2.2: Probability Theory
Programme leader: W.Th.F. den Hollander

Description of the project

The research in **Probability Theory** concentrated on interacting stochastic systems. Such systems consist of a large number of interacting random components that interact with each other and with their environment. The interaction is typically local, and may be either deterministic or random. The latter occurs in systems with disorder.

Even when the interaction is local, interacting stochastic systems typically exhibit a complex global behavior, with a long-rang dependence resulting in anomalous fluctuations and phase transitions. To mathematically understand these systems requires the use of powerful probabilistic ideas and techniques. The challenge is to introduce simple models, which serve as paradigms, and to unravel the complex random spatial structures arising in these models. Statistical physics and ergodic theory provide the conceptual ideas, while probability theory provides the mathematical language and framework. The important challenge is to give a precise mathematical treatment of the physics that arises from the underlying complexity.

Much of the knowledge that has been built up in mathematical statistical physics over the past decades is currently making its way into biology. One of the tasks is to help facilitate this cross-fertilization and to address concrete biological questions at the interface. Examples are coming from population genetics, and immune system biology.

The research focused on phase transitions (percolation, random polymers, random walks in dynamic random environments, parabolic Anderson model, porous media, meta-stability), ergodic properties of random processes (dynamical Gibbs-non-Gibbs transitions, hidden Markov chains), and topics from mathematical biology (population dynamics). Key tools were large deviation theory, stochastic analysis, variational calculus and combinatorics.

There is an interesting link between algebraic dynamical systems and solvable models of statistical mechanics. It turns out that entropies of apparently different systems often coincide, and that this coincidence is not accidental. It is also interesting to understand whether the probabilistic properties of these systems are related.

Research aims at providing an explanation for this phenomenon. A powerful combinatorial technique to study high-dimensional systems is the lace expansion. The aim is to obtain a rigorous understanding of phase transitions in high dimensions, including diffusion on critical spatial structures.

The research in **Operations Research** concentrated on Markov chains, Markov decision processes and Markov games, with applications to problems in stochastic networks, in particular, queueing control models and inventory control.

One of the main issues concerns stability. How can stability be checked? If stable, how fast does the network reach its stationary distribution? If unstable, what does the quasi-stationary distribution look like? How can efficient algorithms be developed to control the network according to certain pre-set optimisation criteria? Are these algorithms amenable to practical implementation? What can one say about the structure of optimal policies? Which type of customer should be prioritised to optimise network performance? How to choose the optimal

re-order point and optimal order quantity in a single product inventory model? These questions are studied within the framework of Markov chain theory.

Often the situation arises where there are conflicting interests, for instance, maximizing server efficiency while minimizing customer dissatisfaction. This may be studied through Markov game models.

Research results in 2011
In 2011 F. den Hollander worked on the following projects:

With F.R. Nardi (Eindhoven) and A. Troiani: Metastability and nucleation for a two-dimensional lattice gas consisting of two types of particles subject to Kawasaki dynamics.

With R. dos Santos: Random walk on top of a supercritical contact process.

With R. Fernandez (Utrecht) and J. Martinez: Dynamical Gibbs-non-Gibbs transitions for the Curie-Weiss model.

With D. Erhard and G. Maillard (Marseille): Quenched Lyapunov exponents and intermittency for the Parabolic Anderson Model in a dynamic random environment.

With E. Bolthausen (Zürich) and A. Opoku: Variational characterization of the free energy of a copolymer chain near a selective interface.

With J. Goodman: Large deviations for the inradius of the complement of a Brownian motion on a torus.

With A. Greven (Erlangen), S. Kliem (Essen) and A. Klimovsky (EURANDOM): Renormalization of hierarchically interacting Cannings processes.

With A. Gaudillière (Marseille), F.R. Nardi (Eindhoven), E. Olivieri (Rome) and E. Scoppola (Rome): Metastability and nucleation for the two-dimensional lattice gas subject to Kawasaki dynamics in large volumes.

With N. Pétrélis (Nantes): Free energy of a copolymer in a micro-emulsion.

With M. Birkner (Mainz): Scaling behavior of random polymers near random interfaces.

With A. Bovier (Bonn): Preparation of a monograph "Metastability - a Potential-Theoretic Approach".

In 2011 F. Spieksma worked on the following projects:

Stability conditions for parametrised collections of Markov processes.

With S. Bhulai (VU): Structural properties of the value function in Markovian control problems. Resource allocation in synchronised queueing models.

With M. Katehakis (Newark, USA): Lumping method in optimal control of single-product inventory models.

In 2011 E. Verbitskiy worked on the following projects:

Renormalization of Gibbs measures in one dimension.

With D. Lind (Seattle) and K. Schmidt (Vienna): Entropy and growth rate of periodic points of algebraic Zd-actions.

With M. Goll (Leiden) and K. Schmidt (Vienna): Correspondence between solvable and algebraic lattice systems.

With R. Fernandez (Utrecht): Cluster expansions and hidden Markov processes

In 2011 M. Heydenreich worked on the following projects:

With R. van der Hofstad (Eindhoven), T. Hulshof (Eindhoven), G. Miermont (Orsay): Scaling limits of high-dimensional incipient infinite clusters.
Random walk on the incipient infinite cluster.

With J. van den Berg (CWI) and J. Björnborg (Uppsala): A probabilistic model related to vegetation patterns and desertification.

With D. Kiss (CWI): Backbone density of high-dimensional percolation.

With N. Berger (Jerusalem): Diffusion constant of random walk on supercritical percolation clusters.

With R. Meester (VU): Poisson Matching.

Research Programme 2.3: Mathematical and Applied Statistics
Programme leader: R.D. Gill

Description of the project

Statistics is the art of drawing conclusions about phenomena in which chance plays a role. Randomness may arise through a variety of reasons: the intrinsic random nature of a phenomenon, unavoidable noise in an experiment, conscious randomization of experimental or measurement units, or as a best approximation to reality. Chance phenomena occur in a broad range of situations. This has rendered Statistical Science a highly multidisciplinary undertaking, but with a core body of concepts and methods that are common to the diverse applications. In the stochastics group at MI we concentrate on a few of the many strands in Statistical Science. Those chosen have in common that they represent areas of rapid development and strong relevance to science and society, and have substantial and challenging mathematical components. These are: forensic statistics; high throughput "omics" data; statistical and machine learning; and quantum statistics.

Forensic statistics is developing into a field of statistics with a rather special flavour, where neither classical frequentist nor classical Bayesian approaches fit the need to communicate the weight of evidence of some crime-related findings to a judge or jury. The focus lies on the likelihood ratio, and in the cases that the statistical analysis is really significant, this involves extrapolation into the tails of distributions, small data sets, and unreliable modeling. A particular example is given by estimating the probability of a random match of a DNA profile. Here the research relies also on statistical genetics and the probability models used in that area.

Development and applications of multivariate analysis/statistical learning techniques have especially been directed toward the field of systems biology, particularly genomics, transcriptomics, proteomics and metabolomics, where there is a high demand for data analysis techniques for high-volume data sets. These high-throughput "omics" data can be characterized as consisting of few objects compared to very many variables. Objects (e.g., patients) may cluster on small subsets of variables (e.g., measurements obtained by LC-mass spectrometry). Other interest is in the structure of fluorescence intensity data of SNP arrays. Modeling of this structure may result in parameter estimates that can be used to improve the results of "calling algorithms" that assign alleles to one of three genotypes.

In statistical learning/machine learning one deals with data arising from complex, often ill-understood phenomena. The aim is to find patterns in such data, and use these to predict future data, based on robust methods that make only few assumptions. Such methods can be very different in nature: they include structural risk minimization for classification and regression, but also nonparametric Bayesian methods. One may also use more traditional unions of parametric models combined with model selection and/or averaging procedures and analyze their behaviour under the assumption that they are all wrong, yet still useful in prediction. The research concerns both theoretical analysis of such methods and development of new, practical methods that combine the advantages of several existing ones.

Quantum statistics refers to the role of statistical inference for data on measurements from quantum systems. This field is making a rapid transition from a theoretical academic exercise to the laboratory and beyond, to technology, fueled by the rise of quantum information and quantum communication.

Research results in 2011

Part of the research time of R. Gill at Netherlands Institute of Advanced Studies was devoted to problems of communicating results from statistics and probability to non-specialists, whether in a professional context (e.g., when a forensic statistician gives advice in a police investigation or a court case) or in public outreach. This led to original new research results on some classical probability puzzles: the Monty Hall problem (three door problem, quizmaster problem) and the Two Envelope Problem (exchange problem). A journal article appeared in Statistica Neerlandica on the three doors problem, as well as invited contributions on the problem to two encylopaedia projects (one an encyclopaedia on statistical science published by Springer). The workshop he organized at the Lorentz Center as part of his distinguished Lorentz Fellowship also addressed these problems and resulted in a "state of the art" paper which has been submitted for publication in an interdisciplinary forensic science journal.

In 2011, P. Grünwald continued work with W. Kotlowski on the behaviour of ML estimators for exponential families when the models are wrong. He also continued work on his VICI project "safe statistics", leading to a publication at the annual COLT (Conference on Learning Theory) on "safe learning" and (jointly with T. van Erven, W. Koolen and S. de Rooij) at the prestigious NIPS conference on "adaptive hedging". Both publications are about "learning the learning rate", the parameter which determines the level of conservativeness of Bayesian-style learning algorithms.

In 2011 J. J. Meulman worked on the following projects:

With J. Friedman (Stanford) on multiple regression with multiple outcomes.

With A. van der Kooij (FSW) on regularized multiple regression with optimal scaling.

With S. Amodio and R. Siciliano (Naples) on generalized boosted additive models.

With R. Rippe (Leiden UMC) and P. Eilers (Erasmus MC): Advanced statistical tools for SNP arrays, including signal calibration, copy number estimation, and single array genotyping.

With H. Draisma (VU), Th. Hankemeier (LACDR) and D. Boomsma (VU) on hierarchical clustering analysis of blood plasma lipidomics profiles from mono- and dizygotic twin families.

With H. van Wietmarschen (LACDR), A. van der Kooij (FSW) and J. van der Greef (TNO) on characterization of rheumatoid arthritis sub-types using symptom profiles, clinical chemistry and metabolomics measurements.

Project Mathematics, Computer Science and Society
Project leader: F.A.J. Birrer

Description of the project
Research area:
Mathematics & Society, Computer Science/Chemistry/Science & Society.
Mission/themes:
Understanding and supporting argumentative, procedural and ethical quality in societal debate, deliberation and decision making that relate to (or draw upon) science and technology, particularly information technology, mathematical models and statistics, environmental issues and biotechnology

Research results in 2011
The work with W. Mensink was finished, resulting in his PhD thesis on innovation in health care, successfully defended in December. A start was made with the construction of a political analysis framework that fits with the framework elements developed earlier

Kloosterman Professor

In 1986 the Mathematical Institute established a visiting professorship in Mathematics, for two months a year, called the Kloosterman Chair. Hendrik Douwe Kloosterman was born on April 9, 1900. After studying in Leiden, Copenhagen, Oxford, Göttingen and Hamburg, he was appointed "lector" in Leiden in 1930 and full professor in 1947. He died on May 6, 1968. He is mostly known for his work in analytic number theory on what we now call "Kloosterman sums".

The Kloosterman professor of 2011 was Jean-Louis Colliot-Thélène, from the University of Paris-sud in Orsay (CNRS), invited by B. Edixhoven. He visited the Mathematical Institute during the months of March and April.

Jean-Louis Colliot-Thélène is one of the main authorities on questions involving algebraic geometry and number theory, aimed at the study of rational points on algebraic varieties. His scientific career started in 1968, in Paris, when algebraic geometry was going through a revolution. He has obtained many important deep results in various areas, including K-theory, Chow groups, algebraic groups and torsors, and the arithmetic of varieties in general.

He has received many awards and invitations to give distinguished lectures, including:

Médaille Albert Châtelet (1980),
Prix de l'Académie des Sciences (Charles-Louis de Saulses de Freycinet, 1985),
Prix Fermat de Recherche en Mathématique (1991),
Grand Prix Léonid Frank de l'Académie des Sciences de Paris (2009),
International Congress of Mathematicians, Berkeley (1986),
Sackler distinguished lectures, Tel Aviv (2003).

He has been a long-term visitor at various highly-regarded institutions around the world.

During his visit, Colliot-Thélène has given four lectures of two hours each on the Hasse principle in the Number Theory Intercity Seminar in Amsterdam (VU), Leiden, and Groningen, as well as the traditional Kloosterman colloquium lecture in Leiden on sums of squares.

In Leiden, he has had much interaction in the form of lively discussions with many members of the Geometry, Algebra, and Number Theory group, and in particular with the local PhD students.

International and National Programmes

***International Programmes**:*

Erasmus Mundus Master and Doc programs Algebra, Geometry and Number Theory
2010-2015
Cooperation with Bordeaux and Padova and Orsay, Milano, Stellenbosch and Montreal.
See: www.math.u-bordeaux1.fr/ALGANT/
Coordinators: P. Stevenhagen, S.J. Edixhoven.

ERC grant: Variational Approach to Interacting Stochastic Systems
2011-2015
Project leader: W.Th.F. den Hollander.

Long term collaboration with Tokyo Metropolitan University in the project Algebras associated with dynamical systems. The collaboration is supported by an NWO visitor's grant for Prof.Em. J. Tomiyama
Coordinator: M.F.E. de Jeu.

FOM Programme Active Control of Magneto-hydrodynamic modes in Burning Plasmas
B. Koren (co-leader).

Multivariate clustering in high-volume data sets
With Jerome H. Friedman, Stanford University
Project leader: J.J. Meulman.

Development of user-friendly software for nonlinear multivariate data analysis by optimal scaling transformations
With SPSS Inc, Chicago
Project leader: J.J. Meulman.

PASCAL2 (European Network of Excellence)
2008-2012
Project leaders: P. Grünwald and J.J. Meulman.

Erasmus programme Bilateral Agreement with Universita degli Studi di Padova
Project leader: J.J. Meulman.

NWO-EW programme "Forensic Science"
Project member: R.D. Gill.

***National Programmes**:*

NWO cluster: Discrete, interactive & algorithmic mathematics, algebra and number theory. (DIAMANT)
Project leader: P.Stevenhagen.

NWO VICI-premie: The Mathematics of Secure Computation
1/4/2007-1/4/2013
Project leader: R. Cramer.

NWO Vrije Competitie Quantum Cryptography
2008-2012
Project leaders: Fehr and Cramer, Bouman (PhD student).

NWO Vrije Competitie project: Banach algebra dynamical systems and positivity
1/9/2009-1/9/2013
Project leader: M. de Jeu.

NWO VENI-project Special Values and t-Motives
July 2010-July 2013
Project leader: L. Taelman.

NWO Veni-grant: Random spatial models at the critical point
2011-2014
Project leader: M. Heydenreich.

NWO Veni-project Multifractal analysis of Bernoulli convolutions through beta-expansions
1/12/2011-1/12/2015
Projectleader: C.C.C.J. Kalle.

NWO VIDI-premie: Formation of singularities in natural systems
1/1/2007-1/1/2012
Project leader: V. Rottschäfer.

NWO VICI Project Safe Statistics
1/7/2010 - 1/7/2015
Project Leader: P. Grünwald.

Participation in the national stochastics cluster STAR: Stochastics - Theoretical and Applied Research
2009-2011
Project leader: W.Th.F. den Hollander.

Random Polymers
2010-2011
Project leader: W.Th.F. den Hollander with V. Sidoravicius.

Variational characterization of copolymers near selective interfaces
2010-2012
Project leader: W.Th.F. den Hollander with V. Sidoravicius.

The Plant BioDynamics Laboratory (PBDL)
Cooperation with the Institute for Biology Leiden (IBL)
Project leader: L.A. Peletier.

Critical transitions and early-warning signals in spatial ecosystems
Cooperation between A. Doelman, J. Rademacher (CWI) and M. Rietkerk (Environmental Sciences, Utrecht).

NWO programme ‘ERGO’ project: Quantifying introgression risks of transgenes with hazard rates, using carrot as a model species

2008-2012
Collaboration with CML and IBL (Leiden university)
Project leader: P. Haccou.

NWO programme “CLS” project: The evolution of stochastic heterogeneous networks as bet-hedging adaptations to fluctuating environments
2009-2011
Collaboration with CML and LIACS (Leiden university) and Groningen Biomolecular Sciences and Biotechnology Institute (University of Groningen)
Project leader: P. Haccou.

Development and application of statistical learning techniques for biomedical high-volume data sets. With Th. Hankemeier, LACDR (Leiden-Amsterdam Center for Drug Research) and Metabolomics Center, Leiden, J. van der Greef, TNO Quality of Life, Zeist, and D. Boomsma, Department of Biological Psychology, VU University Amsterdam. Sponsored by NDNS+ (NWO)
Project leader: J.J. Meulman.

Glucose modeling in patients with diabetes and critically-ill patients
joint with AMC (UvA), UMCG (RuG)
Project leader: E. Verbitskiy.

Master Theses

J. J. van Wamelen
title: Bayesian Networks in Forensic DNA Analysis
advisor: Prof. dr. R.D. Gill
date: 18-01-2011

A.K.A. Kalsbeek
title: Continuous-time GARCH(1,1) processes
advisor: Dr. O. van Gaans
date: 21-01-2011

T. van Ommen
title: Combining predictions from linear models using the switch distribution
advisor: Prof. Dr. P. Grünwald
date: 10-03-2011

J. Rozendaal
title: Decomposing positive representations in L^p-spaces for Polish transformation groups
advisor: Dr. M.F.E. de Jeu
date: 26-04-2011

W. Ellens
title: Effective resistance
advisor: Dr. F.M. Spieksma
date: 29-04-2011

F.H.S. Offergelt
title: SAPHYRE Cooperation among competitors
advisor: Dr. F.M. Spieksma
date: 01-07-2011

S.D. Ramawadh
title: Symbolic dynamics of β-expansions in negative base
advisors: Dr. K. Dajani & Dr. M.F.E. de Jeu
date: 19-08-2011

S. Ding
title: Multi-class fork-join queues & the stochastic knapsack problem
advisor: Dr. F.M. Spieksma
date: 26-08-2011

F.W. van Rest
title: Advance appointment booking in chemotherapy
advisor: Dr. F.M. Spieksma
date: 26-08-2011

Y. Achnine
title: On the main conjecture on algebraic-geometric MDS codes
advisor: Dr. R.S. de Jong
date: 29-08-2011

L.C. Smit
title: Efficient Computations for a Class of Markov Chains and Related Applications
advisor: Dr. F.M. Spieksma
date: 30-08-2011

E.P.J.A. Siero
title: A H2 well-posedness result for second order quasilinear parabolic PDE's on the real line with an application to a generalisation of the Gray-Scott model
advisor: Dr. J. Rademacher
date: 01-09-2011

R.H. Eggermont
title: Generalizations of a theorem by Brauer and Nesbitt
advisor: Prof. Dr. H.W. Lenstra
date: 26-09-2011

M. Fung
title: Lovász number of the Keller graphs
advisor: Dr. D. Gijswijt & Dr. F.M. Spieksma
date: 29-09-2011

S.L. van Lieshout
title: Δ-normality versus functional-Δ-normality
advisor: Dr. K.P. Hart
date: 07-10-2011

M.M.D. Kampert
title: Statistical analysis in genome-wide association studies on genotype imputed family data: a research strategy to compare various toolsets
advisor: Prof.Dr. J.J. Meulman
date: 27-10-2011

J. Jin
title: Point counting formulae on universal elliptic curves
advisor: Prof. Dr. S.J. Edixhoven
date: 19-12-2011

ALGANT Master Theses

The ALGANT MASTER is a two-year master programme in pure mathematics, with a strong emphasis on Algebra, Geometry and Number Theory. It has been offered since September 2005, and it involves the partner universities of Bordeaux (France), Leiden (Holland), Milano (Italy), Padova (Italy) and Paris-Sud (France). It is a European Erasmus Mundus Master and provides European Community grants to students from non-EC-countries.

Every student participating in the Algant Master studies one year each in TWO of the four partner universities. At the end of the second year, the student defends a master thesis and is awarded the Algant master diploma in an Algant Graduation Ceremony.

Davide Calliari
title: Reconstruction of Cubic Surfaces
thesis advisors: Dr. R.S. de Jong, Dr. R.M. van Luijk
date: 7-7-2011

Alfonso Cevallos Manzano
title: Reducing the Share Size in Robust Secret Sharing
thesis advisors: Prof.dr. R.J.F. Cramer (CWI & UL), S. Fehr (CWI)
date: 18-10-2011

Oliver Lenz,
title: The classifying space of a monoid
thesis advisor: L. Taelman
date: 20-12-2011

Weidong Zhuang
title: HASSE-WEIL zeta-function in a special case
thesis advisor: Prof.dr. M. Harris
date: 8-7-2011

PhD Theses

I. Stojković April 19, 2011	Geometric approach to evolution problems in metric spaces Thesis advisor: prof.dr. S.M. Verduyn Lunel Leiden University
H. Draisma May 10, 2011	Analysis of Metabolomics data from twin studies Thesis advisor: Prof.dr.J.J.Meulman Leiden University
A. Stolk June 15, 2011	Discrete tomography for integer-valued functions Thesis advisor: prof.dr. S.J. Edixhoven Leiden University
B.E. van Dalen September 20, 2011	Discrete tomography with two directions Thesis advisor: prof.dr. R. Tijdeman, prof.dr. K.J. Batenburg Leiden University
K. Vafayi December 13, 2011	Duality, bosonic particle systems and some exactly solvable models of non-equilibrium Thesis advisor: prof.dr. F. Redig, prof.dr. F. den Hollander Leiden University
E.T. Torreão Dassen December 20, 2011	Basis reduction for layered lattices Thesis advisor: prof.dr. H.W. Lenstra Leiden University

Publications

1. Number theory, Algebra and Geometry

1.1 Number Theory and Algebra

Papers in Journals and Proceedings

Batenburg, K., Fortes, W., Hajdu, L., Tijdeman, R., Bounds on the difference between reconstructions in binary tomography, *LNCS 6607 (2011), 369-380.*

Cascudo, I., Cramer, R., Xing, C., The Torsion-Limit for Algebraic Function Fields and its Application to Arithmetic Secret Sharing, *Proceedings of 31st Annual IACR CRYPTO (2011), Santa Barbara, Ca., USA, Springer Verlag, LNCS Vol. 6841, 685-705.*

Dalen, B.E. van, Boundary length of reconstructions in discrete tomography, *SIAM Journal of Discrete Mathematics 25 (2011), 645-659.*

Győry, K., Hajdu, L., Tijdeman, R., Irreducibility criteria of Schur-type and Polya-type, *Monatsh. Math. 163 (2011), 415-443.*

L. Hajdu, R. Tijdeman, Representing integers as linear combinations of powers, *Publ. Math. Debrecen 79 (2011), 461-468.*

Hitt, L., McGuire, G., Naehrig, M., Streng, T.C., A CM construction for curves of genus 2 with p-rank 1, *Journal of Number Theory 131 (5) (2011), 920-935.*

Luijk, R.M. van, Wehler K3 surfaces with Picard number 3 and 4. Appendix to: "Orbits of points on certain K3 surfaces", by Arthur Baragar, in: *Journal of Number Theory 131 (3) (2011), 600-603.*

Luijk, R.M. van, Cubic points on cubic curves and the Brauer-Manin obstruction on K3 surfaces in: *Acta Arithmetica 146 (2) (2011), 153-172.*

Luijk, R. van, Macasieb, M., Petersen, K., On character varieties on two-bridge knot groups, *Proc. London Math. Soc. (2) 103 (2011), 473-507.*

Luca, F., Najman, F., On the largest prime factor of x^2-1, *Math. Comp. 80 (2011), 429-435*. Tables: odd solutions, even solutions.

Najman, F., Torsion of elliptic curves over cyclotomic quadratic fields, *Math. J. Okayama Univ. 53 (2011), 75-82.*

Najman, F., Large strings of consecutive smooth integers, *Archiv der Mathematik 97 (4) (2011), 319-324.*

Salgado Guimaraes de Silva, C., On the rank of the fibers of elliptic K3 surfaces, *Bulletin of the Brazilian Math. Soc. New Series 42 (4)(2011), 1-10.*

Smit, B. de, Gornet, R., Sutton, C.J., Isospectral surfaces with distinct covering spectra via Cayley Graphs, *Geometriae Dedicata ("Online first" July 13, 2011).*

PhD Thesis

B.E. van Dalen, Discrete tomography with two directions, defended on September 20.

E.T. Torreão Dassen, Basis reduction for layered lattices, defended on December 20.

Other publications

Borger, J., Smit, B. de, Lambda actions of rings of integers, *arXiv:1105.4662*

Bartel, A., Smit, B. de, Index formulae for integral Galois modules, *arXiv:1105.3876 [pdf, ps, other]*.

Evertse, J.-H., A survey on monogenic orders, special volume in honour of the 70th birthday of K. Győry and A. Sarkőzy and the 60th birthday of A. Pethő and J. Pintz, *Publ. Math. Debrecen 79 (2011), 411-422.*

Lenstra Jr, H.W., Moree, P., Stevenhagen, P., Character sums for primitive root densities, math > arXiv:1112.4816

1.2 Arithmetic Geometry

Papers in Journals and Proceedings
Jong, R.S. de, One half log discriminant and division polynomials, *Archiv der Mathematik 97 (2011), 251-257.*
Jong, R.S. de, Symmetric roots and admissible pairing, *Transactions of the AMS* 363 (2011), 4263-4283.
Jong, R.S. de, Edixhoven, S.J., Short introduction to heights and Arakelov theory, In: *J.-M. Couveignes, J.S. Edixhoven (eds.), Computational aspects of Modular Forms and Galois Representations. Annals of Mathematics Studies 176, Princeton University Press 2011.*
Jong, R.S. de, Edixhoven, S.J., Applying Arakelov theory, In: *J.-M. Couveignes, J.S. Edixhoven (eds.), Computational aspects of Modular Forms and Galois Representations. Annals of Mathematics Studies 176, Princeton University Press 2011.*
Jong, R.S. de, Edixhoven, S.J., Bounds for Arakelov invariants of modular curves, In: *J.-M. Couveignes, J.S.. Edixhoven (eds.), Computational aspects of Modular Forms and Galois Representations. Annals of Mathematics Studies 176, Princeton University Press 2011.*
Taelman, L.D.J., The Carlitz shtuka, *Journal of Number Theory 131(3)(2011), 410-418.*

PhD Thesis
A. Stolk, Discrete tomography for integer-valued functions, defended on June 15.

Other publications
Edixhoven, S.J., Appendix to “Special points and Poincaré bi-extensions” by Daniel Bertrand, arXiv:1104.5178
Edixhoven, S.J., Snelle algoritmen in de getaltheorie, Vakantiecursus voor leraren, CWI, August 26.
Edixhoven, S.J., Représentations galoisiennes et théorème de Fermat-Wiles, Text for the commemoration of the bicentenary of Galois' birth, November, IHP, Paris.

Books
Edixhoven, S.J., Computational aspects of modular forms and Galois representations. Edited with J-M. Couveignes, and with contributions by Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong, and Franz Merkl, Volume 176 of Annals of Mathematics Studies, Princeton University Press, 2011.

2. Analysis and Stochastics

2.1 Analysis and Dynamical Systems

Papers in Journals and Proceedings
Ahlström, C., Peletier, L.A., Jansson-Löfmark, R., Gabrielsson, J., Feedback modeling of non-esterified fatty acids in rats after nicotinic acid infusions, *J. Pharmacokinet Pharmacodyn 38 (1) (2011), 1-24.*
Ahlström, C., Peletier, L.A., Gabrielsson, J., Quantitative analysis of rate and extent of tolerance of biomarkers: Application to nicotinic acid-induced changes in non-esterified fatty acids in rats, *European Journal of Pharmaceutical Sciences (2011) (digitaal verschenen).*

Chen, G., Asymptotic behavior of solutions to a class of linear non-autonomous neutral delay differential equations, *Electronic Journal of Differential Equations 2011(85) (2011), 1-7.*
De Jong, I.G., Haccou, P., Kuipers, O.P., Bet hedging or not? A guide to proper classification of microbial survival strategies, *Bioessays 33 (2011), 215-223.*
Hassen, Y., Koren, B., A two-dimensional embedded-boundary method for convection problems with moving boundaries, *Proceedings Sixth International Conference on Computational Fluid Dynamics, St. Petersburg, 2010, (A. Kuzmin, ed.), Springer, Berlin (2011), 613-620.*
Haverkort, J.W., Blank, H.J. de, Koren, B., Low-frequency Alfven gap modes in rotating tokamak plasmas, *Plasma Physics and Controlled Fusion 53(2011), 1-10.*
Heijster, P.J.A. van, Doelman, A., Kaper T.J., Nishiura, Y., Ueda, K.-I., Pinned fronts in heterogeneous media of jump type, *Nonlinearity 24 (2011), 127.*
Hundsdorfer, W., Spijker, M.N., Boundedness and strong stability of Runge-Kutta methods, *Math. Comp. 80(2011), 863-886.*
Hundsdorfer, W., Mozartova, A., Spijker, M.N., Special boundedness properties in numerical initial value problems, *BIT Numerical Mathematics 51(2011), 909-936.*
Klebaner, F.C., Sagitov, S., Vatutin, V.A., Haccou, P., Jagers, P., Stochasticity in the adaptive dynamics of evolution: the bare bones, *Journal of Biological Dynamics 5(2011),147-162.*
Sanderse, B., Pijl, S.P. van der, Koren, B., Review of computational fluid dynamics for wind turbine wake aerodynamics, *Wind Energy 14(2011), 799-819.*
Schmidt, S., Post, T.M., Peletier, L.A., Boroujerdi, M.A., Danhof, M., Coping with time scales in disease systems analysis: application to bone remodeling, *J. Pharmacokinet Pharmacodyn 38 (2011), 873-900.*
Stojković, I., van Gaans, O., Invariant measures and a stability theorem for locally Lipschitz stochastic delay equations, *Ann. Inst. Henri Poincaré Probab. Stat. 47 (2011) (4), 1121-1146.*
Wackers, J., Koren, B., Raven, H.C., Ploeg, A. van der, Starke, A.R., Deng, G.B., Queutey, P., Visonneau, M., Hino, T., Ohashi, K., Free-surface viscous flow solution methods for ship hydrodynamics, *Archives of Computational Methods in Engineering 18(2011), 1-41.*
Worm, D.T.H., Hille, S.C., Ergodic decompositions associated to regular Markov operators on Polish spaces, *Ergodic Theory and Dynamical Systems 31 (2)(2011), 571-597.*
Worm, D.T.H., Hille, S.C., An ergodic decomposition defined by regular jointly measurable Markov semigroups on polish spaces, *Acta Appl. Math. 116 (2011), 27-53.*
Zagaris, A., Doelman, A., Emergence of steady and oscillatory localized structures in a phytoplankton-nutrient model, *Nonlinearity 24 (2011), 3437-3486.*

PhD Thesis
I. Stojković, Geometric approach to evolution problems in metric spaces, defended on April 19.

Other Publications
Dijk, G. van, Leidse hoogleraren Wiskunde 1575 - 1975, Leiden, Mathematisch Instituut, 2011.
Dijk, G. van, Very elementary introduction to representation theory, *Lecture Notes, Kyushu University (Japan), 2011.*
Frank, J., Hundsdorfer, W., Koren, B., In memoriam Jan Verwer (1946-2011). “Een dag zonder fouten is een dag zonder wiskunde”, *Nieuw Archief voor Wiskunde 59(2011), 91-93.*
Koren, B., Recht door zee, *In Jan Karel Lenstra, the Traveling Science Man, CWI, Amsterdam (2011), 117-119.*

Books
M. van der Heijden, B. Koren, R. van der Mei and C. van Vonderen (eds.), Jan Karel Lenstra,

the Traveling Science Man, *CWI, Amsterdam (2011), ISBN 978 90 6196 559 6, (274 pages).*
Koren, B., Numerieke wiskunde: wetenschap en gereedschap, oratie, Universiteit Leiden (2011).

2.2 Probability Theory

Papers in Journals and Proceedings
Avena, L., Hollander, F. den, Redig, F., Law of large numbers for a class of random walks in dynamic random environments, *Electronic Journal of Probability 16 (2011) 587-617.*
Birkner, M., Greven, A., Hollander, F. den, Collision local time of transient random walks and intermediate phases in interacting stochastic systems, *Electronic Journal of Probability 16 (2011), 552-586.*
Blachère, S. , Hollander, F den, Steif, J.E., A crossover for the bad configurations of random walk in random scenery, *Annals of Probability 39 (2011) 2018-2041.*
Bon, A.C. van, Verbitskiy, E.A., Basum, G. van, Hoekstra, J.B.L., DeVries, J.H., Exercise in closed-loop control: A major hurdle, *Journal of Diabetes Science and Technology 5 (November 2011), (6), 1337-1341.*
Brinker, A.C. den, Krishnamoorthi, H., Verbitskiy, E.A., Similarities and Differences Between Warped Linear Prediction and Laguerre Linear Prediction, *IEEE Audio, Speech, and Language Processing 19 (1), 24-33.*
Heydenreich, M., Hofstad, R. van der, Random graph asymptotics on high-dimensional tori. II. Volume, diameter and mixing time, *Probability Theory and Related Fields 149 (3-4) (2011), 397-415.*
Heydenreich, M., Long-range self-avoiding walk converges to alpha-stable processes, *Annales de l'Institut Henri Poincaré (B) Probabilités et Statistiques 47 (1), 20-42 (2011).*
Hollander, F. den, Nardi, F.R., Troiani, A., Kawasaki dynamics with two types of particles: stable/metastable configurations and communication heights, *Journal of Statistical Physics 145 (2011) 1423-1457.*
Kallenberg, L.C.M., Derman's book as inspiration: some results on linear programming for Markov decision problems, *Annals of Operations Reseach, (On-line first by Digital Object Identifier 10.1007/s10479-011-1047-4).*
Schmidt, K., Verbitskiy, E.A., New directions in algebraic dynamical systems, *Regul. Chaotic Dyn. 16 (2011) (1-2), 79-89.*
Škoric, B., Obi, C.,Verbitskiy, E.A., Schoenmakers, B., Sharp lower bounds on the extractable randomness from non-uniform sources, *Information and Computation 209 (8)(2011), 1184-1196.*
Spieksma, F.M., Ellens, W., Mieghem, P. van, Jamakovic, A., Kooij, R.E., Effective graph resistance, *Linear Anal. Applic. 435 (2011), 2491-2506.*
Verbitskiy, E.A., On factors of measures, *Indagationes Mathematicae 22 (2011), (3- 4), 315-329,* Devoted to: Floris Takens (1940-2010).
Verbitskiy, E.A., Thermodynamics of Hidden Markov Processes, in: Entropy of Hidden Markov Processes and Connections to Dynamical Systems, *B. Marcus, K. Petersen, T. Weissman (eds.), Cambridge University Press, London Mathematical Society Lecture Note Series 385, 258-272.*

Other Publications
Spieksma, F.M., Spelen met Intuitie. Voorbeelden uit de Mathematische Besliskunde, *Eureka! 34 (2011), 19-21.*

PhD Thesis
K. Vafayi, Duality, bosonic particle systems and some exactly solvable models of non-equilibrium, defended on December 13.

2.3 Mathematical and Applied Statistics

Papers in journals and proceedings
Erven, T. van, Grünwald, P.D., Koolen, W., Rooij, S. de, Adaptive Hedge,. *Advances in Neural Information Processing Systems 24 (NIPS 2011), 1656-1664, Granada, Spain.*
Gill,R.D., Keiding,N., Product-limit estimators of the gap time distribution of a renewal process under different sampling patterns, *Lifetime Data Analysis 16 (4)(2010), 571-579.*
Gill,R.D., The Monty Hall problem is not a probability puzzle (It's a challenge in mathematical modelling), *Statistica Neerlandica 65 (1)(2011), 58-71.*
Gill,R.D., Monty Hall Problem: solution, *In: International Encylopedia of Statistical Science, Lovric, M.(ed.), Springer, New York (2011), 858-863.*
Grünwald, P.D., Safe Learning: bridging the gap between Bayes, MDL and statistical learning theory via empirical convexity, *Proceedings of the 24th Conference on Learning Theory (COLT 2011), 551-573, Budapest 2011.*
Grünwald, P.D., Halpern, J.Y., Making decisions using sets of probabilities: Updating, time consistency, and calibration, *Journal of Artificial Intelligence Research (JAIR) 42(2011),393-426.*
Hindriks, R., Bijma, F., Dijk, B.W. van, Stam, C.J., Werf, Y. van der, Someren, E. van, Munck, J. de, Vaart, A.W. van der, Uncovering neuronal synchronization mechanisms from oscillatory data, *Human Brain Mapping 32 (2011), 1161-1178.*
Hindriks, R., Bijma, F., Dijk, B. van, Werf, Y. van der, Someren, E.J.W. van, Vaart, A.W. van der, Zanten, J.H. van, Information rates of nonparametric Gaussian process methods, *Journal of Machine Learning Research 12 (2011), 2095-2119.*
Hindriks, R., Jansen, R., Bijma, F., Mansvelder, H., Gunst, M. de, Vaart, A.W. van der, Unbiased estimation of Langevin dynamics from time series with application to hippocampal field potentials in vitro, *Physical Review E 84 (2)(2011), 021133, 13 p.*
Jonker, M.A., Bochdanovits, Z., Boomsma, D.M., Vaart, A.W. van der, Estimating linkage disequilibrium from sib data, *Statistica Neerlandica 65 (3)(2011), 239-258.*
Kotlowski, W., Grünwald, P.D., Maximum Likelihood vs. Sequential Normalized Maximum Likelihood in On-line Density Estimation, *Proceedings of the 24th Conference on Learning Theory (COLT 2011), 761-779, Budapest., 2011.*
Li, L., Tchetgen, E., Vaart, A.W. van der, Robins, J., Higher order inference on a treatment effect under low regularity conditions, *Statistics and Probability Letters 81 (2011), 821-828.*
Linting, M., Os, B.J. van, Meulman, J.J., Statistical significance and the contributions of variables to the PCA solution: An alternative permutation study. *Psychometrika 76(2011), 440-460.*
Meulman, J.J., Hubert, L.J., Arabie, P., Optimal ordering of objects under nonlinear transformation of variables, *In: B. Fichet, D. Piccolo, R. Verde (Eds.), Classification and Multivariate Analysis for Complex Data Structures*, *Berlin: Springer Verlag (2011), 29-40.*
Meulman, J.J., Dusseldorp, E., Os, B.J. van, An exact dynamic programming algorithm for regression and classification trees, *In: M. van der Heijden, B. Koren, R. van der Mei, C. van Vonderen (Eds.), The Traveling Science Man, Amsterdam: CWI (2011), 198-208.*
Rooij, S. de, Grünwald, P.D., Luckiness and regret in minimum description length inference, *In: Handbook of the Philosophy of Science 7: Philosophy of Statistics, P. S. Bandyopadhyay and M. Forster(eds.), Elsevier Science Publishers (2011), ISBN 0444518622, 865-900.*
Vaart, A.W. van der, Dynamics underlying autocorrelations in spontaneous MEG alpha oscillations: a data-driven approach, *Neuroimage 57 (2011), 440-451.*

Vaart, A.W. van der, Wellner, J.A., A local maximum inequality under uniform entropy, *Electronic Journal of Statistics 5 (2011), 192-203*.
Wieringen, W.N. van, Vaart, A.W. van der, Statistical analysis of the cell's molecular entropy using high-throughput data, *Bioinformatics 27 (2011), 556-563*.
Wietmarschen, H.A.van, Reijmers, T.H., Kooij, A.J. van der, Wei, H., Schroën, J., Meulman, J.J., Greef, J. van der, Systems diagnosis questionnaire reveals similarities and differences between patients with rheumatic diseases, *PLoS One, 6, e24846*.
Zwet, W.R. van, Remembering Erich Lehmann, Annals of Statistics 39 (2011), 2266-2279.

3. Mathematics, Computer Science and Society

Papers in Journals and Proceedings

Birrer, F.A.J., Mensink, W., The virtual world of policy arguments: The case of the Electronic Health Record, *In: F.H. van Eemeren, B. Garssen, D. Godden, G.Mitchell (eds.): Proceedings of the 7th Conference of the International Society for the Study of Argumentation, (2011), Rozenberg/SicSat, Amsterdam, 96-106.*
Mensink, W., Birrer, F.A.J., Constituting the "good patient" – The effect of "clustered argumentation" in Dutch personal healthcare budget policy, *In: F.H. van Eemeren, B. Garssen, D. Godden, G. Mitchell (eds.): Proceedings of the 7th Conference of the International Society for the Study of Argumentation, (2011), Rozenberg/SicSat, Amsterdam, 1266-1283.*

Mathematical Institute Reports

MI 2011-01
F. den Hollander, F.R. Nardi, A. Troiani
Metastability for Kawasaki dynamics at low temperature with two types of particles

MI 2011-02
F. den Hollander, R. dos Santos, V. Sidoravicius
Law of large numbers for non-elliptic random walks in dynamic random environments

MI 2011-03
A. Bérczes. J.-H. Evertse, K. Győry
Multiply monogenic orders

MI 2011-04
S. Dirksen, M. F.E. de Jeu, M.M.R. Wortel
Crossed products of Banach algebras. I.

MI 2011-05
F. den Hollander, F.R. Nardi, A. Troiani
Kawasaki dynamics with two types of particles stable/metastable configurations and communication height

MI 2011-06
M.F.E. de Jeu, J. Tomiyama
Maximal abelian subalgebras and projections in two Banach algebras associated with a topological dynamical system

MI 2011-07
F. Caravenna, F. den Hollander, N. Pétrélis
Lectures on random polymers

MI 2011-08
J.-H. Evertse, K. Győry
Effective results for unit equations over finitely generated domains

MI 2011-09
M.F.E. de Jeu, M.M.R. Wortel
Positive representations of finite groups in Riesz spaces

MI 2011-10
R.S. de Jong
One half log discriminant and division polynomials

MI 2011-11
E. Bolthausen, F. den Hollander, A.A. Opoku
A copolymer near a selective interface: variational characterization of the free energy

MI 2011-12
M.N. Katehakis, L.C. Smit
On computing optimal (Q,r) replenishment policies under quantity discounts

MI 2011-13
R.J. Kooman
Diagonalization of matrix sequences

MI 2011-14
M.F.E. de Jeu, M.M.R. Wortel
Compact groups of positive operators on Banach lattices

MI 2011-15
V. Rottschäfer
Asymptotic analysis of a new type of multi-bump, self-similar, blowup solutions of the Ginzburg Landau equation

MI 2011-16
M.N. Spijker
The existence of stepsize-coefficients for boundedness of linear multistep methods

MI 2011-17
T. Alkurdi, S.C. Hille, O. van Gaans
A dynamical system perturbed by stochastic interventions

Workshops, Seminars a.o.

This chapter summarizes the workshops, seminars and others (co-) organised by (researchers of) the Mathematical Institute. The following data are given:
- *Title*
- *City and date*
- *(Co-) organizers*

CWI/LEIDEN Research on Information Security and Cryptology Seminar (RISC)
scheduled regularly
Organizer: R. Cramer

Abel in Holland, Leiden
February 24
Organized by the Norwegian Academie of Science and L. Taelman

Mathematics of Information-Theoretic Cryptography
Institute for Pure and Applied Mathematics (IPAM), University of California at Los Angeles, USA
February 28 - March 4
Scientific organizers: R. Cramer, Y. Ishai (Technion, Israel), T. Kaufman (MIT, USA), C. Padro' (Singapore), C. Xing (Singapore)

CIRM, Arithmetic geometry and coding theory
March 2011
C. Salgado Guimaraes da Silva

Workshop "Control of Burning Plasmas"
Lorentz Center Leiden, The Netherlands
March 21-25
Organizer: B. Koren et al.

Workshop Science meets Justice: Forensic Statistics at the Interface
Lorentz Center
April 26-29
Organizers: R.D. Gill en J.F. Nijboer (Law, Leiden)

International Conference on Information-Theoretic Security (ICITS)
KNAW Trippenhuis, Amsterdam, The Netherlands
May 21-24
General chairs: R. Cramer and K. Pietrzak

Workshop on "Cohen-Lenstra heuristics"
AIM, Palo Alto, USA
June 13-17
H.W. Lenstra

Extreme-Value Statistics in Mathematics, Physics and Beyond
Lorentz Center, Leiden, The Netherlands
July 4-8

Organizers: Y. Fyodorov (Nottingham), F. den Hollander (Leiden), S. Nechaev (Paris)
H. Rootzen (Gothenburg), S. Shlosman (Marseille)

Transgenes going wild?
Lorentz Center Leiden, The Netherlands
July 11-15
Organizers: B.-R. Lu (Shanghai, China), A. Snow (Columbus, USA), D. Bartsch (Berlin, Germany), P. Haccou (Leiden, The Netherlands), J. Rong (Leiden, The Netherlands),T. de Jong (Leiden, The Netherlands), G. De Snoo (Leiden, The Netherlands), H. Bergmans (Bilthoven, The Netherlands)

International Mathematical Olympiad
Amsterdam, The Netherlands
July 12-24
Organizers: B. van Dalen, B. de Smit, R. van Luijk

Workshop on "Explicit methods in number theory"
Mathematisches Forschungsinstitut Oberwolfach, Germany
July 18-22
Co-Organizer: H.W. Lenstra

BIRS workshop "Localized Multi-Dimensional Patterns in Dissipative Systems: Theory, Modeling, and Experiments"
Banff, Canada
July 24-29
Organizers: A. Doelman (Leiden), B. Deconinck (Washington), E. Knobloch (Berkeley), Y. Nishiura (Sapporo), B. Sandstede (Brown) and M. Ward (UBC)

Summer School: Group Schemes, an introduction to the SGA 3 seminar of Demazure-Grothendieck
Luminy, France
2011/08/29-2011/09/09
Organizers: S.J. Edixhoven, P. Gille, P. Polo, G. Prasad

Zesendertigste Woudschoten Conferentie van Werkgemeenschap Scientific Computing,
Zeist, The Netherlands
October 5-7
Organizer: B. Koren et al

Editorial Board Meeting Journal of Computational Physics
Amsterdam, The Netherlands
October 31
Organizer: B. Koren

The Traveling Science Man
Symposium voor Jan Karel Lenstra, Amsterdam, The Netherlands
November 4
Organizer: B. Koren

Conference "Geometric Methods for Infinite-Dimensional Dynamical Systems"
November 4-6, Brown University, Providence, USA

Organizers: A. Doelman, S. Balasuriya (Connecticut), T. Kaper (Boston), B. Sandstede (Brown University)

Criptografia
Bogota, Colombia
November 15-18
Organizers: R. van Luijk, A. Onshuus, M. Velasco

Semigroups
Leiden, regularly scheduled seminar in Spring 2011
Organizer: M. de Jeu

Choquet theory
Leiden and Delft, regularly scheduled seminar in Fall 2011
Organizers: M. de Jeu and B. de Pagter (Delft)

Edixhoven participates in the organisation of the Cryptography seminar of the university of Rennes and the CELAR (Centre Electronique de l'Armement), since December 2001.
See: www.math.univ-rennes1.fr/crypto/seminaire.html

Intercity number theory seminar
13 meetings in 2011 in Leiden, Delft, Amsterdam, Utrecht, Groningen, Leuven, Gent
Organizer: Bart de Smit
webpage: http://www.math.leidenuniv.nl/~desmit/ic

Algebra, geometry and number theory seminar
Leiden, regularly scheduled seminar (17 meetings in 2011)
Organizer: L. Taelman

Most Informal Probability Seminar
Weekly seminar of the chair of Probability, Leiden (17 meetings in 2011)
Organizer: M. Heydenreich

Invited Lectures

1.1 Number theory and Algebra

R. Cramer
- The Torsion Limit for Algebraic Function Fields and Its Applications in Cryptography and Complexity, Paris, France, January 20-21.
- The Arithmetic Codex, Los Angeles, Ca., USA, February 28-March 4.
- The Arithmetic Codex, Groningen, The Netherlands, March 23.
- The Arithmetic Codex, Tallinn, Estonia, May 15-19.
- The Arithmetic Codex, Lausanne, Switzerland, July 25-29.
- The Arithmetic Codex, Singapore, October 14.
- The Arithmetic Codex, Bonn, Germany, December 9.

J.-H. Evertse
- The Subspace Theorem and twisted heights, Tossa de Mar, Spain, April 26-30.
- Effective results on unit equations over finitely generated domains, Budapest, August 22-26.
- Multiply monogenic orders, Leiden, The Netherlands, December 9.

H.W. Lenstra
- Modeling finite fields, Leiden, The Netherlands, February 24.
- Escher and the Droste effect, The Hague, The Netherlands, March 9.
- Modeling finite fields, Berkeley, USA, March 31.
- Finite fields and field topologies, Stanford, USA, April 7.
- Escher and the Droste effect, Eindhoven, The Netherlands, May 9.
- Cohen-Lenstra heuristics, Palo Alto, USA, June 13.
- Discriminants of wild extensions, Warwick, USA, November 28.
- Escher and the Droste effect, Warwick, USA, November 28.
- Standard models for finite fields, Graz, Austria, December 6-16.
- Escher en het Droste effect, Amsterdam, The Netherlands, December 17.

R. van Luijk
- Computability of Picard numbers, Amsterdam, The Netherlands, March 11.
- K3 surfaces: rational points and Picard numbers, Paris, France, May 13.
- Lectures on algebra, factoring, elliptic curves and cryptography, Bogota, Colombia, November 14-18.
- Computing Picard groups of surfaces, Bogota, Colombia, November 21.

C. Salgado Guimaraes de Silva
- Comparing generic and special ranks of elliptic surfaces, Rio de Janeiro, Brazil, January 11.
- Zariski density of rational points on del Pezzo surfaces of degree one, Marseille, France, March 15.
- Zariski density of rational points on del Pezzo surfaces of low degree, CUNY Number Theory Seminar, April 1.

B. de Smit
- Escher en het Droste effect (ASV Prometheus) Leiden, The Netherlands, January 12.
- Escher en het Droste effect (Symmetrie: de spiegel van de wetenschap), Amsterdam, The Netherlands, January 26.

- Escher and the Droste effect, Villige, Zwitserland, March 17.
- The valuation criterion for normal basis generators, Luminy, France, March 25.
- Identifying number fields with L-functions, Philadelphia, USA, April 1.
- Escher and the Droste effect (MAA distiguished lecture), Washington DC, USA, April 4.
- Escher and the Droste effect, Grinnell, USA, April 6.
- Escher en het Droste-effect, Leiden, The Netherlands, April 16.
- Characterizing number fields with abelian L-functions, Gent, Belgium, June 10.
- Mass formulas for groups and modules, Stanford, USA, June 16.
- Escher en het Droste-effect, Amsterdam, The Netherlands, October 10.
- Escher en het Droste-effect, Delft, The Netherlands, October 12.

P. Stevenhagen
- Character sums for primitive root densities, Palo Alto, USA, January 14.
- Efficient CM-algorithms in low genus, San Diego, USA, February 20.
- Escher en het Droste-effect, Velsen, The Netherlands, March 17.
- Constructing algebraic objects by analytic means, Enschede, The Netherlands, May 14.
- Elliptic curves for cryptography, Bremen, Germany, May 24.
- Character sums for primitive root densities, Bastia, France, June 21.
- Complex multiplication, 6 hours of lectures, Leuven, Belgium, July 14-16.
- Artin's conjecture and character sums, Oberwolfach, Germany, July 21.
- Radical extensions and primitive roots, Bordeaux, France, September 21.
- Cryptographic curves from complex analysis, Athens, Greece, October 27.
- Mathematics in the art of M.C. Escher, Bogotá, Colombia, November 11.
- Lectures on algebra, factoring, elliptic curves and cryptography, Bogotá, Colombia, November 14-18.
- Elliptic curves and cryptography, Bogotá, Colombia, November 21.

R. Tijdeman
- Irrationality of infinite sums of rational numbers, Nijmegen, The Netherlands, February 16.
- Irrationality of Cantor and factorial series, Gent, Belgium, March 7.
- Turán's power sum method, Budapest, Hungary, Augustus 22.
- Smooth numbers, Amsterdam, The Netherlands, December 2.

1.2 Arithmetic Geometry

S.J. Edixhoven
- On Daniel Bertrand's counterexample to relative Manin-Mumford for semi-abelian schemes, Pisa, Italy, March 30.
- Le contre-exemple par Daniel Bertrand pour la conjecture de Manin-Mumford relatif semi-abelien, Strasbourg, France, May 6.
- Comment compter rapidement les vecteurs à coordonnées entières de longueur donnée?, Strasbourg, France, May 6.
- (Counter)example to semi-abelian relative Manin-Mumford, Luminy, France, May 19.
- Computation of modular 2-dimensional Galois representations, Lyon, France, June 6.
- Fast computation of the number of vectors of given length in a lattice, Bayreuth, Germany, July14.
- Relative Manin-Mumford in the semi-abelian case, Bayreuth, Germany, July15.
- Snelle algoritmen in de getaltheorie, Amsterdam, The Netherlands, August 26.
- Gauss's theorem on sums of three squares, via group schemes, Leiden, The Netherlands, October 24.
- Le théorème de Gauss sur les sommes de 3 carrés en termes de schémas en groupes, Bordeaux, France, November 15.
- Modular curves and Galois representations: computational aspects, 6 lectures, Beijing, China, November 27-December 10.

R.S. de Jong
- Normal functions and the height of Ceresa cycles, Regensburg, Germany, December 1.
- Green's functions for the Arakelov metric on hyperelliptic Riemann surfaces, I, II, Delmenhorst, Germany, September 15 and 16.
- On a line bundle on $M_{\{g,1\}}$ associated to Ceresa's cycle, Park City, USA, July 14.
- On a formula of Zhang on the height of Gross-Schoen cycles, Tossa de Mar, Spain, April 28.

L.D.J. Taelman
- Cyclotomic function fields and cohomology of the Carlitz module, Stellenbosch, South Africa, January 27.
- Une formule de nombres de classes analytique en caractéristique positive, Grenoble, France, March 16.
- Believing in the Kummer-Vandiver conjecture, Amsterdam, The Netherlands, May 4.
- Special values in characteristic p, Berlin, Germany, May 10.
- Cohomology of the Carlitz module, Londen, UK, June 14.
- The Carlitz module and a function field Herbrand-Ribet Theorem, Caen, France, June 20.
- A Herbrand-Ribet Theorem for function fields, Oberwolfach, Germany, July 20.
- An analytic class number formula in positive characteristic, Leuven, Belgium, September 5.
- Un théorème à la Herbrand-Ribet en caractéristique p, Lille, France, October 6.
- Herbrand-Ribet in positive characteristic, Zürich, Switzerland, October 21.
- Herbrand-Ribet in positive characteristic, Essen, Germany, October 27.
- Lower bounds for the gonality of curves with many automorphisms, Madrid, Spain, November 10.
- Un théorème à la Herbrand-Ribet en caractèristique p, Lyon, France, November 17.
- Herbrand-Ribet over function fields, Leuven, Belgium, November 30.

2.1 Analysis and Dynamical Systems

G. van Dijk
- Course on "Very elementary introduction to representation theory", Fukuoka, Japan, January 16-February 15.
- Gelfand pairs, old and new, Fukuoka, Japan, February 1.
- Gelfand pairs, old and new, Kagoshima, Japan, February 7.

A. Doelman
- An explicit theory for pulses in two-component, singularly perturbed reaction-diffusion equations, Kyoto, Japan, Plenary presentation conference "Far-From-Equilibrium Dynamics", January 4-8.
- The mathematics of desertification: searching for early warning signals, Eindhoven, The Netherlands, April 14.
- The mathematics of desertification: searching for early warning signals, Enschede, The Netherlands, May 9.
- The Pearling Instability in Polymer Electrolyte Solutions, Snowbird, USA, May 23.
- The Dynamics of Phytoplankton-Nutrient Interactions, Columbus Ohio, USA, June 24.
- Emergence and bifurcations of localized patterns in a coupled phytoplankton- nutrients model, Columbus Ohio, USA, June 27.
- The mathematics of desertification: searching for early warning signals, Rotterdam, The Netherlands, September 16.
- The mathematics of desertification: searching for early warning signals, Princeton, USA, November 7.
- The mathematics of desertification: searching for early warning signals, East Lansing, USA, November 11.
- An explicit theory for pulses in two-component, singularly perturbed reaction-diffusion equations, San Diego, USA, November 15.

P. Haccou
- Stochastic models for population dynamics, Eindhoven, March 14-18.

M.F.E. de Jeu
- Group representations in Banach lattices, Tianjin, China, June 24.

B. Koren
- Het zonnetjes in huis, Leiden, The Netherlands, February 23
- A physical model and numerical method for compressible two-fluid flow, Leiden, The Netherlands, February 23.

L.A. Peletier
- Pharmacokinetics, or "How a drug reaches its target", Split , Kroatia, June 14.
- Plasma protein binding and CNS receptor occupancy, Sandwich, UK, August 24.

V. Rottschäfer
- Asymptotic analysis of a specific type of multi-bump blowup solutions of the Ginzburg-Landau Equation, Snowbird, Utah, USA, May 22-26.
- Asymptotic analysis of a new type of multi-bump, blowup solutions of the Ginzburg Landau equation, Bath, UK, November 15.

2.2 Probability Theory

M. Heydenreich
- A survey of high-dimensional percolations, Barbados, March 9.
- On critical behaviour of random spatial models, Berlin, Germany, October 24.

W. Th.F. den Hollander
- Master course on Random Polymers, Bonn, Germany, Winter and Spring of 2011.
- Random walk in dynamic random environment, Bonn, Germany, January 20.
- The parabolic Anderson model in a dynamic random environment, Zürich, Switzerland, April 20.
- Disordered catalytic diffusion, Bonn, Germany, July 13.
- Disordered catalytic diffusion, Bielefeld, Germany, August 4.
- Disordered catalytic diffusion, Delft, The Netherlands, September 2.
- How universal is the Arrhenius law?, Utrecht, The Netherlands, October 12.
- Disordered catalytic diffusion, Bristol, United Kingdom, December 9.

F.M. Spieksma
- A new device for analyzing Markov (Decision) Chains: the Smoothed Rate Truncation Principle, Newark, USA, November 18.

2.3 Mathematical and Applied Statistics

R.D. Gill
- "Lessons from Lucia", The Hague, The Netherlands, January 18.
- "Lessons from Lucia", Amsterdam, The Netherlands, January 19.
- "Lessons from Lucia", The Hague, The Netherlands, January 23.
- "Lessons from Lucia", Seattle, USA, July 21.

P.D. Grünwald
- The Catch-Up Phenomenon in Model Selection and Model Averaging, Vienna, Austria, March 21.
- Updating Probabilities & Characterizing CAR: when conditioning succeeds and when it fails, Eindhoven, The Netherlands, May 9.
- Over het bedrijven van Statistiek in Kansloze Situaties, Zwolle, The Netherlands, May 18.
- The Catch-Up Phenomenon in Model Selection and Model Averaging, Amsterdam, The Netherlands, September 20.
- Kansloze Situaties: van Willem Ruis tot Lucia de B, The Hague, The Netherlands, September 26.
- Safe Testing, Amsterdam, The Netherlands, September 30.
- Catching Up Faster by Switching Sooner, London, UK, October 16.
- Is bewijsrecht kansloos? Leiden, The Netherlands, November 18.
- Your Honor, this was not a coincidence! About the use of Statistics in the case of Lucia de Berk, Groningen, The Netherlands, November 29.
- We need a BIT more GUTS (=Grand Unified Theory of Statistics), Granada, Spain, December 16.

J.J. Meulman
- Joint prediction of multiple outcomes using regularized regression with optimal scaling, Leiden, The Netherlands, December 8.

W.R. van Zwet
- Remembering Erich Lehmann, Houston, Texas, USA, May 11.
- Special cases, Bielefeld, Germany, August 6.
- The bootstrap: A dynamic future?, Leiden, The Netherlands, October 14.

3 Mathematics, Computer Science and Society

F.A.J. Birrer

- Knowledge inequalities and elites: key issues for democracy, Columbia (SC, USA), April 1.

Memberships of Editorial Boards

R.J.F. Cramer
- Journal of Cryptology, Springer Verlag.
- Journal of Mathematical Cryptology, Walter de Gruyter Publ.
- IEEE Transactions on Information Theory.
- Springer Verlag Book Series on Cryptology and Information Security (Advisory Board).

G. van Dijk
- Vestnik Tambov University

A. Doelman
- Physica D (Nonlinear Phenoma) (Editor-in-Chief)
- Journal of Computational Science

S.J. Edixhoven
- Compositio Mathematica (managing editor)
- Journal of Number Theory
- Expositiones Mathematicae
- Indagationes Mathematicae

J.-H. Evertse
- Compositio Mathematica

R.D. Gill
- Cambridge University Press Series in Statistical and Probabilistic Mathematics
- Annals of Statistics
- Methods of Mathematical Statistics
- Probability and Mathematical Statistics
- Electronic Journal of Statistics
- International Statistical Review

P. Haccou
- Environmental Modeling and Assessment

W.Th.F. den Hollander
- Markov Processes and Related Fields
- Indagationes Mathematicae

B. Koren
- Journal of Computational Physics
- Mathematics and Computers in Simulation

H.W. Lenstra
- Algebra and Number Theory
- Foundations of Computational Mathematics
- Glasgow Mathematical Journal
- Journal of the European Mathematical Society

J.J. Meulman
- Journal of Classification

- British Journal of Mathematical and Statistical Psychology
- Springer Series *Studies in classification, data analysis, and knowledge organization*

J.P. Murre
- Indagationes Mathematicae

L.A. Peletier
- Advances in Differential Equations
- Differential and Integral Equations
- Journal of the European Mathematical Society
- Progress in Nonlinear Differential Equations and their Applications
- Indagationes Mathematicae

B. de Smit
- Journal of the European Mathematical Society

M.N. Spijker
- Journal of Computational and Applied Mathematics
- International Journal of Engineering
- Applicationes Mathematicae

P. Stevenhagen
- Contributions to Discrete Mathematics

L.D.J. Taelman
- Journal of Number Theory.

R. Tijdeman
- Indagationes Mathematicae

E. Verbitskiy
- Journal of Mathematics-for-Industry, Japan

S.M. Verduyn Lunel
- Archiv der Mathematik
- Functional Differential Equations
- Integral Equations and Operator Theory
- Operator Theory Advances and Applications (series of monographs, Birkhäuser)

Honors

P. Bruin
- Stieltjes Prize for the best PhD thesis in mathematics in The Netherlands of the year 2010.

R.J.F. Cramer:
- Invited keynote speaker, 30th Annual IACR EUROCRYPT, 2011, Tallin, Estonia. Subject: The Arithmetic Codex.

R.D. Gill
- "Distinguished Lorentz Fellow" with the Netherlands Institute of Advanced Studies in the Humanities and Social Sciences (NIAS), Wassenaar, The Netherlands.

C. Salgado Guimaraes de Silva
- KNAW- Hendrik Casimir prize 2011.

Foreign Visitors

The following data are given:
name, place and country of the visitor,
name(s) of the host(s)

1. Number theory, Algebra and Geometry

1.1 Number theory and Algebra
C. Xing, Singapore, R.J.F. Cramer
A. Bérczes, Debrecen, Hungary, J.-H. Evertse.
K. Győry, Debrecen, Hungary, J.-H. Evertse.
P. Autissier, Bordeaux, France, J.-H. Evertse and B. de Smit
D. Testa, Oxford, UK, R. van Luijk
M. Bright, Warwick, UK, R. van Luijk
F. Andreatta, Padova, Italy, B. de Smit
L. Hajdu, Debrecen, Hungary. R. Tijdeman.
A. Alpers, München, Germany, R. Tijdeman

1.2 Arithmetic Geometry
C. Peters, Grenoble, France, S.J. Edixhoven and J.P. Murre
A. Telemann, Marseille, France, M. Lübke
B. Totaro, Cambridge, UK, S.J. Edixhoven
A. Rogue and C. Rouffort, Rennes, France, S.J. Edixhoven and P. Stevenhagen
P. Balazs, Szeged, Hungary, S.J. Edixhoven and K.J. Batenburg
J. Sijbers, Antwerpen, Belgium, S.J. Edixhoven and K.J. Batenburg
S. Wahyuni, Yogjakarta, Indonesia, S.J. Edixhoven
K. Sugeng, Jakarta, Indonesia, S.J. Edixhoven
D. Ramakrishnan, Pasadena, USA, J.P. Murre
M. Saito, Kyoto, Japan, J.P. Murre
E. Esteves, Rio de Janeiro, Brazil, L. Taelman and C. Salgado
A. Pál, Londen, UK, L.Taelman
M. Papikian, State College PA, USA, L. Taelman
B. Anglès, Caen, Frankrijk, L. Taelman
A. Facchini, Padova, Italy, L.Taelman and H. Lenstra
P. Jossen, Parijs, France, L. Taelman
D. Ferrand, Rennes, France, L. Taelman
M. Watkins, Sydney, Australia, L. Taelman and P. Stevenhagen

2. Analysis and Stochastics

2*.1. Analysis and Dynamical Systems*
G. Hayrapetyan, East Lansing, USA, A. Doelman
A. Kalauch, Dresden, Germany, O.W. van Gaans
B. Lemmens, Canterbury, UK, O.W. van Gaans
J. Tomiyama, Tokyo, Japan, M. de Jeu
C. Budd, University of Bath, UK, V. Rottschäfer
K.J. In ‘t Hout, Antwerpen, Belgium, M.N. Spijker

Z. Horvath, Gyor, Hungary, M.N. Spijker

2.2. Probability Theory
N. Gaudillière, Marseille, France, F.den Hollander
N. Pétrélis, Nantes, France, F.den Hollander
E. Scoppola, Rome, Italy, F.den Hollander
K. Schmidt, Vienna, Austria, E. Verbitskiy

2.3. *Mathematical and Applied Statistics*
K. Yamaga, Osaka, Japan, R.D. Gill
J.Friedman, Stanford, USA, J.J. Meulman
M. Vichi, Rome, Italy, J.J. Meulman
G. Lubke, Notre Dame, USA, J.J. Meulman
R. Siciliano, Naples, Italy, J.J. Meulman
P. Bentler, Los Angeles, USA, J.J. Meulman

Research Staff

1. Number theory, Algebra and Geometry

1.1 Number theory and Algebra

permanent staff:
prof.dr. R.J.F. Cramer
dr. J.-H. Evertse
prof.dr. H.W. Lenstra
dr. R.M. van Luijk
dr. B. de Smit
prof.dr. P. Stevenhagen

emeritus:
prof.dr. R. Tijdeman

postdocs:
dr. D.C. Gijswijt (till September 1)
dr. C. Salgado Guimaraes de Silva

PhD students:
A. Angelakis, MSc
M.H. Bien, MSc. (from September 1)
drs. J. Bouw
J. Brau, MSc.
drs. J.L.A.H. Daems
B.E. van Dalen, MSc. (till September 1)
K.J. Dorobisz, MSc. (from September 1)
H.D. Duong, MSc.
A. Gioia, MSc.
J.P. van der Horst, MSc. (from January 1)
drs. B.J.H. Jansen
M.F. Kosters, MSc.
J. Liu (from September 1
Drs. W.J. Palenstijn
drs. R. Pannekoek
A. Siviero, MSc. (from September 1)
G. Dalla Torre, MSc.
E.L. Toreao Dassen, MSc.
W. Zhuang, MSc. (from September 1)

guest researcher:
drs. H.M. Matthijsse (LIO)(till September 1)
dr. F. Najman (till September 1)

1.2 Arithmetic Geometry

permanent staff:
prof.dr. S.J. Edixhoven
dr. R.S. de Jong
dr. M. Lübke
dr. L.D.J. Taelman

emeriti:
prof.dr. J.P. Murre
prof.dr. A.J.H.M. van de Ven

PhD students:
S. Anni, MSc.
A. Javanpeykar, MSc.
C. Zhang, MSc.

2. Analysis and Stochastics

2.1 Analysis and Dynamical Systems

permanent staff:
prof.dr. A. Doelman
dr. O.W. van Gaans
dr. S.C. Hille
dr. M.F.E. de Jeu
prof.dr.ir. B. Koren
dr. J.D.M. Rademacher
dr. V. Rottschäfer
prof.dr. S.M. Verduyn Lunel

emeriti:
prof.dr. G. van Dijk
prof.dr.ir. L.A. Peletier
prof.dr. M.N. Spijker

postdoc:
dr. L. Sella (till September 16)

PhD students:
T.S.O. Alkurdi, MSc.
G. Chen, MSc.
W.R. Fortes, MSc.
H.J.M. Messerschmidt, MSc.
drs. M. van der Schans
E.P.J.A. Siero, MSc. (from October 1)
I. Stojković, MSc. (till February 1)
V. Timperio, MSc.
F.W.J. Veerman, MSc.

M. Wortel, MSc.

guest researcher:
dr. P. Haccou (till July 1

2.2 Probability Theory

permanent staff:
dr. M. Heydenreich (STAR cluster)
prof.dr. W.Th.F. den Hollander
prof.dr. V. Sidoravicius (till November 1)
dr. F.M. Spieksma
prof.dr. E. Verbitskiy

Emeritus:
prof.dr. A. Hordijk
prof.dr. L.C.M. Kallenberg

postdocs:
dr. J.A. Goodman (from September 1)
dr. C.C.C.J. Kalle (from December 1)
dr. A. Opoku

PhD students:
H. Blok, MSc. (from June 1)
D. Erhard, Dipl. Math. (from May 1)
D. Ertiningsih, MSc. (from September 1)
M. Göll, MSc. (from May 1)
J.F. Martinez, MSc.
L.C. Smit (from November 1)
R. Soares dos Santos, MSc.
A. Troiani, MSc.
drs. K. Vafayi
F.M. Völlering, Dipl. Math.
F. Wang, MSc.

guest researchers:
prof.dr. K.I. Aardal
prof. dr. F. Redig
prof.dr. V. Sidoravicius (from November 1)

2.3 Mathematical and Applied Statistics

permanent staff:
prof.dr. R.D. Gill
prof.dr. P.D. Grünwald
prof.dr. J.J. Meulman
dr. H.G.J. van Mil

emeritus:
prof.dr. W.R. van Zwet

PhD students:
M. Kampert, MSc. (from December 1)
K. Yamagata (from May 1)

guest researcher:
prof.dr. A.W. van der Vaart

3. Mathematics, Computer Science and Society

permanent staff:
drs. F.A.J. Birrer

Support Staff

managing director:
dr. M. Lübke

management support:
T.A. Dijks

education a.o.:
dr. J. Finkelnberg
dr. R.J. Kooman

secretariat:
T.H. Bakker-Bouma

guest:
drs. F. Bakker

Student Assistants

education:

Y. Achnine	(till July 1)
M. Bargpeter	(from September 1)
B.P.C. Bastiaensen	
T.P.F. Blankevoort	(till July 1)
J.B. Blackshaw	(from September 1)
R. van Bommel	(from September 1)
N. uit de Bos	(from September 1)
W.P.S. Cames van Batenburg	(from September 1)
J.M. Commelin	(from September 1)
J. van Dobben de Bruyn	(from September 1)
R. van Dobben de Bruyn	(till July 1)
R.H. Eggermont	(till July 1)
W. Ellens	(till July 1)
T.E. Feenstra	(till July 1)
M.M.W. Fung	(till July 1)
R.W. Hoogwater	(till July 1)
H. van Imhoff	(from September 1)
A. Javanpeykar	(till July1)
J. Jin	(from September 1)
A.E. de Jonge	(from September 1)
B. Kamphorst	(from September 1)
M.A. Lopuhaä	(from September 1)
E. Massop	(from September 1)
C.J. Meerman	(from September 1)
A. Milburn	(till July 1)
A. Moritz	(from September 1)
F.P.R. Olsthoorn	(till July 1)
B.C.F. Opheusden	(till July 1)
A. Overal	(from September 1)
K. Papadimitropoulou	(from September 1)
S.L. van der Pas	(till July 1)
B. de Rijk	(from September 1)
M. Roelands	(till July 1)
J. Rozendaal	(till July 1)
L. Sewalt	(from September 1)
D.D. Sierag	(from September 1)
S. van der Sluis	(from September 1)
W. Subramanian	(from September 1)
A. Tonkelaar	(from September 1)
H.D. Visse	(from September 1)
R.M.J. Vooys	(till July 1)
V.S.S. Vos	(from September 1)
A.J. Vromans	(from September 1)

J. van Waaij	(from September 1)
T.M.J. van Zalen	(from September 1)
W. Zomervrucht	(from September 1)

tutoren:

M. Assendorp	(from September 1)
R. van Bommel	(from September 1)
N. uit de Bos	(till July 1)
F. Claassens	(from September 1)
J.M. Commelin	(from September 1)
T. Groen	(till July 1)
F. Schouten	(from September 1)
W. Subramanian	(from September 1)
M. Warrens	(till July 1)

webmaster:
F.W. van Rest

Organization

Managing Board

Prof.dr. P. Stevenhagen, scientific director
Prof.dr. S.J. Edixhoven, director of education (till September 15)
Dr. B. de Smit, director of education (from September 15)
Dr. M. Lübke

Science Committee

Prof.dr. A. Doelman
Prof.dr. S.J. Edixhoven
Prof.dr. R.D. Gill.
Prof.dr. W.Th.F. den Hollander
Prof.dr. H.W. Lenstra
Prof.dr. P. Stevenhagen, chairman

Institute Council

Dr. B. de Smit, chairman (till September 29)
Dr. L. Taelman, chairman (from September 29)
Dr. H. Finkelnberg
Dr. V. Rottschäfer