Mathematisch Instituut, Universiteit Leiden

Annual Report 2009

Contents

Mathematisch Instituut, Universiteit Leiden

# Annual Report 2009

Managing Board
Prof.dr. P. Stevenhagen, scientific director
Prof.dr. S.J. Edixhoven, director of education
Drs. F. Bakker, 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 2009*

Cascudo, Cramer, and Xing continued their research into torsion-limits for towers of algebraic function fields and their relation to asymptotically good special codes in secure computation and complexity.

Cascudo, Chen, Cramer, and Xing finished their research on asymptotically good ideal linear secret sharing schemes with strong multiplication over any fixed finite field.

Cascudo, Cramer, and Xing started research on non-trivial upper bounds for asymptotic optimal corruption tolerance in strongly multiplicative secret sharing, and into better bounds for frame-proof codes as well.

Cramer and Damgaard finished their work on amortized complexity of zero knowledge protocols.

Cramer, Hofheinz and Kiltz continued their research on an adaptation of the Naor-Yung paradigm that facilitates efficient CCA-secure encryption from hard search problems.

Evertse continued his project with Győry on writing a book on unit equations and discriminant equations. Related to this, they obtained several new effective results on Diophantine equations with unknowns from an arbitrary finitely generated domain.

Together with Benger and Charlemagne Freeman continued his previous research on pairing-friendly abelian varieties, studying their security and devising improved constructions of pairing-friendly genus 2 curves with Satoh. He also created several fundamental building blocks for cryptographic constructions: a framework for converting pairing-based crypto-systems that use composite-order groups to ones that use prime-order groups, and with Goldreich, Kiltz, Rosen, and Segev he devised new constructions of lossy trapdoor functions. And on the more practical side, he studied methods for avoiding pollution attacks in network coding systems with multiple sources together with Agrawal, Boneh, and Boyen.

Lenstra worked with Eggermont on Modellen voor eindige lichamen, with Pouwelse on Epimorfismen and with Algant master student Gioia on Normal forms in combinatorial algebra.

Van Luijk co-organized, together with Taelman and Chinburg, both a conference and a Stieltjes onderwijsweek on "Counting points on varieties." At that Stieltjesweek he also gave four lectures on the Batyrev-Manin conjectures. He gave talks at various other conferences and seminars, published a paper, and started several more papers.

De Smit and his collaborators Florence (Paris) and Thomas (Lausanne) made substantial progress towards an exact identification of when the so-called valuation criterion for normal basis generators holds.
A new collaboration was started between de Smit and Chinburg (Philadelphia) and Bleher (Iowa City) on the inverse problem of deformations theory of linear representations of finite groups: a preprint is in the making.
Continued work with Sutton (Dartmouth) and Gornet (Arlington, Texas) is leading to new ideas to prove that the covering spectrum is not a spectral invariant for surfaces. The ideas developed last year only work for dimension at least three, but a completely different method is available for surfaces.
With Borger there was further work on Lambda ring actions of Lambda orders in number fields.
With Lenstra work on standard models of finite fields was continued and two students have been involved.
With Palenstijn Artin density results were generalized to tori of dimension 1 over number fields.
Also with Palenstijn, new algorithmic insights gave rise to a dramatically faster software for the large scale collaborative computation project abcathome.com.

Stevenhagen worked with Howe and Lauter (San Diego) on efficient complex multiplication constructions, and on low genus curve constructions using glueing techniques for Jacobians.
With Moree (Bonn) he exploited character sum techniques in primitive root problems.

Streng continued his work on a classification of curves with (l,l)-endomorphisms, and finished his work with Hitt (Dublin), McGuire (Dublin), Naehrig (Eindhoven) on genus-2 curves with p-rank 1.
Streng also started writing his PhD thesis.

Tijdeman continued joint research on irrationality of numbers with Hancl, on Diophantine equations with Győry and Hajdu, and on irreducibility of polynomials with Shorey.
Ekkelkamp and Smeets finished their research on sieves in factorization methods and continued fractions, respectively.
Van Dalen obtained some new results on discrete tomography and related areas.

## *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 result 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 2009*

De Jong worked further on his NWO VENI-project 'The Shafarevich conjecture made effective'. As the result of a study of a recent paper of Zhang he computed the local invariants in that paper for the case of genus 2 curves. In the case of general hyperelliptic curves, he constructed a new local invariant which he conjectured to be equal to one of Zhang's. This has now been proved by Yamaki (non-archimedean case) and de Jong himself. The construction of the new local invariant was based on the arithmetic of symmetric roots and symmetric discriminants.

With Rémond (Grenoble) he obtained an effective Shafarevich result for cyclic covers of the projective line.

Finally, he proved that for superelliptic curves over number fields, the canonical height on the image of the curve in its jacobian satisfies a Mahler type formula, i.e., can be written as a sum, over all places, of suitable local integrals. He also proved that, except for possibly finitely many exceptions, these local integrals can be obtained by averaging over the 'division points' of the curve. These results extend earlier results in the context of elliptic curves due to Everest, Flathuin and Ward, as well as recent results in the context of dynamical systems on the projective line due to Pineiro, Szpiro and Tucker.

Taelman has shown that Drinfeld modules have a canonical finitely generated submodule of the module of rational points, and that this submodule satisfies a kind of Dirichlet unit theorem.

Building on these results he has made progress towards establishing a general result on special values of Goss L-functions, in the style of the class number formula and the Birch and Swinnerton-Dyer conjecture.
In another project, he has shown that for fixed n the "weighted" number of groups of order $p^n$, is (up to a polynomial denominator) the number of $F_p$ rational points on a variety over Z.

Bruin made progress in various areas related to his forthcoming thesis. He developed efficient algorithms for computing in Picard groups of curves over finite fields, based on Khuri-Makdisi's representation of such curves. Furthermore, he found explicit estimates for certain analytic quantities related to modular curves.
The most important of these are maxima of canonical Green functions. These results can be used to give an algorithm for computing modular Galois representations of levels greater than 1 over finite fields, extending the results of Edixhoven et al.

Stolk worked with Batenburg on some problems in discrete tomography. A paper was submitted to the SIAM Journal on Discrete Mathematics describing an algebraic approach to certain discrete tomography problems. The paper focuses on results about linear dependencies between line sums. It shows these dependencies are sufficient to solve the consistency problem in important cases. It also contains results on the number of independent dependencies and a decomposition of the dependencies for finite convex grids into a local and a global contribution. After completing the paper, further research has yielded additional results, including an algorithm to compute global dependencies.

Varma (master student) proved a nice result on sums of even numbers of squares. For k in {1,2,3,4,5} there are explicit formulas for the number of ways in which an integer m can be written as a sum of 2k squares, going back to Fermat, Euler, Lagrange, Legendre, Gauss, Jacobi and Liouville. Varma shows that for larger k there are no longer such formulas.

Edixhoven has spent much time on the fine tuning of the book in progress. With Couveignes, he improved the main result of the book, which was a probabilistic algorithm, into a deterministic one. He proved a criterion for Galois representations attached to modular forms over finite fields to have their image contain the Group $SL_2$ of that finite field.
As a by-product of being in the reading committee for De Deckere's master thesis “Understanding the bounds for the chromatic number of the Erdős-Rényi graph and its subgraphs”, he proved a general result on the covering number of a finite set by translates of a given subset under a group action. This result should make it possible to improve the upper bounds in the master thesis to become of the same order up to log factors as that of the lower bounds.

# Cluster 2. Analysis and Stochastics

## *Research Programme 2.1: Analysis and Dynamical Systems*
## *Programme leader: S.M. Verduyn Lunel*

*Description of the project*
This programme focuses on 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 programme 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. Computing the long-term behavior of dynamical systems by solving the initial data problem can be a time consuming and difficult task. It is often essential to combine numerical methods with methods from dynamical systems theory. Rather than solving 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 dynamical systems with time delays in the feedback loop (such models arise in engineering, life sciences and semi-conductor lasers), differential equations modeled on a lattice (such as the Ising model and Cellular neural networks (CNN)), and partial differential equations with applications to life sciences and chemical engineering.
The current research interests of the group include: Algebras associated with dynamical systems, Ginzburg-Landau equation and semi conductor lasers, differential-difference equations of mixed type, invariant measures for stochastic delay equations, patterns in nonlinear ordinary and partial differential equations and applications to life sciences and chemical engineering.

**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 ambient dynamical system on X, but the even more naturally associated involutive Banach algebra of crossed product type 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.
Calculating Hausdorff dimensions of invariant sets using spectral theory.
In this ongoing project together with R. Nussbaum, we present a new approach to compute the Hausdorff dimension of conformally self-similar invariant sets. The approach is based on a direct spectral analysis of the transfer operator associated with the dynamical system. In the case that the maps defining the dynamical system are analytic, our method yields a sequence of successive approximations that converge to the Hausdorff dimension of the invariant set at a super-exponential rate. This allows us to estimate the dimension very precisely. The results can be illustrated with examples from dynamical systems and from number theory via Diophantine approximations. A number of publications are in progress.

**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.

**Differential-difference equations of mixed type**
Lattice differential equations are continuous-time infinite dimensional dynamical systems, which possess a discrete spatial structure modeled on a lattice. Such equations play an important role in modeling a variety of applications with spatial structure and can be found in chemical reaction theory, image processing and pattern recognition, material science and biology. Travelling waves in lattice differential equations naturally lead to systems of functional differential equations of mixed type, both autonomous and (asymptotically hyperbolic) non-autonomous.

**Invariant measures for stochastic evolution equations**
This project is devoted to a detailed study of the asymptotic behavior of the solutions of stochastic evolution equations. Such equations are of great importance in the applied sciences, since they are used to model processes with stochastic components, such as white noise. In order to apply methods from ergodic theory to study the limit behavior of the distribution of solutions, it is necessary to have the existence of an invariant measure (or stationary distribution).Existing abstract results regarding the existence of an invariant measure for stochastic evolutionary systems require regularity assumptions on the coefficients, which are in many realistic models not satisfied. They also pose strong conditions on the noise processes, which fail in models of financial markets. The asymptotic behavior of solutions is then not yet known. Our main purpose is to provide results on the existence of invariant measures for models with less regularity of the coefficients and for general noise processes. In particular, we investigate Levy processes, non-Lipschitz coefficients, delayed feedback, equations in Banach spaces, and discretizations. This project is part of the NWO VIDI project by van Gaans.

**Numerical analysis and step-by-step methods**
Step-by-step methods are indispensable tools in computing numerical approximations to the solution of initial value problems for ordinary and partial differential equations. The research concentrates on the theoretical analysis of step-by-step methods, with an emphasis on the convergence and stability properties of the numerical methods. There are important open questions and conjectures about these properties.

**Numercial analysis of an immersed boundary method (research carried out at both the Mathematical Institute and CWI)**
The goal of this research is to develop an immersed-boundary method to be applied to incompressible Navier-Stokes problems with moving and deforming boundaries. Bodies of arbitrary shape are immersed in a simple, fixed Cartesian grid, where the corresponding boundary conditions are embedded in the neighboring fluxes.

**Applications to Chemical Engineering**
In reaction engineering it is increasingly important to replace steady state processes by periodic processes. In such processes periodic operation may for instance consist of cyclic reaction-regeneration steps. Depending on the convergence properties of the system at hand, the number of cycles that needs to be computed up to a cyclic steady state is reached, can be large. Hence, direct iterative methods are essential. However, to overcome severe memory constraints many authors have reverted to pseudo-homogeneous onedimensional models and to coarse grid discretization, which renders such models inadequate or inaccurate. In joint work van der Rotten and Verduyn Lunel proposed a limited memory iterative method, called the Broyden Rank Reduction method, to simulate a full two-dimensional model with radial gradients taken into account. A number of publications further elaborating these new ideas are in progress.

**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 (semigroup) 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.

**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.

*Research results in 2009*
Bierkens, van Gaans and Verduyn Lunel have derived upper bounds for pathwise Lyapunov exponents for linear stochastic systems with multiplicative noise and constant coefficients by analyzing a Lyapunov type inequality. Controllability properties of the coefficient matrices have been used for conditions for pathwise asymptotic stability. By means of Malliavin calculus, Bierkens has proved the eventual strong Feller property and uniqueness of an invariant measure of a class of infinite dimensional stochastic evolution equations with degenerate noise. In joint work with Kalauch (Dresden) and Lemmens (Canterbury), van Gaans has shown that every Archimedean partially ordered vector space with unit is order dense in the space of continuous functions given by its functional representation, which yields a convenient construction of the Riesz completion of the space.

The research in 2009 has resulted in new criteria for boundedness properties of Runge-Kutta methods. It has been found that boundedness can only be present in methods of general type, when they are monotonic (strongly stable). This research has been carried out by Spijker in cooperation with Hundsdorfer and Mozartova.

Haccou worked on the development of initial model and derivation of hazard rate for introgression in carrot, publication in press in Theoretical Population biology, with an extension of the methodology to time-inhomogeneous hybrid formation.
Haccou also worked on the development of a first population dynamic model for sporulation

in B. subtilis, with random resource renewal.
Further she worked on the derivation of optimal sex allocation strategies for haplodiploid species, when there is lack of information on life time fecundity and sperm supply.

Hille and Worm established a functional analytic framework that is suitable for analyzing measure-valued integral equations that result from a class of structured population models, the modeling of kinetic chemotaxis models in particular. They obtained results on the continuity of the restriction of semigroups in spaces of measures to invariant L1-spaces, e.g. those defined by invariant measures and a corresponding direct sum decomposition of the underlying space of measures. Research continues in the direction of characterization of existence, uniqueness and stability of invariant measures, for which initial results have been obtained (preprint). Application of these results to structured population models in biology will be considered.

Haccou (CML), Emmerich (LIACS) and Hille received a NWO research grant in the Computational Life Science programme for a two-year interdisciplinary project called BetNet (three postdocs, including one experimental microbiologist) on the stochasticity in signaling and gene regulation involved in sporulation of Bacillus subtilis. It will start December 2009.

In a continuing collaboration between De Jeu and Tomiyama (Tokio), new proofs have been found of several results in the final chapter of Svensson's thesis (defended in March), pertaining the structure of the Banach algebra crossed product of C(X) and the integers as associated with a homeomorphism of X. The structure of these algebras, which are more complicated than their C*-algebra versions, is gradually becoming clearer.

Wortel and De Jeu continued their study of Banach algebra dynamical systems and the associated crossed product algebras. The relation between a given set of covariant representations of the systems and representations of the crossed product is now well-understood and a systematic development of the theory is available in a paper at the brink of submission. It is particularly interesting that well-known classical algebras, such as C*-crossed products and $L_1$-algebras, are now seen to fall under the general framework as developed.
Wortel and De Jeu also took the first steps in the development of the theory of positive group representations in Riesz spaces and Banach lattices. The finite dimensional band irreducible representations of finite groups are now understood, and decomposition theorems have been obtained for compact groups acting in finite dimensional spaces and Banach function spaces.

As a follow-up of his Master thesis, Messerschmidt (starting September 1) spent a limited amount of time refining his new results on induced transformations in non-commutative ergodic theory, before moving on to positivity.

For the immersed-boundary-method topic, Hassen and Koren proposed and analyzed a new two-dimensional immersed-boundary algorithm for convection problems. Test cases, such as, an infinitely thin model plate of arbitrary orientation, moving in a uniform 2D flow-field, and a unit model cylinder of arbitrary initial location, moving in a circular flow-field, have been studied. Further, in this project, Fortes and Koren derived second-order accurate diffusive flux formulae with embedded boundary conditions for one dimensional convection-diffusion problems. Using finite volumes, appropriate limiters and TVD restrictions for the convective term were taken into account. To efficiently solve the corresponding system of equations, an IDR method, a new Krylov-projection-based solver, has been implemented and used.
In the wind-energy project, after an initial investigation into vortex methods (2008), Sanderse and Koren shifted the focus to the use of finite-volume methods for the solution of the in-

compressible Navier-Stokes equations. Research has been performed on the use of so-called symmetry-preserving (or 'mimetic') methods for the accurate simulation of turbulence in wind-turbine wakes. Another point of attention was the modeling of the turbine rotor, for which novel actuator-line methods were and still are under development.
In the tokamak-plasma project, which started in February 2010, Haverkort and Koren started with the investigation of ideal MHD equilibria in tokamak plasmas and their stability. The main achievements are the extension of an analytical equilibrium solution including toroidal flow that already existed in literature, a systematic analysis of the stability of the continuous MHD spectrum in the presence of toroidal flow, and the discovery and analysis of low-frequency toroidal flow-induced Alfvén gap modes.

Singular solutions of the generalized Korteweg-de Vries equation (KdV) have been studied by Rottschäfer. The stability of solitary waves of the KdV has already been studied extensively. These solutions can become unstable after which the amplitude starts growing and finally blows up. The structure of these blowup solutions is studied where the travelling structure of the solitary wave is incorporated in the analysis.
After introducing a dynamical rescaling the solutions are found as bounded solutions to an ordinary differential equation (ODE). This ODE is studied using asymptotic methods to construct the solutions. Through the asymptotic analysis, the parameter range is determined over which these solutions may exist.

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

*Description of the project*

The research in Probability Theory is concentrated on interacting stochastic systems (percolation, random polymers, metastability, catalytic branching, sandpile dynamics), ergodic properties of random processes (Gibbs versus non-Gibbs, frequency of local patterns), and topics from mathematical biology (population dynamics, T-cells, sequence alignment). Key tools are large deviation theory and stochastic analysis.

Interacting stochastic systems consist of a large number of interacting random components. These components interact with each other and with their environment. Even when the interaction is local, such systems typically exhibit a complex global behavior, with a long-range 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, immune system biology, and artificial life.

The research in Operations Research is concentrated on Markov chains, Markov decision processes and Markov games with applications to problems in stochastic networks. One of the main issues concerns stability.

How can one check stability? If stable, how quick does the network "become stable"? It is possible for the network to seemingly have "settled down" to the stationary distribution, while it actually has not. This seemingly stationary distribution is called a quasi-stationary distribution. When can such a situation occur? On the other hand, if one wants to compute certain characteristics of stochastic models, such as stationary distributions and fundamental matrices related to the overall deviation from stationarity, then efficient algorithms are needed. These issues can be studied within the framework of Markov chain theory.

One may also wish to determine controls of a network that optimize a certain criterion, for instance, the probability that a mobile network is overloaded. This is typically a problem to be dealt with by Markov decision processes theory. Much research has involved theoretical issues, such as existence of optimal controls and results on the structure of optimal controls ("are they amenable to practical implementation?"). Current research mainly focuses on developing algorithms for computing optimal controls.

Often the situation arises that there are conflicting interests, say, one wants to maximize server efficiency while minimizing customer dissatisfaction. This may be studied through Markov game models.

*Research results in 2009*

With Avena and Redig den Hollander worked on the derivation of limit laws for random walks in dynamic random environments, in particular, a law of large numbers and a large deviation principle for a random walk on an interacting particle system in one dimension that has a local drift to the right on occupied sites and a local drift to the left on vacant sites.

Den Hollander and dos Santos worked on the extension of the results with Avena and Redig to random walk with long-range steps: investigation of the effect of non-locality in the transitions rates.
Together with Troiani den Hollander studied the metastability and nucleation for a two-dimensional lattice gas consisting of two types of particles subject to Kawasaki dynamics (random hopping with exclusion and with binding between neighbouring particles of different type), at low temperature and low density.
With Blachere (Utrecht) and Steif (Gothenburg) den Hollander worked on the identification of bad configurations for random walks in random sceneries: a crossover as a function of the drift of the random walk.
With Gaertner (Berlin) and Maillard (Marseille) den Hollander studied the Lyapunov exponents and intermittency for the Parabolic Anderson Model in a dynamic random environment, in particular, the voter model.
With Cheliotis (EURANDOM) den Hollander studied the variational characterization of the critical curve separating the localized and the delocalized phase of a polymer chain interacting with a linear interface carrying "random charges".
Together with Dawson (Ottawa), Greven (Erlangen), Sun (Singapore) and Xu (EURANDOM) den Hollander analyzed the renormalization tranformation for hierarchically interacting diffusions taking values in the positive quadrant, describing colonies of individuals of two types that evolve through resampling and migration.
With Gaudilliere (Marseille), Nardi (Eindhoven), Olivieri (Rome) and Scoppola (Rome) den Hollander studied the metastability and nucleation for the two-dimensional lattice gas subject to Kawasaki dynamics in large volumes.
With Bovier (Bonn) den Hollander made attempts to develop a new approach to metastability for conserved dynamics.

With Chazottes (Paris) Redig proved the Poincaré inequality via disagreement percolation, with applications in Ising models, Potts models, Ising antiferromagnet.
With Vafayi, Grosskinsky (Warwick) Redig proved the condensation in the asymmetric inclusion process, with extension to a general class of models with non-translation invariant stationary measures.
With Vafayi, Giardina (Eindhoven) Redig proved the reversed Liggett's inequality in the symmetric inclusion process and associated diffusion process. They also proved the propagation of positive correlations for local Gibbs measures, and the existence of infinite profile measures in the asymmetric inclusion process.
With Wang Redig proved the Gibbsianness of transformed and time-evolved one-dimensional Gibbs measures in the uniqueness regime. Both stochastic and deterministic transformations are covered.
With Völlering Redig got general results on concentration inequalities of additive functionals of Markov processes, with applications to diffusion processes and interacting particle systems. This yields an extension of local-time large deviations to general Lipschitz functions for the exclusion process.
With Roelly (Potsdam) and Ruszel (Groningen) Redig proved the short-time conservation of Gibbsianness for an infinite system of coupled stochastic delay equations. As a consequence, they proved the existence of the solution for typical initial conditions.
With Saada (Paris) and Jarai (Bath) Redig made a study of dissipative sandpiles with arbitrary small dissipation. They also proved that the limit of zero dissipation is the critical model, both for stationary measure as well as for dynamics.

## *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 modelling. 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 2009*

Gill, Grünwald and Zohren have common interests in the intersection of forensic statistics and statistical learning. They started a collaboration with Prof. Peter de Knijf (LUMC - human genetics) and Prof. M. Sjerps (NFI - forensic statistics and UvA) on the statistical analysis of forensic DNA profiles. Work has started in collaboration with Steffen Lauritzen (Oxford), Julia Mortera (Rome) and Robert Cowell (London) on analysing DNA profiles observed in a controversial murder case in the Netherlands, where a complex mixture and a spooky drop-in allele caused traditional interpretation techniques to break down. The case is a challenging test-case for the newest methodology based on graphical models and genetic theory.

## *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 2009*

Two case studies were performed together with Wouter Mensink and Benoît Dutilleul: one on the Electronic Health record in the Netherlands, and one on Living Labs. Both drew upon analytical tools developed earlier in the research programme. These tools were particularly used to identify strengths and weaknesses of the strategies observed.

# Kloosterman Professor 2009

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 Chair 2009 was occupied in by Ted Chinburg, professor of mathematics in the University of Pennsylvania, Philadelphia, USA. Chinburg, who obtained his Ph.D. in 1980 at Harvard under John Tate, is one of the world's most versatile arithmetic geometers. His research is characterized by breadth and depth, and his lectures by friendliness and transparency. He is best known for his early and influential work on Galois module structure, but in Leiden he mostly covered different ground.

Ted Chinburg was coorganizer, with Lenny Taelman and Ronald van Luijk, of a two-week event that took place at the Lorentz Centrum, April 14-24, 2009, on the subject of "Counting Points on Varieties". The first week consisted of a "Stieltjes Onderwijsweek", addressing master students, Ph.D. students, and other interested mathematicians. During that week, he presented four one-hour lectures on "Zeta functions, Laplacians, and etale cohomology". The second week, which had the format of an international workshop, attracted many visitors from abroad.

On May 14, 2009, Chinburg presented the Kloosterman Lecture for a general mathematical audience, on "Two note number theory". It comprised an auditory version of the Droste effect that is better known in the visual arts. On May 15, he gave two lectures at an Intercity number theory seminar that took place in the Diamant seminar room at the Technische Universiteit Eindhoven, on "Lifts of group actions on curves from characteristic p to characteristic 0" and on "Katz Gabber covers with extra automorphisms". On May 20, 2009, Chinburg lectured at a combined RISC/Intercity number theory seminar that took place in Leiden. One lecture was about "Deformations of complexes of modules for a profinite group", another about "Rationality of Euler characteristics".

Chinburg's lectures attracted large audiences and gave rise to lively discussions. Altogether, his visit was considered a great success by everybody involved.

# International and National Programmes

***International Programmes**:*

Erasmus Mundus Master program Algebra, Geometry And Number Theory.
2005-2010.
Cooperation with Bordeaux and Padova and Orsay.
See: www.math.u-bordeaux1.fr/ALGANT/.
Coordinators: P. Stevenhagen, S.J. Edixhoven.

Dutch-German Bilateral Research Group (NWO-DFG): Mathematics of Random Spatial Models from Physics and Biology.
2003-2009.
Cooperation with E. Baake (Bielefeld), A. Bovier (Berlin), F. Götze (Bielefeld), A. Greven (Erlangen) and A. Wakolbinger (Frankfurt).
Project leader: W.Th.F. den Hollander.

Long term collaboration with Lund University in the project Algebras associated with dynamical systems. The collaboration is supported by an NWO visitor's grant (8 months) for Dr. S. Silvestrov (Lund University).
Coordinator: M.F.E. de Jeu.

FP6 Research and Training Network: Galois Theory and Explicit Methods.
October 2006 - October 2010.
Cooperation with: Barcelona, Bordeaux, Essen, Heidelberg, Lausanne, Leuven, Lille, Nottingham, Paris, Rome, Tel Aviv.
Project leader: B. de Smit.

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.

Dynamic Programming in Combinatorial Data Analysis.
With Lawrence J. Hubert, University of Illinois at Urbana-Champaign, and Phipps Arabie, Rutgers University, Newark, NJ.
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

***National Programmes**:*

NWO cluster: Discrete, interactive & algorithmic mathematics, algebra and number theory. (DIAMANT).
1/9/2005 - 1/1/2010.
Coordinators: H.W. Lenstra, P.Stevenhagen.

NWO VICI-premie: Arithmetic geometry, motives: computational aspects.
1/1/2005 - 1/1/2010.
Project leader: S.J. Edixhoven.

NWO VICI-premie: The Mathematics of Secure Computation.
1/1/2006-1/1/2011.
Projectleader: R. Cramer.

NWO cluster: Nonlinear Dynamics of Natural Systems (NDNS).
1/1/2006-1/1/2010.
Coordinator: S.M. Verduyn Lunel.

NWO VIDI-premie Stationary dynamics in infinite dimensions.
1/1/2006-1/1/2011.
Project leader: O.W. van Gaans.

NWO VENI-project The Shafarevich conjecture made effective
January 2007-January 2010
Projectleader: R.S. de Jong

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

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

Random Walks on high-dimensional incipient infinite clusters
2009-2010
Project leader: W.Th.F. den Hollander with R. van der Hofstad.

Variational characterization of copolymers near selective interfaces
2009-2011
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.

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 univeirsity)
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

## Master Theses

C. Borghi
title: Discrete choice models for marketing advisor
advisor: Prof. Dr. R.D. Gill
date: 12-11-2009

E.M. de Deckere
title: Understanding the bounds for the chromatic number of the Erdős-Rényi graph and its subgraphs
advisor: Prof. Dr. L.C.M. Kallenberg
date: 25-08-2009

Y.C. Kleinherenbrink
title: Netwerkoptimalisatie
advisor: Prof. Dr. L.C.M. Kallenberg
date: 11-09-2009

M. Pronk
title: An analytical approach to a stochastic process that underlies a class of structured population models
advisor: Dr. S.C. Hille
date: 14-04-2009

G.G.A. Westhoff
title: Modelling Repeated Measurements of Renal Function during dialysis with cut off due to complete kidney failure
advisor: Prof. Dr. R.D. Gill
date: 12-11-2009

J. Xiong
title: Forecasting exchange rate volatility
advisor: Dr. O.W. van Gaans
date: 11-09-2009

# 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), 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.

J. Brau
title: Congruence conditions on supersingular primes
advisor: Prof. Dr. P. Stevenhagen
date: 08-07-2009

A. Gioia
title: Normal forms in combinatorial algebra
advisor: Prof. Dr. H.W. Lenstra
date: 08-07-2009

B. Hajj-Chehade
title: Sheaf cohomology on sites and the Leray spectral sequence
advisor: Dr. G. Chênevert
date: 08-07-2009

C.-Y. Lu
title: Simple Modules of Reductive Groups
advisor: J. Tilouine
date: 08-07-2009

V. Masarotto
title: Metric and arithmetic properties of a new class of continued fraction expansions
advisor: Dr. C. Kraaikamp
date: 08-07-2009

H. Wang
title: Moduli Spaces of p-divisible Groups and Period Morphisms
advisor: J.F. Dat
date: 08-07-2009

A. Kret
title: Galois Representations
advisor: Prof. Dr. S.J. Edixhoven
date: 31-08-2009

F. Trova
title: On the Geometric Realization of Dendroidal Sets
advisor: Prof. I. Moerdijk
date: 20-11-2009

## PhD Theses

| | |
|---|---|
| R. de Haan | Algebraic techniques for low communication secure protocols |
| March 11, 2009 | Thesis advisor: prof.dr. R.J.F. Cramer |
| | Leiden University |
| P.C. Svensson | Crossed product algebras associated with topological dynamical |
| March 25, 2009 | systems |
| | Thesis advisor: M.F.E. de Jeu |
| | Leiden University |
| J. Brakenhoff | Counting problems for number rings |
| December 22, 2009 | 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*

Benger, N., Charlemagne, M., Freeman, D.M., On the security of pairing-friendly abelian varieties over non-prime fields, *In Pairing-Based Cryptography-Pairing 2009, Springer LNCS 5671 (2009), 52-65.*

Bérczes, A., Evertse, J.-H., Győry, K., Effective results for linear equations in two unknowns from a multiplicative division group, *Acta Arith. 136 (2009), 331-349.*

Bérczes, A., Evertse, J.-H., Győry, K., Effective results for points on certain subvarieties of tori, *Math. Proc. Cambridge Philos. Soc. 147 (2009), 69-94.*

Boneh, D., Freeman, D., Katz, J., Waters, B., Signing a subspace: Signatures for network coding, *In: Public-Key Cryptography-PKC 2009, Springer LNCS 5443 (2009), 68-87.*

Bugeaud, Y., Evertse, J.-H., Approximation of complex algebraic numbers by algebraic numbers of bounded degree, *Ann. Scuola Norm. Sup. Pisa, Cl. Scienze (5) 8 (2009), 1-36.*

Cascudo, I., Chen, H., Cramer, R., Xing, C., Asymptotically Good Ideal Linear Secret Sharing Schemes with Strong Multiplication over Fixed Finite Field, *Proceedings of 29th Annual IACR CRYPTO, Santa Barbara, Ca., USA, Springer Verlag LNCS, 5677 (2009), 466-486.*

Cramer, R., Damgaard, I., Amortized Complexity of Zero Knowledge Protocols, *Proceedings of 29th Annual IACR CRYPTO, Santa Barbara, Ca., USA, Springer Verlag LNCS, 5677 (2009), 177-191.*

Dalen, B. van, Stability results for uniquely determined sets from two directions in discrete tomography, *Discrete Mathematics 309 (2009), 3905-3916.*

Dalen, B. van, On the difference between solutions of discrete tomography problems, *J. of Combinatorics and Number Theory 1 (2009), 15-29.*

Hajdu, L., Tengely, Sz., Tijdeman, R., Cubes in products of terms in arithmetic progressions, *Publ. Math. Debrecen, 74 (2009), 215-232.*

Luijk, R. van, Nontrivial elements of Sha explained through K3 surfaces, *Math. Comp. 78 (2009), 441-483.*

Smeets, I., In collaboration with, A. Lenstra, H.W. Lenstra, L. Lovász, and P. van Emde Boas, The history of the LLL algorithm, in: *Phong Q. Nguyen, Brigitte Vallée (eds), The LLL algorithm survey and applications, Springer-Verlag, Berlin ( 2009), 1-17.*

Smit, B. de, Gornet, R., Sutton, C.J., Sunada's method and the covering spectrum, arXiv: 0905.0380v1 [math.DG], May 1 2009, http://arxiv.org/abs/0905.0380v1.

Tijdeman, R., Zamboni, L., Fine and Wilf words for any periods II, *Theor. Comput. Sci. 410 (2009), 3027-3034.*

Tijdeman, R., Zamboni, L., Characterizations of words with many periods, *Integers, 9 (2009), 333-342.*

Tijdeman, R., Het leven van een wiskundige, *Nieuw Arch. Wiskunde Ser. 5, 10 (2009), 156-162.*

Zagaris, A., Doelman, A., Pham Thi, N.N., Sommeijer, B. (2009), Blooming in a non-local, coupled phytoplankton-nutrient mode, *SIAM J. Appl. Math, 69 (4), 3335-3368.*

*PhD Thesis*

Brakenhoff, J., Counting problems for number rings, defended on December 22.

Haan, R.de, Algebraic techniques for low communication secure protocols, defended on March 11.

*Other publications*
Bouw, J., Grafen, Doeboek 24, *Vierkant Wiskunde*, *41 p.*
Lenstra, H.W., Ode aan het getal 43, *Nieuw Arch. Wisk. (5) 10 (2009), 240-244*.
Stevenhagen, P., Spelen met groepentheorie, *in: Tel uit je winst, wiskunde in geld en spelen, CWI Syllabus 59 (2009), 51-62.*

### 1.2 Arithmetic Geometry

*Papers in Journals and Proceedings*
Jong, R. de, Local invariants attached to Weierstrass points, *Manuscripta Mathematica 129 (2009), 273-292.*
Murre, J.P., Ramakrishnan, D., Local Galois symbols on E x E , In "Motives and Algebraic Cycles" ( A Celebration in Honour of Spencer Bloch ), *Fields Institute Communications, 56, (2009), 257-291.*
Stolk, A., Batenburg, K.J., An Algebraic Framework for Discrete Tomography: Revealing the Structure of Dependencies, *arXiv:0906.0711v2 [math.CO], http://arxiv.org/abs/0906.0711.*
Taelman, L., Special L-values of t-motives: a conjecture, *International Mathematics Research Notices. Article-ID: rnp038.*

## 2. Analysis and Stochastics

### 2.1 Analysis and Dynamical Systems

*Papers in Journals and Proceedings*
Ambati, V.R., Asheim, A., Berg, J.B. van der, Gennip, Y. van, Gerasimov, T., Llod, A., Planqué, B., Schans, M. van der, Stelt, S. van der, Vargas Rivera, M., Vondenhoff, E., Some studies on the deformation of the membrane in an RF MEMS switch, *Proceedings 63rd Study Group mathematics with industry 2008, page 65-84.*
Andersen, N.B., Jeu, M. de, Local spectral radius formulas on compact Lie groups, *J. of Lie Theory 19 (2009), 223-230.*
Archer, C., van Daalen, E.F.G., Dobberschuetz, S., Godeau, M.F., Grasman, J., Gunsing, M., Muskulus, M., Pischanskyy, A., Wakker, M., Dynamical models of extreme rolling of vessels in head waves, *In: Molenaar, J. et al. (Eds): Proceedings of the Sixty-Seventh European Study Group Mathematics with Industry (2009), 1-27.*
Bierkens, J., Gaans, O. van, Verduyn Lunel, S.M., Existence of an invariant measure for stochastic evolutions driven by an eventually compact semigroup, *J. of Evolution Equations 9 (4), 771-786.*
Boonstra, T.W., Houweling, S., Muskulus, M., Does asynchronous neuronal activity average out on a macroscopic scale?, *J. of Neuroscience 29 (2009), 8871-8874.*
Carpentieri, G., Tooren, M.J.L. van, Koren, B., Comparison of exact and approximate discrete adjoint for aerodynamic shape optimization, *Proceedings Fourth International Conference on Computational Fluid Dynamics, Gent, 2006, (H. Deconinck and E. Dick, eds.), Springer (2009), 525-530.*
Dirksen, S., Jeu, M.de, Wortel, M., Extending representations of normed algebras in Banach spaces, *in: Operator Structures and Dynamical Systems (M.F.E. de Jeu, S. Silvestrov, C. Skau, J. Tomiyama (Eds.)), Contemporary Mathematics 503, AMS, (2009), 53-72.*
Dijk, G. van, About the relation between multiplicity free and strong multiplicity free, *J. of Lie Theory 19 (2009), 661-670.*
Dijk, G. van, (U(p,q), U(p-1,q)) is a generalized Gelfand pair, *Math. Z. 261 (2009), 525-529.*

Dijk, G. van, Multiplicity free subgroups of semi-direct products. *Indagationes Mathematicae 20 (2009), 49-56.*
Gabrielsson, J. Peletier, L.A., Nonlinear turnover models for systems with physiological limits, *Eur. J. Pharm. Sci. Vol 37, 11-26*.
Doelman, A., Sandstede, B., Scheel, A., Schneider, G. (2009), The dynamics of modulated wave trains, *Memoirs of the AMS 199 (934), 105p.*
Doelman, A., Heijster, P.J.A. van, Kaper, T.J. (2009), Pulse dynamics in a three-component system: existence analysis, *J. Dyn. Diff. Eq., 21 (1), 73-115.*
Grzelak, L., Fatima, T., Hendriks, H., Munao, S., Muntean, A., Schans, M. van der, Approximate solution to a hybrid model with stochastic volatility: a singular-perturbation strategy, *Proceedings of the 67th Study Group mathematics with industry 2009, 67-80.*
Hassen, Y., Koren, B., A finite-volume method for convection problems with embedded moving boundaries, *Proceedings Fifth International Conference on Computational Fluid Dynamics, Seoul, 2008, (H. Choi, H.G. Choi and J.Y. Yoo, eds.), Springer (2009), 499-505.*
Hassen, Y., Koren, B., Finite-volume discretizations and immersed boundaries*, in: Advanced Computational Methods in Computational Science and Engineering, Lecture Notes in Computational Science and Engineering, 71, (B. Koren and C. Vuik, eds.), Springer (2009), 229-268.*
Hille, S.C., Worm, D.T.H., Embedding of semigroups of Lipschitz maps into positive linear semigroups on ordered Banach spaces generated by measures, *Integr. Equ. Oper . Theory 63 (2009), 351-371.*
Hille, S.C., Worm, D.T.H., Continuity properties of Markov semigroups and their restrictions to invariant L1-spaces, *Semigroup Forum 79 (2009), 575-600.*
Hundsdorfer, W., Mozartova, A., Spijker,.M.N., Stepsize conditions for boundedness in numerical initial value problems, *SIAM J. Numer. Anal. 47 (5) (2009), 3797-3819.*
Isaksson, C., Gabrielsson, J., Wallenius, K. Peletier, L.A., Toreson, H., Turnover modeling of non-esterified fatty acids in rats after multiple intravenous infusions of nicotinic acid, *Dose-Response, 7 (2009) 247-269.*
Jeu, M. de, Svensson, P.C., Silvestrov, S., Algebraic curves for commuting elements in the q-deformed Heisenberg algebra, *J. of Algebra 321 (2009), 1239-1255.*
Lemmens, B., Gaans, O. van, Dynamics of nonexpansive maps on strictly convex Banach spaces, *Israel J. Math. 171 (2009), 1, 425-442*.
Martini, X., Haccou, P., Olivieri, I., Hemptinne, J., Evolution of cannibalism and female's response to oviposition-deterring pheromone in aphidophagous predators, *J. of Animal Ecology 78 (2009), 964-972.*
Mourik, S. van, Bierkens, J., Stigter, H., Dirkse, M., Keesman, K., Rottschäfer, V., DHV water pumping optimization, *Proceedings of the sixty-seventh European Study Group with Industry (2009), 99-116,* http://www.math.leidenuniv.nl/%7Evivi/ProceedingsSWI2009.pdf.
Muskulus, M., Houwelings, S., Verduyn Lunel, S., Daffertshofer, A., Functional similarities and distance properties, *J. of Neuroscience Methods 183 (2009), 31-41.*
Muskulus, M., Scheenstra, A.E.H., Braakman, N., Dijkstra, J., Verduyn Lunel, S., Alia, A., de Groot, H.J., Reiber, J.H., Prospects for early detection of Alzheimer's disease from serial MR images in transgenic mouse models, *Current Alzheimer Research 6 (2009), 503-518.*
Muskulus, M., Applications of Page ranking in P systems, *In: Corne D, et al (Eds): WMC9 2008, Lecture Notes in Computer Science 5391 (2009), 311-324.*
Nguyen, H.-M., Peletier, L.A., Monotonicity of time to peak response with respect to drug dose for turnover models, *Differential and Intergral Equations 22 (2009), 1-26.*
Nguyen, H.-M., Peletier, L.A., Monotonicity of the peak time in turnover models, *Comptes Rendus Acad. Sci. Paris, 347 (1), 495-500.*
Peletier, L.A., Benson, N. Graaf, P.H. van der, Impact of plasma-protein binding on receptor occupancy: An analytical description, *J. Theoretical Biology 256 (2009), 253-262.*

Peletier, L.A., Gabrielsson, J., Dynamics of target-mediated drug disposition, *Eur. J. Pharm. Sci. 38 (2009), 445–464.*
Riedle, M., Gaans, O. van, Stochastic integration for Levy processes with values in Banach spaces, *Stochastic Process. Appl. 119 (2009), 6, 1952-1974*.
Scheenstra. A.E.H, Muskulus, M., Staring, M., van den Maagdenberg, A.M.J.V., Verduyn Lunel, S., Reiber, J.H., van der Weerd, L., Dijkstra, J., The 3D Moore-Rayleigh test for the quantitative groupwise comparison of MR brain images, *In: Prince JL, et al (Eds): Proceedings of the 21st International Conference on Information Processing in Medical Imaging (IPMI'09), Lecture Notes in Computer Science 5636 (2009), 564-575*.
Silvestrov, S., Svensson, P.C., Jeu, M.de, Algebraic dependence of commuting elements in algebras, *In: Generalized Lie Theory in Mathematics, Physics and Beyond (S. Silvestrov, E. Paal, V.Abramov, A. Stolin (Eds.)), Springer, 2009, 265-280*.
Svensson, P.C., Silvestrov, S., Jeu, M. de, Dynamical systems associated with crossed products, *Acta Appl. Math. 108 (2009), 547-559.*
Svensson, P.C., Silvestrov, S., Jeu, M. de, Connections between dynamical systems and crossed products of Banach algebras by Z, *In: Methods of Spectral Analysis In: Mathematical Physics (J. Janas, P. Kurasov, A. Laptev, S. Naboko, G. Stolz (Eds.)), Birkhauser, 2009, 391-402*.
Wackers, J., Koren, B., Accurate and efficient solution of 2D steady water flow with surface waves and turbulence, *Proceedings of the Fourth International Conference on Computational Fluid Dynamics, Gent, 2006, (H. Deconinck and E. Dick, eds.), Springer (2009), 655-661.*

*PhD Thesis*
Svensson, P.C., Crossed product algebras associated with topological dynamical systems, defended on March 25.

*Books*
Operator Structures and Dynamical Systems, (M.F.E. de Jeu, S. Silvestrov, C. Skau, J. Tomiyama (Eds.)), proceedings of a workshop at the Lorentz Center, Leiden, July 21-25, 2008, Contemporary Mathematics 503, AMS, 2009.
Advanced Computational Methods in Computational Science and Engineering, (B. Koren, C. Vuik, C. (Eds.)), *Lecture Notes in Computational Science and Engineering, 71, Springer (2009), 498 pages, ISBN 978-3-642-03343-8.*
Dijk, G. van, Introduction to Harmonic Analysis and Generalized Gelfand Pairs, *Walter de Gruyter, Berlin etc. (2009).*

## 2.2 Probability Theory

*Papers in Journals and Proceedings*
Chazottes, J.R., Collet, P., Redig, F., et al, A concentration inequality for interval maps with an indifferent fixed point, E*rgodic Theory and Dynamical Systems 29 (2009), 1097-1117.*
Chazottes, J.R., Redig, F., Concentration inequalities for Markov processes via coupling, *Electronic J. of Probability 14 (2009), 1162-1180.*
Fey, A., Meester, R., Redig, F., Stabilizability and Percolation in the Infinite Volume Sandpile Model, *Annals of Probability 37(2)(2009), 654-675.*
Gärtner, J., Hollander, F. den, Maillard, G., Intermittency on catalysts, *In: Trends in Stochastic Analysis (eds. J. Blath, P. Mörters and M. Scheutzow), London Mathematical Society Lecture Note Series 353, Cambridge University Press, Cambridge, 2009, 235-248*.
Gärtner, J., Hollander, F. den, Maillard, G., Intermittency on catalysts: three-dimensional simple symmetric exclusion, *Electronic J. Prob. 14 (2009), 2091-2129.*

Gaudillière, A., Hollander, F. den, Nardi, F.R., Olivieri, E. Scoppola, E., Ideal gas approximation for a two-dimensional rarified gas under Kawasaki dynamics, *Stoch. Proc. Appl. 119 (2009), 737-774.*
Giardina, C., Kurchan, J., Redig, F., et al, Duality and Hidden Symmetries in Interacting Particle Systems, *Journal of Statistical Physics 135(1)(2009), 25-55*.
Heidergott, B., Hordijk, A., Measure-valued differentiation for the cycle cost performance in the G/G/1 queue in the presence of heavy-tailed distributions, *Markov Processes and Related Fields 15 (2009), 225-253.*
Heidergott, B., Hordijk, A., Leahu, H., Strong bounds on perturbations, *Mathematical Methods of Operations Research 70 (2009), 99-127.*
Hollander, F. den, Three lectures on metastability under stochastic dynamics, *In: Methods of Contemporary Mathematical Statistical Physics (ed. R. Kotecky), Lecture Notes in Mathematics 1970, Springer, Berlin, 2009, 223-246.*
Hollander, F. den, Pétrélis, N., On the localized phase of a copolymer in an emulsion: supercritical percolation regime, *Commun. Math. Phys. 285 (2009), 825-871.*
Hollander, F. den, Pétrélis, N., On the localized phase of a copolymer in an emulsion: subcritical percolation regime, *J. Stat. Phys. 134 (2009), 209-241.*

*Books*:
F. den Hollander, Random Polymers, Lecture Notes in Mathematics 1974, Springer, Berlin, 2009, xiii + 258 pp., ISBN 978-3-642-00332-5.

### 2.3 Mathematical and Applied Statistics

*Papers in journals and proceedings*
Aalen, O.O., Andersen, P.K., Borgan, Ø., Gill, R.D., Keiding, N., History of applications of martingales in survival analysis, *Electronic Journal for History of Probability and Statistics 5 (1) (2009), 28p., (www.jehps.net).*
Ambjørn, J., Loll, R., Westra, W., Zohren, S., Summing over all topologies in CDT string field theory, *Phys. Lett. B 678 (2009), 227-232*.
Ambjørn, J., Loll, R., Westra, W., Zohren, S., Stochastic quantization and the role of time in quantum gravity, *Phys. Lett. B 680 (2009), 359-364*.
Ambjørn, J., Loll, R., Westra, W., Watabiki, Y., Zohren, S., New aspects of two-dimensional quantum gravity, *Act. Phys. Pol. B, 40 (2009), 1001-1031*.
Gill, R.D., Statistics, ethics and probiotica, *Statistica Neerlandica 63, 1-12*.
Jonker, M.A., Bhulai, S., Vaart, A.W. van der, Ligthart, R.S.L., Posthuma, D., Boomsma, D.I., Gamma frailty model for linkage analysis with application to censored survival data, *Biostatistics 10 (2009), 187-200*.
Robins, J., Li, L., Tchetgen, E., Vaart, A.W. van der, Quadratic Semiparametric Von Mises Calculus*, Metrika 69 (2009), 227-247.*
Tchetgen, E., Robins, J., Li, L., Vaart, A.W. van der, Semiparametric minimax rates, *Electronic J. Statistics 3 (2009), 1305-1321.*
Vaart, A.W. van der, Zanten, J.H. van, Adaptive Bayesian estimation using a Gaussian random field with inverse Gamma bandwidth, *Annals of Statistics 37 (2009), 2655-2675.*
Vaart, A.W. van der, Wellner, J.A., A note on bounds for the VC dimensions of unions, intersections, and products of VC classes. *High-Dimensional Probability V (2009).*

# Mathematical Institute Reports

MI 2009-01
W. Hundsdorfer, A. Mozartova, M.N. Spijker
*Stepsize conditions for boundedness in numerical initial value problems*

MI 2009-02
G. van Dijk
*Multiplicity free subgroups of semi-direct products*

MI 2009-03
P.C. Svensson, J. Tomiyama
*On the Banach *-algebra crossed product associated with a topological dynamical system*

MI 2009-04
S.C. Hille, D.T.H. Worm
*Continuity properties of Markov semigroups and their restrictions to invariant $L^1$-spaces*

MI 2009-05
M. Muskulus, A.E.H. Scheenstra, S.M. Verduyn-Lunel,
*A generalization of the Moore-Rayleigh test for testing symmetry of vector data and two-sample problems.*

MI 2009-06
S. Dirksen, M.F.E. de Jeu, M. Wortel,
*Extending representations of normed algebras in Banach spaces*

MI 2009-07
R. Gornett, B. de Smit, C.J. Sutton
*Sunada's method and the covering spectrum*

MI 2009-08
R. de Jong
*Admissible constants for genus 2 curves*

MI 2009-09
Ph. Clément
*An introduction to gradient flows in metric spaces*

MI 2009-10
R. de Jong
*Symmetric roots and admissible pairing*

MI 2009-11
J. Gärtner, F. den Hollander, G. Maillard
*Intermittency on catalysts: voter model*

MI 2009-12
M. Muskulus , S.M. Verduyn Lunel
*Wasserstein distances in the analysis of time series and dynamical systems*

MI 2009-13
A. Kalauch, B. Lemmens, O. van Gaans
*Functional representations and Riesz-completions of partially ordered vector spaces*

MI-2009-14
W. Hundsdorfer, M.N. Spijker .
*Boundedness and strong stability of Runge-Kutta methods*

MI 2009-15
D.T.H. Worm, S.C. Hille
*Ergodic decompositions associated to regular Markov operators on Polish spaces*

Mi 2009-16
L. Avena, W.Th.F. den Hollander, F. Redig
*Law of large numbers for a class of random walks in dynamic random environments*

MI 2009-17
L. Avena, F. den Hollander, F. Redig
*Large deviation principle for one-dimensional random walk in dynamic random environment: attractive spin-flips and simple symmetric exclusion*

MI 2009-18
R. de Jong
*Canonical height and logarithmic equidistribution on superelliptic curves*

MI 2009-19
R. de Jong, G. Rémond
*Conjecture de Shafarevitch effective pour les revêtements cycliques*

# 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-) organisers*

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

Banach lattices
Leiden, regularly scheduled seminar,
Organizer: M.F.E. de Jeu

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

Meeting on "Random Trees", Oberwolfach, Germany,
January 18-24
Organizers: W.Th.F. den Hollander, E. Baake, D. Dawson and A. Greven

Workshop on “Norm residue symbols”
Leiden, The Netherlands, February 2-6
Organizers: H.W. Lenstra and R. van Luijk

Stieltjes instructional workshop Counting points on varieties
Leiden, The Netherlands, April 2009,
Organizers: R. van Luijk, L.Taelman, T. Chinburg

Conference Counting points on varieties
Leiden, The Netherlands, April 2009
Organizers: R. van Luijk, L.Taelman, T. Chinburg

Member of the scientific committee of the CRM-PIMS Thematic Program on "Challenges and Perpectives in Probability"
Montreal and Vancouver, Canada, April-June.
Organizer: W.Th.F. den Hollander

Immersed Boundary Methods
Amsterdam, The Netherlands, June 15-17
B. Koren member advisory committee Academy Colloquium

Meeting on “Explicit methods in number theory”
Oberwolfach, Germany, July 12-18
Co-organizer H.W. Lenstra

Workshop on computing integral closures
Berkeley, USA, August 2-7
Organizer: H.W. Lenstra

Vision on Statistical Science
Leiden, August 20
Organizers: J.J. Meulman and R.D. Gill

EU-NoE Ecrypt-2 Summer School on Provable Security
Barcelona, Spain, September 7-11
Organizers: M. Abdalla, R. Cramer, G. Neven, C. Padró, N. Smart, M.I. González Vasco

3rd annual meeting GTEM
Warwick, UK, Deptember 7-11
Organizers: B. de Smit, Cremona, Frey, Schoof, Siksek

Workshop on: Experiment and discovery in number theory
Toronto, Canada, September 22-26
Organizer: H.W. Lenstra

Frobenius Lifts
Leiden, The Netherlands, October 5-9
Organizers: B. de Smit, J. Borger

Integers conference
University of West Georgia, Carrollton, USA, October 14-17
Organizer: H.W. Lenstra

Advanced Course on Shimura Varieties and L-functions
Barcelona, Spain, October 19 to 24
Organizers: H. Darmon, F. Diamond, L. Dieulefait, S.J. Edixhoven, V. Rotger

Casimir Force, Casimir Operators and the Riemann Hypothesis - Mathematics for Innovation in Industry and Science
Fukuoka, Japan, November 9-13
Organizers: M. Wakayama, G. van Dijk (chairman) R. Howe, E.Verbitskiy, M. Kaneko, S. Taniguchi

Meeting of Stochastics,
Lunteren, November 16-18
R.D. Gill

Workshop Dike-Height Control
Amsterdam, The Netherlands, December 9
Organizer: B. Koren

Workshop on "Dynamic Random Environments"
EURANDOM, Eindhoven, The Netherlands, December 14-18
Organizers: W.Th.F. den Hollander and V. Sidoravicius

Intercity number theory seminar
15 meetings in different places in the Netherlands

# Invited lectures

*1.1 Number theory and Algebra*

*R. Cramer*
- Approaches to Black-Box Secret Sharing from Algebraic Number Theory, Singapore, April 9.
- Towers of Algebraic Functions Fields in Secure Computation, Lake Arrowhead, Ca., USA, June 8-12.
- Towers of Algebraic Functions Fields in Secure Computation, Antalya, Turkey, September 23-29.
- Towers of Algebraic Functions Fields in Secure Computation, The Netherlands, November 27-29.
- Torsion-Limits for Towers of Algebraic Function Fields and Special Codes in Secure Computation and Complexity, Zurich, Switzerland, December 7.
- Torsion-Limits for Towers of Algebraic Function Fields and Special Codes in Secure Computation and Complexity, Darmstadt, Germany, December 10.
- Torsion-Limits for Towers of Algebraic Function Fields and Special Codes in Secure Computation and Complexity, Cirencester, UK, December 14-17.

*B.E. van Dalen*
- On the difference between solutions of discrete tomography problems, Milan, Italy, March 27.

*J.-H. Evertse*
- Effective results for points on certain subvarieties of tori, Bonn, Germany, March 24.
- Results and open problems related to Schmidt's Subspace Theorem, Zurich, Switzerland, June 6.

*D.C. Gijswijt*
- Applications of semidefinite programming, SDP's for block codes: how to bring your algebra into block diagonal form, Amsterdam, The Netherlands, December 3.

*H.W. Lenstra*
- Modeling finite fields, Haifa, Israel, January 11-15.
- Modeling finite fields, Potsdam, Germany, May 29.
- Exceptional polynomials, Nijmegen, The Netherlands, July 9-10.
- Modeling finite fields, Toronto, Canada, September 16, 17 and 18.
- Finding the ring of integers in a number field, Carrollton, USA, October 14.
- Modeling finite fields, Aachen, Germany, October 30.

*R. van Luijk*
- The Brauer-Manin obstruction I, Leiden, The Netherlands, February 12.
- The Brauer-Manin obstruction II, Leiden, The Netherlands, February 19.
- Batyrev-Manin conjecture, I, Leiden, The Netherlands, April 14.
- Batyrev-Manin conjecture, II, Leiden, The Netherlands, April 15.
- Batyrev-Manin conjecture, III, Leiden, The Netherlands, April 16.
- Batyrev-Manin conjecture, IV, Leiden, The Netherlands, April 17.
- Density of rational points on diagonal quartic surfaces, Leiden, The Netherlands, May 7.
- Two-coverings of Jacobians, Berlin, Germany, June 2.
- Two-coverings of Jacobians, Oberwolfach, Germany, July 14.

- Two-coverings of Jacobians, Bristol, United Kingdom, September 4.
- Two-coverings of Jacobians, Warwick, United Kingdom, Sept. 7.
- Unfaking the fake Selmer group, Eindhoven, The Netherlands, September 18.

*B. de Smit*
- Eschers conformal transformations, Delft, The Netherlands, February 27.
- Standard models of finite fields, Rennes, France, March 20.
- Escher and the Droste effect, Dartmouth, UK, April 1.
- Enumerating ABC triples, Dartmouth, UK, April 2.
- The valuation criterion in unequal characteristic, Raleigh USA, April 4.
- Standard models of finite fields, Dagstuhl, Germany, May 28.
- Escher and the infinite, Utrecht, The Netherlands, June 15.
- Enumerating ABC triples, Toronto, Canada, September 24.

*P. Stevenhagen*
- Construction problems for abelian varieties, Irvine, USA, January 15.
- Prime divisors of linear recurrent sequences, San Diego, USA, January 22.
- Factorization algorithms, Lausanne, Switzerland, February, 2.
- The elliptic curve method, Lausanne, Switzerland, February 2.
- The number field sieve, Lausanne, Switzerland, February 3.
- Constructing abelian surfaces of prescribed order, Redmond, USA, March 10.
- Genus-2 curves and Jacobians of given order, Luminy-Marseille, France, March 30.
- Complex multiplication constructions in cryptography, Leiden, The Netherlands, April 21.
- Efficient CM-constructions, Pointe à Pitre, France, April 29.
- Constructing genus 2-curves and Jacobians, Dagstuhl, Germany, May 25.
- Spelen met groepentheorie, Amsterdam, The Netherlands, August 21.
- Spelen met groepentheorie, Eindhoven, The Netherlands, August 29.
- Low genus curves with prescribed point order, Bonn, Germany, October 21.

*M. Streng*
- Igusa class polynomials, Oberwolfach, Germany, July 15.
- Abelian surfaces admitting an (l,l)-endomorphism, Bonn, Germany, September 17.
- Abelian surfaces admitting an (l,l)-endomorphism, Leuven, Belgium, October 28.
- Abelian surfaces admitting an (l,l)-endomorphism, Bordeaux, France, November 17.
- Igusa class polynomials, Lunteren, the Netherlands, November 27.
- Abelian surfaces admitting an (l,l)-endomorphism, Utrecht, The Netherlands, December 4.

*R. Tijdeman*
- An introduction to exponential polynomials, Bonn, Germany, March 4.
- On polynomials which differ a constant from an irreducible polynomial, Bonn, Germany, March 5
- Some results on discrete tomography, Debrecen, Hungary, October 29.

*1.2 Arithmetic Geometry*

*P. Bruin*
- Computing in Picard groups of projective curves over finite fields, Duisburg, Germany, November 10.
- Arakelov theory and height bounds, Berlin, Germany, November 17.
- Computing coefficients of modular forms, Marseille, France, November 30.

*S.J. Edixhoven*
- Calcul de representations galoisiennes associees aux formes modulaires et applications, Paris, January 21.
- Algebraic geometry and complexity bounds in computational number theory, Utrecht, The Netherlands, April 9.
- Introduction to Shimura varieties. Leopoldina-Symposium in Algebraic and Arithmetic Algebraic Geometry, Ascona, Switzerland, May 12.
- Introduction to Shimura varieties, Barcelona, Spain, October 19-21.
- Overview of results on the conjecture of André and Oort, Amsterdam, The Netherlands, November 10.

*R.S. de Jong*
- Symmetric roots, symmetric discriminants, Luminy, France, April 3.
- Logarithmic equidistribution and hyperelliptic Mahler measure, Bonn, Germany, April 22.
- A Mahler measure for hyperelliptic curves, Grenoble, France, June 17.
- Bogomolov for genus 2, Amsterdam, The Netherlands, June 22.
- Logarithmic equidistribution of division points on superelliptic curves, Groningen, The Netherlands, November 13.

*J.P. Murre*
- On the uniqueness of the Picard Motive, Dijon, France, May 29.

*2.1 Analysis and Dynamical Systems*

*O.W. van Gaans*
- Periods of nonexpansive maps on finite dimensional normed spaces, Canterbury, United Kingdom, November 6.

*P. Haccou*
- Modeling biological invasions, Braga, Portugal, April 15-17.
- Modeling invasions and calculating establishment success chances, Turku, Finland, June 22-27.
- What do models tell us about invasions? Helsinki, Finland, June 29.

*M.F.E. de Jeu*
- Paley-Wiener theorems and local spectral radius formulas, Amsterdam, The Netherlands, May 27.

*R.-J. Kooman*
- A class of renormalizations for first order rational difference equations, Poznan, Poland, May 28.

*B. Koren*
- A physical model and numerical method for compressible two-fluid flow, Leuven, Belgium, March 19.
- Accurate and efficient solution of water flows with surface waves and turbulence, Delft, The Netherlands, April 6.
- Two energetic PhD-projects, Amsterdam, The Netherlands, August 25.
- A physical model and numerical method for compressible two-fluid flow, Leiden, The Netherlands, October 14.

*L.A. Peletier*
- Dynamics of Protein Binding, Paris, France, March, 31.
- Dynamical Systems in Pharmaceutical Sciences, Beerse, Belgium, April, 2.
- Dynamics of Protein Binding, Leiden, The Netherlands, April 9.
- Dynamics of Protein Binding, Middletown, USA, April 28.

*V. Rottschäfer*
- Structuren die blijven groeien, The Hague, The Netherlands, October 2.
- Singular solutions of the generalized Korteweg-de Vries equation, Bath, United Kingdom, November 16.

*M.N. Spijker*
- Monotonicity and boundedness in numerical initial value problems, Zaragoza, Spain, September 7.

*2.2 Probability Theory*

*W. Th.F. den Hollander*
- Metastability under stochastic dynamics, Stockholm, Sweden, February 11.
- Intermittency on catalysts, Stockholm, Sweden, February 12.
- Percolation, Lund, Sweden, February 13.
- Percolation, Gothenburg, Sweden, February 19.
- Large deviations, Amsterdam, The Netherlands, March 5.
- Metastability under stochastic dynamics, Eindhoven, The Netherlands, March 17.
- Percolation, Bologna, Italy, April 21.
- Percolation, Bristol, United Kingdom, April 27.
- Probability at crossroads, Eindhoven, The Netherlands, May 15.
- Variational approach to pinning of random polymers, Vancouver, Canada, June 1.
- Random walk in dynamic random environment, Vancouver, Canada, June 19.
- Renormalization of interacting diffusions, Vancouver, Canada, July 05.
- Renormalization of interacting diffusions, Oberwolfach, Germany, August 21.
- Random polymers (three lectures), Bath, United Kingdom, September 7-10.
- Renormalization of interacting diffusions, Bristol, United Kingdom, September 12.
- Random polymers, Utrecht, The Netherlands, October 15.
- Random pinning, Rome, Italy, October 22.

*F.H.J. Redig*
- Concentration via coupling, Paris, France, January27.
- A new view on duality, Warwick, United Kingdom, February 25.
- Hydrodynamic limits and large deviations, Amsterdam, The Netherlands, March 5.
- The symmetric inclusion process Montreal, Canada, May 15.
- Duality and exact correlations in a model of heat conduction, Oberwolfach, Germany, August 20.
- The inclusion process: duality and correlation inequalities, Utrecht, The Netherlands, November 13.
- Duality and bosonic particle systems, Delft, The Netherlands, December 9.
- Duality and hidden symmetries in interacting particle systems, Leiden, The Netherlands, December 10.
- Random walk in dynamic random environment: a perturbative approach, Eindhoven, The Netherlands, December 16.

*F.M. Spieksma*
- Deviation matrices: existence, unicity properties and perturbations, Adelaide, Australia, September 26-27.

*2.3 Mathematical and Applied Statistics*

*R.D. Gill*
- Statistical coincidence in court: the case of Lucia de Berk, Lausanne, Switzerland, February 19.
- Quantum statistics: an introduction, Lausanne, Switzerland, February 20.
- Statistics on trial: the case of Lucia de Berk, Bern, Switzerland, April 24.
- Schrödinger's cat meets Occam's razor, Toulouse, France, July 22.
- Schrödinger's cat meets Occam's razor, Orsay, France, September 29.
- Introduction to Quantum Statistics, Limerick, U.K., November 20.

*P.D. Grünwald*
- Kansloze Situaties, Amsterdam, The Netherlands, April 24.
- The Catch-Up Phenomenon, Amsterdam, The Netherlands, August 3.
- MDL Model Selection, Eindhoven, The Netherlands, October 3.
- The Catch-Up Phenomenon, New Haven, USA, November 13.

*S. Zohren*
- Causal random geometry from stochastic quantization, Maresias, Brazil, August 02-08.
- A quantum Bell inequality for infinitely many outcomes, Paraty, Brazil, September 08-11.
- Causal random geometry from stochastic quantization, Büzios, Brazil, October 05-09.
- Causal random geometry from stochastic quantization, Sao Paulo, Brazil, November 25-28.
- Lecture course on Two-dimensional Quantum Gravity, Sao Paulo, Brazil. November 25-28.

*W.R. van Zwet*
- Resampling: Another hype in statistics, Amsterdam, The Netherlands, June 17.
- Student's test: The birth of modern statistics, Prague, Czech Republic, September 1.

*3. Project Mathematics and Society*

*F.A.J. Birrer*

- The role of expectations in radical system innovation: the electronic health record, immoderate goal or achievable necessity? Prague, Czech Republic, October 2 (with W.H. Mensink).
- Unpacking European Living Labs: analysing innovation's social dimensions, Prague, Czech Republic, October 2 (with B. Dutileul and W.H. Mensink).

# Memberships of editorial boards

R. Cramer
- IACR Journal of Cryptology
- Information Security and Cryptology Book Series: advisory board
- Journal of Mathematical Cryptology
- Member of Akademie Werkgroep voor de Wiskunde. Subcommittee of the KNAW ARW (Royal Academy Council for Mathematics).

Ph. Clément
- Journal of Evolution Equations
- PanAmerican Mathematical Journal

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

J. P. Hogendijk
- Ganita-Bharati
- Istoriko-Matematicheskie Issledovaniya
- Suhayl
- Centaurus
- Zeitschrift für Geschichte der arabisch-islamischen Wissenschaften
- Historia Mathematica
- Ta'rikh-e Elm
- Journal for the History of Arabic Science
- Early Science and Medicine

W.Th.F. den Hollander
- Electronic Journal of Probability
- Markov Processes and Related Fields
- Indagationes Mathematicae
- Stochastic Processes and Applications

A. Hordijk
- Advisory Board Mathematical Methods of Operations Research

M.F.E. de Jeu
- Operator Structures and Dynamical Systems

- Symmetry, Integrability and Geometry: Methods and Applications
  (guest editor for the "Special Issue on Dunkl Operators and Related Topics")

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

H.W. Lenstra
- Indagationes Mathematicae
- Ergebnisse der Mathematik und ihrer Grenzgebiete
- Experimental Mathematics
- Arab Journal of Mathematical Sciences
- Foundations of Computational Mathematics
- 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

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

P. Stevenhagen
- Contributions to Discrete Mathematics
- Japan journal of industrial and Applied Mathematics
  (guest associate editor special issue on Algorithmic Number Theory, Vol. 24, No. 3)

R. Tijdeman
- Acta Arithmetica
- Indagationes Mathematicae

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

S.J. Edixhoven
- Nominated as member of the KNAW.

H.W. Lenstra
- Benoeming tot Ridder in de Orde van de Nederlandse Leeuw

J.J. Meulman
- Member of the General Board of The Royal Netherlands Academy of Arts and Sciences
- Vice-Chair "Afdeling Letterkunde", Royal Netherlands Academy of Arts and Sciences.

# 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*
Chaoping Xing, Singapore, Singapore, R. Cramer.
A. Bérczes, Debrecen, Hungary, J.-H. Evertse.
L. Hajdu, Debrecen, Hungary, J.-H. Evertse.
Y. Yang, Taiwan, H.W. Lenstra.
C.-Y. Chang, Taiwan, H.W. Lenstra.
S.-Y. Pan, Taiwan, H.W. Lenstra.
J.-D. Yu, Taiwan, H.W. Lenstra.
M. Stoll, Bayreuth, Germany, R. van Luijk.
J. Voight, Vermont, USA, R. van Luijk.
V. Acciaro, Pescara, Italy, R. van Luijk.
J. Klüners, Düsseldorf, Germany, R. van Luijk.
M. Bright, Bristol, United Kingdom, R. van Luijk.
B. Hanzon, Ireland, B. de Smit.
K. Győry, Debrecen, Hungary, J.-H. Evertse and R. Tijdeman.
J. Hancl, Ostrava, Czech Republic, R. Tijdeman.
L. Hajdu, Debrecen, Hungary, R. Tijdeman.

*1.2Arithmetic Geometry*
R. Menares, Lausanne, Switzerland, P Bruin (MI) and A. Bassa (CWI/MI).
C. Gonzalez, Chile, S.J. Edixhoven.
J.-M. Couveignes, France, S.J. Edixhoven.
B. Erez, France, S.J. Edixhoven.
B. Totaro, UK, S.J. Edixhoven.
F. Breuer, South Africa, S.J. Edixhoven.
A.Mohamed, S.J. Edixhoven.
K. van Zyl, South Africa, S.J. Edixhoven.
M. Saito, Kyoto, Japan, J.P. Murre.

2. Analysis and Stochastics

*2.1. Analysis and Dynamical Systems*
V.F. Molchanov, Tambov, Russia, G. van Dijk.
M. Wakayama, Fukuoka, Japan, G. van Dijk.
A. Kalauch, Dresden, Germany, O.W. van Gaans
M. Riedle, Manchester, United Kingdom, O.W. van Gaans
A. Rusinek, Warsaw, Poland, O.W. van Gaans
P. Jagers, Gothenburg, Sweden, P. Haccou
S. Silvestrov, Lund, Sweden, M.F.E. de Jeu
C. Skau, Trondheim, Norway, M.F.E. de Jeu

J. Tomiyama, Tokyo, Japan, M.F.E. de Jeu
J. Gabrielsson, Goteborg, Sweden, M.F.E. de Jeu
W. Chen, Vancouver, Canada, V. Rottschäfer
R. Kuske, Vancouver, Canada, V. Rottschäfer

*2.2. Probability Theory*

M. Birkner, Frankfurt, Germany, W.Th.F. den Hollander.
A. Bovier, Bonn, Germany, W.Th.F. den Hollander.
J. Gaertner, Berlin, Germany, W.Th.F. den Hollander.
A. Greven, Erlangen, Germany, W.Th.F. den Hollander.
G. Maillard, Marseille, France, W.Th.F. den Hollander.
N. Pétrélis, Berlin, Germany, W.Th.F. den Hollander.
E. Saada, Paris, France, F. Redig.
J.-R. Chazottes, Paris, France, F. Redig
S. Grossinksky, Warwick, United Kingdom, F. Redig

*2.3. Mathematical and Applied Statistics*

M. I. Guta, Nottingham, UK, R.D. Gill
E. Baurdoux, London, UK, R.D. Gill
J. H. Friedman, Stanford, USA, J.J. Meulman
J. O. Ramsay, Montreal, Canada, 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. J.P. Hogendijk (till September 1)
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 (from April 1)
dr. C. Salgado Guimaraes de Silva (from September 1)

*PhD students:*
drs. J. Bouw
drs. J.F. Brakenhoff (till May 1)
drs. J.L.A.H. Daems
B.E. van Dalen, MSc.
drs. R. Pannekoek (from September 1)
ir. I. Smeets (till September 1)
drs. T.C. Streng
E.L. Toreao Dassen, MSc.

*guest researchers:*
dr. D. Freeman
drs. H.M. Matthijsse (LIO)
G. Dalla Torre, MSc.

### 1.2 Arithmetic Geometry

*permanent staff:*
prof.dr. S.J. Edixhoven
dr. R.S. de Jong
dr. M. Lübke

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

*postdocs:*

| | |
|---|---|
| dr. S.Brochard | (till September 1) |
| dr. G. Chênevert | (till September 1) |
| dr. F.R.A. Doray | (till September 1) |
| dr. L.D.J. Taelman | |

*PhD students:*

drs. P.J. Bruin
drs. A.P. Stolk

*guest researchers:*

| | |
|---|---|
| drs. J.V. van Zijl | (till September 1) |

## *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. V. Rottschäfer
prof.dr. S.M. Verduyn Lunel

*emeriti:*

prof.dr. P.J.E. Clément
prof.dr. G. van Dijk
prof.dr.ir. L.A. Peletier
prof.dr. M.N. Spijker

*postdoc*

| | |
|---|---|
| dr. P. Haccou | (from May 1) |

*PhD students:*

| | |
|---|---|
| ir. G.N.J.C. Bierkens | (till September 1) |
| G. Chen, MSc. | (from September 1) |
| H.J.M. Messerschmidt, MSc. | (from September 1) |
| M. Muskulus, Dipl.Math. | |
| drs. M. van der Schans | |
| I. Stojkovic, MSc. | |
| P.C. Svensson, MSc. | (till April 1) |
| V. Timperio, MSc. | (from September 1) |
| F.W.J. Veerman, MSc. | (from September 1) |
| drs. D. Worm | |
| M. Wortel, MSc. | |

*guest researchers:*
prof.dr. H. Metz
prof.dr. S. van Strien (till September 1)

## 2.2 Probability Theory

*permanent staff:*
prof.dr. W.Th.F. den Hollander
prof.dr. L.C.M. Kallenberg
dr. F.H.J. Redig
prof.dr. V. Sidoravicius
dr. F.M. Spieksma

*Emeritus:*
prof.dr. A. Hordijk

*PhD students:*
drs. L. Avena
R. Soares dos Santos, MSc.
A. Troiani, M.Sc.
drs. K. Vafayi
F.M. Völlering, Dipl. Math.
F. Wang, M.Sc.

*guest researcher:*
prof. R. Fernandez (till September 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. E.W. van Zwet (till February 1)

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

*PhD student:*
Drs. S. Zohren

*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:*
drs. F. Bakker

*management support:*
T.A. Dijks

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

*computer systems:*
X. Cheng (till September 1)
M.F. Feleus
M. Vijn

*secretariat:*
T.H. Bakker-Bouma

# Student Assistants

*education:*

| | |
|---|---|
| Y. Achnine | |
| J.A. Boon | (from September 1) |
| H.P. Chang | (from September 1) |
| X. Cheng | (from September 1) |
| M. Derickx | (till September 1) |
| R.H. Eggermont | (from September 1) |
| W. Ellens | |
| T.E. Feenstra | |
| M.M.W. Fung | |
| C.S.L. de Graaf | (till September 1) |
| A.G. Hauwert | (from September 1) |
| F. van Helden | |
| J. Jin | |
| A.K.A. Kalsbeek | |
| Y. Kiliç | (from September 1) |
| M. Kosters | |
| S.A. van Lieshout | (from September 1) |
| J. Michielsen | |
| A. Nooitgedagt | (till February 1) |
| B.C.F. Opheusden | (from September 1) |
| S.L. van der Pas | (from September 1) |
| S. Ramawadh | |
| P. Rogaar | (till September 1) |
| E. Siero | (till September 1) |
| L. Smit | (till September 1) |
| R.M.J. Vooys | (from September 1) |
| T. Vorselen | (till September 1) |
| J. van Wamelen | |
| W. Zomervrucht | (from September 1) |

*tutor:*

| | |
|---|---|
| M. Assendorp | (from September 1) |
| J.B.A. Hemerik | (till July 1) |
| S.A. van Lieshout | (till July 1) |
| M. Lopuhaä | (from September 1) |
| E. Massop | (from September 1) |
| St. Pouwelse | (from September 1) |
| E. Visse | (from September 1) |
| R.M.J. Vooys | (till July 1) |
| R.A.C.H. Wols | (till July 1) |

*webmaster:*
F.W. van Rest

*pr:*
V. Hisken (till November 16)
F. Offergelt
B. de Rijk
R. Winter (from November 16)

# Organization

*Board of Trustees*

Ir. B. van Nederveen, chairman
Dr. M. Elkenbracht-Huizing
Prof.dr. G. Nienhuis
Prof.dr. H.A. van der Vorst
Prof.dr. W.R. van Zwet

*Managing Board*

Prof.dr. P. Stevenhagen, scientific director
Prof.dr. S.J. Edixhoven, director of education
Drs. F. Bakker, managing director

*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. L.C.M. Kallenberg
Prof.dr. H.W. Lenstra
Prof.dr. P. Stevenhagen, chairman
Prof.dr. S.M. Verduyn Lunel

*Institute Council*

Dr. B. de Smit, chairman
Dr. H. Finkelnberg
Dr. V. Rottschäfer