Mathematisch Instituut, Universiteit Leiden

Annual Report 2008

Contents

Mathematisch Instituut, Universiteit Leiden

Annual Report 2008

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 2008

Chen (Shanghai), Cramer, de Haan and Cascudo (Oviedo) completed their work on (strongly) multiplicative ramp schemes from higher degree places in algebraic function fields, with applications to communication efficient secure multi-party computation.

Cramer, Dodis (NYU), Fehr (CWI), Padró (Barcelona), and Wichs (NYU) completed their work on algebraic manipulation detection codes and their application to fuzzy extractors and robust secret sharing.

Cramer, Hofheinz (CWI) and Kiltz (CWI) commenced work on hard algebraic set systems and applications to chosen ciphertext-secure encryption.

Cramer and Damgaard (Aarhus) completed their work on amortized linear complexity of large classes of zero knowledge protocols, by combining Sigma-protocols and a new black-box secret sharing scheme.

Cramer, Daza (Barcelona), Gracia (Barcelona), Jimenez Urroz (Barcelona), G. Leander (Toulon), J. Marti-Farre (Barcelona), C. Padró (Barcelona) finished their work on the connections between codes, matroids and secure multi-party computation from linear secret sharing schemes.

Cascudo (Oviedo), Chen (Shanghai), Cramer, and Xing (Singapore) started several new works on strongly multiplicative ideal linear secret sharing over arbitrary finite fields from algebraic function fields (dedicated field-descent techniques, divisor-exclusion techniques).
Van Dalen continued her investigations on discrete tomography. She completed two papers on the differences between solutions which have the same binary images from two directions.

Daems continued her research on the history of mathematics. She studied 19th century descriptions of the 32 crystal classes.
Ekkelkamp finished her study of estimates for the expected run time of factorization algorithms. She is expected to defend her thesis in 2009.
Together with Györy (University of Debrecen) Evertse continued his work on a book about unit equations and about related results on polynomials of given discriminant.
Evertse completed some work, jointly with Bérczes, Györy (Debrecen) and Pontreau (Caen) on effective results on points lying on the intersection of a subvariety of a linear torus, and a subgroup of finite rank of this torus.
Tijdeman and Zamboni gave various characterizations of words with many periods. Shorey and Tijdeman generalized some irreducibility results of Schur. Gyory, Hajdu and Tijdeman started a study on a completely different type of irreducibility results started by Schur. Hancl and Tijdeman continued their investigations of irrationality properties of factorial series.
Smeets worked with Kraaikamp (Delft) and Schmidt (Corvallis, USA) on properties of natural extensions for α-Rosen continued fractions.

Lenstra worked on several subjects in algebra and number theory, in many cases as part of a collaboration with others or a supervision of a student.
With bachelor students Rozendaal and Michielsen he worked on groups with few conjugacy classes and on semisimplicity and finite groups, respectively.
With "leraar in onderzoek" Zevenhek he worked on pro-eindige Fibonaccigetallen.
With Hogendijk and "leraar in onderzoek" Matthijsse he worked on Archimedes and Dijksterhuis.
With master students Liu and Gioia he worked on trinomials and exponential diophantine equations and on normal forms in combinatorial algebra, respectively.
Further, he supervised the Ph.D. work of Bouw on computing norm residue symbols; of Brakenhoff on counting problems in algebraic number theory, of Dalla Torre on the unit residue group; of Dassen on layered lattices; and, jointly with de Smit, of Jansen on Mersenne primes and class field theory.
He worked with Smeets on the history of the LLL algorithm, with Aardal on integer programming, with Pomerance on primality testing in polynomial time, with Zannier on the distribution of quadratic non-residues, and with de Smit on a variety of subjects, including the modelling of finite fields.
Finally he worked on degrees of field automorphisms and on cyclic affine permutations.
Van Luijk organized and lectured in two week-long workshops for students: one in Warwick, England (geometry and arithmetic of surfaces), and one in Bogotá, Colombia (the Hasse principle). He also organized an international conference on the arithmetic of K3 surfaces in Banff, Canada, gave several more talks at conferences and various seminars, and worked on three papers.

The distributed computation project abcathome.com which is run by Palenstijn and de Smit, made substantial progress collecting data related to the ABC conjecture. In addition, De Smit and Palenstijn developped a new algorithm which will enable us to obtain these results much faster than before. Thus, a new and much wider search range becomes feasible.

De Smit collaborated with Thomas and Florence of the EPFL Lausanne on a valuative criterion for normal basis generators in a wildly ramified extension of local fields. Only a few stubborn cases remain. Together with Sutton (Dartmouth) and Gornet (U. Texas, Arlington) he completed a detailed study of the covering spectrum of isospectral Riemannian manifolds.
De Smit continued his collaboration with Hanzon (Cork) which aims to apply Galois theory to mathematical finance: several key examples are now fully analyzed.
Lenstra and De Smit started a new line of research in the algorithmic theory of finite field. In particular they found a semideterministic method that on input a prime power q produces an explicit model of a finite field of q elements.
In cooperation with Howe (CCR San Diego), Stevenhagen found an algorithm to efficiently construct genus 2 curves over finite fields with prescribed number of points. With Howe and Lauter (Microsoft), he proved that similar efficient constructions do not exist for the Jacobians of these curves.
Streng worked on constructions of algebraic curves of genus two and finished his analysis of the runtime of computing Igusa class polynomials. He worked with Bröker (Microsoft) and Lauter (Microsoft) on a classification of curves with (l,l)-endomorphisms.

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 2008

Bosman has computed a polynomial of degree 33, with rational coefficients, whose Galois group is the group of 2 by 2 matrices of determinant one with coefficients in the field with 32 elements.

Brochard proved some partial results on a conjecture of de Smit. If B is a flat A-algebra with A and B Artin local rings with the same embedding dimension, the conjecture tells that any A-flat B-module should be B-flat. Brochard proved the conjecture in embedding dimension 2, and also in embedding dimension n under an additional assumption on the ring B/m_A.B. The conjecture has its origin in Wiles proof of Fermat's last theorem, and a positive answer might help to simplify some arguments in the commutative algebra part of the proof.

In an other preprint, Brochard proved that the main finiteness theorems for the Picard functor of a scheme (given in SGA6, exp. XII and XIII) are still valid for the Picard functor of a tame algebraic stack (in the sense of Abramovich-Olsson-Vistoli 2008). In particular, if f is a surjective morphism of proper and tame stacks over an integral noetherian base scheme S, then the induced morphism f^* between the Picard functors is quasi-affine and of finite presentation over an open subscheme of S. If S is the spectrum of a field, f^* is affine. As a consequence, the Picard functor of a tame and proper stack over a field is a scheme which is a disjoint union of quasi-projective and finite type open subschemes. Brochard also deduces some finiteness theorems for the torsion component of the Picard functor (which classifies the points of the Picard functor, a power of which lies in the neutral component) and some other results that are more arithmetic in nature, e.g. the finite generation of the Neron-Severi groups.

Chênevert extended the Faltings-Serre method used to prove the equivalence of l-adic representations by means of a finite amount of data. The main application of this is to global Galois representations coming from geometry, which encode the number of points of arithmetic varieties over finite fields. Showing that pieces of the representations are equivalent to more well-understood ones allows to decrease the complexity of point-counting, and reduces the problem of counting points on certain complicated varieties to e.g. computing the coefficients of modular forms, tying in with a central research theme of the group. Chênevert filled a gap in the existing literature for 2-dimensional 2-adic representations, sorted certain problems in the actual implementation, and made some progress toward the goal of exhibiting an explicit checkable criterion in certain cases of higher complexity.
Chênevert obtained results about the equidistribution on average of certain exponential sum over finite fields, as the size of the field tends to infinity. He can express the moments of these exponential sums in terms of the dimension of the cohomology groups of certain varieties of high dimension, for which a closed-form formula can sometimes be given using tools from representation theory. These results fit nicely in a (generalized) "Sato-Tate" equidistribution conjectural philosophy, as developped by Katz and Sarnak.

De Jong worked in the framework of his VENI project "The Shafarevich conjecture made effective". His work on the "symmetric root" on a moduli space of stable hyperelliptic curves of 2007 has led to a formula that relates the "log discriminant" of a complex separable polynomial f to the integral of log|f| over the hyperelliptic curve given by f. This generalises results on elliptic curves.
With Remond (Grenoble) he works on bounds for theta heights of low degree cyclic coverings of the projective line. With Roessler (Orsay) he studies lower bounds for the p-adic distance between a torsion point and a theta divisor on the jacobian of a curve.
Doray worked with Karpenkov and Schepers on the geometry of configuration spaces of tensegrities. They consider a graph G with n vertices, and study geometric conditions for an n-tuple of points in R^d to admit a tensegrity with underlying graph G. They introduce and investigate a natural stratification, depending on G, of the configuration space of all n-tuples in R^d. In particular they find surgeries on graphs that give relations between different strata. Based on numerous examples they give a description of geometric conditions defining the strata for plane tensegrities, they conjecture that the list of such conditions is sufficient to describe any stratum. They conclude their paper with particular examples of strata for tensegrities in the plane with a small number of vertices. Doray made a short animation movie to illustrate what tensegrity is about.

Edixhoven worked with de Jong and Schepers on bounds on the Faltings height of covers of a curve over a function field over the complex numbers, unramified outside a fixed divisor and a fixed set of places of the function field, polynomial in the degree of the cover. First a quadratic bound was obtained. After suggestions of Esnault and Viehweg, this was improved to a linear bound. They try to transpose this to the arithmetic case, where it is important for proving the existence of a polynomial time algorithm that computes mod l Galois representations arising as etale cohomology of a given smooth projective geometrically connected surface over the rational numbers.
The preprint "On the computation of coefficients of a modular form", in collaboration with Couveignes, de Jong, Merkl and Bosman, has been accepted for publication as a book in the series "Annals of Mathematics Studies", of Princeton University Press. Edixhoven has started updating the preprint and transforming it into a book.

Karpenkov continued his work on conjugacy classes in the group SL(n,Z). Gauss Reduction Theory gives the answer for the case n=2, for $n \geq 3$ the problem is still open. He introduced a

new approach to this problem based on reduction to reduced Hessenberg matrices. An important tool used in his approach is to determine minima of Markoff-Davenport characteristics at the vertices of Klein-Voronoi continued fractions. Mostly, he worked in the case of three-dimensional matrices having a real and two complex-conjugate eigenvalues, nevertheless, his techniques can be applied both to the totally real case and to the multidimensional case.

Schepers described a class of isolated nondegenerate hypersurface singularities that give a polynomial contribution to Batyrev's stringy E-function. The singularities are defined by imposing a natural condition on the facets of the Newton polyhedron and they are strictly canonical. He proved that, in many cases, Batyrev's conjecture concerning the nonnegativity of stringy Hodge numbers is true for complete varieties with such singularities. The proof uses combinatorics on lattice polytopes. The results form a strong generalization of previously obtained results for Brieskorn singularities.

Stolk has worked with Batenburg on a problem in discrete tomography, and he has continued working on the function field analog of the complexity of computation of Galois representations. Together with Bruin he started studying how to apply Khuri-Makdisi's methods for computation in the jacobians in the context of the computation of Galois representations.

Taelman has obtained a precise conjecture relating characteristic p special values (of so-called t-motives) with certain regulators, based on numerical experiments and a close study of the analogy with classical motives.

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. Of special interest, and 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. Another main line of investigation 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 (ordered) Banach spaces and induction procedures in these spaces.

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.

Ginzburg-Landau equation and semi conductor lasers.
Lasers are highly nonlinear devices and the competition between nonlinear and dispersive effects can lead to exciting pattern formation, quasi-periodic, chaotic, and blow-up structures. Semi-conductor lasers subject to delayed optical feedback can be described by the so-called Lang-Kobayashi equations, that form a three dimensional delay differential system. In work of Rottschäfer, the regions of existence and stability of certain types of solutions for these equations in 3-dimensional parameter-space, thereby laying out the `ECM-backbone' of the LK-equations. Furthermore, using asymptotic analysis combined with numerical simulations, Rottschäfer constructed multi-bump, blow-up structures for the Ginzburg-Landau equation considered as a small perturbation of the nonlinear Schrödinger equation. 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 an initial value problems for ordinary and partial differential equations. The research concentrates on the theoretical analysis of step-by-step methods. The emphasis lies on the convergence and stability properties of the numerical methods. There are important open questions and conjectures about these properties. The research has in view to contribute to the settlement of these questions.

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 method are essential. However, to overcome severe memory constraints many authors have reverted to pseudo-homogeneous one-dimensional 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 modelling, 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 signalling and plant (secondary) metabolism. From a mathematical modelling 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 focusses 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.

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.

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.

Research results in 2008

Bierkens, van Gaans, and Verduyn Lunel have investigated semilinear stochastic differential equations in Hilbert spaces where the linear part generates an eventually compact semigroup. They have proved that existence of a bounded solution implies existence of a stationary solution, provided the nonlinear terms in the drift and diffusion have finite dimensional ranges.

Es-Sarhir and van Gaans in collaboration with M. Scheutzow have shown the existence of stationary solutions of stochastic functional differential equations with a dissipative drift which is stronger than linear and an arbitrary Lipschitz diffusion coefficient.

In joint work A. Kalauch and van Gaans have proceeded their extension of the notions of ideals and bands of vector lattice theory to partially ordered vector spaces. They have identified when these objects correspond to extensions and restrictions of ideals and bands in larger vector lattices and applied their results to extend a theorem of Ogasawara.

The stability of self-similar, radially symmetric blowup solutions of the Ginzburg-Landau equation (GL) for all dimensions $2<d<4$ has been studied by Rottschäfer and the Ph.D. student van der Schans. These solutions were previously found in numeric simulations, asymptotic analysis and were proved to exist via geometric construction. As a first step in the stability analysis, linear stability with respect to radially symmetric perturbations is considered.

The asymptotic construction of the solution and Evans function techniques are used to analyse the discrete spectrum. However, due to the nature of the solutions that were found in the asymptotic analysis, Evans function techniques are not directly applicable. The essential spectrum is also analysed. Not only stable solutions are found (as in the numerics), but more interestingly, there also exist regions in parameter space where the solutions become unstable.

For the immersed-boundary method topic, together with a PhD- and MSc-student, Koren derived second-order accurate diffusive flux formulae with embedded boundary conditions, and investigated total variation diminishing (TVD) requirements. Appropriate limiters and TVD restrictions for the time step were derived. Further, research concentrated on the analysis, implementation and testing of a second-order accurate, adaptive time-integration method (Adaptive Modified Euler).

In the dike-height-control project, Koren and CWI-colleagues studied literature on dynamic programming and the Hamilton-Jacobi-Bellman (HJB) equation. A numerical method for the latter equation was developed, a method especially suited for the control of dike heights over very long time intervals. The discretization of the HJB equation exploits an existing essentially non-oscillatory (ENO) discretization of the drift term. This discretization can be of arbitrary high order of accuracy. A novelty was the development of an ENO discretization for the HJB equation's diffusion term.

For the wind-farm-aerodynamics theme, Koren and Sanderse (PhD-student of the Mathematical Institute seconded at CWI) started by making an extensive literature survey of the numerical simulation of wind-farm aerodynamics.

Wind-farm aerodynamics is dominated by vortices generated by the turbine rotors. Classical, mathematically elegant computational methods for simulating vortical flows are vortex methods. A start was made with the investigation of the suitability of vortex methods for wind-

farm aerodynamics. A challenge is to accurately and efficiently include the turbulent atmospheric boundary layer in a vortex method**.**

In a continuing collaboration with Prof. Tomiyama (Tokio), new structural results about crossed product C*-algebras associated with dynamical systems have been obtained, leading to, amongst others, the new insight that the commutant of the coefficient algebra is much better behaved than the coefficient algebra itself. Also with Tomiyama the, in a sense more natural, l_1-type crossed product algebras associated with a dynamical system have been investigated, revealing both parallels and differences with their C*-counterparts. These two projects have completed Svensson's thesis, which will be defended in March 2009.
The study of Banach algebra dynamical systems and the associated crossed product algebras by Wortel is well under way, partially in collaboration with Dirksen (Delft), and will be published in 2009. As a side product several new insights about extending representations from ideals to normed algebras, as well as about modules over centralizer algebras originating from modules over normed algebras, have beeen obtained. These include several well-known results on C*-algebras as special cases.

Research Programme 2.2: Probability Theory
Programme leader: 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 2008

Birkner, Greven and den Hollander proved a quenched large deviation principle for words drawn from a random letter sequence according to a renewal process. This large deviation principle was subsequently used to prove a conjecture about the existence of an intermediate phase for a class of interacting stochastic systems, including interacting diffusions, coupled branching processes, and directed polymers in random environment.

Bovier, den Hollander and Spitoni proved that the two-dimensional lattice gas subject to Kawasaki dynamics at low temperature and low density exhibits homogeneous nucleation in large volumes, i.e., the nucleation time between the gas phase and the liquid phase is inversely proportional to the volume, as predicted by the Arrhenius law. The proof is based on potential theory and extends ideas developed earlier by Gaudilliere, den Hollander, Nardi, Olivieri and Scoppola.
Den Hollander and Spitoni completed the analyis of the phase diagram for a copolymer, consisting of a random concatenation of hydrophobic and hydrophilic monomers, in an emulsion, consisting of random blocks of oil and water arranged in a percolation-type fashion. Especially the subcritical regime, where neither the oil nor the water percolates, shows a compllex phase diagram, with three critical curves meeting at two tricritical points.
Gärtner, den Hollander and Maillard completed the analysis of intermittency in a catalytic model consisting of A-particles performing simple symmetric exclusion and B-particles performing branching random walk with a branching rate that is proportional to the number of A-particles present at the same location. It turns out that the scaling behavior of the Lyapunov exponents, describing the growth rate of the density of B-particles, is markedly different in three dimensions than in higher dimensions.
Avena and den Hollander proved a quenched and an annealed large deviation principle for the empirical speed of a random walk in a dynamic random environment, driven by a simple exclusion process. The behavior of the rate function is qualitatively different from that in the static environment.
Cheliotis and den Hollander studied pinning of copolymer by an interface carrying random charges. It was shown that the quenched critical curve and the annealed critical curve, separating the localized phase from the delocalized phase, have a variational characterization. This characterization can be used to determine when the disorder is relevant, i.e, when the two critical curves are different.
Giardina, Kurchan, Redig and Vafayi obtained a duality for a general class of models, of which the Kipnis-Marchioro-Presutti (KMP) model of heat conduction is a special case. The relation between duality functions and symmetries of the generator is analyzed and applied in several cases with SU(2) symmetry (exclusion processes) as well as SU(1,1) symmetry (KMP-like models).

Redig and Vafayi considered a model for the Fourier law and studied its behavior close to equilibrium (weak coupling to the heat bath). They obtained that the stationary measure, up to first order in the non-equilibrium parameter, is a product of Gaussian measures associated to the linear temperature profile.
Chazottes and Redig obtained concentration inequalities for Markov processes in a general metric space, using a coupling method. Depending on the existence of moments of the expected coupling time, they obtain Gaussian or moment bounds for general Lipschitz functions along the trajectory of a Markov chain.
Chazottes, Collet, Redig and Verbitskiy obtained a variance inequality for Lipschitz functions along the orbit of the Manneville-Pomeau map (a dynamical system with intermittency used in the study of turbulence).
Kuelske and Redig studied a large deviation principle for the trajectory of the empirical magnetization conditioned on a given magnetization at a given time, in the context of mean-field dynamics and Glauber dynamics. For a low-temperature initial measure, as a function of time, both a unique minimizer or several minimizers of the rate function can appear.
Redig and Wang studied single-site transformations of one-dimensional Gibbs measures with infinite-range interaction. They use a house-of-cards coupling to show that the transformed measure is Gibbs. In the case of an exponentially decaying interaction, the transformed

measure also has an exponentially decaying interaction, and thus the transformation can be viewed as a flow on the space of interactions.

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. The 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 great 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 2008 (highlights)
Kahn, PhD student of Gill and Massart (Orsay), defended his 300 page Leiden PhD thesis "Quantum Local Asymptotic Normality (and other questions of Quantum statistics)" in June,

2008. This thesis - of which many chapters have been or will soon appear in major journals in mathematical physics and in quantum information - lays the groundwork for the quantum analogue of LeCam's celebrated theory of local asymptotic normality. The latter unifies and explains a large part of asymptotic theory in classical statistics, and at last this becomes also possible in quantum asymptotic statistics, which so far has consisted of many disparate results, hard to relate to one another.
A four page joint work of Gill and Zohren on a generalized Bell inequality known as 'CGLMP' appeared in Physics Review Letters. Gill and Zohren assembled very strong evidence that quantum physics asympotically violates the bound as strongly as any non-local theory, as the dimension of the Hilbert spaces goes to infinity. Zohren - completing a PhD in theoretical physics at Imperial College, London - started a new PhD program in mathematics in Leiden under Gill's supervision.
In November Grünwald joined the group as one-day-a-week special professor, in an exchange agreement with CWI. Gill, Grünwald and Zohren have common interests in the intersection of forensic statistics and statistical learning. They started a collaboration with Knijffs (LUMC - human genetics) and Sjerps (NFI - forensic statistics) on the statistical analysis of forensic DNA profiles.

Meulman, working part-time at the mathematical institute and part-time at the pharmaceutical research institute LACDR, completed in collaboration with medical statistician Eilers and PhD student Rippe two papers on analysis of different kinds of SNP micro-array gene-expression data, succesfully applying novel multivariate techniques from psychometrics. She gave an invited address to a joint meeting at Caserta, Italy, of the French Classification Society and the Classification and Data Analysis Group of the Italian Statistical Society.
Gill continued to devote much time to the celebrated case of the 'serial killer nurse' Lucia de B. He was invited to give the LeCam lecture to the combined meetings of the French and the Canadian statistical societies at Montreal, Canada, and devoted his lecture to that topic. A similar recent case in Canada helped generate large interest in the lecture. Several papers are in preparation on various statistical aspects of the case.
Van Zwet worked on several multidisciplinary collaborations (traffic detectors, depression, DNA profiling, electricity pricing), and papers are in preparation on all these topics.

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 2008
Currently the focus is on one major project: developing an epistemological framework for the study of (the social role of) science and scientific expertise.

Kloosterman Professor 2008

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 was occupied in 2008 by Prof. Viacheslav (Slava) P. Belavkin, professor of applied mathematics at the Mathematics Department of the University of Nottingham, UK. Originally from the Ukraine, Slava Belavkin was educated at Moscow State University, where he was a student of Stratonovich, who independently developed the stochastic calculus known by his name – the main competitor of the Ito calculus. Belavkin works in quantum stochastic processes, with special emphasis on the interface between the underlying quantum world and the classical world around us. His theory of quantum filtering and prediction is nowadays used by state of the art experimenters to control macroscopic individual quantum systems such as Bose-Einstein condensates. It also underlies his novel approach to the infamous "measurement problem" of how to reconcile deterministic Schrödinger evolution of the wave function with its random collapse on measurement, when measurement itself is a physical process governed by the laws of quantum physics.

Belavkin gave research seminars to large audiences at Leiden, Amsterdam and Nijmegen, as well as the Kloosterman lecture itself in Leiden. He also met and talked with researchers in the field at other locations (Utrecht, Eindhoven) during informal visits. Though not yet formally organised in a research network, there does exist an active informal network with many PhD students working on the foundations of quantum theory between mathematics, physics and philosophy/history of science (among them, the groups of Dieks in Utrecht, Landsman in Nijmegen, Nieuwenhuizen in Amsterdam). Also researchers in quantum optics and in cosmology share interests (Bell tests, locality).

So far the main concrete research of the visit is a paper in preparation by Gill and Belavkin with the provisional title "Schrödinger's cat meets Occam's razor".

International and National Programmes

European Programmes:

Dutch-Russian Research Cooperation (NWO-RBFR): Geometric aspects of quantum theory and integrable systems.
2005-2008.
Cooperation with Moscow, St. Petersburg, Tambov, Twente, Utrecht, Amsterdam.
Project leader: G. van Dijk.

RTN: Arithmetic Algebraic Geometry.
2004-2008.
Cooperation with Barcelona (Spain), Bonn (Germany), Cambridge (England), Durham (England), Jerusalem (Israel), Milano (Italy), Münster (Germany), Padova (Italy), Paris 11 (France), Paris 13 (France), Regensburg (Germany), Rennes (France), Strasbourg (France), Tokyo (Japan).
Coordinator: S.J. Edixhoven.

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: 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, Not` ``ing-ham, Paris, Rome, Tel Aviv.
Project leader: B. de Smit.

Socrates program: Number Theory.
2006-2008.
Cooperation with Debrecen (Hungary).
Project leader: R. Tijdeman.

Socrates program: Number Theory.
2001-2008.
Cooperation with Ostrava (Czech Republic).
Project leader: R. Tijdeman.

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

National Programmes:

NWO SPINOZA-premie.
1999 – 2008.
Project leader: H.W. Lenstra.

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

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 program: Number Field Sieve.
2004-2008.
Cooperation with CWI.
Coordinator: R. Tijdeman.

NWO project: Radicals in arithmetic.
1/4/2004-1/4/2008.
Project leader: B. de Smit

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

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

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

Master Theses

E.D. van Werkhoven
title: Imputation methods for non-response in economical survey data
advisor: prof.dr. L.C.M. Kallenberg
date: 11-07-2008

R.P.M.J. Jurrius
title: Classifying polynomials of linear codes
advisor: dr. R.S. de Jong
date: 27-06-2008

M. Walenkamp
title: Forecasting stock index volatility
advisor: dr. E.W. van Zwet
date: 17-07-2008

J.H. Bakker
title: De partitieformule van Euler
advisor: dr. H. Finkelnberg
date: 29-08-2008

P.C. Hutter
title: Generic extensibility for the scheduler of an advanced planning system
advisor: prof.dr. L.C.M. Kallenberg
date: 22-08-2008

J. Wang
title: An heuristic approach to Markov decision processes based on the Interior point method
advisor: prof.dr. L.C.M. Kallenberg
date: 26-08-2008

A.A. van Boxtel
title: A Banach Space-Valued Stochastic Integral with respect to a Jump Process
advisor: dr. O. van Gaans
date: 19-09-2008

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.

M.E. Aharpour
title: Diagonalization and maximal torus reduction
advisor: dr. M. Lübke
date: 09-07-2008

Z. Chen
title: Correspondence between cubic algebras and twisted cubic forms
advisor: dr. L.D.J. Taelman
date: 09-07-2008

W.-W. Li
title: The Weil Representation and Its Character
advisor: dr. J.-L. Waldspurger
date: 09-07-2008

S. Liu
title: Trinomials and exponential Diophantine equations
advisor: prof.dr. H.W. Lenstra
date: 09-07-2008

A. Mohajer-Naser
title: Algebraic and analytic multiplier ideals and their applications
advisor: dr. R.S. de Jong
date: 09-07-2008

Hu Yong
title: R-equivalence and Zero-Cycles on 3-Dimensional Tori
advisor: dr. F.R.A. Doray
date: 09-07-2008

PhD Theses

S.W. Rosema June 3, 2008	Induced substitutions Thesis advisor: prof.dr. R. Tijdeman Leiden University
T. van den Bogaart June 4, 2008	Links between cohomology and arithmetic Thesis advisor: prof.dr. S.J. Edixhoven Leiden University
H.J. Hupkes June 12, 2008	Invariant Manifolds and Applications for Functional Differential Equations of Mixed Type Thesis advisor: prof.dr. S.M. Verduyn Lunel Leiden University
J. Kahn June 17, 2008	Quantum local asymptotic normality and other questions of quantum statistics Thesis advisor: prof.dr. R.D. Gill Leiden University
J.G. Bosman December 15, 2008	Explicit computations with modular Galois representations Thesis advisor: prof.dr. S.J. Edixhoven Leiden University

Publications

1. Number theory, Algebra and Geometry

1.1 Number Theory and Algebra

Papers in Journals and Proceedings

Borger,J., Smit, B. de, Maximal Lambda-orders over Z, Bull. London, *Math. Soc. (2008), 40(3) 439-446*

Brochard, S., Foncteur de Picard d'un champ algébrique, Mathematische Annalen, 62 pages.

Cramer, R. (Editor), Proceedings of 11th Annual IACR PKC, Springer Verlag, *LNCS (2008), vol. 4939, 396p.*

Cramer, R., Dodis, Y., Fehr, S., Padro, D., Wichs, D., Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors. In: Proceedings of 27th Annual IACR EUROCRYPT, Istanbul, Turkey, Springer Verlag, *LNCS (2008), vol. 4965, 471-488.*

Cramer, R., Daza, V., Gracia, I., Urroz, J.J., Leander, G., Marti-Farre, J., Padro, C., On Codes, Matroids, and Secure Multiparty Computation From Linear Secret-Sharing Schemes, *IEEE Transactions on Information Theory (2008), 54(6), 2644-2657.*

Chen, H., Cramer, R., Haan, R. de, Cascudo Pueyo, I., Ramp schemes with multiplication from high degree rational points on curves, in: Proceedings of 27th Annual IACR EUROCRYPT, Istanbul, Turkey, Springer Verlag, *LNCS (2008), vol. 4965, 451-470.*

Evertse, J.-H., Ferretti, R., A generalization of the Subspace Theorem with polynomials of higher degree, *In: Diophantine Approximation, Festschrift for Wolfgang Schmidt, H.P. Schlickewei, K.G. Schmidt, R.F. Tichy, eds., Proc. Conf. in honour of W. Schmidt's 70th birthday, Vienna, 2003, Springer Verlag, 2008, 175-198.*

Evertse, J.-H., Zannier, U., Linear equations with unknowns from a multiplicative group in a function fields, *Acta Arith. 133 (2008), 157-170, volume dedicated to Wolfgang Schmidt in honour of his 75th birthday.*

Evertse, J.-H., Bugeaud, Y., On two notions of complexity of algebraic numbers, *Acta Arith. 133 (2008), 221-250, volume dedicated to Wolfgang Schmidt in honour of his 75th birthday.*

Freeman, D., Stevenhagen, P., Streng, M., Abelian varieties with prescribed embedding degree, *Algorithmic Number Theory, Lecture Notes in Computer Science 5011 (2008), 60-73.*

Hajdu, L. Tijdeman, R., A criterion for polynomials to divide infinitely many k-nomials, *Diophantine Approximation, Developments in Mathematics, 16 (2008), Springer-Verlag, Wien, 211-220.*

Hancl, J. Tijdeman, R., On the irrationality of polynomial Cantor series, *Acta Arith. 133 (2008), 37-52.*

Hogendijk, J.P.,Ancient and modern secrets of Isfahan, *Nieuw Archief voor Wiskunde, fifth series, 9 (2008), p. 121.*

Kraaikamp, C., Schmidt, Th.A., Smeets, I., Tong's spectrum for Rosen continued fractions, *Journal de théorie des nombres de Bordeaux, 19, 3 (2007), 641-661.*

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

Luijk, R.M. van, The diameter of the circumcircle of a Heron triangle, *Elem. Math. 63, Issue 3, (2008), 118-121.*

Luijk, R.M. van, Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on K3 surfaces, *Mathematical Intelligencer 30,vol.4 (2008), 4-10..*

Saradha, N., Tijdeman, R., Arithmetic progressions with common difference divisible by small primes, *Acta Arith. 131 (2008), 267-279.*

Stevenhagen, P., The number field sieve, in: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press (2008), 83-100.*
Stevenhagen, P., The arithmetic of number rings, in: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press (2008), 209-266.*
Stevenhagen, P., Bröker, R., Constructing elliptic curves of prime order, *AMS Contemporary Math. 463 (2008), 17-28.*
Stevenhagen, P., Cohen, H., Computational class field theory, in: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press (2008), 497-534.*
Streng, M., Divisibility sequences for elliptic curves with complex multiplication. *Algebra & Number Theory 2 (2008), no. 2, 183-208.*
Tijdeman, R., Highlights in the research work of T.N. Shorey, in: *Diophantine Equations, ed. by N. Saradha, TIFR, Narosa Publ., New Delhi, India, 1-18.*
Tijdeman, R., On irrationality and transcendency of infinite sums of rational numbers, in: *Diophantine Equations, ed. by N. Saradha, TIFR, Narosa Publ., New Delhi, India, 279-296*

PhD Thesis
Rosema, S.W., Induced Substitutions, Ph.D. thesis, June 3, 2008.

Books
Buhler, J.P., Stevenhagen, P.(eds.), Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, *Mathematical Sciences Research Institute Publications vol. 44, Cambridge University Press (2008).*
H.W. Lenstra: Solving the Pell equation, 1-25, Lattices, 127-183, in: *Buhler, J.P., Stevenhagen, P.(eds.), Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, *Mathematical Sciences Research Institute Publications vol. 44, Cambridge University Press (2008).*

Other publications
Tijdeman, R., Het leven van een wiskundige, afscheidsrede, August 29, 2008

1.2 Arithmetic Geometry

Papers in Journals and Proceedings
Doray, F., Karpenkov, O., Schepers, J., Geometry of configuration spaces of tensegrities, *J. Discrete & Computational Geometry, arXiv: 0806.4976*
Jong, R.S. de, Gauss map on the theta divisor and Green's functions. In: *S.J. Edixhoven, G. van der Geer and B. Moonen (eds.), Modular Forms on Schiermonnikoog, Cambridge University Press 2008.*
Taelman, L., Artin t-motifs, *Journal of Number Theory, Available online 7 October 2008.*

PhD Theses
Bogaart, Th. Van den, Links between cohomology and arithmetic, defended on June 4, 2008.
Bosman, J. Explicit computations with modular Galois representations, to be defended on December 15, 2008.
Chênevert, G., Exponential sums, hypersurfaces with many symmetries and Galois representations, Ph.D. thesis, McGill University, Montreal, Canada (2008), 172 p.

Books
Edixhoven, S.J., Geer, G. van der, Moonen, B.(editors), Modular forms on Schiermonnikoog, *Cambridge University Press, (2008). ISBN-13-987-0-521-49354-3.*

Other publications
Bogaart, Th. van den, About the choice of a basis in Kedlaya's algorithm, *arXiv:0809.1243*.
Bogaart, Th. van den, The de Rham comparison theorem for Deligne-Mumford stacks, *arXiv:0809.1242.*
Edixhoven, S.J., Jong, R.S. de, Schepers, J.A.W., Covers of surfaces with fixed branch locus, *Preprint. Arxiv:math.AG/0807.0184.*

2. Analysis and Stochastics

2.1 Analysis and Dynamical Systems

Papers in Journals and Proceedings
Besseling, N., Bokhove, O., Kolechkina, A., Molenaar, J., Nooyen, R. van, Rottschäfer, V., Stein, A., Stoorvogel, A., Math Fights Flooding, Proceedings of the sixty-third European Study Group with Industry *(2008), 47-63*.
Brijder, R.; Hoogeboom, H.J.; Muskulus, M. Strategies of Loop Recombination in Ciliates, *Discrete Applied Mathematics 156 (2008), 1736-1753, DOI: 10.1016/j.dam.2007.08.032.*
Carpentieri, G., Koren, B., Tooren, M.J.L. van, Development of the discrete adjoint for a 3D unstructured Euler solver, *Journal of Aircraft, 45 (2008), 237-245.*
Cate, A. ten, Geurts, B.J., Muskulus, M., et al., Modeling and simulation of phase-transitions in multi-alloy aluminium castings, In: *Proceedings of the sixty-third European Study Group Mathematics with Industy, Enschede, The Netherlands (2008), Bokhove, O., Hurink, J., Meinsma, G., et al.(eds.), 117-139.*
Clément, P., Desch, W., An elementary proof of the triangle inequality for the Wasserstein metric, *Proc. Amer. Math. Soc. 136 (2008), 333-339*.
Clément, P., Desch, W., Wasserstein metric and subordination, *Studia Math. 189 (1) (2008) 35-52.*
Clément, Ph., Zacher, R., Global Smooth Solutions to a Fourth-order Quasilinear Fractional Evolution Equation, in *Functional Analysis and Evolution Equations, The Gunter Lumer Volume. 131-146, H. Amann and al. eds, (2007) Birkauser Verlag Basel/Switzerland*
Dijk, G. van, Pevzner, M., H*-algebras and quantization of para-Hermitian spaces, *Proc. Amer. Math. Soc. 136 (2008), 2253-2260.*
Dijk, G. van, (*U(p,q), U(p-1,q)*) is a generalized Gelfand pair, DOI 10.1007/s00209-008-0335-4 (online publication in Mathematische Annalen).
Dijk, G. van, *(GL(n+1, R), GL(n,R)) is a generalized Gelfand pair, Russian J. Math. Physics 15 (2008), 548-551*.
Ferracina L., Spijker M.N., Strong stability of singly-diagonally-implicit Runge-Kutta Methods, *Appl.Numer.Math. 58 (2008), 1675-1686.*
Gaans, O. van, Kalauch, A., Bands in pervasive pre-Riesz spaces, *Oper.Matrices 2 (2008), 2, 177-191.*
Gaans, O. van, Kalauch, A., Ideals and bands in pre-Riesz spaces, *Positivity 12 (2008), 4, 591-611.*
Gabrielsson, J., Peletier, L.A., A flexible nonlinear feedback system that captures diverse patterns of adaptation and rebound; *The AAPS Journal; 10(1):70-83*
Geldof, M., Freijer, J I., Peletier, L.A., Beijsterveldt, L. van, Danhof. M., Mechanistic model

for the acute effect of fluvoxamine on 5-HT and 5- HIAA concentrations in rat frontal cortex, *European journal of pharmaceutical sciences, 33(3), 217-229*
Gerritsma, M., Bas, R. van der, Maerschalck, B. de, Koren, B., Deconinck, H., Least-squares spectral element method applied to the Euler equations, *International Journal for Numerical Methods in Fluids, 57 (2008), 1371-1395.*
Hassen, Y., Koren, B. , A monotone, higher-order accurate, fixed-grid finite-volume method for advection problems with moving boundaries, *Proceedings of the Fourth International Conference on Advanced Computational Methods in Engineering (ACOMEN 2008), May 26-28, Liege.* http://www.ltas.ulg.ac.be/acomen2008/proceedings_all.htm
Hille, S.C. Local well-posedness of kinetic chemotaxis models, *J. Evol. Equ.8 (2008), 423-448.*
Hupkes, H.J., Verduyn Lunel, S.M., Center manifolds for periodic functional differential equations of mixed type, *J. Differential Equations 928 (2008), 6, 1526-1565.*
Hupkes, H.J., Augeraud-Véron, E., Verduyn Lunel, S.M., Center projections for smooth difference equations of mixed type, *J. Differential Equations 244 (2008), 4, 803-835.*
Muskulus, M.; Verduyn Lunel, S., Reconstruction of functional brain networks by Wasserstein distances in a listening task, In: *Kakigi, R.; Yokosawa, K.; Kuriki, S. (eds): Biomagnetism: Interdisciplinary Research and Exploration. Hokkaido University Press, Sapporo, Japan (2008), 59-61.*
Muskulus, M.; Verduyn-Lunel, S. The Analysis of Dynamical Diseases by Optimal Transportation Distances, *ERCIM News 73 (2008), 16-17.*
Muskulus, M. Identification of P system models assisted by biochemical databases, In: *Ibarra, O. H.; Sosik, P. (Eds.) Prague International Workshop on Membrane Computing. Preliminary proceedings, Sileasian University in Opava, Faculty of Philosophy and Science (2008), 46-49.*
Muskulus, M.; Slats, A.M.; van der Plas D.T.; Verduyn Lunel S.J., Sterk, P.J., Discrimination of asthma and COPD by reconstructing unbiased probability distributions (attractors) from the dynamics of respiratory impedance, *American Journal of Respiratory and Critical Care Medicine 177 (2008), A947 (Abstracts Issue).*
Rottschäfer, V., Multi-bump, self-similar, blowup solutions of the Ginzburg Landau equation, *Physica D 237 (2008), 510-539.*
Svensson, C., Silvestrov, S., Jeu, M.F.E. de, Connections Between Dynamical Systems and Crossed Products of Banach Algebras by *Z, In:Methods of Spectral Analysis in Mathematical Physics, Conference on Operator Theory, Analysis and Mathematical Physics (OTAMP) 2006, Lund, Sweden, Operator Theory: Advances and Applications 186, Janas, J., Kurasov, P., Laptev, A., Nabokov, S., Stolz, G. (eds.), 391-401, Birkhauser, (2008).*
Wackers, J., Koren, B., Efficient computation of steady water flow with waves, *International Journal for Numerical Methods in Fluids, 56 (2008), 1567-1574.*
Wackers, J., Koren, B., A surface capturing method for the efficient computation of steady water waves, *Journal of Computational and Applied Mathematics, 215 (2008), 618-625*.

Books

Dijk, G. van, Gelfand pairs and beyond, *COE Lecture Note vol. 11, Kyushu Unversity (2008).*

Special journal issue

Brandts, J., Koren, B., Verwer, J.G. (eds.), Special Issue in Honor of Piet Hemker, *Applied Numerical Mathematics, 58 (2008), Issue 12, 1759-1993.*

Other publications
Hille, S.C., Worm, D.H.T., Embedding of semigroups of Lipschitz maps into positive linear semigroups on ordered Banach spaces generated by measures, *to appear in Journal of Integral Equations and Operator Theory.*
Jeu, M. de, Hoeveel is oneindig?, *Euclides 83-5, (2008), 262-264*.
Muskulus, M. Speltheorie voor beginners, *Eureka! 20 (2008), 8-10*.
Muskulus, M., Waal H. de, Over luie studenten, groepsdynamica en pokeren, *Nieuw Archief voor Wiskunde 5/9 (2008), 287-290.*

2.2 Probability Theory

Papers in Journals and Proceedings
Angel, O.,Goodman, J.,Hollander, F. den, Slade, G., Invasion percolation on regular trees, *Annals of Probability 36 (2008), 420-466.*
Chazottes, J.R., Collet, P., Redig, F., Coupling, concentration and stochastic dynamics, *Journal of Mathematical Physics, 49 (2008).*
Cirillo, E.N.M., Nardi, F.R., Spitoni, C., Metastability for reversible probabilistic cellular automata with self-interaction, *Journal of Statistical Physics (2008)*, *132*(3), *431-471.*
Cirillo, E.N.M., Nardi, F.R., Spitoni, C., Competitive nucleation in reversible probabilistic cellular automata, *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics (2008)*, *78(4), 040601-1/4.*
Fey-den Boer, A., Meester, R., Quant, C., Redig, F., A probabilistic approach to Zhang's model *Comm. Math. Phys. 280(2008) , 351-388.*
Fey-den Boer, A., Redig, F., Limiting shapes for deterministic centrally seeded growth models, *J. Stat. Phys., 130 (2008), 579-597.*
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, (2008).*
Heidergott, B., Hordijk A., Weisshaupt, H., Derivatives of Markov kernels and their Jordan decomposition, *J. of Applied Analysis, 14, No. 1 (2008), 13-26*.
Hollander, W.Th.F. den, Senden, W.J.M.,Zwet, W.R.van, EURANDOM: A decade of European stochastics, in: EURANDOM 1998-2008: A random tour through a decade of research (eds. I. Adan, A. Di Bucchianico and R. van der Hofstad), *Statistica Neerlandica 62 (2008), 256-265.*
Hollander, F. den, Abelprijs 2007: S.R. Srinivasa Varadhan, *Nieuw Archief voor Wiskunde 9 (2008), 192-197.*
Jarai, A.A., Redig, F., Infinite volume limit of the abelian sandpile model in dimensions $d \leq 3$ *,Prob. Theory Rel. Fields 141 (2008), 181-212.*
Spieksma, F.M.,Hordijk, A., Popov, N., Discrete scattering and simple and non-simple face-homogeneous random walks. *Prob. Engin. Inf. Sc. 22 (2008)*, *2, 163-189.*

2.3 Mathematical and Applied Statistics

Papers in journals and proceedings
Draisma, H.M., Reijmers, Th.H., Bobeldijk-Pastorova, I., Meulman, J.J., et al, Similarities and differences in lipidomics profiles among healthy monozygotic twin pairs. *OMICS, A journal of integrative biology, 12, 17-31.*
Fisher N.I. and Zwet, W.R. van, Remembering Wassily Hoeffding, *Statistical Science 23 (2008), 4, 536-547.*

Gibescu, M., Kling, W.L., Zwet, E.W. van, Bidding and regulating strategies in a dual imbalance pricing system, *International Journal for Energy Technology and Policy 6 (2008, 240-253.*
Gill, R.D. and Grünwald, P.D., An algorithmic and a geometric characterization of coarsening at random, *Annals of Statistics 36(2008), 2409-2422.*
Gill, R.D., Concilliation of Bayes and pointwise quantum state estimation, in: *V.P. Belavkin and M. Guta (eds), Quantum Stochastics and Information: statistics, filtering and control, 239-261 (2008), World Scientific.*
Meulman, J.J., Heiser, W.J. *Categories 18.0, Chicago: SPSS inc*.
Posthuma, B., Cator, E.A., Veerkamp, W., Zwet, E.W. van, Combined Analysis of Paid and Incurred Losses, *Proceedings Casualty Loss Reserve Seminar, Washington, DC. On-line: Fall CAS e-forum, 272-293.*
Zohren, S., Ambjørn, J., Loll, R., Watabiki, Y., Westra, W., A new continuum limit of matrix models, *Phys. Lett. B670(2008), 224-230.*
Zohren, S., Ambjørn, J., Loll, R., Watabiki, Y., Westra, W., A Causal Alternative for c=0 Strings, *Acta Phys. Polon. B39 (2008),3355-3364.*
Zohren, S. and Gill, R.D., On the maximal violation of the Collins-Gisin-Linden-Massar-Popescu inequality for infinite dimensional states, *Phys. Rev.Lett. 100 (2008), 120406(4).*

PhD Thesis
Kahn, J., Quantum local asymptotic normality and other questions of quantum statistics,
Ph.D. Thesis, June 17, 2008.

Mathematical Institute Reports

MI 2008-01
F. den Hollander
Abelprijs 2007: S.R. Srinivassa Varadhan

MI 2008-02
N.B. Andersen, M.F.E. de Jeu
Real Paley-Wiener theorems and local spectral radius formulas

MI 2008-03
N.B. Andersen, M.F.E. de Jeu
Local spectral radius formulas on compact Lie groups

MI 2008-04
G. van Dijk
(GL(n + 1), R), GL(n,R)) is a generalized Gelfand pair

MI 2008-05
A. Bovier, F. den Hollander, C. Spitoni
Homogeneous nucleation for Glauber and Kawasaki dynamics in large volumes at low temperatures

MI 2008-06
F.R.A. Doray, O. Karpenkov, J.A.W. Schepers
Geometry of configuration spaces of tensegrities

MI 2008-07
S.J. Edixhoven, R.S. de Jong, J.A.W. Schepers
Covers of surfaces with fixed branch locus

MI 2008-08
O. Karpenkov
Constructing multidimensional periodic continued fractions in the sense of Klein

MI 2008-09
O. Karpenkov
Bernoulli-Euler numbers and multiboundary singularities of type B n^1

MI 2008-10
M. Birkner, A. Greven, F. den Hollander
Quenched large deviation principle for words in a letter sequence

MI 2008-11
F. den Hollander, N. Petrelis
On the localized phase of a copolymer in an emulsion: subcritical percolation regime

MI 2008-12
S.C. Hille, D.T.H. Worm
Embedding of semigroups of Lipschitz maps into positive linear semigroups on ordered Banach spaces generated by measures

MI 2008-13
P.C. Svensson, J. Tomiyama
On the commutant of C(X) in c-crossed products by Z and their representations.*

MI-2008-14
F. van Rest, F.M. Spieksma
Taboos in PageRank Computation

MI-2008-15
J. Bierkens
Pathwise Lyapunov exponents for linear stochastic differential equations

MI-2008-16
A. Bérczes, J.-H. Evertse, K. Győry
Effective results for linear equations in two unknowns from a multiplicative division group

MI-2008-17
A. Bérczes, J.-H. Evertse, K. Győry, C. Pontreau
Effective results for points on certain subvarieties of Tori

MI-2008-18
J. Gärtner, F. den Hollander, G. Maillard
Intermittency on catalysts: three-dimensional simple symmetric exclusion

MI-2008-19
M. Birkner, A. Greven, F. den Hollander
Collision local time of transient random walks and intermediate phases in interacting stochastic systems

MI-2008-20
J.-R. Chazottes, P. Collet, F. Redig, E. Verbitskiy
A concentration inequality for interval maps with an indifferent fixed point

MI -2008-21
J.-R. Chazottes, F. Redig
Concentration inequalities for Markov processes via coupling

MI-2008-22
A.C.D. van Enter, F. Redig, E. Verbitskiy
Gibbsian and non-Gibbsian states at Eurandom

MI-2008-23
C.Giardinà, J. Kurchan, F. Redig, K. Vafayi
Duality and hidden symmetries in interacting particle systems

MI- 2008-24
L.A. Peletier, N. Benson, P.H. van der Graaf
Impact of plasma-protein binding on receptor occupancy:
An analytic description

MI-2008-25
H.-M. Nguyen, L.A. Peletier
Monotonicity of time to peak response with respect to drug dose for turnover models

MI 2008-26
H.-M. Nguyen, L.A. Peletier
Monotonicity of the Peak Time in Turnover Models

MI 2008-27
J. Gabrielsson, L.A. Peletier
Nonlinear turnover models for systems with physiological limits

MI 2008-28
R. Tijdeman, L.Q. Zamboni
Fine and Wilf words for any periods II

MI 2008-29
R. Tijdeman, L.Q. Zamboni
Characterizations of words with many periods

MI 2008-30
T.N. Shorey, R. Tijdeman
Generalizations of some irreducibility results by Schur

MI 2008-31
J. Hancl, R. Tijdeman
On the irreducibility of factorial series II

MI 2008-32
J.-H. Evertse
On the quantitative subspace theorem

MI 2008-33
B.E. van Dalen
Stability results for uniquely determined sets from two directions in discrete tomography

MI 2008-34
B.E. van Dalen
On the difference between solutions of discrete tomography problems

MI 2008-35
Rippe, R.A.H., Eilers, P.H.C, Meulman, J.J.
Psychometric modeling of structure in fluorescence intensities of SNP arrays

MI 2008-36
Rippe, R.A.H., Eilers, P.H.C, Meulman, J.J.
SNP calibration of illumina bead arrays

MI 2008-37
R.D. Gill
Statistics, ethics, and probiotica

MI 2008-38
Kraaijkamp, I. Smeets
Sharp bounds for symmetric and asymmetric Diophantine approximation

MI 2008-39
L.D.J. Taelman
Special L-values of t-motives: a conjecture

MI 2008-40
S.J. Edixhoven
On the computation of the coefficients of modular forms

MI 2008-41
T.C. Streng
Computing Igusa class polynomials

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*

Metastability,
EURANDOM, Eindhoven, January 9-11.
W.Th.F. den Hollander

Mathematics of Operations Research,
Lunteren, January 15-16.
L.C.M. Kallenberg

Seminar Operations Research and Energy
Lunteren, January 17
L.C.M. Kallenberg

Special Session on Low Genus Curves and Applications
San Diego, California, January 2008.
P. Stevenhagen.

Intercity Number Theory Seminar
Amsterdam, The Netherlands, February 29
H.W. Lenstra

4th IACR PKC Conference
Barcelona, Spain, March 9-12
R. Cramer

A special day in the Intercity Number Theory Seminar, on the occasion of Wilberd van der Kallen's 61st birthday
Utrecht, The Netherlands, March 14
S.J. Edixhoven

Intercity Number Theory Seminar
Amsterdam, The Netherlands, April 4
H.W. Lenstra

Workshop "Brauer-Manin obstructions",
Warwick, United Kingdom, April 14-18
R.M. van Luijk

Intercity Number Theory Seminar
Amsterdam, The Netherlands, April 18
H.W. Lenstra

Intercity Number Theory Seminar
Amsterdam, The Netherlands, May 9
H.W. Lenstra

Diamant-symposium
Oegstgeest, The Netherlands, May 29-30
H.W. Lenstra

Hash functions in cryptology: theory and practice
Leiden, The Netherlands, June 2-6
R. Cramer

Number Fields, Lattices and Curves
Cetraro, Italia, June 2-6
Bart de Smit

Summer School on Noncommutative Integration
Leiden, The Netherlands, June 9 - 13
M.F.E. de Jeu

Fifth European Congress of Mathematics
Amsterdam, The Netherlands, June 14-18
H.W. Lenstra

Workshop on Computational number theory
Hong Kong, June 2008.
P. Stevenhagen and H. W. Lenstra

Organisation of the workshop “Algebraic Geometry”
Leiden, The Netherlands, June 30-July 4
S.J. Edixhoven

Mini-symposium on Mathematical Cryptology
Amsterdam, The Netherlands, July 16
R. Cramer

Galois Theory and Explicit Methods
Amsterdam, The Netherlands, July 18
B. de Smit

Invited paper sessions on quantum statistics
Singapore, July 18
R.D. Gill

Workshop "Operator Structures and Dynamical Systems"
Leiden, The Netherlands, July 21-25
M.F.E. de Jeu

Symposium Number Theory & Discrete Mathematics
Leiden, The Netherlands, August 27-28
J.-H. Evertse

Seminar De toekomst van de wiskunde in Nederland
Leiden, The Netherlands, August 29
J.-H. Evertse, L.C.M. Kallenberg, F. Bakker and J. Batenburg

N.G. de Bruijn 90 jaar
Eindhoven, The Netherlands, September 5
H.W. Lenstra

Intercity Number Theory Seminar
Leiden, The Netherlands, September 12
H.W. Lenstra

3rd Mathematics Foundations of Cryptology
Barcelona, Spain, September 22-26
R. Cramer

Intercity Number Theory Seminar
Leiden, The Netherlands, October 10
H.W. Lenstra

Galois Theory and Explicit Methods
Bordeaux, France, October 13-17
B. de Smit

Workshop “The Hasse principle”,
Bogota, Columbia, October 21-25
R.M. van Luijk

DIAMANT meets GQT
Leiden, The Netherlands, October 27-31
H.W. Lenstra

Meeting of Stochastics,
Lunteren, November 12-14
R.D. Gill

Intercity Number Theory Seminar
Groningen, The Netherlands, November 14
H.W. Lenstra

Conference “Arithmetic of K3 surfaces,”
Banff, Canada, November 30-December 5
R.M. van Luijk

Intercity Number Theory Seminar
Amsterdam, The Netherlands, December 12
H.W. Lenstra

Interacting Particle Systems, Statistical Mechanics and Probability Theory
Paris, France, September-December 2008
W.Th F. den Hollander

General Mathematics Colloquium, monthly,
Leiden
J.-H. Evertse and F. Redig

DIAMANT Intercity number theory seminar
Varying locations, bi-weekly
B. de Smit

Research seminar on Faltings heights of covers
Leiden, weekly
S.J. Edixhoven

RISC (Research in Information Security and Cryptology) Seminar
Leiden and Amsterdam, monthly
R. Cramer

Cryptography seminar
Rennes, France
S.J. Edixhoven

Geometry Seminar
Leiden
L. Taelman en A. Stolk

BioScience Colloquium
Leiden, monthly
L.A. Peletier

Joint Leiden/Delft seminar on Banach space theory
Leiden, biweekly.
M.F.E. de Jeu

NDNS+-bioseminar 'Evolutionary theory'
Leiden, biweekly
S.C. Hille and S.M. Verduyn Lunel

Invited lectures

1.1 Number theory and Algebra

R. Cramer
- Computing in the Dark Using Algebraic Geometry, Madrid, Spain, February 15.
- Hoe te overtuigen zonder bewijzen prijs te geven, Amsterdam, The Netherlands, April 25.
- Hoe te overtuigen zonder bewijzen prijs te geven, Utrecht, The Netherlands, June 20.
- How to be convincing without giving proofs away? Secure computation!, Lausanne, Switzerland, July 4.
- Hoe te overtuigen zonder bewijzen prijs te geven, Leiden, The Netherlands, September 17.
- Hoe te overtuigen zonder bewijzen prijs te geven, Amsterdam, The Netherlands, October 19.
- Hoe te overtuigen zonder bewijzen prijs te geven, Leiden, The Netherlands, October 20.
- Algebraic Geometric Aspects of Secure Computation, Dortmund, Germany, November 9.
- Computing in the Dark Using Algebraic Geometry, Singapore, November 17.
- Better bounds on ideal t-strongly multiplicative LSSS using divisor exclusion, Dagstuhl, Germany, December 4.

J.-H. Evertse
- On the Quantitative Subspace Theorem, Bonn, Germany, May 5.
- Approximation of complex algebraic numbers by complex algebraic numbers of bounded degree, Ostravice, Czech Republic, June 10.
- Approximation of complex algebraic numbers by complex algebraic numbers of bounded degree, Waterloo, Canada, July 18.
- Approximation of complex algebraic numbers by complex algebraic numbers, Leiden, The Netherlands, August 27.
- On the Quantitative Subspace Theorem, Toronto, Canada, October 24.

H.W. Lenstra
- Degrees of field automorphisms, Leiden, The Netherlands, February 15.
- Escher and the Droste effect, Trondheim, Norway, February 22.
- Standard models for finite fields, Trondheim, Norway, February 22.
- Zooming in to Escher's Print gallery, Rome, Italy, March 13-16.
- Standard models for finite fields, Pisa, Italy, April 29.
- Escher and the Droste effect, Pisa, Italy, April 30.
- Escher and the Droste effect, Oxford, England, May 24.
- Standard models for finite fields, Hong Kong, Taiwan, June 17-27.
- Cyclic affine permutations, Leiden, The Netherlands, August 27-28.
- Defining F_q, Nijmegen, The Netherlands, September 26.
- Standard models for finite fields, Utrecht, The Netherlands, October 9.
- Het getal nul als fundament van de wiskunde, Leiden, The Netherlands, October 15.
- Wat kost een priemgetal?, Amsterdam, The Netherlands, November 11.

R.M. van Luijk
- K3 surfaces with Picard number one and infinitely many rational points, Vancouver, Canada, February 11.
- Manin conjectures for K3 surfaces, SFU, UK, February 22.

- Canonical divisors on hypersurfaces, Warwick, UK. April 14.
- Picard groups of del Pezzo surfaces, Warwick, UK, April 15.
- Growth of rational points, Warwick, UK, April 16.
- Galois cohomology I, Warwick, UK, April 17.
- Galois cohomology II, Warwick, UK, April 18.
- Density of rational points on diagonal quartic surfaces, Bristol, UK, May 5.
- Density of rational points on diagonal quartic surfaces, Oxford, UK, May 12.
- Density of rational points on diagonal quartic surfaces, Berkeley, USA, May 27.
- Density of rational points on diagonal quartic surfaces, Rennes, France, June 12.
- Density of rational points on diagonal quartic surfaces, Warwick, UK, June 16.
- Density of rational points on diagonal quartic surfaces, Hong Kong, China, June 26.
- Density of rational points on diagonal quartic surfaces, Waterloo, Canada, July 14.
- Density of rational points on diagonal quartic surfaces, Leiden, The Netherlands, September 12.
- Pythagorean Boxes, Leiden, The Netherlands, September 26.
- Introduction to the Hasse Principle, Bogota, Colombia, October 21.
- Quadratic forms I, Bogota, Colombia, October 22.
- Quadratic forms II, Bogota, Colombia, October 23.
- Density of rational points on diagonal quartic surfaces, Bogota, Colombia, October 23.
- Classification of quadratic forms over Q, Bogota, Colombia, October 24.
- Character varieties, Leiden, The Netherlands, November 17.
- Batyrev-Manin conjecture for K3 surfaces, Banff, Canada, December 2.

B. de Smit
- Escher en the Droste effect, Zeist, The Netherlands, March 5.
- Enumerating ABC triples, Eindhoven, The Netherlands, April 1.
- Escher and the Droste effect, Amsterdam, The Netherlands, May 28.
- Escher and the Droste effect, Spijkenisse, The Netherlands, June 11.
- Escher en het Droste-effect, Amsterdam, The Netherlands, September 10.
- Consistent isomorphisms between finite fields, Nijmegen, The Netherlands, September 26.
- Standard models for finite fields, Bordeaux, France, October 17.
- Zeta functions, Laplace spectra and G-sets, Leiden, The Netherlands, November 3.

P. Stevenhagen
- CM-constructions in genus 1 and 2, San Diego, USA, January 7.
- Prime densities for linear recurrent sequences, San Diego, USA, January 17
- Being a mathematician, San Diego, USA, January 28.
- Complex multiplication constructions in cryptography, Utrecht, The Netherlands, February 14.
- Escher und der Droste Effekt, Konstanz, Switzerland, February 24.
- Complex multiplication constructions in cryptography, Konstanz, Switzerland, February 25.
- Complex multiplication in low genus, Cetraro, Italy, June 6.
- Efficient CM-constructions, Hong Kong, Taiwan, June 26.
- Cryptografie voor iedereen, Lunteren, The Netherlands, August 7.
- Constructing abelian varieties for cryptographic use, Utrecht, the Netherlands, September 21.
- Escher und der Droste Effekt, Köln, Germany, November 7.
- Continuous methods for discrete problems, Eindhoven, The Netherlands, November 26.

M. Streng
- Igusa Class Polynomials, San Diego, USA, January 7.
- Elliptic Divisibility Sequences with Complex Multiplication, Irvine, USA, January 17.
- Igusa Class Polynomials, Utrecht, Netherlands, April 18.
- Abelian varieties with prescribed embedding degree, Banff, Canada, May 20.
- Igusa Class Polynomials, Cetraro, Italy, June 6.
- Abelian varieties with prescribed embedding degree, Palaiseau, France, June 10.
- Igusa Class Polynomials, Seattle, USA, December 5.

R. Tijdeman
- Words with many periods, Prague, Czech. Republic, May 27.
- Die mühsame Ehe von Addition und Multiplikation, Vienna, Austria, June 12.
- On irreducibility of polynomials, Vienna, Austria, June 13.
- Irreducibility results of Schur-type, Debrecen, Hungary, November 14.

1.2 Arithmetic Geometry

S.J. Edixhoven
- How to count vectors with integral coordinates and given length in n-dimensional space Düsseldorf, Germany, January 18.
- Computation of Galois representations associated to modular forms: numerical part using finite fields, after Couveignes, Essen, Germany, January 22.
- Computation of Galois representations associated to modular forms, with an application to lattices, Leuven, Belgium, March 5.
- On the computation of cooefficients of modular forms, Amsterdam, Netherlands, July 14.
- Subvarieties of Shimura varieties, Oberwolfach, Germany. September 30.
- Néron models, Leiden, The Netherlands, October 17.
- Sur les sommes de carrés d'entiers, Rennes, France, November 13.
- Arakelov theory and bounding the complexity of computing Galois representations, Rennes, France, December 19.

G. Chênevert
- The quartic fields method, Leiden, The Netherlands, September 12.
- Exponential sums, hypersurfaces with many symmetries and Galois representations, Montreal, Canada, August 22.

R.S. de Jong
- Arithmetic positivity of line bundles on the moduli space of stable curves, Bonn, January 9.
- On the discriminants of hyperelliptic curves, Warwick, United Kingdom, July 14.
- Hitchin fibration and Neron models Utrecht, The Netherlands, November 21.
- Heights of ramified covers, Rennes, France, December 19.

J.P. Murre
- The Picard motive revisited", Mumbai, India, January 6.
- Introduction to the Theory of Motives, Mumbai, India, February 15.
- On Grothendieck's work on the algebraic fundamental group, Peyresq, France, August 26.

L. Taelman
- Torsors and transcendental numbers, Heidelberg, Germany, February 4.
- Special values of L-functions: conjectures, variations, computations, Oegstgeest, The Netherlands, May 21.
- Characteristic p special L-values, Amsterdam, The Netherlands, November 20.
- Special L-values of t-motives: a conjecture, Essen, Germany, November 13.
- Hodge structures for t-motives, Essen, Germany, November 14.

2.1 Analysis and Dynamical Systems

Ph. Clément
- Schauder estimates for a degenerate second-order elliptic operator on a cube, Pau, France, January 7
- Schauder estimates for a degenerate second-order elliptic operator on a cube, Toulouse, January 8
- An elementary proof of the triangle inequality for the Wasserstein metric, Trieste, Italy, February 28
- An introduction to gradient flows in metric spaces, Kagurazaka Analysis Seminar, Tokyo, Japan, June 26
- An introduction to gradient flows on probability spaces, Lausanne, Switzerland, October 25-December 11

G. van Dijk
- Gelfand pairs and beyond, Tokio, Japan, April/May.

O.W. van Gaans
- Periods of nonexpansive maps on finite dimensional normed spaces, Nijmegen, The Netherlands, February 27.
- Stochastic integration in Banach spaces relative to Levy processes, Delft, The Netherlands, April 7
- Stationary solutions of stochastic delay differential equations, Dresden, Germany, December 18

S.C. Hille
- Long-term dynamics of kinetic chemotaxis models: motivation, first results and long-term perspectives, Utrecht, The Netherlands, February 20.
- Embedding of semigroups of Lipschitz maps into linear semigroups on Banach spaces generated by measures, Delft, The Netherlands, December 11.

B. Koren
- Applications of advanced numerical methods for fluid dynamics, Eindhoven, The Netherlands, March 14.
- ECCOMAS and CFD, the flow goes on, Barcelona, Spain, April 25.
- A monotone, higher-order accurate, fixed-grid finite-volume method for convection problems with moving boundaries, Venice, Italy, July 1.
- Computing compressible two-fluid flow, Delft, The Netherlands, September 19.
- Computational methods for compressible flows, Delft, The Netherlands, October 15.
- A physical model and numerical method for compressible, two-fluid flow, Leiden, The Netherlands, November 18.

L.A. Peletier
- Dynamical Systems in Pharmaceutical Science, Tours, France, January 31.
- Dynamical Systems in Pharmaceutical Science, Amsterdam, The Netherlands, April 8.
- Dynamical Systems in Pharmaceutical Science, Haifa, Israel, May 26.
- The Turnover Model in Pharmacodynamics, Parijs, France, July 3.
- Turnover and Feedback Models in Pharmacodynamics, München, Germany, July 23.
- Dynamical Systems Methods for Analysing Turnover Models, Stockholm, Sweden, September 9.
- Dynamical Systems in Pharmaceutical Science, Swansea, UK, September 15.

- Elliptic Equations with Critical Exponent on Spherical Caps of S^3, Middletown, USA, October 30.
- Dynamical Systems in Pharmaceutical Science, Boston, USA, November 3**.**
- Dynamics of Protein Binding, Leiden, The Netherlands, November 10.

M.N. Spijker
- Monotonicity in the numerical solution of initial value problems, Vienna, Austria, September 19.

V. Rottschäfer
- Dynamics between CWI and Leiden, Leiden, The Netherlands, April 10.

C. Svensson
- Ideal intersection properties of commutative subalgebras of C*-crossed products, Leiden, The Netherlands, July 21.

M. Wortel
- Crossed products associated with Banach algebra dynamical systems, Leiden, The Netherlands, July 25.
- Groepsacties op Banachruimten, Nijmegen, The Netherlands, October 23.

2.2 Probability Theory

W. Th.F. den Hollander
- Invasiepercolatie, Noordwijk, The Netherlands, February 2.
- Invasion percolation, Aachen, Germany, February 6.
- Copolymers near selective interfaces, Strasbourg, France, May 29.
- Metastability under stochastic dynamics, Amsterdam, The Netherlands, June 11.
- A quenched large deviation principle for words in a letter sequence, Oberwolfach, Germany, June 6.
- Random walk in random scenery, Sao Paulo, Brazil, July 31.
- Percolation, Sao Paulo, Brazil, August 1.
- On the potential-theoretic approach to metastability, Ouro Preto, Brazil, August 5.
- Intermittency on catalysts, Vienna, Austria, October 2.
- Percolation, Namur, Belgium, October 16.
- Metastability, Paris, France, December 15-19.

F. Redig
- Sandpile percolation, Rouen, France, May 27.
- Abelian sandpiles, Paris, France, December 3-5.

2.3 Mathematical and Applied Statistics

R.D. Gill
- Health Care Serial Killers (HCSKs): a world epidemic, or just bad statistics?, Liverpool, Great Brittain, April 10.
- Perfect passion at a distance (how to win at Polish poker with quantum dice), München, Germany, January 25.
- Science versus Justice: the case of Lucia de Berk, Leiden, The Netherlands, February 26.
- Introduction to Forensic Statistics, Leiden, The Netherlands, February 27.
- Epidemiological and statistical flaws in the judicial process of Lucia de B, Amsterdam, The Netherlands, March 25.
- Why Bell's Theorem is Relevant and still Untested, Berlin, Germany, April 29.
- Hunting serial killer nurses with statistics, Ottawa, Canada, May 26.
- Careless Statistics Costs Lives, Rotterdam, The Netherlands, June 24.
- Why Bell's Theorem is more relevant than ever, Växjö, Sweden, August 27.
- Careless Statistics Costs Lives: the probiotica trial, Delft, The Netherlands, September 17.
- Careless Statistics Costs Lives: the probiotica trial, Amsterdam, The Netherlands, September 17.
- Forensic statistics: not ready for consumption?, Leusden, The Netherlands, September 27.
- Polish poker and the Bell inequality, Utrecht, The Netherlands, October 28.

J.J. Meulman
- Ordering and scaling objects in multivariate data under nonlinear transformations of variables. Caserta, Italy, June 13.
- Clustering of Objects on Subsets of SNPs. Philadelphia, USA, November 10.

W.R. van Zwet
- The birth of modern statistics: A centenary of Student's test, Vilnius, Lithuania, June 6.
- A decade of EURANDOM, Eindhoven, The Netherlands, August 28.

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

F. den Hollander
- Annals of Probability
- Annales Henri Poincaré
- Electronic Communications in Probability
- Electronic Journal of Probability
- Markov Processes and Related Fields
- Indagationes Mathematicae
- Stochastic Processes and Applications

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
- Applied Numerical Mathematics (guest editor special issue on the occasion of P.W. Hemker's retirement)

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

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 (managing editor)
- Operator Theory Advances and Applications (series of monographs, Birkhäuser)

Honors

R.D. Gill
- LeCam lecture at joint meeting of Statistical Society of Canada and French Statistical Society at Ottawa, May 26.

R. Tijdeman
- Benoeming tot ridder in de Orde van de Nederlandse Leeuw

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

- S. Akiyama, Niigata, Japan, R. Tijdeman.
- B. Baran, Roma, Italy, B. de Smit.
- J. Batenburg, Antwerpen, Belgium, R. Tijdeman.
- A. Berczes, Debrecen, Hungary, J.-H. Evertse.
- F. Beukers, Utrecht, The Netherlands, R. Tijdeman.
- J. Borger, Canberra, Australia, B. de Smit.
- Y. Bugeaud, Strasbourg, France, R. Tijdeman.
- K. György, Debrecen, Hungary, J.-H. Evertse.
- L. Hajdu, Debrecen, Hungary, R. Tijdeman.
- J. Hancl, Ostrava, Czech Republic, R. Tijdeman.
- B. Hanzon, Cork, Ireland, B. de Smit.
- M. Keane, Connecticut, USA, R. Tijdeman.
- P. Moree, Bonn, Germany, R. Tijdeman.
- C.Popescu, USA, P.Stevenhagen.
- K.-T. Rühl, Lausanne, Switzerland, B. de Smit.
- S. Siksek, Warwick, United Kingdom, R. Tijdeman.
- I. Suarez, Lausanne, Switzerland, B. de Smit.
- L. Thomas, Lausanne, Switzerland, B. de Smit.
- L. Zamboni, Denton,.USA, R. Tijdeman.

1.2.Arithmetic Geometry

- Chia-Fu Yu, China, S.J. Edixhoven.
- A. Perucca, Rome, Italy, S.J. Edixhoven.
- B. Marmeth, Rennes, S.J. Edixhoven.
- J.-M. Couveignes, Toulouse, France, Edixhoven.
- K. van Zyl, Stellenbosch, South Africa, S.J. Edixhoven.
- B. Totaro, Cambridge, USA, S.J. Edixhoven.
- J. Klueners, Düsseldorff, Germany, S.J. Edixhoven.
- G. Wiese, Essen, Germany, S.J. Edixhoven.
- G. Remond, Grenoble, France, R.S. de Jong.
- D. Roessler, Paris, France, R.S. de Jong.
- U. Kuhn, Hamburg, Germany, R.S. de Jong.
- M. Saito, Kyoto, Japan, J.P. Murre.
- J. D. Lewis, Edmonton, Canada, J.P. Murre.

2. Analysis and Stochastics

2.1. Analysis and Dynamical Systems

- A. Kalauch, Dresden, Germany, O. van Gaans

- B. Lemmens, Warwick, United Kingdom, O. van Gaans
- M. Riedle, Manchester, O. van Gaans
- J. Tomiyama, Tokio, Japan, M.F.E. de Jeu
- V. Timperio, Turin, Italy, V. Rottschäfer.
- J.-W. van de Meent, Cambridge, United Kingdom, V. Rottschäfer

2.2. Probability Theory

- M. van den Berg, Bristol, United Kingdom, W.Th.F. den Hollander.
- M. Birkner, Berlin, Germany, W.Th.F. den Hollander.
- A. Bovier, Bonn, Germany, W.Th.F. den Hollander.
- D. Dawson, Ottawa, Canada, W.Th.F. den Hollander.
- A. Gaudillière, Rome, Italy, W.Th.F. den Hollander.
- J. Gärtner, Berlin, Germany, W.Th.F. den Hollander.
- J. Goodman, Vancouver, Canada, W.Th.F. den Hollander.
- A. Greven, Erlangen, Germany, W.Th.F. den Hollander.
- G. Maillard, Marseille, France, W.Th.F. den Hollander.
- F. Manzo, Rome, Italy, W.Th.F. den Hollander.
- E. Olivieri, Rome, Italy, W.Th.F. den Hollander.
- N. Petrelis, Berlin, Germany, W.Th.F. den Hollander.
- E. Scoppola, Rome, Italy, W.Th.F. den Hollander.
- G. Slade, Vancouver, Canada, W.Th.F. den Hollander.
- J. R. Chazottes, Paris, France, F. Redig.
- L. Levine, Boston, USA, F. Redig.

2.3. Mathematical and Applied Statistics

- V.P. Belavkin, Nottingham, UK, R.D. Gill.
- P. Massart, Orsay (Paris X), France, R.D. Gill.
- B. Sanctuary, McGill Univ., Canada, R.D. Gill.

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	
prof.dr. H.W. Lenstra	
dr. R.M. van Luijk	(from March 1)
dr. B. de Smit	
prof.dr. P. Stevenhagen	
prof.dr. R. Tijdeman	(till August 1)

emeritus:

prof.dr. R. Tijdeman	(from August 1)

PhD students:

drs. J. Bouw	
drs. J.F. Brakenhoff	
drs. J.L.A.H. Daems	
B.E. van Dalen, MSc.	
drs. W.H. Ekkelkamp	(CWI)(till October 1)
drs. W.J. Palenstijn	
drs. S.W. Rosema	(till June 1)
ir. I. Smeets	
drs. T.C. Streng	
E.L. Toreao Dassen, MSc.	

guest researchers:

drs. H.M. Matthijsse	(LIO)(from September 1)
drs. B. Zevenhek	(LIO)(till August 1)
G. Dalla Torre, MSc.	(from September 1)

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	(from September 1)
dr. G. Chênevert	(from September 1)

dr. F.R.A. Doray
dr. O. Karpenkov (till September 1)
dr. J.A.W. Schepers (till September 1)
dr. L.D.J. Taelman

PhD students:
drs. J.G. Bosman (till September 1)
drs. P.J. Bruin
drs. A.P. Stolk

guest researchers:
drs. J.V. van Zijl (from September 1)

2. Analysis and Stochastics

2.1 Analysis and Dynamical Systems

permanent staff:
dr. O. van Gaans
dr. S.C. Hille
dr. M.F.E. de Jeu
prof.dr.ir. B. Koren (from March 1)
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

postdocs:
dr. A. Es-Sahir (till November 1)
dr. B.A. van de Rotten (till September 1)

PhD students:
ir. G.N.J.C. Bierkens
drs. H.J. Hupkes (till May 1)
M. Muskulus, Dipl.Math.
drs. M. van der Schans
I. Stojkovic, MSc.
P.C. Svensson, MSc.
drs. D. Worm
M. Wortel, MSc.

guest researchers:
dr. P. Haccou
prof.dr. H. Metz
prof.dr. S. van Strien (from 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 (from November 1)
dr. F.M. Spieksma

emeritus:
prof.dr. A. Hordijk

postdocs:
dr. C. Spitoni (UL/Eurandom)(till November 1)

PhD student:
drs. L. Avena
A. Troiani, M.Sc. (from September 1)
drs. K. Vafayi (from February 1)
F.M. Völlering, Dipl. Math. (from October 1)
F. Wang, M.Sc. (from September 1)

guest researcher:
prof. R. Fernandez

2.3 Mathematical and Applied Statistics

permanent staff:
prof.dr. R.D. Gill
prof.dr. P.D. Grünwald (from November 1)
prof.dr. J.J. Meulman
dr. E.W. van Zwet

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

PhD student:
Drs. S. Zohren (from August 1)

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

3. Mathematics, Computer Science and Society

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

Support Staff

managing director:
drs. F. Bakker

management support:
T.A. Dijks

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

computer systems:
X. Cheng
M.F. Feleus
M. Vijn

secretariat:
T.H. Bakker-Bouma

Student Assistants

education:

Y. Achnine	(from September 1)
L. de Boer	(from September 15)
A.A. van Boxtel	(till September 1)
H.P. Chang	(till September 1)
M. Derickx	
W. Ellens	(from September 1)
T.E. Feenstra	(from September 1)
M.M.W. Fung	(from September 1)
C.S.L. de Graaf	(from September 1)
F. van Helden	(from September 1)
A. Javanpeykar	(till September 1)
J. Jin	(from September 1)
A.K.A. Kalsbeek	
M. Kosters	
J. Michielsen	(from September 15)
A. Nooitgedagt	
S. Ramawadh	
P. Rogaar	
A. Schouten	(till September 1)
E. Siero	
L. Smit	
A. Stolwijk	(till September 1)
T. Vorselen	
J. van Wamelen	(from September 1)
J. Weimar	(till September 1)

tutor:

J.B.A. Hemerik	(from November 24)
S.A. van Lieshout	(from November 24)
R.M.J. Vooys	(from November 20)
R.A.C.H. Wols	(from November 20)

webmaster:

F.W. van Rest

pr:

W. Ellens	(till September 1)
G. Hauwert	(till September 1)
V. Hisken	(from November 1)
F. Offergelt	
B. de Rijk	(from September 1)
J. Rozendaal	(till November 1)

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. 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. R. Tijdeman (till August 1)
Prof.dr. S.M. Verduyn Lunel

Institute Council

Dr. B. de Smit, chairman
Dr. H. Finkelnberg
Drs. H.J. Hupkes (till May 1)
Dr. V. Rottschäfer