Martin Barlow (University of British Columbia)

The Directors of the three institutes, CRM, Fields and PIMS are pleased to announce that Martin Barlow from UBC is the recipient of the 2009 CRM – Fields – PIMS Prize. Martin Barlow is a leading figure in probability and the leading international expert in diffusion on fractals and other disordered media. In addition, the impact of his work has been important in such diverse fields as partial differential equations, including major progress on the De Giorgi conjecture, stochastic differential equations, the mathematical finance of electricity pricing, filtration enlargement and branching measure diffusions.

Already in the 1980s, Martin Barlow settled a long open problem of probability theory, by providing necessary and sufficient conditions (the latter with J. Hawkes) for the continuity of local times of Lévy processes. This was the resolution of a thirty-year old problem which had attracted the efforts of Hale Trotter, Ronald Getoor and Harry Kesten among others. His conditions have paved the way for the study of the connection between local times and Gaussian processes.

In the 1990s his detailed study of diffusions on a variety of fractals and fractal-like sets opened a new area of study in probability, making him the leading international expert in the behaviour of diffusions on fractals and other disordered media. The study of the diffusion on the Sierpinski gasket and carpet, started with Ed Perkins in 1986 and then Richard Bass in 1988, served as a testing ground for diffusion in highly inhomogeneous media, a domain of interest for the physics community which is now within mathematical reach. Barlow remains at the leading edge of this research with his recent work giving sharp results for the behaviour of transition probabilities for random walks on supercritical percolation clusters. The pioneering papers on the diffusion on the Sierpinski carpet attracted to the domain experts in Dirichlet forms, diffusions on manifolds and statistical mechanics. Martin Barlow currently is at the forefront of a program to study the transport properties of a broad class of graphs and manifolds.

Martin Barlow received his undergraduate degree from Cambridge University in 1975 and completed his doctoral degree with David Williams at the University College of Swansea in Wales in 1978. He held Royal Society University Research Fellowship at Cambridge University from 1985 to 1992, when he joined the Mathematics Department at University of British Columbia. He currently is Professor of Mathematics at UBC. He has held a number of visiting professorships at leading universities including University of Tokyo, Cornell University, Imperial College London, and Université de Paris.

Martin Barlow gave an invited lecture at the 1990 ICM in Kyoto and was an invited lecturer at the prestigious Saint-Flour Summer School in 1995. In 2008 he received the Jeffery – Williams Prize of the Canadian Mathematical Society. Other past distinctions include the Rollo Davidson Prize from Cambridge University, the Junior Whitehead Prize from the London Mathematical Society. He has been a leader of the international probability community, as a lead organiser of numerous conferences, Associate Editor of all the top probability journals and Editor-in-Chief of the Electronic Communications in probability. He is a Fellow of the Institute of Mathematical Statistics since 1995, of the Royal Society of Canada since 1998 and in 2006 was elected Fellow of the Royal Society (London).

I am honoured to have been awarded the 2009 CRM – Fields – PIMS Prize. I have been asked to write a short account of my research, and find it easiest to do so chronologically. In retrospect, a unifying theme for much of my research in the last 20 years has been random walks (or diffusion) in irregular media.

In the first few years after my Ph.D. I worked on a variety of problems in the theory of martingales and stochastic differential equations. In the summer of 1985 Ron Horgan, an applied mathematician at Cambridge, showed me a physics paper on the spectral properties of the Sierpinski gasket. (This is a triangle-based fractal constructed by a procedure analogous to the usual Cantor set.) I realised that the construction of a limiting diffusion on this set was an interesting problem, and the following January, when I visited Ed Perkins at UBC, we began to work on this. We found later that S. Goldstein (continued on page 10)
Grande Conférence du CRM

Le mouvement chaotique du système solaire
Jacques Laskar (Observatoire de Paris)
de Christiane Rousseau (Université de Montréal)

Le 9 octobre, Jacques Laskar donnait la première grande conférence de l’automne 2008 sous le titre provocateur « Le système solaire est chaotique ». Le public s’est présenté nombreux, incluant des groupes d’étudiants de collèges et des moins jeunes que l’exploration du ciel a toujours fascinés.

La conférence a commencé par un historique du sujet et des nombreuses preuves de stabilité du système solaire. Jacques Laskar a rappelé les lois de Kepler. Il a parlé des « preuves de stabilité » d’Euler et de Lagrange qui se sont initialement révélées en désaccord avec les données expérimentales, pour finalement conduire à l’introduction de nouvelles méthodes : les méthodes perturbatives pour Euler et l’invariance des grands axes des planètes pour Lagrange, ceci provenant de l’étude du système linéarisé. Le conférencier a montré les données historiques des Chaldéens, transmises par Ptolémée, qui ont conduit Halley à conclure que Jupiter se rapprochait du soleil tandis que Saturne s’en éloignait. Le triomphe de Laplace a consisté à regarder des termes perturbatifs d’ordre supérieur. Cette étude lui a permis de découvrir la présence des oscillations périodiques des grands axes des planètes (avec une période de l’ordre de 800 ans), laquelle expliquait parfaitement les variations observées depuis l’antiquité. Jacques Laskar a ensuite expliqué la découverte du chaos par Henri Poincaré et le fait qu’il était théoriquement possible dans le système solaire, tout en insistant sur un écrit ultérieur de Poincaré, montrant clairement que ce dernier ne s’attendait pas à trouver du chaos dans le système solaire.

Jacques Laskar a ensuite sauté à la période moderne, marquée par la simulation du système solaire à l’ordinateur. Il a parlé de la divergence exponentielle des trajectoires et des difficultés que cela pose pour la simulation numérique : le pas ne doit pas être trop grand par rapport à la période. Après un certain nombre de pas, on perd le contrôle sur les trajectoires à cause de l’accumulation des erreurs. D’où l’intérêt de regarder le système moyenné sur le temps rapide, ce qui permet de se concentrer sur les mouvements lents. Comme la période est beaucoup plus grande, cela permet de prendre des pas de temps beaucoup plus grands et de garder le contrôle des simulations sur des périodes de temps beaucoup plus longues. Ces simulations permettent de suivre l’évolution des paramètres caractérisant l’orbite : l’excentricité, la précession (la rotation de l’axe de la Terre), etc.

Jacques Laskar a fait état des études récentes mettant en évidence la remarquable corrélation entre les oscillations de l’axe de la Terre et les périodes glaciaires, lesquelles sont explorées via l’étude des sédiments marins.

Les résultats de Jacques Laskar des années 1990 montrent l’existence de chaos parmi les planètes internes du système solaire (Mercure, Terre, Vénus). Il est expliqué par la présence de résonances dans les paramètres des orbites de ces planètes. Il permet une faible expansion de l’excentricité des orbites de ces planètes. L’expansion de ces excentricités permet à son tour de faire varier les périodes de révolution des planètes. Lors de ces variations on s’approche de résonances, ce qui accélère le phénomène et permet de montrer l’existence de trajectoires où l’orbite de Mercure croise celle de Vénus. Lorsqu’on simule le système moyenné sur cinq milliards d’années, on observe que les excentricités de Mercure et de Vénus peuvent subir des variations suffisantes pour permettre des collisions. Le conférencier a comparé des simulations sur un modèle contenant la relativité générale et sur un modèle l’excluant. Il s’avère que lorsqu’on enlève la relativité, le chaos est beaucoup plus fort.

Jacques Laskar a expliqué comment on pouvait contrer le problème de la divergence exponentielle pour simuler des trajectoires réalistes. On simule des ensembles de trajectoires ayant des conditions initiales proches sur des périodes de temps pas trop longues. Ensuite, on simule un nouvel ensemble de trajectoires ayant des conditions initiales proches de la condition d’arrivée. On se trouve ainsi à simuler des trajectoires par morceaux. Lorsqu’on cherche des trajectoires pouvant mener à une collision, on choisit parmi ces trajectoires celles qui conduisent à la plus grande excentricité pour Mercure. On montre ainsi l’existence de trajectoires par morceaux conduisant à une collision. Une technique de « lemme d’ombrage » permet de conclure à l’existence d’une vraie trajectoire qui lui ressemble, pour une condition initiale très proche.

(suite à la page 10)
Admitted to Uppsala University at the age of thirteen, Svante Janson received his BA at the age of fourteen and his doctoral degree in functional analysis on his 22nd birthday in 1977. This was followed by a second doctoral degree in probability theory in 1984, all at Uppsala University, where he was appointed professor in 1985.

He had a bicephalous career, making a mark in functional analysis starting with his influential 1981 paper “Minimal and maximal methods of interpolation” (Journal of Functional Analysis), and moving into probability theory and its applications in combinatorics, random structures and algorithms during the last three decades. He was awarded several prizes, including the prestigious Göran Gustafsson Prize in 1992.

He wrote over 200 papers, and four books. Probability theorists know his books “Poisson Approximation” (with Andrew D. Barbour and Lars Holst, 1992) and “Random Graphs” (with Tomasz Łuczak and Andrzej Rucinski, 2000) very well. In the field of random graphs, which was created in 1959 by Erdős and Rényi, many consider Janson’s 126-page paper “The birth of the giant component” (1993, with Knuth, Łuczak, and Pittel) one of the finest ever written. It gives a precise description of the nature of the phase transition in random graphs when the edge probabilities are about 1/n. Janson is also known for his analyses and ingenious proof methods of many newer random graph models that are being created to explain social, web, computer, and other networks.

Introduction

In 1959, Erdős and Rényi proposed and analysed the basic model for random graphs, now known as “the $G_{n,p}$” model, which is at the root of hundreds of modern applications. A graph is a pair $(V,E)$, where $V$ is a set of $n$ vertices labelled 1 through $n$, and the set of edges, $E$, is a subset of $V \times V$. In a $G_{n,p}$, each possible edge $(i,j)$ is selected independently with probability $p$. This graph exhibits a phase transition at $p = 1/n$, that is, when $p = c/n$, with $0 < c < 1$, the graph consists with high probability (abbreviated whp in this report) of small connected components of size $O(\log n)$. For $c > 1$, there is whp just one large component, whose size is linear in $n$, while all other components remain small ($O(\log n)$). At $c = 1$, there is an interesting sudden transition called “the birth of the giant,” in which some components of size $n^{2/3}$ briefly coexist. Janson himself has written a book with Ruczinski and Łuczak on this model, and has analysed the transition in depth in a hundred-page paper with Knuth, Łuczak and Pittel.

The physical web, the Internet of links on web pages, computer networks, cellular phone networks, and other communication networks can be modelled by graphs, but the simplistic $G_{n,p}$ is usually inadequate. The two main reasons for this lack of fit are the distribution of the degrees (number of neighbours) of the vertices, and the association between vertices and a physical location in some Euclidean space. Thus were born many probabilistic models to fill the void. In his Aisenstadt lecture for a general public, Janson described various models.

In the first group, we find the so-called small world models, in which the number of nodes of degree $d$ are asymptotic to a constant times $n/d^d$, where typically, $\gamma \in [2,3]$. A few popular high-degree nodes exist, and this causes the (graph) distances between nodes to be small. More generally, one can consider degree-driven models, with $(V,E)$ having nodes of prescribed degrees $d_1, \ldots, d_n$, and all graphs with such a degree sequence being equally likely. More about this model, proposed by Molloy and Reed, below. Related to this are models based on activity levels $a_i$, $1 \leq i \leq n$, where we connect $i$ with $j$ with probability $\lambda_{ij} a_i a_j$, and $\lambda_{ij}$ depends upon $n$ only. Finally, the web link model and social networks demand incrementally defined models. The earliest model in this group is the preferential attachment model, in which vertex $i$ is born at time $i$, and connects to node $j < i$ with probability proportional to $(1 + d_j)^\alpha$. The choice $\alpha = 1$ describes the original model of Barabási and Albert, while the choice $\alpha > 2$ is almost trivial—one vertex will receive almost all connections.

Each of Janson’s three technical lectures focused on a particularly interesting generalisation of $G_{n,p}$. The main task at hand is to investigate the component structure and to identify the phase transition for the birth of the giant. Secondary tasks in-
clude the analysis of the sizes of the connected components and their combinatorial parameters such as the diameter and maximal degree. Janson focused mainly on the phase transitions.

In 2006, Bollobas and Riordan, both at Cambridge then, and authors of a recent book on percolation, teamed up with Janson on a project in which they defined and analysed homogeneous random graphs. The goal was to add a geometric element to the random graph structure. Given are \( n \) independent identically distributed random points \( x_1, \ldots, x_n \) on \([0,1]\), which provide a geometric anchor for the \( n \) vertices. Let \( K: [0,1]^2 \to [0,\infty) \), the kernel, be a nonnegative symmetric function, and let us connect \( i \) to \( j \) with probability \( p_{ij} = K(x_i,x_j)/n \), independently for all pairs \((i,j)\). When \( K \) is constant, this yields the \( G_{n,p} \) model. One can in general replace \([0,1]\) and the Lebesgue measure on it by a space \( S \) and a probability measure \( \mu \) on \( S \). Janson attacked this problem by partitioning \([0,1]\) (or \( S \)) into a finite grid, and calling all members of each set in the partition a tribe. Edges between members of different tribes appear with certain nearly constant probabilities if \( K \) is smooth enough. Using the theory of multitype Bienaymé–Galton–Watson branching processes, Janson was able to deduce a necessary and sufficient condition for the existence of a giant component, under some regularity conditions on \( K \). If \( T \) is the integral operator \( T f(x) = \int_{[0,1]} K(x,y)f(y) \, dy \) on \( L^2([0,1],dx) \), then a giant exists if and only if the spectral radius of \( T \) is strictly greater than one.

The following growth paradigm is often useful when studying giant components of random graphs. Start at a vertex \( v \) and visit the neighbours (generation one), then the neighbours of the neighbours (generation two), and so forth, halting either when the process becomes extinct or the number of nodes visited is substantial (a suitably large number \( \omega_n \), which diverges to \( \infty \) but remains \( o(n) \)). This is often modelled as a Bienaymé–Galton–Watson branching process, possibly of multitype. Roughly then, the probability that \( v \) is in a giant component is the probability \( \rho \) that the approximating branching process survives, plus \( o(1) \), and the expected size of all giants together is then \( \rho n + o(n) \), so that one only needs to take care of the matter of establishing that there is only a single giant. This link with Bienaymé–Galton–Watson processes leads to a fascinating number of relatively easy analyses, because it is well known that such processes survive with a positive probability if and only if the mean offspring is greater than one. Furthermore, the survival probability is easily derived from the offspring distribution.

The main starting point in these studies is the fundamental paper by Molloy and Reed and its extension by Luczak and Janson. Assume that the degrees of a graph on \( n \) nodes are fixed as \( d_1,\ldots,d_n \). Let \( D = D_X \) where \( X \) is uniformly drawn from \( \{1,\ldots,n\} \): it is the degree of a randomly drawn node. Assume also that the graph is equally likely among all graphs with the given degree sequence. As \( n \) varies, so do the degree sequences and the distribution of \( D \). To fix things, assume however that \( D \) tends in distribution to a random variable \( D_\infty \) which has a positive and finite mean. Assume also that \( E D^2 \) is uniformly bounded over \( n \) and that \( P\{D_\infty = 1\} > 0 \). Then analysis based on the survival or extinction of the Bienaymé–Galton–Watson process shows that three phases exist, according to whether \( \mu = E\{D_\infty(D_\infty - 2)\} \) is positive, zero, or negative. In the positive mode, the largest giant component is of size \( pn + o(n) \) whp, where \( p > 0 \) depends upon the distribution of \( D_\infty \) and can be explicitly derived. If \( \mu < 0 \), the largest component is \( o(n) \) whp. Interestingly, Janson was also able to describe the behaviour at the threshold itself, when \( \mu = 0 \), and obtain the rate of convergence to infinity of the size of the largest component.

The same model is also useful for studying epidemics, which can be regarded as percolation. In a given random graph, edges are kept independently with probability \( p \) (the probability of infection) and are removed otherwise, a case that can be regarded either as noninfection or vaccination. The question now is whether the graph is broken up into a multitude of small components, or whether one large component survives. The latter case would correspond to an ineffective vaccination campaign, for example. Under minor assumptions, a giant component (of linear size) occurs whp for large \( n \) if \( E\{D_\infty(D_\infty - (1 + 1/p))\} > 0 \). For example, in a random regular graph of degree \( 4 \), all such graphs being equally likely, a giant occurs whp if and only if \( p > \frac{1}{2} \). To avoid a disastrous epidemic, therefore, a proportion of the population strictly greater than \( \frac{1}{2} \) should be vaccinated, but vaccinating more is not necessary.

In his last lecture, Janson considered the susceptibility of a random graph, i.e., the average size of the components in which the vertices live, \((1/n) \sum C_i^2\), where the component sizes are denoted by \( C_i \). For the \( G_{n,p} \), when \( 1 - np \) is much larger than \( n^{-1/3} \), a range that includes the so-called subcritical case and the lower part of the critical case, he showed an elegant proof that shows that the susceptibility is whp asymptotic to \( 1/(1 - np) \). Again, the idea of random clocks for births of edges and continuous time turned out to be useful, because averages and variances are functions of time which satisfy tractable differential equations.

Svante Janson has placed all his work on his web site. He has laid the analytic, combinatorial and probabilistic foundations for studying many models of random graphs and networks. At this early point in this developing field, it is essential to have results for models that are as broad as possible, and to have proofs that are as transparent and straightforward as possible. For the most interesting aspect of such random networks, the moment of percolation or birth of the giant component, he has done just that.
Random Functions, Random Surfaces and Interfaces

by Senya Shlosman (Centre de physique théorique) and Steve Zelditch (Johns Hopkins University)

This is a report on the workshop on Random functions, Random Surfaces and Interfaces, organised by Dick Bond (Toronto), Michael R. Douglas (Rutgers), Scott Sheffield (Courant, NYU), Senya Shlosman (CPT, Marseille) and Steve Zelditch (Johns Hopkins), which took place Jan. 4 – 10, 2009.

First, a word on what random functions or surfaces are. Examples from nature include the surface of the sea in heavy weather, the cosmic microwave radiation background, the electric field intensity of a laser speckle pattern, or random noise in signals. Random surfaces and interfaces are often modelled as graphs of Gaussian random functions. Classics include the book of Paley-Wiener in the 30s (with a chapter on random functions), the work of S. A. Rice and M. Kac on peaks of random functions of one variable, the work of M. S. Longuet-Higgins in the early 60s on the higher dimensional case with applications to water waves. The initial matter distribution of the universe was modelled as a Gaussian random function by Ya. B. Zeldovich in the 70s. Random surfaces form a chapter in A. Polyakov’s well-known book on Gauge Fields and Strings, and are the basis of his string theory. They are also used to model the early universe in current string theory and quantum gravity. In another direction they arise as interfaces in statistical mechanics.

The simplest random fields are the Gaussian random fields \( f(x) \sim \sum_{j=1}^{\infty} a_j(\omega) \phi_j(x) \) where \( \{\phi_j\} \) is an orthonormal basis for a Hilbert space \( \mathcal{H} \) and where the coefficients \( a_j(\omega) \) are independent (real or complex) Gaussian random variables of mean zero and variance one. If the sum is finite, the field is smooth and one can study the landscape formed by its graph. When the random graph is \( L^2 \) normalised, one may visualise it as a random mountain chain with a characteristic height. Imagine submerging it under water and slowly lowering the sea level. At first one sees an isolated peak. Then as the level is lowered one sees a collection of peaks. When further lowered, one sees ridges and land bridges. These features are easily seen in computer graphics and immediately generate obvious questions as to the height at which new features form and the distribution of the peaks or zeros.

Gaussian infinite series are often very singular as functions, but are also important. For instance, the Gaussian free field on a Riemannian manifold is a random eigenfunction expansion, where the inner product is defined by \( \langle f, g \rangle \nabla = \int_M \nabla f \cdot \nabla g \) dV.

The workshop was interdisciplinary, with participants ranging from astrophysics to string theory to statistical mechanics to probability and geometry.

For mathematicians, a focal point was the recent work of Duplantier–Sheffield giving a rigorous definition of Polyakov’s Liouville field theory and a proof of the so-called KPZ formula. Liouville theory is a theory of random metrics on a Riemann surface. Duplantier–Sheffield define its area form on a bounded planar domain \( D \) as the weak limit as \( \epsilon \to 0 \) of the random measure

\[
\mu_\epsilon := e^{\gamma^2/2} e^{h_\epsilon(z)} d^2 z,
\]

where \( h_\epsilon \) is the mean value of an instance of the Gaussian free field on \( D \) on the circle of radius \( \epsilon \) centred at \( z \). They prove that for \( \gamma \in [0, 2) \) along powers of \( 2 \), the measures \( \mu_\epsilon \) converge weakly to a limiting measure \( \mu_\gamma = e^{\gamma h} d^2 z \). The KPZ relation is a relation between Euclidean scaling exponent

\[
x = \lim_{\epsilon \to 0} \frac{\log E \mu_\epsilon(B_\epsilon(X))}{\log \epsilon^2},
\]

where \( B_\epsilon(X) \) is the \( \epsilon \)-neighbourhood of \( X \subset D \), and is the quantum scaling exponent,

\[
\Delta = \lim_{\epsilon \to 0} \frac{\log E \mu(B^\delta(X))}{\log \delta},
\]

where

\[
B^\delta(X) = \{ z : B^\delta(z) \cap X \neq 0 \},
\]

where \( B^\delta(z) \) is the isothermal quantum ball of area \( \delta \) centred at \( z \), i.e., the Euclidean ball so that \( \mu(B^\delta(z)) = \delta \). The KPZ relation asserts that

\[
x = \frac{\gamma^2}{4} \Delta^2 + \left( 1 - \frac{\gamma^2}{4} \right) \Delta.
\]

The astrophysicists spoke largely about the distribution of “matter” in the universe. It is believed that the fluctuations in the initial distribution of matter were Gaussian random. The evolution in time of the matter distribution is often modelled as the evolution of Gaussian random initial data under the Euler–Poisson equation. The distribution seems to remain roughly Gaussian for a few hundred thousand years, but eventually gravitational attraction causes matter to clump in non-Gaussian filamentary structures. This is a modification of the original Zeldovich picture whereby matter clumped in the walls of a cell-like structure (“pancake model”). Matter clumps near highest peaks in the original matter distribution and forms ridges between them. An approximate and almost geometric picture of this evolution is given by a random map known as the Zeldovich approximation. The astrophysicists pointed out that for a random set, numerical simulations and data on the matter distribution. A lot of interest was focused on the Morse–Smale complex of a Gaussian random function, i.e., the gradient lines connecting critical points which differ
by one in their index. Pogosyan presented a mathematically convincing picture whereby the ridges or filaments were concentrated along the directions where the gradient of the random field is an eigenvector of its Hessian. M. R. Douglas gave a survey of questions and results pertaining to the landscape problem in string theory and in chaotic inflation, which raises a number of problems he has studied with his collaborators Ashok, F. Denef, B. Shiffman, S. Zelditch. Ben Baugher, a postdoc, spoke on his recent proofs of a number of conjectures of Douglas–Shiffman–Zelditch on the growth rate of the number of critical points of the relevant Gaussian random fields as the dimension tends to infinity or as the degree of the field tends to infinity. Graduate student S. Klevtsov discussed his joint work with Douglas on balanced Kähler metrics and their connection to black hole physics, the main idea being that both objects maximise related notions of entropy.

The talks by Richard Kenyon, Pavel Bleher and Senya Shlosman were dealing with random surfaces arising in certain exactly solvable models. One such model is obtained by considering the dimer coverings or random tilings of lattices and other periodic graphs. The most famous one concerns the tiling of the two-dimensional plane by lozenges. Such tilings can be naturally viewed as surfaces, carrying the corresponding probability distribution. The most known problem here is the existence of the asymptotic shape of the random surface as the mesh of the lattice goes to zero. This problem is closely related to the study of the ground states of certain modes of statistical physics, in particular, the Ising model, with appropriate boundary conditions, which force the interface to appear. It turns out that the asymptotic shape in question does exist, and is given by precise algebraic-geometric construction, involving Harnak curves. Moreover, the Harnak curves are parametrised by the dimer coverings with periodic weights, which is in itself a striking result.

P. Bleher was investigating the related circle of problems for the six-vertex model with the domain-wall boundary condition. Again, the problem there is about the study of the asymptotic limit shape of the corresponding random surface and the determination of the location of the arctic circle line. This problem can be solved on the free-fermion line of the phase diagram.

K. Khanin was discussing problems related to directed polymers in quasi-stationary random potentials. Such potentials correspond to disordered systems interacting with a chaotic external field. He have shown that the transversal fluctuations for such directed polymers are of the same order as the Kardar–Parisi–Zhang scaling \( n^{2/3} \), although the system belongs to a different universality class. Until recently the results of that type were obtained by reduction of the problem to the question of the random matrix theory, though it seems that the above scaling has to be valid in much more broad situation. So this result deals with the problem directly, without using random matrices.

Sergei Nechaev was computing the asymptotic distribution of scaled height in various \((1+1)\)-dimensional anisotropic ballistic deposition model. Some of them can be mapped to the Ulam problem of finding the longest nondecreasing subsequence in a random sequence of integers. The known results for the Ulam problem imply that the scaled height in the model has the Tracy–Widom distribution, appearing in the theory of random matrices near the edges of the spectrum. This result supports the hypothesis that various growth models in \((1+1)\) dimensions that belong to the Kardar–Parisi–Zhang universality class share the same universal Tracy–Widom distribution for the suitably scaled height variables.

Finally, there were several talks on the more “geometric” aspects of smooth random surfaces such as defined by random holomorphic polynomials or power series in several variables or by real Gaussian random fields on Riemannian manifolds. R. J. Adler gave a survey of his works with J. Taylor and A. Takamura on the Euler characteristic approximation to high excursion sets. This approximation at least heuristically is based on the fact that a high excursion set (= the mountain chain above a high sea level) appears to have just one component which is a ball. Hence its Euler characteristic is zero. So the probability that the top of a random surface is above that level is the expected value of the Euler characteristic. The actual rigorous proof is based on integral geometry and tube volumes. M. Sodin presented some of his many results with Tsirelson, Nazarov, Volberg and others on Gaussian random analytic functions and their zeros. Among other things, he discussed his results on the random Morse-Smale complex of the weighted norm square \( \lvert f \rvert^2 e^{-\phi} \) of a random entire analytic function \( f \) on \( C \). Its local minima occur at the zeros of the function. The basins of attraction of the local minima decompose the plane into domains of fixed area. Computer graphics of M. Krishnapur show that each of these basins (which all have area one) tend to have eight tentacle like arms separating them from neighbouring basins. Sodin presented many results and conjectures on this picture, which were close to the problems of interest to the astrophysicists. Each basin should have on average \( \frac{3}{5} \) neighbours with which it shares a gradient line as boundary. On average 8 basins should meet at each local maximum.

S. Zelditch discussed joint results with O. Zeitouni on large deviations for empirical measure of zeros for random holomorphic polynomials and their generalisations to Riemann surfaces. The inner product defining the Gaussian structure is defined as in weighted potential theory, and as the degree of the polynomials tend to infinity, their zeros concentrate exponentially fast in a limit configuration defined by the weighted equilibrium measure. I. Wigman spoke on his work with J. A. Toth, Z. Rudnick and others on Gaussian random combinations of eigenfunctions. In particular, he discussed a subtle variance estimate that proved a conjecture of M. V. Berry.
The 2009 André-Aisenstadt Prize
Valentin Blomer (University of Toronto)

It is with great pleasure that the CRM awards the 2009 André-Aisenstadt Prize to Dr. Valentin Blomer in recognition of his exceptional research achievements. The Prize will be awarded at a ceremony to be held on March 20, 2009 at the CRM.

Following his master’s degree in 2001, Valentin Blomer burst onto the number theory scene by solving a deep and difficult problem of Paul Erdős, allowing him to obtain his Ph.D. in 2002 under Jörg Brüdern at the University of Stuttgart, after just one year! After spending the 2003–2004 academic year as a postdoctoral fellow at the University of Toronto, he returned to Germany to start as an assistant professor at Göttingen, and has been back in Toronto, as an assistant professor, since 2005.

Blomer’s solution to Erdős’s problem revolved around getting precise estimates for the number of integers up to a given point represented by a given binary quadratic form, where that point is small enough that the coefficients of the form will have significant impact on the shape of the solution. This type of question going back to Lagrange and Gauss, so it is not surprising that Blomer’s work on this has had such an impact.

Recently, Blomer has focused on the subconvexity problem for automorphic L-functions, obtaining in papers with Harcos and Michel the best results known in this central question, in several different aspects. Also recently Blomer and Harcos obtained the complete spectral decomposition for the shifted convolution problem, a question that goes back to Selberg.

Blomer has many other fine works in all sorts of different directions. He seems to generate a wealth of ideas, aided by great technical prowess. There is obviously much more to come.

Valentin Blomer’s exceptional research has been recognised by several prizes and honours, including a 2005 Heinz Maier–Leibnitz award in Germany and a 2008 Sloan Research Fellowship.

My area of research is analytic number theory, in particular

- the arithmetic of quadratic and higher-degree forms
- and the theory of automorphic forms and L-functions.

Quadratic Forms

The representation of integers by quadratic forms is a classical area of number theory that combines analytic and algebraic aspects. For a d-ary integral positive quadratic form \( q \) of discriminant \( D_q \) one is typically interested in the representation function \( r_q(n) := \#\{x \in \mathbb{Z}^d \mid q(x) = n\} \).

Let me start with a seemingly unrelated question. Erdős calls a positive \( n \) integer squarefull (or powerful) if every prime divisor \( p \) of \( n \) occurs with multiplicity at least 2. For example, every perfect square is squarefull, but also numbers like \( 72 = 2^3 \cdot 3^2 \) are squarefull. Erdős was interested in the additive behaviour of squarefull numbers and asked for the number \( V(x) \) of sums of two squarefull numbers up to \( x \). What does this have to do with quadratic forms? Every squarefull number \( n \) can be written uniquely as \( n = a^2 b^3 \) with \( b \) squarefree, so we are interested in the representation numbers of the set of binary quadratic forms \( b_1^2 x_1^2 + b_2^2 x_2^2 \). The main point here is that we are looking at many forms simultaneously, so we need uniform results.

Together with A. Granville [6] I obtained sharp bounds and asymptotics for all moments

\[
\sum_{n \leq x} r_q(n)^\beta, \quad \beta \in \mathbb{R}_{\geq 0}, x \rightarrow \infty
\]

of binary quadratic forms \( q \) with the special feature of uniformity in the essentially largest possible range \( |D_q| = o(x) \). Here the case \( \beta = 0 \) (which in some sense is the hardest) is interpreted as the characteristic function on the representable integers. This result is based on a new method developed in my thesis that combines analysis with combinatorial group theory. As a corollary we can solve Erdős’ problem [3,6]:

\[
V(x) = x (\log x)^{2+\Theta(1)}, \quad \alpha = 1 - 2^{-1/3}.
\]

This result came as a surprise, in particular the shape of the exponent \( \alpha \) was against the more popular existing conjectures \( \alpha = \frac{1}2 \) (Erdős), \( \alpha = \frac{1}{\delta} \) or \( \alpha = \frac{1}{\theta} \), cf. [1, 15]. The underlying methods can for example be applied to fairly general systems of Abelian norm forms [10] instead of quadratic forms, or—in a different direction—coupled with sieve methods to count points with prime coordinates on higher-dimensional quadrics [5].

Automorphic Forms

Automorphic forms are functions on \( \Gamma \backslash G \) where \( G = \text{PSL}_2(\mathbb{R}) \), or a more general Lie group, and \( \Gamma \) is an arithmetic subgroup \( G \). The space \( L^2(\Gamma \backslash G) \) is naturally equipped with a \( G \)-action, but it has more structure: the Hecke algebra \( \{ T(n) \mid n \in \mathbb{N} \} \) forms a large family of naturally defined commuting endomorphisms that also commute with the \( G \)-action. The rich structure makes the space of automorphic forms an interesting object to consider; the theory lies at the interface of number theory, representation theory, (nonabelian) harmonic analysis and arithmetic geometry, and it combines a variety of techniques from these areas, see for example [12–14].
From a number theoretical point of view one is particularly interested in the Hecke eigenvalues $\lambda(n)$, since they carry important information on the structure of geometric or algebraic objects like elliptic curves and algebraic number fields. The method of analytic number theory is to encode this sequence of complex numbers into a generating function

$$L(s) := \sum_{n=1}^{\infty} \lambda(n) n^{-s},$$

a so-called $L$-function that reflects the arithmetic information very precisely in its analytic properties (zeros, poles, growth, special values). This fruitful interplay between arithmetic and analysis is at the core of the first proof of the prime number theorem $\#\{\text{primes } \leq x\} \sim x/\log x$ more than 100 years ago, and is reflected in two of the Clay Mathematics Millenium Problems.

The series representation for $L(s)$ converges absolutely only in $\Re s > 1$, but it can be continued to a meromorphic function that, as every decent zeta-function, comes equipped with a functional equation relating $L(s)$ to $L(1-s)$. It is one of the magic features of analytic continuation that $L$-functions reveal the most relevant information in the region $0 < \Re s < 1$ outside of absolute convergence, and in particular on the critical line $\Re s = \frac{1}{2}$. The functional equation together with some standard complex analysis provides bound for an $L$-function on the critical line, the so-called convexity bounds. The Generalised Riemann Hypothesis (GRH) implies much stronger and essentially best possible bounds, but a proof seems completely out of reach at the moment. For many applications, GRH is not necessary, but it is crucial to prove a bound that is just a little bit better than the convexity bound: a subconvexity bound. Partly in joint work with G. Harcos and P. Michel (e.g., [2, 9]) I could prove a number of new subconvex results for classical families of $L$-functions. There are numerous applications:

- Waldspurger’s theorem [17] translates central values of $L$-functions into Fourier coefficients of half-integer weight modular forms that for example come up in the theory of ternary quadratic forms [4]. The above mentioned subconvex bounds yield the strongest currently known bounds in this direction.
- Watson’s formula [18] translates subconvex bounds of certain $L$-functions into a quantitative version of the quantum ergodicity conjecture of Rudnick–Sarnak for CM-forms.
- The analysis of our subconvexity bounds is needed as an input for estimates of several types of higher-degree $L$-functions [9] and a crucial ingredient for various equidistribution results, e.g., of Heegner points and generalisations of Linnik-type problems [14].

One of the ingredients to prove subconvexity results are bounds for so-called shifted convolution sums of Hecke eigenvalues of the type $\sum_{n} \lambda(n) \lambda(n+h)$ for $h \neq 0$. Although perhaps not apparent at first sight, these sums play an important role in the theory. One reason is that they constitute a typical off-diagonal term when squaring out $(\sum_{n} \lambda(n))^2$. Combining the spectral theory of automorphic forms with the representation theory of the Lie group $GL_{2}(\mathbb{R})$, I obtained together with G. Harcos [7] an exact spectral decomposition of such sums, also over totally real number fields. This solves (and generalises) a forty-year-old problem of A. Selberg [16].

Let me finish by describing a very recent result on automorphic forms that has (at least at first sight) nothing to do with $L$-function. If $K = \text{PSO}(2)$ denotes the maximal compact subgroup of $G = \text{PSL}_2$, then $\Gamma \backslash G/K$ is a noncompact quotient of the upper half plane, a so-called modular curve. It is a Riemannian manifold, and comes equipped with the action of Hecke operators and the Laplace–Beltrami operator. Given an $L^2$-normalised eigenform for the Hecke and the Laplace operator, what can we say about its $L^\infty$-norm, that is, pointwise bounds? We have three options: we can give bounds in terms of the Laplacian eigenvalue for a fixed group $\Gamma$, we can give bounds in terms of the size of $\Gamma$ for fixed Laplacian eigenvalue, or we can give hybrid bounds. A nontrivial bound in the first case was given by Iwaniec and Sarnak [11], but the case of a varying group remained open, and one can imagine that this is a hard problem since we are shooting on a moving target: we want to bound functions while the underlying space varies. Jointly with R. Holowinsky [8] I proved the first nontrivial $L^\infty$-bound for an $L^2$-normalised automorphic cusp form in terms of the group (we are only considering here the most interesting case of so-called Hecke congruence groups). Coupling our ideas with the paper of Iwaniec and Sarnak, we also obtain hybrid bounds in terms of the group and the Laplacian eigenvalue. These techniques are powerful and flexible enough to be used for other spaces than modular curves, for example quotients of quaternion algebras.

Depuis quelque temps, le CRM parraine une série de conférences appelées les « Grandes Conférences (GC) du CRM ». Il s’agit d’exposés grand public donnés par d’excellents conférenciers.

Vendredi soir, le 28 novembre 2009, la GC du CRM se donnait à la magnifique salle Hydro-Québec de l’Université Laval, et le conférencier invité était le professeur Yvan Saint-Aubin (U. de Montréal). Pour souhaiter la bienvenue, M. André Darveau, vice-doyen à la recherche de la faculté des sciences et de génie de l’Université Laval, fit l’éloge du CRM comme moyen de regrouper les différents départements de mathématiques et de statistique (et même un département de physique) de la province. Il en profita aussi pour expliquer que l’Université Laval est un endroit merveilleux pour faire des études.

Puis le professeur Yvan Saint-Aubin commença son exposé intitulé Désordre et beauté. Sur les affiches publicitaires, on mentionnait : « Le mathématicien qui découvre de nouveaux motifs ou structures utilisera souvent le mot beauté pour décrire la compréhension ainsi gagnée, car sa réussite s’apparente à l’expérience esthétique. Ce sentiment est particulièrement singulier quand l’objet d’étude est le désordre. ». Le conférencier se proposait donc de « décrire des sujets où les mathématiques ont réussi à trouver des structures là où seul le désordre était visible ». Tout un défi que le conférencier a réussi à relever avec un brio alimenté de plusieurs pointes d’humour, et cela devant plus de 250 personnes.

On apprit d’abord que Jackson Pollock est reconnu comme un des plus grands peintres américains du XXe siècle. Sa méthode de travail est particulière : il semble lancer de la peinture au hasard sur une toile. Bien qu’à première vue, le résultat semble complètement désordonné, ses peintures sont plaisantes à regarder. Mais pourquoi donc ? Richard Taylor, physicien théoricien et artiste amateur (ne pas le confondre avec le coauteur de Andrew Wiles), explique ce phénomène en émettant l’hypothèse que les œuvres de Pollock, dites de dripping, ont des propriétés fractales. Mais d’abord quel est donc cet objet géométrique, qu’on appelle « fractale », et que l’on construit habituellement à l’aide d’un ordinateur ?

Yvan Saint-Aubin utilise alors pour exemple le fameux flocon de von Koch, soit une des premières courbes fractales décrite au début du XXe siècle, nommée ainsi à cause du mathématicien suédois Helge von Koch (1870-1924). La construction itérative du flocon de Koch (très bien illustrée visuellement) arrive à nous convaincre qu’il s’agit bien d’une courbe fermée, de périmètre infini et dont la dimension est supérieure à l’unité. Pour calculer cette « dimension fractale », Saint-Aubin effectue un décompte des coups de pinceaux nécessaires pour recouvrir le flocon de Koch. Il arrive ainsi à montrer que sa dimension est effectivement entre 1 et 2, et on peut calculer qu’elle est égale à $\log 4 / \log 3 \approx 1,26$.

C’est ce même décompte qui a été effectué par Taylor pour démontrer que les œuvres de Pollock sont en réalité des fractales dont on peut estimer la dimension. Ceci nous amène à émettre l’hypothèse que le cerveau est bien « filé » pour apprécier les objets fractales.

Saint-Aubin mentionne même que Taylor aurait réussi à identifier de faux Pollock en effectuant un calcul de dimension fractale sur ces fausses peintures pour constater que la dimension fractale était nulle, ce qui prouvait que l’on était en présence de faux. Comme quoi, les mathématiques se portent même au secours de l’art en épinglant les faussaires. Toute une surprise pour d’aucunes personnes présentes !


Une modélisation simple du phénomène de percolation : les hexagones les plus foncés représentent les sites où la mouture est située, les plus pâles ceux occupés par le liquide qui percole. L’interface entre ces deux plages est indiquée par un trait plus épais.
Einstein utilisa ce mouvement désordonné pour suggérer une façon de mesurer le nombre d’Avogadro (une quantité qui correspond au nombre d’atomes de carbone dans 12 grammes de l’isotope 12 du carbone). Cette expérience a été menée par Jean Perrin qui obtiendra le prix Nobel pour ses expériences décisives sur l’hypothèse atomique.

En fait, le mouvement brownien peut se comparer à une marche aléatoire, soit à la limite, quand le pas, et le temps entre les pas, tendent vers zéro. Saint-Aubin illustre cette modélisation en nous faisant entendre un clip de Madame Butterfly. Mais en réalité, les désordres ne sont pas les mêmes ! Il y a donc émoi chez les mathématiciens : le mouvement brownien est presque sûrement continu, mais il n’est différentiable en aucun point !

S’ensuivent, pour le plus grand plaisir de l’auditoire, les explications du professeur Saint-Aubin sur la percolation, via la modélisation d’un filtre à café, toujours avec de petites vidéos à l’appui de ses dires, en particulier pour localiser le point très particulier où la densité de la mouture est au « point critique ». Il explique que les transformations conformes forment un ingrédient crucial dans la description de ce point critique. Il montre même des images décrivant des transformations conformes et d’autres images mettant en évidence des transformations qui ne sont pas conformes. Décidément, ses preuves sont convaincantes. On voit en action une famille de transformations conformes pour retirer des fentes dans le demi-plan complexe. Il s’avère que si la fente est une interface entre café et eau, le point le long de l’axe réel d’où sort la fente est un « multiple du » mouvement brownien. Décidément, nous avons l’impression que le lendemain notre petit café aura meilleur goût.

La fin approche, mais pas la fin des temps. C’est l’épilogue. Ne laissant pas la chance au café de se refroidir, Saint-Aubin cite alors Poincaré : « Si un résultat nouveau a du prix, c’est quand, laissant pas la chance au café de se refroidir, Saint-Aubin cite

Jacques Laskar
(suite de la page 2)

Ces méthodes permettent de passer de l’étude du système moyennisé dont les grands résultats datent d’une quinzaine d’années à l’étude du système réel, lequel inclut la position de la planète sur son orbite. Une vaste simulation est en cours pour montrer la possibilité de vraie collision entre Mercure et Vénus.

Jacques Laskar a également discuté l’étude statistique des demi-grands axes des planètes internes. La distribution statistique de ces valeurs est très régulière lorsqu’on fait de nombreuses simulations sur des périodes de temps très longues.

Martin Barlow
(continued from page 1)

and S. Kusuoka had already solved this problem; however, in the end Ed and I were able to obtain very detailed information on the behaviour of the limiting process.
The Winter 2010 CRM Thematic Semester:
Number Theory as an Experimental and Applied Science
by Henri Darmon and Eyal Goren (McGill University)

The year 2010 marks the 50th anniversary of the publication of Eugene Wigner’s famous essay on the “unreasonable effectiveness of mathematics in the natural sciences.” The intervening five decades have witnessed an explosion in the variety and scope of the applications of mathematics, to the extent that one can now speak of an ongoing “mathematization” of many branches of science and indeed of society as a whole. Number theory, traditionally viewed as far removed from the sphere of applications, now plays a central role in questions pertaining to the design of efficient networks as well as in areas like robotics, computer vision, statistics, coding theory, computer security, and cryptography. By extending the reach of calculation and the potential of the experimental method, ever-more powerful and sophisticated software packages like MAPLE, MAGMA and SAGE are transforming the way in which number theorists approach their subject.

The 2010 winter semester (January 1 – April 31) will be devoted to recent developments in number theory with a specific focus on significant practical applications, as well as on the many ways in which the field stands to be affected by the emergence of new software and technologies.

The first event of the theme semester will be the Summer School (SMS) Automorphic Forms and L-Functions: Computational Aspects organised by Mike Rubinstein (Waterloo) and Andreas Strömbergsson (Uppsala) and held at the CRM from June 22 to July 3, 2009. The purpose of the summer school is to bring together a number of experts who are leaders in both the theoretical and computational aspects of the theory of automorphic forms to offer introductory-level courses presenting to graduate students and postdoctoral fellows the state of the art in the subject, and reporting on new advances which have not yet been covered in a forum of this sort. The Aisenstadt Chair for the theme semester will be Akshay Venkatesh (Stanford), and he will give a series of lectures during the SMS. For students and junior researchers who would like to apply for funding to participate to the summer school, please contact Sakina Benhimma at benhimma@CRM.UMontreal.CA.

A cornerstone of the special semester activities will be a collection of five workshops covering related themes.

**MAGMA 2010 Conference on p-adic L-functions**
Organisers: Matthew Greenberg (Calgary), Xavier Roblot (Lyon 1), Mark Watkins (Sydney), Christian Wüthrich (Nottingham)
Date: February 22 – 26, 2010

This workshop is being run under the auspices of the MAGMA Computer Algebra Group (University of Sydney), and is devoted to computational aspects of the theory of p-adic L-functions. This topic has a rich history both in itself and in relation to global L-functions. It is only recently that the ability to explore various conjectures has become practical. An explicit example is the one of p-adic variants of Stark’s conjectures, which have been investigated at least in the abelian case. In some contexts, the computations have truly acted as an “experimental science,” in that the final refinements of the conjectures were largely aided by the numerical data. Another development has been the application of overconvergent modular symbols to facilitate the computation of the p-adic L-functions of modular forms, and here the connection with elliptic curves is also of interest. Finally, the well-known cross-germinations with Iwasawa theory will also be highlighted. Our goal is to bring together a targeted group of experts on both the theoretical and computational sides of this subject, to share and expose the latest results, and determine the viable prospects for future work.

**Graphs and Arithmetic**
Organisers: Winnie Li (Penn State), Eyal Goren (McGill), An-
There is a long history of interaction between number theory and combinatorics. In the past two decades, deep results in automorphic forms and number theory were used to construct (optimal) expanders, which are known to have wide applications in computer science and communication networks. These techniques were generalised to construct higher-dimensional analogues. In the meanwhile, zeta functions for graphs and complexes are better understood. Recent exciting developments in arithmetic combinatorics provide new tools to construct families of good expanders, and these expanders in turn are used to obtain deep number theoretic results. At the same time, the concept of expansion is extended in group theory and computer science to a different context.

In view of these fruitful developments, we think the time is ripe to hold a week long conference to review recent results in this area. Both theories and applications will be emphasised.

**Computer Methods for L-functions and Automorphic Forms**

**Organisers:** Bas Edixhoven (Leiden), Mike Rubinstein (Waterloo), William Stein (Seattle)

**Date:** March 22–26, 2010

For years, computers have also played a key role in investigating the most central questions in the analytic theory of automorphic forms such as the existence of Maass wave forms. Recently, a team of researchers, including M. Rubinstein (Waterloo) and W. Stein (Seattle), has embarked on an ambitious collaborative effort to systematically gather vast amounts of data concerning, among other things, automorphic forms on higher rank groups. This effort is part of a three year (2008–2011) NSF funded Focused Research Group (FRG) grant dealing with L-functions and automorphic forms. The FRG effort is sure to generate challenges and new questions for people working both on the theoretical and the experimental side of the subject, as well as gathering valuable data that will be precious in suggesting conjectures or revealing new lines of enquiry.

A parallel theme of the workshop will be the emerging role of specialised software in number theory. While they have been on the scene for many years, symbolic algebra systems have become a lot more powerful and integrated in recent years. The possibilities offered by the world wide web have caused some packages (the computer system SAGE, notably) to embrace the “wikipedia model” whereby all members of the community can contribute code in a decentralised manner. The possibilities of such an approach are tremendously exciting, but also raise a host of challenges.

This workshop will bring together the “experimentalists” who develop the software and the “theoreticians” who are primarily interested in using it to test conjectures or discover patterns, so that each group can become better aware of each other’s needs, priorities, and capabilities.

**Computer Security and Cryptography**

**Principal organisers:** Kristin Lauter (Microsoft) and Joseph Silverman (Brown)

**Date:** April 12–16, 2010

Among the exciting new directions in cryptography that this one-week workshop will attempt to touch upon are the following: proliferating hardness assumptions and protocols in pairing-based cryptography; provable security and the random oracle model in theory and practice; design and selection of new cryptographic hash functions; new security models for deterministic encryption and searchable encryption; new number theoretic constructs in cryptography such as expander graphs, lattice-based systems, elliptic divisibility sequences, etc.; the trade-off between security and privacy in emerging applications such as cloud storage; new applications of pairings to areas such as e-cash and Attribute Based Encryption. A major goal of the workshop will be to foster exchanges between mathematicians working on the theoretical end of cryptography and the leading practitioners in government, finance and industry, so that each community can be more aware of the other’s basic assumptions and priorities.

**Counting Points: Theory, Algorithms, and Practice**

**Organisers:** Kiran Kedlaya (MIT), Jean-François Mestre (Paris 7)

**Date:** April 19–23, 2010

The development of efficient (polynomial time) algorithms for counting the number of points on varieties over finite fields represents a highly attractive area of application, in part because it relies on sophisticated mathematical theories like the étale and $p$-adic cohomology theories whose development was a cornerstone of number theory in the second half of the 20th century. The workshop will be devoted to recent advances in this area and its applications.

There will be several courses in support of the special semester.

A mini-course on *Expander Graphs* which will be taught by Eyal Goren (McGill) in January and February. It will be geared at graduate students and young researchers, and present them with the required background for the workshop on *Graph and Arithmetic* held in March.

A mini-course on *Cohomology and Point Counting* will be given by Henri Darmon (McGill) during March–April. This course will be geared at covering the prerequisites for the workshop *Counting Points: Theory, Algorithms, and Practice*.

A graduate course on *Computational Aspects of Quaternion Algebras and Shimura Curves* will be given by John Voight (Vermont). This course will cover background material that will be relevant to several of the workshops that will be held: quaternion algebras play an important role in some constructions of expanders, they are central, as a source of key examples, to the

(continued on page 14)
General Program and External Activities

Arithmetic and Hyperbolic Geometry
by Steven LU (UQÀM)

On the weekend of November 8, 2008, the workshop Arithmetic and Hyperbolic Geometry was held in the Science Complex of UQÀM at the heart of downtown Montréal. It was organised by J. Bland (Toronto), A. Granville (Montréal), S. Lu (UQÀM), P. Russel (McGill) and N. Yui (Queen’s) and jointly funded by CIRGET (the Geometry and Topology laboratory of the CRM) and the Fields Institute.

It was intended to be a small followup of the workshop Geometry of Holomorphic and Algebraic Curves in Complex Algebraic Varieties held at the CRM in the spring of 2007, and it took ample advantage of the very much related thematic program on Arithmetic Geometry, Hyperbolic Geometry and Related Topics that was held at the Fields Institute for the second half of 2008. Since there was little overlap in the contents of the talks in the workshop and those at the thematic program at the Fields, it has served as a very useful and inspiring complement to the thematic program. As a result, it was very well attended with over 50 participants from which about 20 came from the thematic program, and saw some intense activities for a day and a half that have produced and certainly will continue to bring fruits among the participants for time to come.

Almost all the talks related directly to the geometry of algebraic or holomorphic curves in algebraic varieties, and many also addressed the questions of rational points and the relations to hyperbolicity. New techniques were given in every talk and often in details, even though many were only works in progress. We single out the examples of the two pre-eminent scholars from the thematic program: Y. T. Siu (Harvard), Fields Senior Scholar, who talked about how one can try to produce rational curves on Fano varieties analytically (thereby giving an analytic approach to one of the key ingredients in Mori’s Minimal Model Program in the classification of algebraic varieties) and H. Gillet (UIC), Clay Institute Senior Scholar, who spoke on the relationship between heights of conics (an arithmetic object) and the derivative at 0 of the zeta function of the Laplacian of the conic (an analytic object). We also single out the fact that Paul Vojta (Berkeley) introduced a new conjecture on diophantine geometry in his talk and that J. Noguchi (Tokyo) discussed new questions concerning rational points and holomorphic curves in semi-abelian varieties that have now been solved at least in part by some of the participants and the organizers. X. Chen (Alberta), E. Rousseau (Strasbourg) and B. de Oliveira (Harvard/Miami) gave eye-opening talks on some new approaches to hyperbolicity, and Č. Gasbarri (Rome/Strasbourg), P. Corvaja (Udine) and M. McQuillan (IHES/Glasgow) did the same for arithmetic.

The workshop was therefore very successful as a model joint program of the two institutes and a followup meeting would be quite appropriate in the near future.

Hilbert Spaces of Analytic Functions
by Javad Mashreghi (Laval)

The workshop entitled Hilbert Spaces of Analytic Functions was held at the CRM from December 8 to December 12, 2008. The event was organized by Javad Mashreghi (Université Laval), Thomas Ransford (Université Laval) and Kristian Seip (NTNU, Norwegian University of Science and Technology), and 62 mathematicians attended the workshop. It brought together a blend of researchers with a common interest in spaces of analytic functions, but seen from many different angles. About fifteen students and postdoctoral fellows attended the conference, and half of them presented talks.

Hilbert spaces of analytic functions are currently a very active field of complex analysis. The Hardy space \( H^2 \) is the most senior member of this family. Its relatives, such as the Bergman space \( A_p \), the Dirichlet space \( D \), the de Branges–Rovnyak spaces \( H(b) \), and various spaces of entire functions, have been extensively studied by prominent mathematicians since the beginning of the last century. They have been exploited in different fields of mathematics and also in physics and engineering. For example, de Branges used them to solve the Bieberbach conjecture, and J. Zames, a late professor of McGill University, applied them to construct his theory of \( H^\infty \) control. But there are still many open problems, old and new, that attract a wide spectrum of mathematicians.

To highlight the vast scope of this domain and the variety of applications, we provide a representative sample of the topics discussed at the workshop: completeness of translates in weighted spaces; analytic continuation in backward-shift-invariant subspaces; multivariable extensions of de Branges–Rovnyak spaces; Bernstein-type inequalities in de Branges–Rovnyak spaces; interpolation and sampling in Fock spaces; pointwise estimates for the Bergman kernel of the weighted Fock space; multiplication operators on the Bergman space; compactness criteria for composition operators on BMOA; approximation of and by the Riemann zeta function; curvature and maximal Blaschke products; trigonometric and Hausdorff moments; Poincaré variational problem in potential theory; singularities of solutions to the Dirichlet problem and complex lightning bolts; Hankel forms on the Dirichlet space; cyclicity in the Dirichlet space; the positivstellensatz in Weyl’s algebra; operator H"older–Zygmund functions; power-boundedness on function spaces; function theory on the tetrablock; uniqueness sets for Nevanlinna–Pick interpolation in two variables.
Dixième Conférence Québec-Maine

Les 4 et 5 octobre 2008 se tenait à l’Université Laval la dixième édition de la conférence Québec-Maine de théorie des nombres, et cette année, elle se tenait en l’honneur des 80 ans du professeur Paulo Ribenboim. En fait, il était très difficile de passer sous silence la passion de Paulo pour les nombres, « des amis qui nous donnent des problèmes ».


Andrew Granville (le dernier né de Paulo parmi ses étudiants au doctorat, et le premier récipiendaire du prix Ribenboim) y est allé d’une conférence toute spéciale intitulée « Mon cher Paulo, c’est à ton tour de te laisser parler d’amour » (Gilles Vigneault). Un portrait de Paulo au fil des ans, avec photos d’archives à l’appui ! L’émotion était palpable.

Cette année, une trentaine d’exposés ont été donnés. Voici la liste des conférenciers selon l’ordre chronologique de leurs présentations : Andrew Granville (Montréal), Ernst Kani (Queen’s), Bao Chau Ngo (Orsay), Adrian Iovita (Concordia), Florian Luca (UNAM, Morelia), Henri Darmon (McGill), Hershy Kisilevsky (Concordia), Damien Roy (Ottawa), John Labute (McGill), Carl Pomerance (Dartmouth), Trueman MacHenry (York), Bram Brer (Montréal), Gary Walsh (Ottawa), Romyar Sharifi (McMaster), Cam Stewart (Waterloo), Chantal David (Concordia), Mitsuo Kobayashi (Dartmouth), John Voight (Vermont), Enrique Trevino (Dartmouth), Lloyd Simons (Saint Michael’s College), Alain Togbé (Purdue), David Bradley (Maine), Omar Kihel (Brock), John Cullinan (Bard College), Youness Lamzouri (Montréal), Hugo Chapdelaine (Laval), Nicolas Doyon (Laval), Chris Cummins (Concordia), Mark Sheingorn (CUNY).

On se donne rendez-vous à Orono, University of Maine, les samedi et dimanche, 3 et 4 octobre 2009, pour la onzième édition du congrès de théorie des nombres Maine-Québec.

Valentin Blomer

(continued from page 8)


Winter 2010

(continued from page 12)

study of modular forms and Shimura varieties, and the computational focus of Voight’s course will make this course directly relevant to the workshop dedicated to computer methods for L-functions.

Additional graduate courses are planned during the theme semester. For updated information see crm.math.ca/NT2010.

The planned presence of a large and active group of visitors and postdoctoral fellows is an important feature of any special semester. Some postdoctoral fellows could be joint with the Centre de Recerca Matemàtica in Barcelona, who is organizing a special year on Arithmetic Geometry at the same period. For more information about the theme semester, in particular for graduate students and post-doctoral fellows who would like to apply for funding, please contact the organisers, or the CRM scientific activities coordinator Louis Pelletier at pelletier@CRM.UMontreal.CA. More details are also available at crm.math.ca/NT2010.
Mot de la directrice
(suite de la page 16)

la Société mathématique du Canada, MITACS et le CNRC. Bruno Rémillard de HEC Montréal a accepté d’être l’organisateur local. L’ensemble de la communauté canadienne en sciences mathématiques est derrière le projet et prête à participer à des activités reliées au congrès. La visite de site aura lieu à Montréal les 25 et 26 mars 2009.

Peter Russell, a accepté de prendre la direction du CRM pour un mandat de deux ans commençant le 1er juin 2009. Auparavant, il a fait carrière à l’Université McGill et dirigé le département de mathématiques et de statistique de 1988 à 1994, années pendant lesquelles son département connut un essor important. Peter Russell est un spécialiste de la géométrie algébrique. Ses intérêts couvrent la géométrie des variétés algébriques non complètes, en particulier les variétés affines et les actions de groupes sur ces variétés. Peter et moi avons déjà commencé à coopérer et échanger sur les grands dossiers du CRM. Nous lui sommes reconnaissants et l’assurons du soutien enthousiaste de la communauté scientifique du CRM.

Christiane Rousseau

Word of the Director
(continued from page 16)

Peter Russell, has accepted to take over as Director of CRM for a two-year period starting June 1st 2009. He spent his career at the Department of Mathematics and Statistics of McGill University and chaired his department from 1988 to 1994, a great period for his department. He is a specialist of algebraic geometry. His interests include the geometry of non complete algebraic varieties and the group actions on these varieties. Peter and I have started cooperation and discussion on the main dossiers of CRM. We are greatful to him for accepting the position and assure him of the enthusiastic support of the scientific community of CRM.

Christiane Rousseau

2009 Fall Thematic Semester
Mathematical Problems in Imaging Science

Workshops
- Brain Activity Modeling: From Fine to Coarse Scale (August 17 – 22, 2009)
- Inverse Problems in Brain Imagery and Multimodal Fusion (August 24 – 29, 2009)
- Quantum Dynamic Imaging (October 19 – 23, 2009)

Aisenstadt Chairs
- Stéphane Mallat (École Polytechnique, Paris; Courant Institute, NYU)
- Claude Le Bris (École Nationale des Ponts ParisTech)

La thématique de l’automne 2009 portera sur les problèmes mathématiques en imagerie, avec trois ateliers sur l’imagerie cérébrale et la modélisation de l’activité neuronale et un atelier sur l’imagerie dynamique quantique. La portion du semestre sur l’imagerie cérébrale et neuronale est pilotée par le laboratoire PhysNum du CRM, lequel travaille en étroite collaboration avec l’INSERM à Paris et l’Institut de gériatrie de Montréal. Stéphane Mallat (École Polytechnique, Paris; Courant Institute, NYU) sera le conférencier Aisenstadt attaché à ce thème. L’imagerie dynamique quantique est une nouvelle science multidisciplinaire créée par André Bandrauk (Sherbrooke), chercheur en chimie théorique et membre du CRM, ainsi que Paul Corkum, physicien, travaillant au Conseil National de Recherches du Canada à Ottawa. Claude LeBris (CERMICS, École des Ponts ParisTech) sera le conférencier Aisenstadt associé à ce deuxième thème.

Suiira pendant l’hiver 2010 un semestre sur la théorie des nombres comme science expérimentale et appliquée, avec comme conférencier Aisenstadt, Akshay Venkatesh (Stanford). Le Séminaire de mathématiques supérieures de l’été 2009 aura pour thème Formes automorphes et fonctions L : aspects computationnels, et nous sommes reconnaisants à Michael Rubinstein (Waterloo) et Andreas Strömbergsson (Uppsala) de s’occuper de l’organisation.


La communauté mathématique canadienne et le CNRC (Conseil national de recherches du Canada) ont déposé en novembre dernier la candidature de Montréal pour le Congrès international des mathématiciens de 2014. Ce projet est un partenaire entre les trois instituts canadiens (CRM, Fields et PIMS),

\[\text{(suite à la page 15)}\]