### MOSCOW MATHEMATICAL JOURNAL

Published by the Independent University of Moscow

The Moscow Mathematical Journal (MMJ) is an international quarterly published (paper and electronic) by the Independent University of Moscow and distributed worldwide by the American Mathematical Society. MMJ presents highest quality research and research-expository papers in mathematics from all over the world. Its purpose is to bring together different branches of our science and to achieve the broadest possible outlook on mathematics, characteristic of the Moscow mathematical school in general and of the Independent University of Moscow in particular.

An important specific trait of the journal is that it especially encourages research-expository papers, which must contain new important results and include detailed introductions, placing the achievements in the context of other studies and explaining the motivation behind the research. The aim is to make the articles—at least the formulation of the main results and their significance—understandable to a wide mathematical audience rather than to a narrow class of specialists.

 $\,$  MMJ is covered by the Mathematical Reviews Database and by Zentralblatt MATH.

### Subscription Information

Subscriptions are available beginning with the 2002 subscription year. All paid subscriptions to MMJ will qualify subscribers to receive the inaugural 2001 issues free of charge. The subscription entitles the subscriber to the paper and electronic versions of MMJ.

Subscriptions are available from the AMS in the USA to Institutional Subscribers in the following world regions: North America (USA, Canada, and Mexico), European Union, Norway, Switzerland, Japan, Australia, Taiwan, Israel, South Korea, New Zealand.

List Price: US \$160 (at least four issues, hard copies and electronic version). Free samples are available to Institutional Subscribers in these regions upon request.

A 30 day free trial of the electronic version of Moscow Mathematical Journal is available to institutions in the above countries.

Subscriptions can be placed through subscription agents, or ordered directly from the AMS:

Moscow Mathematical Journal P.O. Box 845904, Boston, MA 02284–5904, U.S.A. Tel: (401) 455–4081, Fax: (401) 331–3842,

E-mail: cust-serv@ams.org

Subscriptions are available directly from MMJ in Russia to: Individual Subscribers worldwide and Institutional Subscribers in regions other than those listed above.

Individual and Special Price: US \$80.00 (at least four issues, hard copies and electronic version), available to individual subscribers and institutional subscribers in regions other than those listed above. Still lower prices are available for Russian residents and libraries. Please direct these subscription inquiries and sample requests to:

Moscow Mathematical Journal Independent University of Moscow,

11, B. Vlasievsky per., Moscow 121002, Russia. Tel: (7-095) 241-0500, Fax: (7-095) 291-6501,

E-mail: mmj@mccme.ru

### DYNAMICS OF TRAFFIC JAMS: ORDER AND CHAOS

#### MICHAEL BLANK

ABSTRACT. By means of a novel variational approach, we study the ergodic properties of a model of a multi lane traffic flow, considered as a (deterministic) wandering of interacting particles on an infinite lattice. For a class of initial configurations of particles (roughly speaking satisfying the Law of Large Numbers) the complete description of their limit behaviour (in time) is obtained, as well as estimates of the transient period. In this period the main object of interest is the dynamics of 'traffic jams', which is rigorously defined and studied. It is shown that the dynamical system under consideration is chaotic in the sense that its topological entropy (calculated explicitly) is positive. Statistical quantities describing limit configurations are obtained as well.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 1, January—March 2001, Pages 27–47

### THE DUCK AND THE DEVIL: CANARDS ON THE STAIRCASE

#### J. GUCKENHEIMER AND YU. ILYASHENKO

ABSTRACT. Slow-fast systems on the two-torus  $T^2$  provide new effects not observed for systems on the plane. Namely, there exist families without auxiliary parameters that have attracting canard cycles for arbitrary small values of the time scaling parameter  $\varepsilon$ . In order to demonstrate the new effect, we have chosen a particularly simple family, namely  $\dot{x} = a - \cos x - \cos y$ ,  $\dot{y} = \varepsilon$ ,  $a \in (1, 2)$  being fixed. There is no doubt that a similar effect may be observed in generic slow-fast systems on  $T^2$ . The proposed paper is the first step in the proof of this conjecture.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 1, January–March 2001, Pages 49–63

#### INTRODUCTION TO FAMILY ALGEBRAS

### A. A. KIRILLOV

ABSTRACT. Classical and quantum family algebras, previously introduced by the author and playing an important role in the theory of semi-smiple Lie algebras and their representations are studied. Basic properties, structure theorems and explicit fomulas are obtained for both types of family algebras in many significant cases. Exact formulas (based on experimental calculations) for quantum eigenvalues, their multiplicities, and the trace of the so-called matrix of special elements are conjectured.

## DIMENSIONS OF QUANTIZED TILTING MODULES

#### VIKTOR OSTRIK

ABSTRACT. Let U be the quantum group with divided powers at p-th root of unity for prime p. To any two-sided cell A in the corresponding affine Weyl group, one associates the tensor ideal in the category of tilting modules over U. In this note we show that for any cell A there exists a tilting module T from the corresponding tensor ideal such that the greatest power of p which divides dim T is  $p^{a(A)}$ , where a(A) is Lusztig's a-function. This result is motivated by a conjecture of J. Humphreys.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 1, January–March 2001, Pages 73–89

# RANDOM LATTICES AND RANDOM SPHERE PACKINGS: TYPICAL PROPERTIES

#### SENYA SHLOSMAN AND MICHAEL A. TSFASMAN

ABSTRACT. We review results about the density of typical lattices in  $\mathbb{R}^n$ . This density is of the order of  $2^{-n}$ . We then obtain similar results for random (non-lattice) sphere packings in  $\mathbb{R}^n$ : after suitably taking a fraction  $\nu$  of centers of spheres in a typical random packing  $\sigma$ , the resulting packing  $\tau$  has density  $C(\nu)2^{-n}$  with a reasonable  $C(\nu)$ . We obtain estimates of  $C(\nu)$ .

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 1, January–March 2001, Pages 91–123

# COMBINATORIAL FORMULAS FOR COHOMOLOGY OF KNOT SPACES

### V. A. VASSILIEV

ABSTRACT. We develop homological techniques for finding explicit combinatorial formulas for finite-type cohomology classes of spaces of knots in  $\mathbb{R}^n$ ,  $n \geq 3$ , generalizing the Polyak—Viro formulas for invariants (i. e., 0-dimensional cohomology classes) of knots in  $\mathbb{R}^3$ .

As the first applications, we give such formulas for the (reduced mod 2) generalized Teiblum—Turchin cocycle of order 3 (which is the simplest cohomology class of long knots  $\mathbb{R}^1 \hookrightarrow \mathbb{R}^n$  not reducible to knot invariants or their natural stabilizations), and for all integral cohomology classes of orders 1 and 2 of spaces of compact knots  $S^1 \hookrightarrow \mathbb{R}^n$ . As a corollary, we prove the nontriviality of all these cohomology classes in spaces of knots in  $\mathbb{R}^3$ .

## ISOGENY CLASS AND FROBENIUS ROOT STATISTICS FOR ABELIAN VARIETIES OVER FINITE FIELDS

S. G. VLĂDUŢ

ABSTRACT. Let I(g, q, N) be the number of isogeny classes of g-dimensional abelian varieties over a finite field  $\mathbb{F}_q$  having a fixed number N of  $\mathbb{F}_q$ -rational points. We describe the asymptotic (for  $q \to \infty$ ) distribution of I(g, q, N) over possible values of N. We also prove an analogue of the Sato—Tate conjecture for isogeny classes of g-dimensional abelian varieties.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 2, April-June 2001, Pages 145–156

# TRUNCATION OF FUNCTIONAL RELATIONS IN THE XXZ MODEL

A. A. BELAVIN, S. YU. GUBANOV, AND B. L. FEIGIN

ABSTRACT. The integrable XXZ model with a special open boundary condition is considered. We study the Sklyanin transfer matrices after the quantum group reduction at roots of unity. In this case, the Sklyanin transfer matrices satisfy a closed system of truncated functional equations. The algebraic reason for the truncation is found. An important role in the proof of the result is played by the Zamolodchikov algebra introduced in the paper.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 2, April-June 2001, Pages 157-220

# MATRIX BALLS, RADIAL ANALYSIS OF BEREZIN KERNELS, AND HYPERGEOMETRIC DETERMINANTS

#### YURII A. NERETIN

ABSTRACT. Consider the pseudounitary group  $G = \mathrm{U}(p,q)$  and its compact subgroup  $K = \mathrm{U}(p) \times \mathrm{U}(q)$ . We survey the analysis of the Berezin kernels on the symmetric space G/K. We also explicitly construct unitary intertwining operators from the Berezin representations of G to the representation of G in the space  $L^2(G/K)$ . This implies the existence of a canonical action of the group  $G \times G$  in  $L^2(G/K)$ .

# INDUCTIVE FORMULAS FOR THE INDEX OF SEAWEED LIE ALGEBRAS

#### DMITRI I. PANYUSHEV

ABSTRACT. A seaweed subalgebra of a semisimple Lie algebra  $\mathfrak g$  is a generalization of the notion of parabolic subalgebra. In the case  $\mathfrak g=\mathfrak{sl}(V)$ , seaweed subalgebras were recently introduced by Dergachev and Kirillov. We give an inductive procedure for computing the index of seaweed subalgebras of classical Lie algebras. This allows us to prove that the index of any seaweed in  $\mathfrak{sl}(V)$  or  $\mathfrak{sp}(V)$  is at most the rank of  $\mathfrak g$ . For  $\mathfrak{so}(V)$ , the problem is reduced to the case of parabolic subalgebras.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 2, April-June 2001, Pages 243-286

## SMALL ELLIPTIC QUANTUM GROUP $e_{\tau,\gamma}(\mathfrak{sl}_N)$

#### V. TARASOV AND A. VARCHENKO

ABSTRACT. The small elliptic quantum group  $e_{\tau,\gamma}(\mathfrak{sl}_N)$ , introduced in the paper, is an elliptic dynamical analogue of the universal enveloping algebra  $U(\mathfrak{sl}_N)$ . We define highest weight modules, Verma modules, and contragradient modules over  $e_{\tau,\gamma}(\mathfrak{sl}_N)$ , the dynamical Shapovalov form for  $e_{\tau,\gamma}(\mathfrak{sl}_N)$ , and the contravariant form for highest weight evaluation modules. We show that any finite-dimensional  $\mathfrak{sl}_N$ -module and any Verma module over  $\mathfrak{sl}_N$  can be lifted to the corresponding evaluation module on the same vector space. For the elliptic quantum group  $E_{\tau,\gamma}(\mathfrak{sl}_N)$  we construct the evaluation morphism  $E_{\tau,\gamma}(\mathfrak{sl}_N) \to e_{\tau,\gamma}(\mathfrak{sl}_N)$ , thus making any evaluation module into an evaluation module.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 2, April-June 2001, Pages 287–299

# EQUIVARIANT SYMPLECTIC GEOMETRY OF COTANGENT BUNDLES

#### E. B. VINBERG

ABSTRACT. It is proved that, for any action of a reductive algebraic group G on a quasiaffine algebraic variety X, there is a canonical G-equivariant symplectic rational Galois covering  $f: T^* \operatorname{Hor} X \to T^* X$ , where  $\operatorname{Hor} X$  is the variety of horospheres (orbits of maximal unipotent subgroups of G) in X.

## EUCLIDEAN GIBBS STATES OF QUANTUM CRYSTALS

# SERGIO ALBEVERIO, YURI KONDRATIEV, TATIANA PASUREK, AND MICHAEL RÖCKNER

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. We prove existence and uniform a priori estimates for Euclidean Gibbs states corresponding to quantum anharmonic crystals. Our method is based on a characterization of Gibbs measures in terms of their Radon—Nikodym derivatives with respect to local shifts of the configuration space and corresponding integration by parts formulas.

 $\begin{array}{l} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\rm Volume~1,~Number~3,~July-September~2001,~Pages~315-344} \end{array}$ 

# PERRON-FROBENIUS SPECTRUM FOR RANDOM MAPS AND ITS APPROXIMATION

### MICHAEL BLANK

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. To study the convergence to equilibrium in random maps, we develop the spectral theory of the corresponding transfer (Perron—Frobenius) operators acting in a certain Banach space of generalized functions (distributions). The random maps under study in a sense fill the gap between expanding and hyperbolic systems, since among their (deterministic) components there are both expanding and contracting ones. We prove the stochastic stability of the Perron—Frobenius spectrum and develop its finite rank operator approximations by means of a 'stochastically smoothed' Ulam approximation scheme. A counterexample to the original Ulam conjecture about the approximation of the SBR measure and the discussion of the instability of spectral approximations by means of the original Ulam scheme are presented as well.

### RIGIDITY OF THE CRITICAL PHASES ON A CAYLEY TREE

P. BLEHER, J. RUIZ, R. H. SCHONMANN, S. SHLOSMAN, AND V. ZAGREBNOV

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. We discuss statistical mechanics on nonamenable graphs, and we study the features of the phase transition, which are due to nonamenability. For the Ising model on the usual lattice it is known that below the critical temperature fluctuations of magnetization are much less likely in the states with nonzero magnetic field than in the pure states with zero field. We show that on the Cayley tree the corresponding fluctuations have the same order.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 3, July–September 2001, Pages 365–380

# $T^{-1/4}$ -NOISE FOR RANDOM WALKS IN DYNAMIC ENVIRONMENT ON $\mathbb Z$

C. BOLDRIGHINI AND A. PELLEGRINOTTI

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. We consider a discrete-time random walk  $X_t$  on  $\mathbb{Z}$  with transition probabilities  $P(X_{t+1} = x + u \mid X_t = x, \xi) = P_0(u) + c(u; \xi(t, x))$ , depending on a random field  $\xi = \{\xi(t, x) : (t, x) \in \mathbb{Z} \times \mathbb{Z}\}$ . The variables  $\xi(t, x)$  take finitely many values, are i.i.d. and  $c(u; \cdot)$  has zero average. Previous results show that for small stochastic term the CLT holds almost surely, with dispersion independent of the field. Here we prove that the first correction in the CLT asymptotics is a term of order  $T^{-1/4}$  depending on the field, with asymptotically gaussian distribution as  $T \to \infty$ .

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 3, July–September 2001, Pages 381–388

# A QUASILINEAR APPROXIMATION FOR THE THREE-DIMENSIONAL NAVIER-STOKES SYSTEM

E. I. DINABURG AND YA. G. SINAI

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. In this paper a modification of the 3-dimensional Navier—Stokes system which defines some system of quasilinear equations in Fourier space is considered. Properties of the obtained system and its finite-dimensional approximations are studied.

# ORNSTEIN-UHLENBECK AND RENORMALIZATION SEMIGROUPS

WILLIAM G. FARIS

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. The Ornstein—Uhlenbeck semigroup combines Gaussian diffusion with the flow of a linear vector field. In infinite-dimensional settings there can be non-Gaussian invariant measures. This gives a context for one version of the renormalization group. The adjoint of the Ornstein—Uhlenbeck semigroup with respect to an invariant measure need not be an Ornstein—Uhlenbeck semigroup. This adjoint is the appropriate semigroup to analyze the local stability of the invariant measure under the renormalization group.

 $\begin{array}{l} {\rm MOSCOW~MATHEMATICAL~JOURNAL}\\ {\rm Volume~1,~Number~3,~July-September~2001,~Pages~407-419} \end{array}$ 

### STEADY SOLUTIONS FOR FIFO NETWORKS

K. KHANIN, D. KHMELEV, A. RYBKO, AND A. VLADIMIROV

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. We consider the fluid model of a reentrant line with FIFO discipline and look for solutions with constant flows (steady solutions). In the case of constant viscosities we prove the uniqueness of such a solution. If viscosities are different, we present an example with multiple steady solutions. We also prove that for some classes of reentrant lines uniqueness holds even if the viscosities are different.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 3, July-September 2001, Pages 421-438

### FROM GLOBAL TO LOCAL FLUCTUATION THEOREMS

CHRISTIAN MAES, FRANK REDIG, AND MICHEL VERSCHUERE

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. The Gallavotti—Cohen fluctuation theorem suggests a general symmetry in the fluctuations of the entropy production, a basic concept in the theory of irreversible processes, based on results in the theory of strongly chaotic maps. We study this symmetry for some standard models of nonequilibrium steady states. We give a general strategy to derive a *local* fluctuation theorem exploiting the Gibbsian features of the stationary space-time distribution. This is applied to spin flip processes and to the asymmetric exclusion process.

### TWO-DIMENSIONAL LORENTZIAN MODELS

V. MALYSHEV, A. YAMBARTSEV, AND A. ZAMYATIN

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. The goal of this paper is to present rigorous mathematical formulations and results for Lorentzian models, introduced in physical papers. Lorentzian models represent two dimensional models, where instead of a two-dimensional lattice one considers an ensemble of triangulations of a cylinder, and natural probability measure (Gibbs family) on this ensemble. It appears that correlation functions of this model can be found explicitly. Such models can be considered as an example of a new approach to quantum gravity, based on the notion of a causal set. Causal set is a partially ordered set, thus having a causal structure, similar to Minkowski space. We consider subcritical, critical and supercritical cases. In the critical case the scaling limit of the light cone can be restored.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 3, July–September 2001, Pages 457–468

# THE LIMIT SHAPE AND FLUCTUATIONS OF RANDOM PARTITIONS OF NATURALS WITH FIXED NUMBER OF SUMMANDS

A. VERSHIK AND YU. YAKUBOVICH

Dedicated to Robert Minlos on the occasion of his 70<sup>th</sup> birthday

ABSTRACT. We consider the uniform distribution on the set of partitions of integer n with  $c\sqrt{n}$  numbers of summands, c>0 is a positive constant. We calculate the limit shape of such partitions, assuming c is constant and n tends to infinity. If  $c\to\infty$  then the limit shape tends to known limit shape for unrestricted number of summands (see references). If the growth is slower than  $\sqrt{n}$  then the limit shape is universal  $(e^{-t})$ . We prove the invariance principle (central limit theorem for fluctuations around the limit shape) and find precise expression for correlation functions. These results can be interpreted in terms of statistical physics of ideal gas, from this point of view the limit shape is a limit distribution of the energy of two dimensional ideal gas with respect to the energy of particles. The proof of the limit theorem uses partially inversed Fourier transformation of the characteristic function and refines the methods of the previous papers of authors (see references).

### ON FIRST ORDER LOGIC OF PROOFS

SERGEI ARTEMOV AND TATIANA YAVORSKAYA (SIDON)

To the memory of I. G. Petrovskii on the occasion of his 100<sup>th</sup> anniversary

ABSTRACT. The Logic of Proofs LP solved long standing Gödel's problem concerning his provability calculus (cf. [1]). It also opened new lines of research in proof theory, modal logic, typed programming languages, knowledge representation, etc. The propositional logic of proofs is decidable and admits a complete axiomatization. In this paper we show that the first order logic of proofs is not recursively axiomatizable.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 4, October–December 2001, Pages 491–520

# ON SOLUTIONS FOR THE KADOMTSEV-PETVIASHVILI I EQUATION

J. COLLIANDER, C. KENIG, AND G. STAFFILANI

To the memory of I. G. Petrovskii on the occasion of his 100<sup>th</sup> anniversary

ABSTRACT. Oscillatory integral techniques are used to study the well-posedness of the KP-I equation for initial data that are small with respect to the norm of a weighted Sobolev space involving derivatives of total order no larger than 2.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 4, October-December 2001, Pages 521-537

# MIXED SPECTRUM REPARAMETERIZATIONS OF LINEAR FLOWS ON $\mathbb{T}^2$

BASSAM FAYAD, ANATOLE KATOK, AND ALISTAR WINDSOR

To the memory of great mathematicians of the 20th century, Andrei Nikolaevich Kolmogorov and Ivan Georgievich Petrovskii

ABSTRACT. We prove the existence of mixed spectrum  $C^{\infty}$  reparameterizations of any linear flow on  $\mathbb{T}^2$  with Liouville rotation number. For a restricted class of Liouville rotation numbers, we prove the existence of mixed spectrum real-analytic reparameterizations.

# LOWER BOUNDS FOR THE NUMBER OF ORBITAL TOPOLOGICAL TYPES OF PLANAR POLYNOMIAL VECTOR FIELDS "MODULO LIMIT CYCLES"

#### ROMAN M. FEDOROV

To the memory of I. G. Petrovskii on the occasion of his 100<sup>th</sup> anniversary

ABSTRACT. We consider planar polynomial vector fields. We aim to find the (asymptotic) upper and lower bounds for the number of orbital topological equivalence classes for the fields of degree n. An evident obstacle for this is the second part of Hilbert's 16th problem. To circumvent this obstacle we introduce the notion of equivalence modulo limit cycles. Both upper and lower bounds can be obtained for this type of equivalence. In this paper we use the Viro gluing method to obtain the lower bound  $2^{cn^2}$ , where c > 0 is a constant.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 4, October–December 2001, Pages 551–568

# GROMOV-WITTEN INVARIANTS AND QUANTIZATION OF QUADRATIC HAMILTONIANS

### ALEXANDER B. GIVENTAL

ABSTRACT. We describe a formalism based on quantization of quadratic hamiltonians and symplectic actions of loop groups which provides a convenient home for most of the known general results and conjectures about Gromov–Witten invariants of compact symplectic manifolds and, more generally, Frobenius structures at higher genus. We state several results illustrating the formalism and its use. In particular, we establish Virasoro constraints for semisimple Frobenius structures and outline a proof of the Virasoro conjecture for Gromov–Witten invariants of complex projective spaces and other Fano toric manifolds. Details will be published elsewhere.

# ARITHMETIC CODING AND ENTROPY FOR THE POSITIVE GEODESIC FLOW ON THE MODULAR SURFACE

#### BORIS GUREVICH AND SVETLANA KATOK

This article, whose authors had the privilege and good fortune of studying at Moscow University when I. G. Petrovsky was its Rector, is dedicated to his memory.

ABSTRACT. In this article we study geodesics on the modular surface by means of their arithmetic codes. Closed geodesics for which arithmetic and geometric codes coincide were identified in [9]. Here they are described as periodic orbits of a special flow over a topological Markov chain with countable alphabet, which we call the *positive geodesic flow*. We obtain an explicit formula for the ceiling function and two-sided estimates for the topological entropy of the positive geodesic flow, which turns out to be separated from one: the topological entropy of the geodesic flow on the modular surface.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 4, October–December 2001, Pages 583–599

# SOME UPPER ESTIMATES OF THE NUMBER OF LIMIT CYCLES OF PLANAR VECTOR FIELDS WITH APPLICATIONS TO LIÉNARD EQUATIONS

### YU. ILYASHENKO AND A. PANOV

To the memory of Ivan Georgievich Petrovskii, great personality and great mathematician

ABSTRACT. We estimate the number of limit cycles of planar vector fields through the size of the domain of the Poincaré map, the increment of this map, and the width of the complex domain to which the Poincaré map may be analytically extended. The estimate is based on the relationship between the growth and zeros of holomorphic functions [IYa], [I]. This estimate is then applied to getting the upper bound of the number of limit cycles of the Liénard equation  $\dot{x}=y-F(x)$ ,  $\dot{y}=-x$  through the (odd) power of the monic polynomial F and magnitudes of its coefficients.

# AN APPLICATION OF POTENTIAL ANALYSIS TO MINIMAL SURFACES

#### NIKOLAI NADIRASHVILI

ABSTRACT. We study complete proper minimal immersions in a bounded domain in Euclidean space. We show that for certain domains there are no such immersions. The existence of such unproper immersions is known.

MOSCOW MATHEMATICAL JOURNAL Volume 1, Number 4, October–December 2001, Pages 605-628

# SECOND ORDER CASIMIRS FOR THE AFFINE KRICHEVER–NOVIKOV ALGEBRAS $\widehat{\mathfrak{gl}}_{a,2}$ AND $\widehat{\mathfrak{sl}}_{q,2}$

#### O. K. SHEINMAN

To the memory of I. G. Petrovskii on the occasion of his  $100^{th}$  anniversary

ABSTRACT. The second order casimirs for the affine Krichever–Novikov algebras  $\widehat{\mathfrak{gl}}_{g,2}$  and  $\widehat{\mathfrak{sl}}_{g,2}$  are described. More general operators which we call semi-casimirs are introduced. It is proven that the semi-casimirs induce well-defined operators on conformal blocks and, for a certain moduli space of Riemann surfaces with two marked points and fixed jets of local coordinates, there is a natural projection of its tangent space onto the space of these operators.

# SINGULAR DIFFERENTIAL, INTEGRAL AND DISCRETE EQUATIONS: THE SEMIPOSITONE CASE

R. P. AGARWAL AND DONAL O'REGAN

ABSTRACT. Fixed point methods play a major role in the paper. In particular, we use lower type inequalities together with Krasnoselskii's fixed point theorem in a cone to deduce the existence of positive solutions for a general class of problems. Moreover, the results and technique are applicable also to positione problems.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 1, January–March 2002, Pages 17–33

# MULTIPLICITIES IN THE BRANCHING RULES AND THE COMPLEXITY OF HOMOGENEOUS SPACES

#### DMITRI AKHIEZER AND DMITRI PANYUSHEV

ABSTRACT. Let H be an algebraic subgroup of a connected algebraic group G defined over an algebraically closed field  $\mathbbm{k}$  of characteristic zero. For a dominant weight  $\lambda$  of G, let  $V_{\lambda}$  be a simple G-module with highest weight  $\lambda$ ,  $d_{\lambda} = \dim V_{\lambda}$ , and denote by  $\mathbbm{k}[G/H]_{(\lambda)}$  the isotypic  $\lambda$ -component in  $\mathbbm{k}[G/H]$ . For G/H quasi-affine, we show that the ratio  $\dim \mathbbm{k}[G/H]_{(\lambda)}/d_{\lambda}$  grows no faster than a polynomial in  $\|\lambda\|$  whose degree is the complexity of the homogeneous space G/H. If H is reductive and connected, this yields an estimate of branching coefficients for the pair (G, H) in terms of the complexity of  $G/B_H$ , where  $B_H$  is a Borel subgroup of H. We classify all affine homogeneous spaces G/H such that G is simple and the complexity of  $G/B_H$  is at most 1. Some explicit descriptions of branching rules are also given.

 $\begin{array}{l} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\rm Volume~2,~Number~1,~January-March~2002,~Pages~35-40} \end{array}$ 

### SEMIINFINITE COHOMOLOGY OF TATE LIE ALGEBRAS

### SERGEY ARKHIPOV

ABSTRACT. In this note we give a definition of semiinfinite cohomology for Tate Lie algebras using the language of differential graded Lie algebroids with curvature (CDG Lie algebroids).

## NOTES ON THE QUANTUM TETRAHEDRON

### R. COQUEREAUX

ABSTRACT. This is a set of notes describing several aspects of the space of paths on ADE Dynkin diagrams, with a particular attention paid to the graph  $E_6$ . Many results originally due to A. Ocneanu are described here in a very elementary way (manipulation of square or rectangular matrices). We recall the concept of essential matrices (intertwiners) for a graph and describe their module properties with respect to right and left actions of fusion algebras. In the case of the graph  $E_6$ , essential matrices build up a right module with respect to its own fusion algebra, but a left module with respect to the fusion algebra of  $A_{11}$ . We present two original results: 1) Our first contribution is to show how to recover the Ocneanu graph of quantum symmetries of the Dynkin diagram  $E_6$  from the natural multiplication defined in the tensor square of its fusion algebra (the tensor product should be taken over a particular subalgebra); this is the Cayley graph for the two generators of the twelve-dimensional algebra  $E_6 \otimes_{A_3} E_6$  (here  $A_3$  and  $E_6$  refer to the commutative fusion algebras of the corresponding graphs). 2) To every point of the graph of quantum symmetries one can associate a particular matrix describing the "torus structure" of the chosen Dynkin diagram; following Ocneanu, one obtains in this way, in the case of  $E_6$ , twelve such matrices of dimension  $11 \times 11$ , one of them is a modular invariant and encodes the partition function of which corresponding conformal field theory. Our own next contribution is to provide a simple algorithm for the determination of these matrices.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 1, January—March 2002, Pages 81–97

# MACWILLIAMS DUALITY AND THE ROSENBLOOM-TSFASMAN METRIC

STEVEN T. DOUGHERTY AND MAXIM M. SKRIGANOV

ABSTRACT. A new non-Hamming metric on linear spaces over finite fields has recently been introduced by Rosenbloom and Tsfasman [8]. We consider orbits of linear groups preserving the metric and show that weight enumerators suitably associated with such orbits satisfy MacWilliams-type identities for mutually dual codes. Furthermore, we show that the corresponding weight spectra of dual codes are related by transformations which involve multi-dimensional generalizations of known Krawtchouk polynomials. The relationships with recent results by Godsil [5] and Martin and Stinson [7] on MacWilliams-type theorems for association schemes and ordered orthogonal arrays are also briefly discussed in the paper.

### TORIC GEOMETRY AND GROTHENDIECK RESIDUES

#### O. A. GELFOND AND A. G. KHOVANSKII

ABSTRACT. We consider a system of n algebraic equations  $P_1 = \cdots = P_n = 0$  in the torus  $(\mathbb{C} \setminus 0)^n$ . It is assumed that the Newton polyhedra of the equations are in a sufficiently general position with respect to one another. Let  $\omega$  be any rational n-form which is regular on  $(\mathbb{C} \setminus 0)^n$  outside the hypersurface  $P_1 \cdots P_n = 0$ . Formerly we have announced an explicit formula for the sum of the Grothendieck residues of the form  $\omega$  at all roots of the system of equations. In the present paper this formula is proved.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 1, January–March 2002, Pages 113–126

# THE DUAL HOROSPHERICAL RADON TRANSFORM FOR POLYNOMIALS

J. HILGERT, A. PASQUALE, AND E. B. VINBERG

ABSTRACT. Let X=G/K be a semisimple symmetric space of non-compact type. A horosphere in X is an orbit of a maximal unipotent subgroup of G. The set Hor X of all horospheres is a homogeneous space of G. The horospherical Radom transform suggested by I. M. Gelfand and M. I. Graev in 1959 takes any function  $\varphi$  on X to a function on Hor X obtained by integrating  $\varphi$  over horospheres. We explicitly describe the dual transform in terms of its action on polynomial functions on Hor X.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 1, January–March 2002, Pages 127–160

# ORBITS OF BRAID GROUPS ON CACTI

### GARETH A. JONES AND ALEXANDER ZVONKIN

ABSTRACT. One of the consequences of the classification of finite simple groups is the fact that non-rigid polynomials (those with more than two finite critical values), considered as branched coverings of the sphere, have exactly three exceptional monodromy groups (one in degree 7, one in degree 13 and one in degree 15). By exceptional here we mean primitive and not equal to  $S_n$  or  $A_n$ , where n is the degree. Motivated by the problem of the topological classification of polynomials, a problem that goes back to 19th century researchers, we discuss several techniques for investigating orbits of braid groups on "cacti" (ordered sets of monodromy permutations). Applying these techniques, we provide a complete topological classification for the three exceptional cases mentioned above.

## THE BOTT FORMULA FOR TORIC VARIETIES

#### EVGENY N. MATEROV

ABSTRACT. The purpose of this paper is to give an explicit formula which allows one to compute the dimension of the cohomology groups of the sheaf  $\Omega^p_{\mathbb{P}}(D) = \Omega^p_{\mathbb{P}} \otimes \mathcal{O}_{\mathbb{P}}(D)$  of p-th differential forms Zariski twisted by an ample invertible sheaf on a complete simplicial toric variety. The formula involves some combinatorial sums of integer points over all faces of the support polytope for  $\mathcal{O}_{\mathbb{P}}(D)$ . Comparison of two versions of the Bott formula gives some elegant corollaries in the combinatorics of simple polytopes. Also, we obtain a generalization of the reciprocity law. Some applications of the Bott formula are discussed.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 1, January–March 2002, Pages 183–196

# ELLIPSOIDS, COMPLETE INTEGRABILITY AND HYPERBOLIC GEOMETRY

### SERGE TABACHNIKOV

Dedicated to the memory of J. Moser

ABSTRACT. We describe a new proof of the complete integrability of the two related dynamical systems: the billiard inside the ellipsoid and the geodesic flow on the ellipsoid (in Euclidean, spherical or hyperbolic space). The proof is based on the construction of a metric on the ellipsoid whose nonparameterized geodesics coincide with those of the standard metric. This new metric is induced by the hyperbolic metric inside the ellipsoid (the Caley–Klein model of hyperbolic space).

# METRIC DIOPHANTINE APPROXIMATION: THE KHINTCHINE-GROSHEV THEOREM FOR NONDEGENERATE MANIFOLDS

V. V. BERESNEVICH, V. I. BERNIK, D. Y. KLEINBOCK, AND G. A. MARGULIS

Dedicated to Yu. I. Manin on the occasion of his 65<sup>th</sup> birthday

ABSTRACT. The main objective of this paper is to prove a Khintchine type theorem on divergence of linear Diophantine approximation on nondegenerate manifolds, which completes earlier results for convergence.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 2, April–June 2002, Pages 227–248

## CATÉGORIES TENSORIELLES

#### P. DELIGNE

à Yu. I. Manin, en témoignage d'admiration

ABSTRACT. We give a super mathematics analogue to the theorem that, over an algebraically closed field of characteristic zero, categories of representations of affine group schemes, with their associative, commutative and unital tensor product, are characterized by the property that for any object large enough exterior powers vanish. Exterior powers are replaced by arbitrary Schur functors.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 2, April-June 2002, Pages 249-279

### GROUP SCHEMES WITH STRICT $\mathcal{O}\text{-}\text{ACTION}$

### GERD FALTINGS

To my colleague Yu. Manin

ABSTRACT. Let  $\mathcal{O}$  denote the ring of integers in a p-adic local field. Recall that  $\mathcal{O}$ -modules are formal groups with an  $\mathcal{O}$ -action such that the induced action on the Lie algebra is via scalars. In the paper this notion is generalised to finite flat group schemes. It is shown that the usual properties carry over. For example, Cartier duality holds with the multiplicative group replaced by the Lubin–Tate group. We also show that liftings over  $\mathcal{O}$ -divided powers are controlled by Dieudonné modules or, better, by complexes. For these facts new proofs have to be invented, because the classical recipe of embedding into abelian varieties is not available.

## COUNTING ELLIPTIC SURFACES OVER FINITE FIELDS

#### A. J. DE JONG

Respectfully dedicated to Yu. Manin

ABSTRACT. We count the number of isomorphism classes of elliptic curves of given height d over the field of rational functions in one variable over the finite field of q elements. We also estimate the number of isomorphism classes of elliptic surfaces over the projective line, which have a polarization of relative degree 3. This leads to an upper bound for the average 3-Selmer rank of the aforementionned curves. Finally, we deduce a new upper bound for the average rank of elliptic curves in the large d limit, namely the average rank is asymptotically bounded by 1.5 + O(1/q).

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 2, April—June 2002, Pages 313–328

# A NEW METHOD OF CONSTRUCTING p-ADIC L-FUNCTIONS ASSOCIATED WITH MODULAR FORMS

### ALEXEI PANCHISHKIN

To Yuri Ivanovich Manin for his sixty-fifth birthday

ABSTRACT. We give a new method of constructing admissible p-adic measures associated with modular cusp eigenforms, starting from distributions with values in spaces of modular forms. A canonical projection operator is used onto the characteristic subspace of an eigenvalue  $\alpha$  of the Atkin–Lehner operator  $U_p$ . An algebraic version of nearly holomorphic modular forms is given and used in constructing p-adic measures.

# INFINITE GLOBAL FIELDS AND THE GENERALIZED BRAUER-SIEGEL THEOREM

M. A. TSFASMAN AND S. G. VLĂDUŢ

To our teacher Yu. I. Manin on the occasion of his 65th birthday

ABSTRACT. The paper has two purposes. First, we start to develop a theory of infinite global fields, i. e., of infinite algebraic extensions either of  $\mathbb Q$  or of  $\mathbb F_r(t)$ . We produce a series of invariants of such fields, and we introduce and study a kind of zeta-function for them. Second, for sequences of number fields with growing discriminant, we prove generalizations of the Odlyzko–Serre bounds and of the Brauer–Siegel theorem, taking into account non-archimedean places. This leads to asymptotic bounds on the ratio  $\log hR/\log \sqrt{|D|}$  valid without the standard assumption  $n/\log \sqrt{|D|} \to 0$ , thus including, in particular, the case of unramified towers. Then we produce examples of class field towers, showing that this assumption is indeed necessary for the Brauer–Siegel theorem to hold. As an easy consequence we ameliorate existing bounds for regulators.

MOSCOW MATHEMATICAL JOURNAL Volume 2, Number 2, April–June 2002, Pages 403–431

# VERY SIMPLE 2-ADIC REPRESENTATIONS AND HYPERELLIPTIC JACOBIANS

YURI G. ZARHIN

To my teacher Yuri Ivanovich Manin

ABSTRACT. Let K be a field of characteristic zero,  $n \geq 5$  an integer, f(x) an irreducible polynomial over K of degree n, whose Galois group is either the full symmetric group  $\mathcal{S}_n$  or the alternating group  $\mathcal{A}_n$ . Let  $C\colon y^2=f(x)$  be the corresponding hyperelliptic curve and X=J(C) its Jacobian defined over K. For each prime  $\ell$  we write  $V_\ell(X)$  for the  $\mathbf{Q}_\ell$ -Tate module of X and  $e_\lambda$  for the Riemann form on  $V_\ell(X)$  attached to the theta divisor. Let  $\mathfrak{sp}(V_\ell(X), e_\lambda)$  be the  $\mathbf{Q}_\ell$ -Lie algebra of the symplectic group of  $e_\lambda$ . Let  $\mathfrak{g}_{\ell,X}$  be the  $\mathbf{Q}_\ell$ -Lie algebra of the image of the Galois group  $\mathrm{Gal}(K)$  of K in  $\mathrm{Aut}(V_\ell(X))$ . Assuming that K is finitely generated over  $\mathbb{Q}$ , we prove that  $\mathfrak{g}_{\ell,X} = \mathbf{Q}_\ell \operatorname{Id} \oplus \mathfrak{sp}(V_\ell(X), e_\lambda)$  where Id is the identity operator.

# TORIC RESIDUES AND MIRROR SYMMETRY

#### VICTOR V. BATYREV AND EVGENY N. MATEROV

To Yuri Ivanovich Manin on his 65th birthday

ABSTRACT. We develop some ideas of Morrison and Plesser and formulate a precise mathematical conjecture which has close relations to toric mirror symmetry. Our conjecture, we call it Toric Residue Mirror Conjecture, claims that the generating functions of intersection numbers of divisors on a special sequence of simplicial toric varieties are power series expansions of some rational functions obtained as toric residues. We expect that this conjecture holds true for all Gorenstein toric Fano varieties associated with reflexive polytopes and give some evidences for that. The proposed conjecture suggests a simple method for computing Yukawa couplings for toric mirror Calabi-Yau hypersurfaces without solving systems of differential equations. We make several explicit computations for Calabi-Yau hypersurfaces in weighted projective spaces and in products of projective spaces.

 $\begin{array}{l} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\it To~appear.} \end{array}$ 

## $\mathcal{E} ext{-}\mathbf{FACTORS}$ FOR GAUSS-MANIN DETERMINANTS

ALEXANDER BEILINSON, SPENCER BLOCH, AND HÉLÈNE ESNAULT

To Yuri Manin, with gratitude and admiration

ABSTRACT. We define  $\varepsilon$ -factors in the de Rham setting and calculate the determinant of the Gauß-Manin connection for a family of (affine) curves and a vector bundle equipped with a flat connection.

# NORMALIZED INTERTWINING OPERATORS AND NILPOTENT ELEMENTS IN THE LANGLANDS DUAL GROUP

#### ALEXANDER BRAVERMAN AND DAVID KAZHDAN

To Yuri Ivanovich Manin on the occasion of his 65th birthday

ABSTRACT. Let F be a local non-archimedian field and G be a split reductive group over F whose derived group is simply connected. Set G = G(F). Let also  $\psi \colon F \to \mathbb{C}^{\times}$  be a non-trivial additive unitary character of F. For two parabolic subgroups P and Q in G with the same Levi component M we construct an explicit unitary isomorphism  $\mathcal{F}_{P,Q,\psi} \colon L^2(G/[P,P]) \overset{\sim}{\to} L^2(G/[Q,Q])$  commuting with the natural actions of the group  $G \times M/[M,M]$  on both sides. In some special cases  $\mathcal{F}_{P,Q,\psi}$  is the standard Fourier transform. The crucial ingredient in the definition is the action of the principal  $\mathfrak{sl}_2$ -subalgebra in the Langlands dual Lie algebra  $\mathfrak{m}^{\vee}$  on the nilpotent radical  $\mathfrak{u}_{\mathfrak{p}}^{\vee}$  of the Langlands dual parabolic.

For M as above and using the operators  $\mathcal{F}_{P,Q,\psi}$  we define a *Schwartz space*  $\mathcal{S}(G, M)$ . This space contains the space  $\mathcal{C}_c(G/[P, P])$  of locally constant compactly supported functions on G/[P, P] for every P for which M is a Levi component (but does not depend on P). We compute the space of spherical vectors in  $\mathcal{S}(G, M)$  and study its global analogue.

Finally we apply the above results in order to give an alternative treatment of automorphic L-functions associated with standard representations of classical groups.

 $\begin{array}{l} \text{MOSCOW MATHEMATICAL JOURNAL} \\ To \ annear \end{array}$ 

# ON m-QUASI-INVARIANTS OF A COXETER GROUP

### PAVEL ETINGOF AND VICTOR GINZBURG

To Yuri Ivanovich Manin on his 65-th birthday

ABSTRACT. Let W be a finite Coxeter group in a Euclidean vector space V, and let m be a W-invariant  $\mathbb{Z}_+$ -valued function on the set of reflections in W. Chalykh and Veselov introduced an interesting algebra  $Q_m$ , called the algebra of m-quasi-invariants for W, such that  $\mathbb{C}[V]^W \subseteq Q_m \subseteq \mathbb{C}[V]$ ,  $Q_0 = \mathbb{C}[V]$ , and  $Q_m \supseteq Q_{m'}$  whenever  $m \le m'$ . Namely,  $Q_m$  is the algebra of quantum integrals of the rational Calogero–Moser system with coupling constant m. The algebra  $Q_m$  was studied in [CV], [VSC], [FeV] and [FV]. In particular, in [FV] Feigin and Veselov proposed a number of interesting conjectures concerning the structure of  $Q_m$  and verified them for dihedral groups and constant functions m. Our objective is to prove some of these conjectures in the general case.

## Q-CHARACTERS OF THE TENSOR PRODUCTS IN $\mathfrak{sl}_2$ -CASE

#### B. FEIGIN AND E. FEIGIN

Dedicated to Yu. I. Manin on the occasion of his 65th birthday

ABSTRACT. Let  $\pi_1, \ldots, \pi_n$  be irreducible finite-dimensional  $\mathfrak{sl}_2$ -modules. Using the theory of representations of current algebras, we introduce several ways to construct a q-grading on  $\pi_1 \otimes \cdots \otimes \pi_n$ . We study the corresponding graded modules and prove that they are essentially the same.

 $\begin{array}{l} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\it To~appear.} \end{array}$ 

# ÉTALE COHOMOLOGY, LEFSCHETZ THEOREMS AND NUMBER OF POINTS OF SINGULAR VARIETIES OVER FINITE FIELDS

SUDHIR R. GHORPADE AND GILLES LACHAUD

Dedicated to Professor Yuri Manin for his 65th birthday

ABSTRACT. We prove a general inequality for estimating the number of points of arbitrary complete intersections over a finite field. This extends a result of Deligne for nonsingular complete intersections. For normal complete intersections, this inequality generalizes also the classical Lang-Weil inequality. Moreover, we prove the Lang-Weil inequality for affine, as well as projective, varieties with an explicit description and a bound for the constant appearing therein. We also prove a conjecture of Lang and Weil concerning the Picard varieties and étale cohomology spaces of projective varieties. The general inequality for complete intersections may be viewed as a more precise version of the estimates given by Hooley and Katz. The proof is primarily based on a suitable generalization of the Weak Lefschetz Theorem to singular varieties together with some Bertini-type arguments and the Grothendieck-Lefschetz Trace Formula. We also describe some auxiliary results concerning the étale cohomology spaces and Betti numbers of projective varieties over finite fields, and a conjecture along with some partial results concerning the number of points of projective algebraic sets over finite fields.

# AN ANALYTIC SEPARATION OF SERIES OF REPRESENTATIONS FOR $SL(2; \mathbb{R})$

#### SIMON GINDIKIN

To Yuri Manin with warmest regards

ABSTRACT. For the group  $SL(2;\mathbb{R})$ , holomorphic wave fronts of the projections on different series of representations are contained in some disjoint cones. These cones are convex for holomorphic and antiholomorphic series, which corresponds to the well-known fact that these projections can be extended holomorphically to some Stein tubes in  $SL(2;\mathbb{C})$  [GG]. For the continuous series, the cone is not convex, and the projections are boundary values of 1-dimensional  $\bar{\partial}$ -cohomology in a non-Stein tube.

 $\begin{array}{ll} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\it To~appear.} \end{array}$ 

### COMPLEXITY OF SEMI-ALGEBRAIC PROOFS

DIMA GRIGORIEV, EDWARD A. HIRSCH, AND DMITRII V. PASECHNIK

ABSTRACT. It is a known approach to translate propositional formulas into systems of polynomial inequalities and to consider proof systems for the latter ones. The well-studied proof systems of this kind are the *Cutting Planes* proof system (CP) using linear inequalities and the *Lovász–Schrijver calculi* (LS) utilizing quadratic inequalities. We introduce generalizations  $LS^d$  of LS that operate with polynomial inequalities of degree at most d.

It turns out that the obtained proof systems are very strong. We construct polynomial-size bounded degree  $\mathrm{LS}^d$  proofs of the clique-coloring tautologies (which have no polynomial-size CP proofs), the symmetric knapsack problem (which has no bounded degree Positivstellensatz Calculus proofs), and Tseitin's tautologies (which are hard for many known proof systems). Extending our systems with a division rule yields a polynomial simulation of CP with polynomially bounded coefficients, while other extra rules further reduce the proof degrees for the aforementioned examples.

Finally, we prove lower bounds on Lovász–Schrijver ranks and on the "Boolean degree" of Positivstellensatz Calculus refutations. We use the latter bound to obtain an exponential lower bound on the size of  $static\ LS^d$  and  $tree-like\ LS^d$  refutations.

# UNRAMIFIED RECIPROCAL POLYNOMIALS AND COXETER DECOMPOSITIONS

BENEDICT H. GROSS

Dedicated to Yu. I. Manin on the occasion of his 65th birthday

ABSTRACT. We classify certain automorphisms of an even, unimodular lattice L with fixed characteristic polynomial, assumed to be irreducible and unramified. We then investigate which automorphisms are conjugate to their inverses in the orthogonal group of L.

 $\begin{array}{l} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\it To~appear.} \end{array}$ 

# GOOD AND BAD USES OF ELLIPTIC CURVES IN CRYPTOGRAPHY

### NEAL KOBLITZ

 $Dedicated\ to\ Yuri\ I.\ Manin\ on\ the\ occasion\ of\ his\ 65th\ birthday$ 

ABSTRACT. In the first part of this article I describe the construction of cryptosystems using elliptic curves, discuss the Elliptic Curve Discrete Logarithm Problem (upon which the security of all elliptic curve cryptosystems rests), and survey the different types of elliptic curves that can be chosen for cryptographic applications. In the second part I describe three unsuccessful approaches to breaking various cryptosystems by means of liftings to global elliptic curves. I explain how the failure of these attacks is caused by fundamental properties of the global curves.

# ISOMONODROMY EQUATIONS ON ALGEBRAIC CURVES, CANONICAL TRANSFORMATIONS AND WHITHAM EQUATIONS

#### I. KRICHEVER

Dedicated to Yu. I. Manin on the occasion of his 65<sup>th</sup> birthday

ABSTRACT. We construct the Hamiltonian theory of isomonodromy equations for meromorphic connections with irregular singularities on algebraic curves. We obtain an explicit formula for the symplectic structure on the space of monodromy and Stokes matrices. From these we derive Whitham equations for the isomonodromy equations. It is shown that they provide a flat connection on the space of spectral curves of Hitchin systems.

MOSCOW MATHEMATICAL JOURNAL To~annear.

#### GENERALIZED HARISH-CHANDRA MODULES

### IVAN PENKOV AND VERA SERGANOVA

To Yuri Ivanovich Manin with admiration

ABSTRACT. Let  $\mathfrak g$  be a complex reductive Lie algebra and  $\mathfrak h$  be a Cartan subalgebra of  $\mathfrak g$ . If  $\mathfrak k$  is a subalgebra of  $\mathfrak g$ , we call a  $\mathfrak g$ -module M a strict  $(\mathfrak g, \mathfrak k)$ -module if  $\mathfrak k$  coincides with the subalgebra of all elements of  $\mathfrak g$  which act locally finitely on M. For an intermediate  $\mathfrak k$ , i.e., such that  $\mathfrak h \subset \mathfrak k \subset \mathfrak g$ , we construct irreducible strict  $(\mathfrak g, \mathfrak k)$ -modules. The method of construction is based on the  $\mathcal D$ -module localization theorem of Beilinson and Bernstein. The existence of irreducible strict  $(\mathfrak g, \mathfrak k)$ -modules has been known previously only for very special subalgebras  $\mathfrak k$ , for instance when  $\mathfrak k$  is the (reductive) subalgebra of fixed points of an involution of  $\mathfrak g$ . In this latter case strict irreducible  $(\mathfrak g, \mathfrak k)$ -modules are Harish-Chandra modules.

We also give separate necessary and sufficient conditions on  $\mathfrak{k}$  for the existence of an irreducible strict  $(\mathfrak{g}, \mathfrak{k})$ -module of finite type, i. e., an irreducible strict  $(\mathfrak{g}, \mathfrak{k})$ -module with finite  $\mathfrak{k}$ -multiplicities. In particular, under the assumptions that the intermediate subalgebra  $\mathfrak{k}$  is reductive and  $\mathfrak{g}$  has no simple components of types  $B_n$  for n > 2 or  $F_4$ , we prove a simple explicit criterion on  $\mathfrak{k}$  for the existence of an irreducible strict  $(\mathfrak{g}, \mathfrak{k})$ -module of finite type. It implies that, if  $\mathfrak{g}$  is simple of type A or C, for every reductive intermediate  $\mathfrak{k}$  there is an irreducible strict  $(\mathfrak{g}, \mathfrak{k})$ -module of finite type.

### SYMMETRIES OF MODULES OF DIFFERENTIAL OPERATORS

H. GARGOUBI, P. MATHONET, AND V. OVSIENKO

ABSTRACT. Let  $\mathcal{F}_{\lambda}(M)$  be the space of tensor densities of degree  $\lambda$  on a smooth manifold M. The space  $\mathcal{D}_{\lambda,\mu}^k(M)$  of k-th order linear differential operators, from  $F_{\lambda}(M)$  to  $F_{\mu}(M)$  has a natural structure of  $\mathrm{Diff}(M)$ -module. We study the algebra of symmetries of the modules  $\mathcal{D}_{\lambda,\mu}^k(M)$ , i.e., of all intertwining linear maps on  $\mathcal{D}_{\lambda,\mu}^k(M)$ .

MOSCOW MATHEMATICAL JOURNAL

# PERIODIC SCHRÖDINGER OPERATORS AND AHARONOV-BOHM HAMILTONIANS

B. HELFFER, T. HOFFMANN-OSTENHOF, AND N. NADIRASHVILI

ABSTRACT. Let  $H=-\Delta+V$  be a two-dimensional Schrödinger operator defined on a domain  $\Omega\subset\mathbb{R}^2$  with Dirichlet boundary conditions. Suppose that H and  $\Omega$  are invariant with respect to translations in the  $x_1$ -direction, so that  $V(x_1,x_2)=V(x_1+1,x_2)$  and that in addition  $V(x_1,x_2)=V(-x_1,x_2)$  and that  $(x_1,x_2)\in\Omega$  implies  $(x_1+1,x_2)\in\Omega$  and  $(-x_1,x_2)\in\Omega$ . We investigate the associated Floquet operator  $H^{(q)}$ ,  $0\leq q<1$ . In particular we show that the lowest eigenvalue  $\lambda_q$  is simple for  $q\neq 1/2$  and strictly increasing in q for 0< q<1/2 and that the associated complex valued eigenfunction  $u_q$  has empty zero set.

For the Dirichlet realization of the Aharonov–Bohm Hamiltonian in an annuluslike domain with an axis of symmetry,

$$H_{A,V} = (i\partial_{x_1} + A_1)^2 + (i\partial_{x_2} + A_2)^2 + V,$$

we assume that the magnetic field curl A vanishes identically and we obtain similar results, where the parameter q is now replaced by the  $\frac{1}{2\pi}$ -flux through the hole.

# SET-THEORETICAL SOLUTIONS TO THE YANG–BAXTER RELATION FROM FACTORIZATION OF MATRIX POLYNOMIALS AND $\theta$ -FUNCTIONS

#### ALEXANDER ODESSKII

To V. I. Arnold

ABSTRACT. New set-theoretical solutions to the Yang–Baxter Relation are constructed. These solutions arise from the decompositions "in different order" of matrix polynomials and  $\theta$ -functions. We also construct a "local action of the symmetric group" in these cases, i.e., generalizations of the action of the symmetric group  $S_N$  given by the set-theoretical solution.

 $\begin{array}{ll} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\it To~appear.} \end{array}$ 

# THE MULTIPLE ERGODICITY OF NON-DISCRETE SUBGROUPS OF $Diff^{\omega}(\mathbb{S}^1)$

J. C. REBELO AND R. R. SILVA

ABSTRACT. In this work we deal with non-discrete subgroups of  $\mathrm{Diff}^{\omega}(\mathbb{S}^1)$ , the group analytic diffeomorphisms of the circles preserving the orientation. If  $\Gamma$  is such a group, we consider its natural diagonal action  $\widetilde{\Gamma}$  on the n-dimensional torus  $\mathbb{T}^n$ . Then we obtain a complete characterisation of groups  $\Gamma$  whose corresponding  $\widetilde{\Gamma}$ -action on  $\mathbb{T}^n$  is not piecewise ergodic for all  $n \in \mathbb{N}$ . This result can also be interpreted as an extension of Lie's classification of Lie algebras on  $\mathbb{S}^1$  to general non-discrete subgroups of  $\mathbb{S}^1$ .

# HODGE STRUCTURE ON THE FUNDAMENTAL GROUP AND ITS APPLICATION TO p-ADIC INTEGRATION

#### VADIM VOLOGODSKY

ABSTRACT. We study the unipotent completion  $\Pi_{un}^{DR}(x_0, x_1, X_K)$  of the de Rham fundamental groupoid [De] of a smooth algebraic variety over a local non-archimedean field K of characteristic 0. We show that the vector space  $\Pi_{un}^{DR}(x_0, x_1, X_K)$  carries a certain additional structure. It is a  $\mathbb{Q}_p^{ur}$ -space  $\Pi_{un}(x_0, x_1, X_K)$  equipped with a  $\sigma$ -semilinear operator  $\phi$ , a linear operator N satisfying  $N\phi = p\phi N$  and a weight filtration  $W_{\bullet}$  together with a canonical isomorphism  $\Pi_{un}^{DR}(x_0, x_1, X_K) \otimes_K \bar{K} \simeq \Pi_{un}(x_0, x_1, X_K) \otimes_{\mathbb{Q}_p^{ur}} \bar{K}$ . We prove that an analog of the Monodromy Conjecture holds for  $\Pi_{un}(x_0, x_1, X_K)$ .

As an application, we show that the vector space  $\Pi_{un}^{DR}(x_0, x_1, X_K)$  possesses a distinguished element. In the other words, given a vector bundle E on  $X_K$  together with a unipotent integrable connection, we have a canonical isomorphism  $E_{x_0} \simeq E_{x_1}$  between the fibers. The latter construction is a generalization of Colmez's p-adic integration (rk E=2) and Coleman's p-adic iterated integrals ( $X_K$  is a curve with good reduction).

In the second part we prove that, if  $X_{K_0}$  is a smooth variety over an unramified extension of  $\mathbb{Q}_p$  with good reduction and  $r \leq \frac{p-1}{2}$  then there is a canonical isomorphism  $\Pi_r^{DR}(x_0, x_1, X_{K_0}) \otimes B_{DR} \simeq \Pi_r^{et}(x_0, x_1, X_{\bar{K}_0}) \otimes B_{DR}$  compatible with the action of Galois group.  $(\Pi_r^{DR}(x_0, x_1, X_{K_0}))$  stands for the level r quotient of  $\Pi_{un}^{DR}(x_0, x_1, X_K)$ .) In particular, it implies the Crystalline Conjecture for the fundamental group (for  $r \leq \frac{p-1}{2}$ ).

# THE COMBINATORIAL GEOMETRY OF SINGULARITIES AND ARNOLD'S SERIES $E,\ Z,\ Q$

EGBERT BRIESKORN, ANNA PRATOUSSEVITCH, AND FRANK ROTHENHÄUSLER

To Vladimir Igorevich Arnold With affection and admiration

ABSTRACT. We consider discrete co-compact subgroups  $\Gamma$  of the simply connected Lie group  $\widetilde{\mathrm{SU}}(1,\,1)$ . This Lie group has the structure of a 3-dimensional Lorentz manifold coming from the Killing form.  $\Gamma$  acts on  $\widetilde{\mathrm{SU}}(1,\,1)$  by left translations. We want to describe the Lorentz space form  $\Gamma\backslash\widetilde{\mathrm{SU}}(1,\,1)$  by constructing a fundamental domain F for  $\Gamma$ . We want F to be a polyhedron with totally geodesic faces. We construct such F for all  $\Gamma$  satisfying the following condition:  $\Gamma$  intersects the centre Z of  $\widetilde{\mathrm{SU}}(1,\,1)$  over a subgroup of finite index K, and  $\Gamma = \Gamma/\Gamma \cap Z$  has a fixed point K0 order K2 in the unit disk. The construction depends on  $\Gamma$ 3 and  $\Gamma$ 4.

The Lorentz space form  $\Gamma\backslash \widetilde{\mathrm{SU}}(1,\,1)$  is the link of a quasi-homogeneous Gorenstein singularity. The quasi-homogeneous singularities of Arnold's series  $E,\,Z,\,Q$  are of this type. We compute the fundamental domains for the corresponding group. They are represented by polyhedra in Lorentz 3-space. Each series exhibits a regular characteristic pattern of its combinatorial geometry related to classical uniform polyhedra.

 $\begin{array}{ll} \text{MOSCOW MATHEMATICAL JOURNAL} \\ \textit{To appear.} \end{array}$ 

# INFINITE-DIMENSIONAL FAMILIES OF EXACT SOLUTIONS TO VISCOUS MHD AND NAVIER-STOKES EQUATIONS

OLEG I. BOGOYAVLENSKIJ

This paper is dedicated to V. I. Arnold

ABSTRACT. Infinite families of exact solutions are derived for viscous magnetohydrodnamics equations and for the Navier–Stokes equations. The solutions depend on all four variables  $t,\,x,\,y,\,z,$  are non-symmetric in general and form infinite-dimensional linear spaces. Appplications to Taylor's plasma relaxation theory are presented.

### MAXIMALLY INFLECTED REAL RATIONAL CURVES

#### VIATCHESLAV KHARLAMOV AND FRANK SOTTILE

To V. I. Arnold

ABSTRACT. We introduce and begin the topological study of real rational plane curves, all of whose inflection points are real. The existence of such curves is a corollary of results in the real Schubert calculus, and their study has consequences for the important Shapiro and Shapiro conjecture in the real Schubert calculus. We establish restrictions on the number of real nodes of such curves and construct curves realizing the extreme numbers of real nodes. These constructions imply the existence of real solutions to some problems in the Schubert calculus. We conclude with a discussion of maximally inflected curves of low degree.

 $\begin{array}{ll} {\rm MOSCOW~MATHEMATICAL~JOURNAL} \\ {\it To~appear.} \end{array}$ 

# $L ext{-} ext{CONVEX-CONCAVE SETS IN REAL PROJECTIVE SPACE}$ $AND \ L ext{-} ext{DUALITY}$

A. KHOVANSKII AND D. NOVIKOV

To V. I. Arnold

ABSTRACT. We define a class of L-convex-concave subsets of  $\mathbb{R}P^n$ , where L is a projective subspace of dimension l in  $\mathbb{R}P^n$ . These are sets whose sections by any (l+1)-dimensional space L' containing L are convex and concavely depend on L'. We introduce an L-duality for these sets, and prove that the L-dual to an L-convex-concave set is an  $L^*$ -convex-concave subset of  $(\mathbb{R}P^n)^*$ . We discuss a version of Arnold hypothesis for these sets and prove that it is true (or wrong) for an L-convex-concave set and its L-dual simultaneously.

# EFFECTIVISATION OF A STRING SOLUTION OF 2D TODA HIERARCHY AND RIEMANN THEOREM ABOUT COMPLEX DOMAINS

S. M. NATANZON

Dedicated to V. I. Arnold

ABSTRACT. Let  $0 \in D_+$  be a connected domain with analytic boundary on complex plane  $\mathbb{C}$ . Then according to Riemann theorem there exists a function  $w(z) = \frac{1}{r}z + \sum_{j=0}^{\infty} p_j z^{-j}$ , mapping biholomorphically  $D_- = \mathbb{C} \setminus D_+$  to the exterior of the unit disk  $\{w \in \mathbb{C}||w| > 1\}$ . It follows from Wiegmann and Zabrodin rezults that this function is described by the formula  $\log w = \log z - \partial_{t_0} (\frac{1}{2} \partial_{t_0} + \sum_{k \geqslant 1} \frac{z^{-k}}{k} \partial_{t_k})v$ , where  $v = v(t_0, t_1, \bar{t}_1, t_2, \bar{t}_2, \dots)$  is a function of infinite number of moments of domain  $D_-$ . This function is independent from the domain and satisfies the dispersionless Hirota equation for 2D Toda lattice hierarchy. In the paper we find recursion relations for coefficients of Taylor series of v.

 $\begin{array}{ll} \text{MOSCOW MATHEMATICAL JOURNAL} \\ \textit{To appear.} \end{array}$ 

# DEFORMATIONS OF POLYNOMIALS, BOUNDARY SINGULARITIES AND MONODROMY

DIRK SIERSMA AND MIHAI TIBĂR

Dedicated to Vladimir Igorevich Arnold on the occasion of his 65th anniversary

ABSTRACT. We study the topology of polynomial functions by deforming them generically. We explain how the non-conservation of the total "quantity" of singularity in the neighbourhood of infinity is related to the variation of topology in certain families of boundary singularities along the hyperplane at infinity.

# SPACES OF HERMITIAN OPERATORS WITH SIMPLE SPECTRA AND THEIR FINITE-ORDER COHOMOLOGY

#### V. A. VASSILIEV

To V. I. Arnold

ABSTRACT. V. I. Arnold has studied the topology of spaces of Hermitian operators in  $\mathbb{C}^n$  with non-simple spectra in the relation with the theory of adiabatic connections and the quantum Hall effect. The natural filtration of these spaces by the sets of operators with fixed numbers of eigenvalues defines a spectral sequence providing interesting combinatorial and homological information on this stratification.

We construct a different spectral sequence, also converging to homology groups of these spaces; it is based on the universal techniques of topological order complexes and conical resolutions of algebraic varieties, generalizing the combinatorial inclusion-exclusion formula and is similar to the construction of finite-order knot invariants

This spectral sequence stabilizes at the term  $E_1$ , is (conjecturally) multiplicative, and for  $n \to \infty$  it converges to a stable spectral sequence calculating the cohomology of the space of infinite Hermitian operators without multiple eigenvalues, all whose terms  $E_r^{p,q}$  are finitely generated. This allows us to define the finite-order cohomology classes of this space, and to apply well-known facts and methods of the topological theory of flag manifolds to the problems of geometrical combinatorics, especially concerning continuous partially ordered sets of subspaces and flags.

### INFORMATION FOR AUTHORS

Articles, as a rule, should be submitted in English (British spelling preferred, except for North American authors) in a reasonable electronic version, sent by email to mmj@mccme.ru, preferably as a source file in AMSIATEX (or AMSTEX). Figures (if any) should be included in separate Postscript files or files in one of the formats BMP, PCX, TIFF, JPEG with resolution no less than 600dpi; the size of the figures as they should appear in print must also be indicated. Exceptionally, readable hard copies (two of them) of articles and/or figures will also be considered, but it should be understood that their processing will take substantially longer.

The article must include a title (and a short title, if the title does not fit in one line of the running head), the name(s) of the author(s), their affiliations and addresses (including e-mail), a short (not more than 200 words) abstract, a list of key words or phrases (from 3 to 10), and the primary (and secondary, if any) subjects of the article, specified in accordance to the 2000 Mathematics Subject Classification (accessible at www.ams.org/msc/). Russian speaking authors are also asked to include a Russian translation of the summary.

More detailed technical information about the typesetting (style files, requirements concerning figures, etc.) may be obtained at mmj@mccme.ru. An appropriate electronic author package is available at www.ams.org/tex/.

The English of the articles may be corrected in the process of editing. Authors will be sent one set of proofs.

Publishing a paper in the Moscow Mathematical Journal, the author transfers the copyright to the Independent University of Moscow, retaining all rights for non-commercial use of the published material.

Author(s) of each article receive gratis 50 offprints of his/her/their article. Additional offprint demands should be sent not later than the proofs to mmj@mccme.ru.

### Copying and reprinting

Materials in this journal may be reproduced by any means for educational and scientific purposes without fee or permission (provided that the customary acknowledgment of the source is given). This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Independent University of Moscow.