David Kohel
Curriculum Vitæ

Institut de Mathématiques de Marseille
163, avenue de Luminy, case 907
13288 Marseille cedex 9

né le 27 février 1966
nationalités :
américaine, australienne, française

Déroulement de carrière

Institut de Mathématiques de Luminy

— Professeur 1^e classe, depuis 2011.

— Professeur, équipe d'Arithmétique et Théorie de l'Information, depuis décembre 2007.

Université de Sydney

— Senior Lecturer, équipe de Théorie des Nombres, 2005–2007.

— Sesqui Lecturer in Cryptography, équipe d'Algèbre Computationnelle, 2002–2004.

En 2001, l'Université de Sydney a créé 15 postes permanents, dans des disciplines ciblées, pour la commémoration du 150ième anniversaire de l'université (le sesquicentenniel). Dans ce poste en cryptographie, j'avais la responsabilité de créer un programme d'enseignement en cryptographie dans le département de mathématiques.

Mathematical Sciences Research Institute

— Postdoctorant, pendant le semestre *Algorithmic Number Theory*, août–décembre 2000.

Université de Sydney

— Senior Research Associate, équipe Computational Algebra, 1999–2000, 2001.

National University of Singapore

— Postdoctorant, National Science and Technology Board, Singapore, 1997–1999.

University of California, Berkeley

— National Science Foundation Graduate Research Fellow, U.C. Berkeley.
Thèse, *Endomorphism rings of elliptic curves over finite fields*, décembre 1996.
Jury : Hendrik W. Lenstra, Jr. (directeur), Paul Vojta, John Canny.

Charges d'enseignement

Je suis enseignant-chercheur titulaire depuis 2002, d'abord à l'University de Sydney et depuis la fin 2007 à Aix-Marseille Université.

En Australie, j'ai effectué la service normale : trois cours magistrales par année plus une repartition des TD. J'ai beneficié d'un semestre "sabbatique" en 2005 (y inclus un peu d'enseignement pendant un mois de professeur invité à Toulouse). J'ai passé également deux mois de professeur invité à Nancy au printemps 2007 (sans reduction d'enseignement à Sydney).

Depuis mon arrivée en France en décembre 2007, venant d'Australie, j'ai commencé avec un surcharge de 50% (144h dans un semestre), et effectue depuis une service pleine de 192h, à l'exception d'un semestre de CRCT au printemps 2012 et un semestre de délégation CNRS du printemps 2014 avec l'objectif d'organiser un mois thematique "Arithmétique" et l'accueiller et animer des activités autour de l'invitation de la Chaire Morlet Igor Shparlinski.

Je note également ma participation à l'enseignement et organisation de plusiers Ecoles d'été internationaux (voir ci-dessous dans le cadre de Rayonnement).

Fonctions d'intérêt collectif

Activités en matière d'administration

Institut de Mathématiques de Luminy

— Membre élu du Conseil de laboratoire de l'I2M, depuis 2014.

— Responsable de l'équipe *Arithmétique et Théorie de l'Information*, 2014–2015.

— Responsable, Master M2 Mathématiques générales, parcours *Mathématiques Discrètes et Fondements de l'Informatique*, depuis 2010, (`http://iml.univ-mrs.fr/MDFI/`)

University of Sydney

— Responsable de l'équipe *Number Theory*, 2005–2007.

— Responsable du séminaire *Number Theory*, 2003–2005.

— Responsable du séminaire *Computational Algebra*, 2001–2002.

Responsabilités collectives nationales

Commissions de spécialistes

— Maître de conferences, Aix-Marseille, 2015 (Président).

— Maître de conferences, Aix-Marseille, 2014.

— Maître de conferences, Caen, 2012.

— Maître de conferences, Besançon, 2012.

— Professeur des universités, Bordeaux, 2011.

Rapporteur de thèses

— Christophe Tran, U. Rennes I, 2014.
— Peng Tian, U. Roma, Tor Vergata, 2013.
— Emmanuel Hallouin, HDR, U. Toulouse 2, 2013.
— Kisoon Yoon, U. Caen, 2013.
— Jean-Gabriel Kammerer, U. Rennes I, 2013.
— Aurelien Bajolet, U. Bordeaux, 2012.
— Gaetan Bisson, U. Eindhoven, 2011.
— Marco Streng, U. Leiden, 2010.
— Sorina Ionica, U. Paris, Versailles, 2010.
— Stephen Meigher, U. Groningen, 2009.

Activités de recherche

Les thèmes de ma recherche sont l'arithmétique des courbes (elliptiques, hyperelliptiques et modulaires), les algèbres de quaternions (et leurs relations avec les courbes modulaire et courbes de Shimura), le calcul formel en théorie des nombres et en géométrie arithmétique, et les applications éventuelles en cryptographie et en théorie des codes.

Recemment ma recherche a tourné vers les questions de représentations galoisiennes et d'équidistribution, autour des conjectures de Sato-Tate et Lang-Trotter généralisés. En collaboration avec Gilles Lachaud et mon étudiant Yih-Dar Shieh, nous travaillons sur les algorithmes pour la caracterisation des groupes de Sato-Tate en utilisant des caractères irreducibles des groupes compactes de Lie. Nous trouvons des invariants qui permets d'identifier le groupe par une echantillon de la distribution de Frobenius. Ce travaille peut également jouer un rôle dans l'étude des formes automorphes et questions de rang des variétés abéliennes.

Plus de detailles de ma recherche se trouvent dans mon projet scientifique.

Bourses de recherche

Agence Nationale de Recherche

Parameter spaces for Efficient Arithmetic and Curve security Evaluation (PEACE), avec l'Université de Rennes (D. Lubicz, porteur) et INRIA Bordeaux, (J.-M. Couveignes), 2012–2015, (montant €34 000 pour Luminy). Cette proposition constitue une approche globale et cohérente afin de mieux comprendre les aspects théoriques et algorithmiques du problème du logarithme discret sur les courbes algébriques de petit genre.

Courbes Hyperelliptiques, Isogénies et Comptage (CHIC), avec l'Université de Rennes (D. Lubicz, porteur) et INRIA Lorraine Nancy (E. Thomé), 2009–2012, (montant €69 000 pour Luminy). Le principal objectif du projet CHIC est de combler l'écart en terme de sécurité et de performance qui s'est creusé entre d'une part les courbes elliptiques et d'autre part les courbes de petit genre.

Égide (en partenariat avec Procope)

Explicit Methods and Algorithms in Number Theory, projet de recherche en théorie des nombres avec Florian Heß, T. U. Berlin (montant €6600 pour voyages France–Allemagne), 2009–2010.

European Science Foundation

Curves, Coding Theory and Cryptography avec G. Lachaud et C. Ritzenthaler, (montant €15 000), Exploratory Workshop, 15–16 juin 2009.

Australian Research Council

Mathematics of Elliptic Curve Cryptography avec Christophe Doche et Igor Shparlinski, 2008–2011 (montant 210 000 AU$ [€125 000]). Le programme de recherche de ce projet concerne les méthodes effectives pour l'utilisation des courbes elliptiques en cryptographie.

p-Adic Methods in Arithmetic Geometry, 2004–2006 (montant 210 000 AU$ [€125 000]). Le programme de recherche de ce projet concerne les méthodes p-adiques effectives pour la détermination des ordres de jacobiennes de courbes algébriques, dans le but d'une application cryptographique.

Développement de logiciels

1. **ECHIDNA** (responsable D. Kohel) : un répositoire de code source ouvert et bases de données en Magma conçu pour la recherche en théorie des nombres et géométrie arithmétique.
2. **Sage** (responsable William Stein) : Depuis 2005 (pendant une invitation à l'University of California, San Diego), j'ai contribué aux fondations du système (en code et conception). Un des plus important systèmes de calcul formel et l'alternative la plus viable au systèmes propriétaires (Maple, Mathematica, Matlab, etc.).
3. **Magma** (responsable John Cannon) : pendant un postdoc 1999–2002, j'ai mis en place les fondations de la géométrie arithmétique, théorie des nombres, et la cohérence générale des structures algébriques, détaillé dans un dizaine de chapitres de documentation. Actuellement le plus puissant système de calcul formel en théorie des nombres et géométrie arithmétique, avec l'emploi d'une quinzaine de personnes et financement par licenses, bourses, et organismes de défense australiennes et américaines.

Encadrement de thèses et mémoires

Encadrement de thèses

— Yih-Dar Shieh, 2009–2015, *Arithmetic Aspects of Point Counting and Frobenius Distributions*, Université d'Aix-Marseille, 2015.
— Florent Rovetta, 2011–2015, *Étude arithmétique et algorithmique de courbes de petit genre*, codirigé avec C. Ritzenthaler, Université d'Aix-Marseille, 2015.
— Virgile Ducet, 2009–2013, *Construction of algebraic curves with many rational points over finite fields*, Université d'Aix-Marseille, 2013.
— Hamish Ivey-Law, 2007–2012, *Algorithmic Aspects of Hyperelliptic Curves and their Jacobians*, codirigé avec C. Fieker, l'Université d'Aix-Marseille et U. Sydney, 2012.
— Christophe Arene, 2008–2011, *Geometrie et arithmetique explicites des variétés abéliennes et applications à la cryptographie*, codirigé avec C. Ritzenthaler, Université d'Aix-Marseille 2, 2011.
— Ley Wilson, 2006-2009, **Q**-*Curves with Complex Multiplication*, U. Sydney, 2010.
— David Gruenewald, 2004-2008, *Explicit Algorithms for Humbert Surfaces*, U. Sydney, 2009.
— Ben Smith, 2002–2005, *Explicit Endomorphisms and Correspondences*, U. Sydney, 2006.

Stages et mémoires de master

— Yih-Dar Shieh, *Algebraic Curves over Finite Fields*, U. Paris-Sud et U. Leiden (Erasmus Mundus Masters programme ALGANT), 2009.
— Virgile Ducet, *The Arithmetic of CM Elliptic Curves*, ENS Lyon, 2009.
— Steve Enright-Ward, *CM Proofs for Elliptic Curves over Number Fields*, U. Sydney, 2008.
— Thomas Icart, *Cryptologie : multiplication scalaire sur les courbes elliptiques*, École Polytechnique, 2005.
— Alex Unger, *Variétés abéliennes*, U. Leipzig, 2005.

Honours thesis

Dans le système australien, la quatrième année d'université permet aux étudiants d'obtenir leur

diplôme avec mention, pour lequel ils rédigent un mémoire de fin d'études d'une soixantaine de pages. Les étudiants et leur titre de mémoire que j'ai encadré sont :

— Graeme Pope, *Efficient arithmetic on elliptic and hyperelliptic curves*, 2006.
— Gareth White, *Heights on elliptic curves*, 2006.
— Zhuo Jia Dia, *Algebraic geometric coding theory*, 2006.
— Hamish Ivey-Law, *Rational points on higher genus curves*, 2006.
— David Gruenewald, *An introduction to modular forms*, 2003.
— Gordon Childs, *Counting points on hyperelliptic curves over finite fields*, 2001.
— Quy Tuan Nguyen, *Binary quadratic forms*, 2000.

Vacation Scholars

L'University of Sydney donne la possibilité (sur dossier) aux étudiants inscrits en quatrième année de travailler sur un projet de recherche pendant six semaines de l'été, souvent precurseur à un mémoire de quatrième année.

Les étudiants et sujets que j'ai encadré sont : Jacky Chow (Fonctions elliptiques et fonctions abéliennes, 2005), Graeme Pope (Courbes elliptiques et cryptographie, 2005), Gareth White (Groupes de Mordell-Weil des courbes elliptiques, 2005), Peter McNamara (Courbes elliptiques, 2004), Quy Tuan Nguyen (Formes quadratiques, 2000).

Rayonnement

Écoles d'été et d'hiver

— *Frobenius distributions of curves*, École d'hiver, CIRM, 17–21 février 2014. Dans le cadre de l'invitation de la Chaire Morlet Igor Shparlinski, j'ai organisé une école d'hiver avec Shparlinski et Christophe Ritzenthaler. Les cours principaux et orateurs étaient : Chantal David, Nathan Jones et Peter Stevenhagen : *Cebotarev density theorem with application to distributions of Frobenius*, Francesc Fité and Andrew Sutherland : *Sato-Tate groups and Galois endomorphism modules of abelian surfaces*, Igor Shparlinski : *Group and number theoretic properties of points on elliptic curves.*
— *Sage Days 61 : Quaternion Orders and Brandt Modules.* A l'exception des Sage Days precédents, nous avons donné des cours (par moi-même, Lassina Dembelé, Alyson Deines, William Stein, et John Voight) qui ont été validé comme Erasmus Master Class.
— *AMSI Summer School*, University of Sydney (Australian Mathematical Sciences Institute), *Cryptography.* J'ai donné un cours intensif de cryptographie à l'école d'été pour étudiants de master et doctorants, janvier–février 2007.
— *MSRI Summer Graduate Workshop in Computational Number Theory*, Mathematical Sciences Research Institute, Berkeley. *Quaternion algebras and modular forms.* J'ai donné un cours sur les algèbres de quaternions et formes modulaires destinés aux doctorants, 31 juillet au 11 août 2006.

Invitations colloques internationaux

— *Sage Days 61* (Copenhagen, 2014), *Theoretical and Practical Aspects of the Discrete Logarithm Problem* (Ascona, 2014), *International Workshop on Coding and Cryptography* (Qingdao, 2011), *Elliptic Curves and Computation* (Microsoft Research, Redmond, 2010), *Sage-devel Days* (U. Washington, Seattle, 2008), *Computational number theory* FoCM'08 (Hong Kong, 2008), *Symposium on Algebraic Geometry and its Applications* (Papeete, 2007), *Elliptic Curve Cryptography* (Dublin, 2007).

Organisation de colloques

— *Arithmetic, Geometry, Cryptography and Coding Theory 2015* (CIRM, Luminy), avec A. Bassa et A. Couvreur (95 personnes), *Frobenius distributions of curves* (CIRM, Luminy), avec C. Ritzenthaler et I. Shparlinski (50 personnes), *Geocrypt 2011* (Bastia) avec C. Ritzenthaler, et al., (40 personnes), *Arithmetic, Geometry, Cryptography and Coding Theory 2009* (CIRM, Luminy) avec S. Vladuts, (80 personnes), ESF Exploratory Workshop *Curves, Codes, and Cryptography* (Luminy 2009) avec C. Ritzenthaler et G. Lachaud, (30 personnes), *Elliptic Curves and Higher Dimensional Analogues II* (Sydney 2005), (15 personnes). *Elliptic Curves and Higher Dimensional Analogues* (Sydney 2002), (20 personnes). *Algorithmic Number Theory Symposium* (Sydney, 2002) avec J. Cannon et C. Fieker (150 personnes).

European Science Foundation

— *Strategic Workshop with Exploratory Workshop Convenors*, invité par ESF Standing Committee for Physical & Engineering Sciences, Egelsbach, 1 septembre 2010.

— *Round Table Meeting of ESF Member Organisations*, invité par ESF Standing Committee for Physical & Engineering Sciences, Berlin, 15-16 juin 2009.

Rapporteur des bourses

— Rapporteur pour Australian Research Council, ANR, European Science Foundation, Hong Kong Grant Council, INRIA, National Science Foundation (USA).

Exposés grand public

— *Théorie des nombres et cryptographie*, Journée Annuelle de l'SMF, Institut Henri Poincaré, 14 avril 2014.

— *Sage dans l'enseignement : Cryptographie*, Journée Sage dans l'enseignement, Luminy, 24 février 2010.

— *Sage : Open source software for mathematics*, Sage Days 20, Luminy, 22 février 2010.

— *SAGE notions of computing with schemes*, SAGE Days, U.C. San Diego, 5 février 2006.

— *Introduction to Magma and Applications*, Institut africain pour les sciences mathématiques (AIM), Afrique du Sud, 2 février 2005.

— *The Magma Language and Vistas*, Computer Education Seminar, Mathematical Sciences Research Institute, Berkeley, 6 octobre 2000.

Invitations de recherche internationales

Depuis Singapour :

— Université de Sydney, (invité par J. Cannon), décembre 1997, mai 1998.

— Reed College (invité par R. Crandall), juin 1998.

Depuis Sydney :

— École Polytechnique (invité par F. Morain, LIX), juillet 2001, décembre 2001.

— Université de Rome 2, Tor Vergata (invité par R. Schoof), fin novembre–décembre 2002.

— Université de Californie à San Diego (invité par W. Stein), septembre 2005.

— Institut de Technologie de Tokyo (invité par T. Satoh), 11–21 novembre 2005.

— Université Toulouse le Mirail, GRIMM (Professeur invité) fin novembre–décembre 2005.

— Université Henri Poincaré, Nancy, (Professeur invité) fin avril–juin 2007.