

# Curriculum vitæ — David Madore

## État-civil et coordonnées

- *Nom* : David Alexander MADORE
- *Date et lieu de naissance* : 3 août 1976 à Paris (13<sup>e</sup>)
- *Situation familiale* : célibataire
- *Nationalité* : française et canadienne (double nationalité)
- *Adresse personnelle* : 11 rue Simonet, 75 013 Paris
- *Adresse professionnelle* : DMA, ENS, 45 rue d’Ulm, 75 230 Paris cedex 05
- *Tél.* : 01 44 32 20 54 (pro.) / 01 45 88 39 61 (perso.) / 06 98 03 41 80 (mobile)
- *Mél.* : david.madore@ens.fr

## Études et diplômes

- *2005* : Doctorat de mathématiques de l’Université de Paris-Sud XI (Orsay).  
Thèse réalisée sous la direction de Jean-Louis Colliot-Thélène (DR CNRS),  
ayant pour titre « Hypersurfaces cubiques : équivalence rationnelle, R-  
équivalence et approximation faible. »  
Rapporteurs : Brendan Hassett (Assoc. Prof., Rice Univ.) et Laurent Moret-  
Bailly (Prof. Univ. Rennes 1).  
Soutenue le 8 avril 2005. Mention très honorable.
- *1999* : Magistère de mathématiques fondamentales et appliquées et d’in-  
formatique (MMFAI) de l’École Normale Supérieure et de l’Université de  
Paris-Sud XI.
- *1998* : DEA de mathématiques à l’Université de Paris-Sud XI. Mémoire  
« Diviseurs thêta et morphisme de Frobenius », effectué sous la direction  
de Michel Raynaud (Prof. Univ. Paris XI), mention très bien. Soutenu le  
4 novembre 1998.
- *1998* : Reçu à l’Agrégation externe de mathématiques (option mathéma-  
tiques appliquées à l’informatique) avec rang 4.
- *1997* : Maîtrise de mathématiques pures, mention très bien. Mémoire de  
maîtrise sur « le théorème de Belyĭ », sous la direction d’Yves Laszlo.
- *1997* : Licence de mathématiques, mention très bien.

- 1996 : Admis à l'École Normale Supérieure de Paris (concours C/S : mathématiques) avec rang 3.
- 1994–1996 : Classes préparatoires scientifiques (math. sup., math. spé.  $M'$ ) au lycée Louis le Grand (Paris).
- 1994 : Reçu au baccalauréat (série C) avec mention très bien et félicitations du jury.
- 1994 : Troisième prix au concours général des lycées, mathématiques.
- 1994 : Premier prix au concours général des lycées, sciences physiques.
- 1991 : Brevet des collèges.

## Publications et prépublications

### Parues ou à paraître

- 2006 : « Équivalence rationnelle sur les hypersurfaces cubiques de mauvaise réduction », à paraître au *J. Number Theory*.
- 2004 : « Approximation faible aux places de bonne réduction sur les surfaces cubiques sur les corps de fonctions », à paraître au *Bulletin de la SMF*.
- 2003 : « Surfaces de del Pezzo sans point rationnel sur un corps de dimension cohomologique un », en collaboration avec Jean-Louis Colliot-Thélène, paru au *J. Inst. Math. Jussieu*, **3** (2004), 1–16.
- 2002 : « Équivalence rationnelle sur les hypersurfaces cubiques sur les corps  $p$ -adiques », paru à *Manuscripta Math.*, **110** (2003), 171–185.
- 1999 : « Theta Divisors and the Frobenius Morphism », paru dans le volume *Courbes semi-stables et groupe fondamental en géométrie algébrique* (Jean-Benoît Bost, François Loeser et Michel Raynaud éditeurs), Progress in Mathematics (Birkhäuser).

### Prépublications

- 2007 : « Consum v0 : An Experimental Cipher » (article de cryptographie).
- 2003 : « Sur la spécialisation de la  $R$ -équivalence », à soumettre (cité par P. Gille, dans « Spécialisation de la  $R$ -équivalence pour les groupes réductifs », *Trans. Amer. Math. Soc.*, **356** (2004), 4465–4474).
- 2003 : « Very free  $R$ -equivalence on toric models », à soumettre.

*Tous ces textes sont disponibles en ligne sur <http://www.dma.ens.fr/~madore/>*

### En cours d'élaboration

- 2007 : « Quelques remarques sur le principe de Hasse pour les hypersurfaces cubiques singulières », en cours d'amélioration.
- 2006 : « Les hypersurfaces cubiques sont séparablement rationnellement connexes », en cours d'amélioration.

### **Exposés, colloques**

#### Exposés donnés sur invitation

- 2006 (14 décembre) : « Introduction aux surfaces cubiques », séminaire de mathématiques et réseaux du département Informatique et Réseaux, École nationale supérieure des télécommunications.
- 2006 (23 juin) : « Dégénérescence des variétés de Fano et une conjecture d'Ax (d'après J. Kollár) », séminaire *Variétés rationnelles*, Université de Paris-Sud XI.
- 2006 (27 janvier) : « Équivalence rationnelle sur une hypersurface cubique de mauvaise réduction », séminaire de théorie des nombres du laboratoire Nicolas Oresme, Université de Caen Basse Normandie.
- 2004 (19 juin) : « Weak Approximation at Places of Good Reduction on Cubic Surfaces over the Function Field of a Curve », conférence *Diophantine Geometry* (18–22 juin 2004) organisée par Yuri Tschinkel, Georg-August-Universität de Göttingen.
- 2003 (11 décembre) : « Approximation faible aux places de bonne réduction sur les surfaces cubiques sur les corps de fonctions », séminaire de géométrie algébrique de l'IRMAR, Université de Rennes 1.
- 2003 (22 novembre) : « Approximation faible aux places de bonne réduction sur les surfaces cubiques sur les corps de fonctions », séminaire *Variétés rationnelles*, École normale supérieure.
- 2003 (30 juin) : « Surfaces de del Pezzo sans point rationnel sur un corps de dimension cohomologique un », colloque *Groupes algébriques, formes quadratiques* (20 juin – 4 juillet 2003), Université de Franche-Comté à Besançon.
- 2003 (7 février) : « Surfaces cubiques et corps de dimension cohomologique un », séminaire *Variétés rationnelles*, École normale supérieure.

- 2002 (6 novembre) : «  $R$ -équivalence très libre sur les modèles toriques », séminaire de théorie des nombres de l’Institut Fourier, Université Joseph Fourier de Grenoble.
- 2002 (15 février) : «  $R$ -équivalence sur les surfaces cubiques », séminaire *Variétés rationnelles*, École normale supérieure.
- 2001 (13 janvier) : « Groupes fondamentaux des variétés rationnellement connexes (d’après J. Kollár) », séminaire *Variétés rationnelles*, École normale supérieure.
- 1998 (4 décembre) : « Theta Divisors and the Frobenius Morphism », rencontre jeunes chercheurs « Groupe fondamental en géométrie algébrique » (30 novembre – 4 décembre 1998) au CIRM de Luminy.

### Autres

- 2002 : Participation en tant qu’auditeur à l’école d’été sur la conjecture de Birch et Swinnerton-Dyer à Chevaleret.
- 2001 : Participation en tant qu’auditeur au congrès « Higher dimensional varieties and rational points » à l’institut Alfréd Rényi de Budapest.
- 1998–1999 : Organisation d’un groupe de travail d’élèves « Logique, Théorie des Ensembles et Forcing » (classiques et intuitionnistes) à l’École normale supérieure.

### **Enseignement**

- 2007– : Examineur au concours d’entrée des ENS (épreuve de TIPE).
- 2004– : Agrégé-préparateur (« caïman ») à l’École normale supérieure (Paris) :
  - organisation de la préparation à l’Agrégation de l’ENS (algèbre et mathématiques générales 2004–, et option algèbre et calcul formel 2005–), sous la direction de François Loeser ;
  - travaux dirigés d’Algèbre, niveau maîtrise (cours par Marc Rosso en 2004–2006, par Bernhard Keller en 2006–) pour la FIMFA ;
  - encadrement d’exposés de maîtrise des élèves de première année (sujets proposés et encadrés : « variétés toriques et polytopes », « degrés de Turing et problème de Post », « résolution de l’équation du cinquième degré », « modèles à permutation et indépendance de l’axiome du choix »).

- 2005– : Donné un cours accéléré d’algèbre commutative et applications à l’informatique (19–23 septembre 2005 et 11–15 septembre 2006) au master parisien de recherche en informatique (MPRI) à l’invitation de Louis Granboulan (département d’informatique de l’ENS, équipe de cryptographie).
- 2000–2004 : Donné des travaux dirigés en 1<sup>ère</sup> année de DEUG MIAS à l’Université de Paris-Sud XI (Orsay), en tant que moniteur (2000–2003) puis en tant qu’ATER (2003–2004), sous la coordination de François Cottet-Emard. (Également, en 2004, séances de travaux dirigés en licence de mathématiques pour le cours de Guy Henniart.)
- 1996–1999 : Examineur (« khôlleur ») en mathématiques en classes préparatoires au lycée Blaise Pascal à Orsay puis au lycée Louis le Grand à Paris.

## Divers

- Intérêts mathématiques* : Géométrie algébrique (hypersurfaces cubiques, déformation des courbes, variétés toriques, fondements de la géométrie algébrique), géométrie arithmétique (variétés rationnelles, toseurs universels, problème de Hasse), théorie des nombres (cohomologie galoisienne, problème de Galois inverse, dessins d’enfants, corps de classes), théorie des corps, méthodes effectives (bases de Gröbner), cryptographie; calculabilité, logique mathématique (arithmétique, mathématiques à rebours), théorie des ensembles, théorie des catégories (topoi et logique intuitionniste); vulgarisation mathématique, histoire des mathématiques (histoire des fondements).
- Langues* : Anglais courant; allemand parlé, écrit, lu; italien et espéranto lus; connaissances de russe, latin, grec ancien.
- Informatique* : Très bonne connaissance des systèmes Unix. Bonne maîtrise de T<sub>E</sub>X et L<sup>A</sup>T<sub>E</sub>X. Programmation dans plusieurs langages (C, Perl, Scheme, Java). Auteur des programmes `sha256sum` et `apparentés` (fonctions de hachage cryptographiques SHA-2) sur les systèmes GNU/Linux.
- Loisirs* : Informatique; écriture de nouvelles (en français et en anglais); lecture. Contributeur sur Wikipédia anglophone. Blogueur.