

# 1 Notice individuelle

---

Christophe Ritzenthaler

Né le 4 janvier 1976 à Creutzwald (57)

Nationalité : française

Situation actuelle : Maître de conférences à l'université de la Méditerranée.

Adresse personnelle :

3, cours Jean Ballard

13001 Marseille

France

Tél. : 00 33 (0)4 91 33 59 40

Adresse professionnelle :

Institut de Mathématiques de Luminy

163 av. de Luminy Case 907

13288 Marseille

France

Tél. : 00 33 (0)4 91 26 95 84

E-mail : [ritzenth@iml.univ-mrs.fr](mailto:ritzenth@iml.univ-mrs.fr)

Internet : <http://www.iml.univ-mrs.fr/~ritzenth/>

## 2 Publications les plus significatives

---

Les publications précédées d'un ★ sont jointes au dossier et sont brièvement décrites dans la section 10.

★ G. LACHAUD, C. RITZENTHALER, A. ZYKIN, Jacobians among abelian threefolds : a formula of Klein and a question of Serre, à paraître dans Math. Research Letters.

★ E. HOWE, E. NART, C. RITZENTHALER, Jacobians in isogeny classes of abelian surfaces over finite fields, Annales de l'institut Fourier, 59 :239-289, 2009.

D. LEHAVI, C. RITZENTHALER, An explicit formula for the arithmetic geometric mean in genus 3, Experimental Math., 16, 421-440, 2007.

E. NART, C. RITZENTHALER, Non hyperelliptic curves of genus three over finite fields of characteristic two, J. of Number Theory, 116 :443-473, 2006.

P. GAUDRY, T. HOUTMANN, D. KOHEL, C. RITZENTHALER, A. WENG,  $p$ -adic construction of CM-curves, Asiacrypt 2006, Lecture Notes in Comput. Sci. 4284 :114-129, Springer, Berlin, 2006.

### 3 Formation

---

Sept. 1996	Entrée à l'École Normale Supérieure de Cachan.
1998 - 1999	Agrégation de Mathématiques ( <b>rang 20</b> ).
1996 - 1999	Magistère de Mathématiques et d'Informatique de l'ENS Cachan et de l'université Paris 7 (mention Très honorable avec les Félicitations du jury).
1999 - 2003	Thèse sous la direction du Professeur Jean-François MESTRE, soutenue le 25 juin 2003 à l'Université Paris VII. <i>Titre :</i> Problèmes relatifs à certaines familles de courbes sur les corps finis. <i>Mention :</i> Très honorable. <i>Président :</i> Pr. Loïc MEREL Université Paris VII. <i>Rapporteurs :</i> Pr. Henri COHEN Université Bordeaux I. Pr. René SCHOOF Université Roma Tor Vergata.
Sep. 03-Fév. 04	Post-doctorat à l'IEM (Institut für Experimentelle Mathematik), Essen, Allemagne (Invité par Gerhard Frey, réseau GTEM).
Mars 04-Sep. 04	Post-doctorat à l'institut de mathématiques de Leiden, Pays-Bas (Invité par Bas Edixhoven et Bart de Smit, réseau GTEM).
Oct. 2004	Invitation à l'université de Sydney, Australie (Invité par David Kohel).
Nov. 04-Août 05	Post-doctorat à l'Universitat Autònoma de Barcelone, Espagne (invité par Enric Nart et Xavier Xarles, réseau AAG).
Sep. 2005	Invitation à l'université de Copenhague (DTU), Danemark (Invité par Tanja Lange).
Oct. 05-Déc. 05	Invitation à l'université de Princeton, États-Unis (Invité par Manjul Bhargava).
Jan. 2006 -	Maître de conférences à l'université de la Méditerranée.
Déc. 2009	Habilitation à Diriger des Recherches, soutenue le 2 décembre à l'université de la Méditerranée. <i>Titre :</i> Aspects arithmétiques et algorithmiques des courbes de genre 1, 2 et 3. <i>Président :</i> M. Gerard VAN DER GEER Université d'Amsterdam. <i>Tuteur :</i> M. Gilles Lachaud Université de la Méditerranée. <i>Rapporteurs :</i> M. Gerard VAN DER GEER Université d'Amsterdam. Mme Kristin LAUTER Microsoft Research. M. Felipe VOLOCH Université du Texas. <i>Examineurs :</i> M. Noam D. ELKIES Université de Harvard. M. David KOHEL Université de la Méditerranée. M. Jean-François MESTRE Université Paris VII. M. Enric NART Université autonome de Barcelone.

## 4 Liste de publications et travaux (ordre chronologique inverse)

---

Ces publications peuvent être trouvées à l'adresse suivante :

<http://www.iml.univ-mrs.fr/~ritzenth/research.html>

### Articles dans des revues internationales à comité de lecture

- [1] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of Tate pairings, 2011. À paraître dans *Journal of Number Theory*.
- [2] C. Ritzenthaler. Optimal curves of genus 1, 2 and 3, 2011. À paraître dans les *Publications Mathématiques de Besançon*.
- [3] S. Ballet, C. Ritzenthaler, and R. Rolland. On the existence of dimension zero divisors for function fields over  $\mathbb{F}_q$ . *Acta Arithmetica*, 143(4) :377–392, 2010.
- [4] A. Beauville and C. Ritzenthaler. Jacobians among abelian threefolds : a geometric approach, 2010. À paraître dans *Math. Annal.*
- [5] Gilles Lachaud, Christophe Ritzenthaler, and Alexey Zykin. Jacobians among abelian threefolds : a formula of Klein and a question of Serre. *Math. Res. Lett.*, 17(2), 2010.
- [6] Christophe Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS J. Comput. Math.*, 13 :192–207, 2010.
- [7] A. I. Zykin, Zh. Lasho, and K. Rittsentaler. Jacobians and abelian threefolds : Klein's formula and Serre's question. *Dokl. Akad. Nauk*, 431 :313–315, 2010.
- [8] S. D. Galbraith, J. Pujolàs, C. Ritzenthaler, and B. Smith. Distortion maps for supersingular genus two curves. *J. Math. Cryptol.*, 3(1) :1–18, 2009.
- [9] E. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Annales de l'institut Fourier*, 59 :239–289, 2009.
- [10] E. Howe, D. Maisner, E. Nart, and C. Ritzenthaler. Principally polarizable isogeny classes of abelian surfaces over finite fields. *Math. Research Lett.*, 15 :121–127, 2008.
- [11] E. Nart and C. Ritzenthaler. Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2. *Finite fields and their applications*, 14 :676–702, 2008.
- [12] D. Lehavi and C. Ritzenthaler. An explicit formula for the arithmetic geometric mean in genus 3. *Experimental Math.*, 16 :421–440, 2007.
- [13] M. Girard, D. Kohel, and C. Ritzenthaler. The Weierstrass subgroup of a curve has maximal rank. *Bull. of London Math. Soc.*, 38 :925–931, 2006.
- [14] J. Müller and C. Ritzenthaler. On the ring of invariants of ordinary quartic curves in characteristic 2. *J. of Algebra*, 303 :530–542, 2006.
- [15] E. Nart and C. Ritzenthaler. Non hyperelliptic curves of genus three over finite fields of characteristic two. *J. of Number Theory*, 116 :443–473, 2006.
- [16] C. Ritzenthaler. Automorphism group of  $C: y^3 + x^4 + 1 = 0$  in characteristic  $p$ . *JP J. Algebra Number Theory Appl.*, 4(3) :621–623, 2004.
- [17] C. Ritzenthaler. Automorphismes des courbes modulaires  $X(n)$  en caractéristique  $p$ . *Manuscripta Math.*, 109(1) :49–62, 2002.

## Comptes-rendus de congrès ou colloques

- [18] E. Nart and C. Ritzenthaler. Genus three curves with many involutions and application to maximal curves in characteristic 2. In *Proceedings of AGCT-12*, volume 521, pages 71–85. Contemporary Mathematics, 2010.
- [19] Roger Oyono and Christophe Ritzenthaler. On rationality of the intersection points of a line with a plane quartic. Hasan, M. Anwar (ed.) et al., Arithmetic of finite fields. Third international workshop, WAIFI 2010, Istanbul, Turkey, June 27–30, 2010. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 6087, 224-237 (2010)., 2010.
- [20] S. Flon, R. Oyono, and C. Ritzenthaler. Fast addition on non-hyperelliptic genus 3 curves. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 1–28. World Sci. Publ., Hackensack, NJ, 2008.
- [21] G. Lachaud and C. Ritzenthaler. On some questions of Serre on abelian threefolds. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 88–115. World Sci. Publ., Hackensack, NJ, 2008.
- [22] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in cryptography—ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Comput. Sci.*, pages 114–129. Springer, Berlin, 2006. version Arxiv : <http://arxiv.org/abs/math/0503148>.
- [23] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 379–394. Springer, Berlin, 2004.

## Prépublications, travaux en cours et thèses

- [24] C. Arène, D. Kohel, and C. Ritzenthaler. Complete addition laws on abelian varieties.
- [25] N. D. Elkies, E. Howe, and C. Ritzenthaler. Genus bounds for curves with fixed frobenius eigenvalues.
- [26] E. Nart and C. Ritzenthaler. A new proof of Weber’s formula.
- [27] C. Ritzenthaler. *Aspects arithmétiques et algorithmiques des courbes de genre 1, 2 et 3*. Habilitation à Diriger des Recherches, Université de la Méditerranée, 2009.
- [28] C. Ritzenthaler. Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis. Thèse de doctorat de l’Université Paris VII, 2003.

## Informatique et autres

**Juil. 09.** En collaboration avec G. Lachaud et M.A. Tsfasman, édition de *Arithmetic, Geometry, Cryptography and Coding Theory*, proceedings of AGC2T-11, CIRM (centre international de rencontres mathématiques), Marseille (France), November 5-9, 2007, Contemporary Math. **487**, (2009).

**Sept. 08 -** En collaboration avec E. Howe, K. Lauter et G. van der Geer, nous élaborons un site web dédié aux courbes optimales pour remplacer et compléter les tables disponibles sur <http://www.science.uva.nl/~geer/>. Ce site est disponible à l’adresse

<http://www.manypoints.org/>

**Mai 08.** En collaboration avec R. Lercier, nous avons implémenté des algorithmes d'énumération des courbes de genre 2 sur les corps finis en MAGMA. En sous-routines, nous avons généralisé le calcul d'un modèle à partir des invariants en caractéristiques 2 et 3 et le calcul de toutes les tor- dues (pas uniquement quadratiques) en toute caractéristique. Ces programmes sont disponibles dans la version MAGMA 2.15, voir

<http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm>

## 5 Participation à des colloques et séminaires

---

### Conférences sur invitation, avec communication orale :

Oct. 2010	The higher genus sigma functions and applications, Édimbourg, Écosse.
Sep. 2010	Final GTEM conference, Barcelone, Espagne.
Mai 2010	Computational Number Theory and Arithmetic Geometry, Louvain.
Avr. 2010	Counting points : theory, algorithms and practice, Montréal.
Avr. 2010	Computer security and cryptography, Montréal.
Sep. 2009	Codes, sequences and curves, Antalya, Turquie.
Jan. 2009	Arithmetic geometry, Essen, Allemagne.
Juin 2008	C4 : Computations on Curves for Crypto and Coding, Paris.
Mar. 2008	Journées Codage et Cryptographie C2 2008, Carcans.
Dec. 2007	Cryptography and algebraic curves, Ulm, Allemagne.
Jui. 2007	Conference on global fields, Moscou, Russie.
Sep. 2005	Conférence Elliptic Curves and Cryptography, Copenhague, Danemark.
Dec. 2004	Semestre IHP ‘Méthodes explicites en Théorie des Nombres’, Paris.
Oct. 2003	Conférence “Mathematics of Discrete Logarithm”, Essen, Allemagne.
Sep. 2003	Conférence “Mathematics of Cryptology”, Leiden, Pays-Bas.

### Conférences avec communication orale :

Juin 2010	WAIFI, Istanbul, Turquie.
Mai 2009	Geocrypt, Point-à-Pître, Guadeloupe.
Avril 2009	AGCT-12, Marseille.
Mars 2009	ESF Workshop Curves, Coding Theory and Cryptography, Marseille.
Nov. 2007	AGCT-11, Marseille.
Mai. 2007	SAGA, Papetee, Polynésie Française.
Sep. 2005	Arithmetic Geometry and Coding Theory (AGCT 10), CIRM, Marseille.
Juin 2004	Algorithmic Number Theory Symposium (ANTS 6), University of Vermont, Etats-Unis.

### Séminaire avec communication orale :

Mars 2010	Séminaire de Théorie des Nombres, Orsay.
Mai 2009	Séminaire de Théorie des Nombres, Université autonome de Madrid.
Mar. 2008	Séminaire de Théorie des Nombres, Université de Bordeaux.
Mar. 2008	Séminaire de Théorie des Nombres, Université de Toulouse.
Mar. 2008	Séminaire de Théorie des Nombres, Université de Besançon.
Oct. 2007	Séminaire de Théorie des Nombres, UAM (Madrid).
Dec. 2006	Séminaire de Théorie des Nombres, Université de Toulon.
Dec. 2006	Séminaire de Théorie des Nombres, Université de Rennes.
Oct. 2006	Séminaire de Théorie des Nombres, Université de Marseille II.

Avr. 2006	Séminaire de Théorie des Nombres, Holloway university, Londres.
Jan. 2006	Séminaire de Théorie des Nombres, Université Paris VII.
Jui. 2005	Séminaire de Théorie des Nombres, Université de Berlin-Est, Allemagne.
Mars 2005	Séminaire Arithmétique et Théorie de l'Information, Luminy.
Dec. 2004	Séminaire de Cryptographie de Rennes.
Nov. 2004	Séminaire de Théorie des Nombres de l'UAB, Barcelone, Espagne.
Mars 2004	Séminaire de Théorie des Nombres de Leiden, Pays-Bas.
Dec. 2003	Séminaire de Théorie des Nombres de Lyon.
Dec. 2003	Séminaire de Théorie des Nombres de Barcelone, Espagne.
Oct. 2003	Séminaire de Théorie des Nombres de Bordeaux.
Oct. 2003	Séminaire d'Algorithmique de Bordeaux.
Juin 2003	Séminaire de Cryptographie de Caen.
Jan. 2003	Séminaire du LIX, Palaiseau.
Dec. 2002	Séminaire de Théorie des Nombres de Toulouse.

**Invitations (d'une semaine à un mois) :**

Jan. 2011	IRMAR, Rennes, par R. Lercier.
Avr. 2010	ICIMAF, la Havane, Cuba par J.E. Sarlabous.
Août 2009	Technical University of Berlin, Allemagne par F. Hess.
Mai 2009	UAM, Madrid, Espagne par E.-G. Jimenez.
Juin 2007	UAB, Barcelone, Espagne par E. Nart.
Dec. 2006	Laboratoire de cryptologie de la DGA, par R. Lercier.
Avr. 2006	Holloway university, Londres, par S. Galbraith.
Juin 2005	Université de Berlin-Est par Holzapfel.

## 6 Activités d'enseignement (sur les cinq dernières années)

---

Certains de ces enseignements sont disponibles sur le site

<http://iml.univ-mrs.fr/~ritzenth/enseignement.html>

**Sep. 2010 - Aoû. 2011.** (délégation CNRS).

**Sep. 2009 - Fev. 2010.** (96 heures annuelles -demi délégation CNRS).

1. M1 : Introduction au logiciel de calcul formel MAPLE.
2. Préparation à l'agrégation externe, option C (à U1) (80 heures).
3. Colles L1 et L2.

**Sep. 2008 - Juin. 2009.** (193 heures annuelles).

1. L1 : MAO pour le calcul matriciel.
2. M1 : cours+TD de cryptographie.
3. M1 : Introduction au logiciel de calcul formel MAPLE.
4. Préparation à l'agrégation externe, option C (à U1) (80 heures).
5. Hippocampe pour des élèves de terminale S sur le thème de la cryptographie.

**Sep. 2007 - Juin 2008.** (220 heures annuelles).

1. L1 : TD de calcul matriciel.
2. M1 : introduction à Maple.
3. M1 : cours+TD de cryptographie. J'ai rajouté certains aspects pratiques comme les attaques sur cartes bleues.
4. Agrégation externe option C (à U1) (60 heures).
5. Hippocampe (IREM). Sur le thème de la cryptographie pour des élèves de première.
6. TER mémoire de M1. J'ai supervisé un premier mémoire sur AKS et un autre sur les constructions à la règle et au compas et origami.
7. Colles L1 maths discrètes.

**Sep. 2006 - Juin 2007.** (192 heures annuelles).

1. L1 : TD de fonctions.
2. L1 : TD de mathématiques pour la biologie.
3. L2 : TD de mathématiques pour la biologie 2.
4. Agrégation externe option C (à U1) (40 heures).
5. M1 : cours+TD de cryptographie. J'ai tenu compte des difficultés des élèves sur certains points et modifié le programme. J'ai également rajouté des TP sur MAPLE pour les aider à assimiler le cours.
6. TER mémoire de M1 : AKS (test de primalité en temps polynomial).
7. Colles L2.

## 7 Activités de formation à la recherche

---

### ■ Mémoires de M2 et thèses :

**Jan.09 - Juin 09.** Encadrement du mémoire de Master 2 de Marc Munsch sur les classes d'isogénie des variétés abéliennes en dimension 3.

**Sept. 08 -.** Co-encadrement avec David Kohel de la thèse de Christophe Arène (bourse Axa). Son sujet de thèse porte sur les courbes d'Edwards et leur généralisation en genre supérieur.

**Jan 08 - Juin 08.** Encadrement du mémoire de Master 2 de Christophe Arène sur les courbes d'Edwards. Ce mémoire a débouché sur l'écriture de [1].

### ■ Cours à l'étranger et groupes de travail :

**Mai 2009.** Cours de cryptographie de M2 sur les méthodes de comptages de points pour les courbes elliptiques à l'UAM, Madrid (invitation d'E.-G. Jimenez).

**Sept. 08 -.** Co-animation du groupe de travail pour les doctorants de l'équipe ATI, Marseille.

**Septembre 2005.** Sur l'invitation de T. Lange, j'ai effectué un cours introductif sur les méthodes  $p$ -adiques en cryptographie durant la semaine précédant la conférence E.C.C. à Copenhague.

**Janvier 2005.** Sur l'invitation de V. Rotger, j'ai effectué un cours de 20 heures à l'Universitat Politècnica de Barcelone. Ce cours (98 pages) constitue une introduction aux courbes sur les corps finis pour des étudiants en MASTER et comporte quatre parties : fonctions zêta (conjectures de Weil, théorie d'Honda-Tate),  $p$ -rang et applications ; automorphismes ; courbes maximales ; cryptographie. Il était accompagné de TD sur le logiciel MAGMA pour illustrer les différentes notions.

### ■ Organisation de conférences :

**Juin 2011.** Co-organisateur de la conférence Geocrypt-2 à Furiani du 20 au 24 juin.

**Mar. 2011.** Co-organisateur de la conférence AGCT-13 au CIRM du 14 au 18 mars.

**Mai 2009.** Co-organisateur de la conférence Geocrypt, Guadeloupe.

**Mars 2009.** Co-organisateur du workshop ESF curves, coding theory and cryptography à Marseille du 26 au 28 mars.

**Nov. 2007.** Co-organisateur de la conférence AGC2T-11 au CIRM du 5 au 9 novembre.

## 8 Activités annexes

---

**Mai 2011** Rapporteur pour la thèse de Vijaykumar Singh sous la direction de Gary McGuire.

**Déc. 2010** Rapporteur pour la thèse de Luca De Feo sous la direction de François Morain.

**Août 2010** Membre du comité scientifique de Parings 2010 à Yamanaka Hot Spring, Japon du 13 au 15 décembre.

**2008 -.** Membre de la commission de la bibliothèque du CIRM.

**2008 -.** Membre de la commission de sélection de mathématiques de Luminy.

**2008 -.** Je suis co-responsable du L3 BIM (biologie-informatique-mathématiques). Pour plus de renseignements sur cette filière

<http://www.luminy.univ-mrs.fr/enseignement/enseignement.htm>

**Nov. 2008.** Membre du jury de thèse de Magali Rocher soutenue à Bordeaux I sous la direction de M. Matignon.

## 9 Participations à des réseaux et projets

---

**Jan. 2010.** Membre du projet CHIC (Courbes Hyperelliptiques Isogénies et Comptage) de l'ANR. Voir

[http://chic.gforge.inria.fr/index\\_fr.html](http://chic.gforge.inria.fr/index_fr.html)

**Jan. 2009 -.** Membre du partenariat bilatéral Marseille-Berlin du projet procope d'Egide.

**Sep. 2009 -.** Membre du projet MTM2006-11391 de la MEC (Espagne) avec l'université UAB de Barcelone.

## 10 Travaux et projet de recherche

**Mots-clés.** courbe de bas genre, quartique plane, courbe optimale, classe d'isogénie, jacobienne, obstruction de Serre, invariant, forme modulaire de Siegel, espace des modules, théorème de Torelli explicite.

Les citations [1],[2],[3],... , sont des références aux articles, pré-publications et travaux en cours dont je suis (co)-auteur (voir pages 4 et 5).

### Travaux

Mes recherches s'articulent principalement autour de questions arithmétiques et algorithmiques sur les courbes de genre 1, 2 et 3 : nombre maximal de points sur les corps finis, invariants, reconstruction à partir de la jacobienne,...Mes publications sont diverses et je ne retiendrai dans cette présentation que deux résultats. On pourra consulter pour plus de détails sur ces sujets et sur mes autres publications récentes mon habilitation (soutenue en décembre 2009), à l'adresse :

<http://iml.univ-mrs.fr/~ritzenth/research/HDR-main.pdf>

En genre 2, dans [10] puis [9], nous avons caractérisé les classes d'isogénie de surfaces abéliennes sur un corps fini qui contiennent la jacobienne d'une courbe en termes de leur polynôme de Weil. Ceci parachève en genre 2 de nombreux travaux sur le sujet, initiés par J.-P. Serre en 85 avec une formule pour le nombre maximal de points d'une courbe de genre 2 sur un corps fini (voir l'historique du chapitre 3 de [27]).

Lorsqu'on cherche à réaliser le même projet en genre 3 (ou ne serait-ce que le calcul du nombre maximal de points), on se heurte à un nouvel obstacle, que nous avons nommé *obstruction de Serre en genre 3*. Serre a en effet observé qu'une variété abélienne principalement polarisée  $(A, a)$  sur un corps  $k$  qui est une jacobienne sur  $\bar{k}$  n'est pas nécessairement une jacobienne sur le corps  $k$ . Lorsque cette jacobienne est non hyperelliptique, il peut exister une obstruction. Dans une lettre à J. Top, Serre avait suggéré une piste pour la calculer basée sur l'étude de la forme modulaire de Siegel  $\chi_{18}$  sur l'espace des modules des variétés abéliennes de dimension 3 (en fait, plus précisément, sur le champ). Dans [21], [5],[6] (voir également le chapitre 4 de [27]) nous démontrons les assertions de Serre et illustrons cette méthode avec le calcul de l'obstruction dans le cas le plus intéressant pour les applications, c.-à-d.  $A = E^3$  avec  $E$  une courbe elliptique CM. Nous pouvons ainsi donner de nouvelles valeurs pour le nombre maximal de points d'une courbe de genre 3.

Ces deux travaux ont permis de re-dynamiser l'étude des courbes maximales et ont établi des connexions prometteuses entre ce domaine et celui des formes modulaires. Le site web

<http://www.manypoints.org/>

que nous avons élaboré en collaboration avec E. Howe, K. Lauter et G. van der Geer pour remplacer et compléter les tables disponibles sur <http://www.science.uva.nl/~geer/> permettra de rendre visibles les avancées de la communauté sur ces questions.

## Projet de recherche

Je ne donne ici qu'un résumé de mon programme de recherche. Celui-ci est détaillé dans mon habilitation [27] aux sections 2.5, 4.5 et 5.4.3.

Les avancées sur le calcul de l'obstruction de Serre sont encore loin de fournir une formule pour le nombre maximal de points d'une courbe de genre 3 sur un corps fini comme en genre 2. Une approche globale du problème des courbes optimales est encore hors d'atteinte et nécessite des études fines sur les réductions (singulières, hyperelliptiques, non hyperelliptiques) d'une variété abélienne principalement polarisée  $(E^3, a)$ , avec  $E$  une courbe elliptique, définie sur un corps de nombres. En parallèle, avec l'aide d'A. Beauville, j'explore une approche personnelle et basée sur des constructions géométriques utilisant des courbes de genre 4 et 5 [4].

Le second volet est un travail algorithmique, également entamé ([20],[14],[12],[26]). Il s'agit de généraliser au genre 3, les constructions connues en genre 1 et 2 : reconstruction d'une courbe d'invariants donnés et calcul de tordues (avec R. Lercier), calcul des Thetanullwerte à partir de la courbe et inversement. Parmi les applications possibles, citons la construction de courbes de genre 3 à multiplication complexe, afin de compléter les tables de D. Kohel. Ces applications s'inscrivent dans le cadre de l'ANR CHIC dont je fais partie. Mon étudiant, C. Arène, travaille quant à lui sur la notion de loi de groupe arithmétiquement complète, une généralisation en genre supérieur de la loi de groupe sur les courbes d'Edwards.

En plus de ces travaux en bas genre, j'espère pouvoir prolonger mes résultats récents sur certaines propriétés en tout genre : existence de diviseurs non spéciaux rationnels [3] et jacobiniennes totalement décomposées à isogénie près [25].