CURVES OVER FINITE FIELDS: PAST, PRESENT AND FUTURE

Alp Bassa, Elisa Lorenzo García & Christophe Ritzenthaler (eds.)

Panoramas et Synthèses

Numéro 60 2023

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
`christian.smf@cirm-math.fr`

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 43 € ($ 65)

Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat

Panoramas et Synthèses
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
`panoramas@smf.emath.fr` • `http://smf.emath.fr/`

ISSN 1272-3835

ISBN 978-2-85629-980-7

Directeur de la publication : Fabien Durand

PANORAMAS ET SYNTHÈSES 60

CURVES OVER FINITE FIELDS : PAST, PRESENT AND FUTURE

Alp Bassa, Elisa Lorenzo García
& Christophe Ritzenthaler (eds.)

Société mathématique de France

***Classification mathématique par sujets.* (2010) —** 11G20, 14G15, 14G05, 14H05, 14H25, 14H10, 14H37, 11G10, 11T71.

***Keywords and phrases.* —** Curves over finite fields, maximal curves, rational points, abelian varieties, Weil polynomial, isogeny classes, automorphisms, function fields, coding theory, moduli spaces, towers of curves, recursive towers, Ihara constant, arithmetic statistics.

***Mots-clés et phrases.* —** Courbes sur les corps finis, courbes maximales, points rationnels, variétés abéliennes, polynôme de Weil, classes d'isogénie, automorphismes, corps de fonctions, théorie des codes, espaces de modules, tours de courbes, tours récursives, constante d'Ihara, statistiques arithmétiques.

CURVES OVER FINITE FIELDS: PAST, PRESENT AND FUTURE

Alp Bassa, Elisa Lorenzo García & Christophe Ritzenthaler (eds.)

***Abstract.* —** The present proceedings rely on the plenary lectures that were given during the online conference "Curves over finite fields: past, present and future" in May 2021. Each lecturer was asked to do a survey on a particular aspect of this research area and to point out some compelling open questions. The six lectures gathered here show the richness and diversity of the results in the domain: isogeny classes of abelian varieties, large automorphism groups, recursive towers, error-correcting codes, moduli spaces, arithmetic statistics are so many gates to this vivid area of research.

***Résumé.* (Courbes sur les corps finis : passé, présent et avenir) —** Ces comptes rendus sont constitués des exposés pléniers donnés pendant la conférence en ligne « Curves over finite fields : past, present and future » en mai 2021. Chaque conférencier et conférencière a réalisé un état des lieux sur un aspect particulier de ce sujet de recherche et a fait ressortir certaines questions ouvertes fascinantes. Les six exposés rassemblés ici montrent la richesse et la diversité des résultats du domaine : classes d'isogénie des variétés abéliennes, large groupe d'automorphismes, tours récursives, codes correcteurs d'erreurs, espaces de modules, statistiques arithmétiques sont autant de portes d'entrée dans ce champ de recherche très actif.

TABLE OF CONTENTS

RÉSUMÉS DES ARTICLES

Ayant fixé une classe d'isogénie de variétés abéliennes sur un corps fini, on s'intéresse à des méthodes exploitant son polynôme de Weil afin de déterminer les propriétés des courbes (s'il y en a) dont les Jacobiennes appartiennent à ladite classe d'isogénie. Certaines méthodes sont suffisamment puissantes pour montrer qu'il n'y a pas de courbes ayant un polynôme de Weil donné, alors que d'autres permettent parfois de montrer qu'une courbe avec un polynôme de Weil donné doit posséder des automorphismes non triviaux, ou doit être munie d'une application de degré et de trace connus vers une courbe elliptique. De telles propriétés peuvent parfois fournir des méthodes efficaces pour trouver des courbes ayant un polynôme de Weil fixé.

Les techniques que nous décrivons dans cet article sont pour la plupart inspirées de méthodes utilisées par Serre dans son cours à Harvard de 1985 sur les points rationnels sur les courbes sur les corps finis. La publication récente des notes de ce cours fournit une bonne motivation pour survoler les développements dans le domaine survenus depuis.

Une courbe algébrique (projective, lisse, absolument irréductible) de genre $\mathfrak{g}$ définie sur un corps fini $\mathbb{F}_{q^2}$ d'ordre q^2 est *maximale* si son nombre de points $\mathbb{F}_{q^2}$-rationnels atteint la borne supérieure d'Hasse-Weil, c'est-à-dire s'il est égal à $q^2+1+2\mathfrak{g}q$. Le début d'une étude systématique des courbes maximales (et plus généralement de courbes avec beaucoup de points sur $\mathbb{F}_{q^2}$) a été marqué par une série de séminaires et de leçons par J-P. Serre en 1982/83, voir **[131]**, et en 1985, voir **[132]**. Depuis, les questions principales sur les courbes maximales sur un corps $\mathbb{F}_{q^2}$ donné ont concerné la description du spectre de leurs genres, la classification des courbes maximales avec un genre fixé, la détermination déquations explicites et les applications en théorie des codes. Les résultats des années

suivantes ont fait l'objet des cours de A. Garcìa [**53,52**], G. van der Geer [**67,66**] et J.W.P. Hirschfeld [**86**], et ont été traités en détail dans des monographies et des chapitres de livres [**57,87,89,107,119,122,152,153,151,154**]. Au cours de la dernière décennie, il y a eu un regain d'intérêt pour les courbes maximales et les recherches ont également porté sur les courbes maximales qui n'admettent pas de revêtement par la courbe hermitienne, les courbes maximales munies d'un revêtement galoisien par la courbe hermitienne, ainsi que les semi-groupes de Weierstrass et le groupe d'automorphismes d'une courbe maximale. Notre article vise à présenter ces développements d'un point de vue géométrique.

Depuis que Serre a donné ses célèbres conférences de Harvard en 1985 sur divers aspects de la théorie des courbes algébriques définies sur un corps fini, il y a eu de nombreux développements. Dans cet article, un aperçu sera donné sur ceux concernant la quantité $A(q)$, connue sous le nom de constante d'Ihara. L'accent sera mis sur les techniques explicites et en particulier sur les tours de corps de fonctions définies récursivement sur un corps fini, qui ont donné de bonnes bornes inférieures pour la constante d'Ihara dans le passé.

Cette note complete un exposé donné à la conférence *Curves over finite fields, past, present and future* organisée en l'honneur de la publication du livre *Rational points of curves over finite fields* de J-P. Serre et organisée au *Centro de ciencias de Benasque* en juin 2021. L'article présente une l'histoire des codes géométriques ainsi que des applications modernes de ces derniers. On se focalise en particulier sur la structure « multiplicative » de ces codes, autrement dit leur comportement vis-à-vis du produit termes à termes. Quelques problèmes ouverts sont discutés.

Cet article traite de certains aspects des espaces de modules de courbes algébriques sur un corps fini. Nous y discutons le comptage de points sur de tels espaces. Les formules pour le nombre de points sur ces espaces de modules nous conduisent vers des formes modulaires. De cette façon, le comptage des courbes et de leurs points sur les corps finis offre une manière d'obtenir des informations sur les traces des opérateurs de Hecke sur certains espaces de formes modulaires. Nous discutons également certaines stratifications des espaces de modules des courbes et de leur pertinence pour les courbes sur les corps finis.