Séminaires & Congrès

COLLECTION SMF

ARITHMETICS, GEOMETRY, AND CODING THEORY (AGCT 2005)

Numéro 21

François Rodier, Serge Vladut, eds.

SOCIÉTE MATHÉMATIQUE DE FRANCE

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
smf@smf.univ-mrs.fr

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

Tarifs 2010

Vente au numéro : 40 € ($ 60)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Nathalie Christiaën

Séminaires et Congrès
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
revues@smf.ens.fr • http://smf.emath.fr/

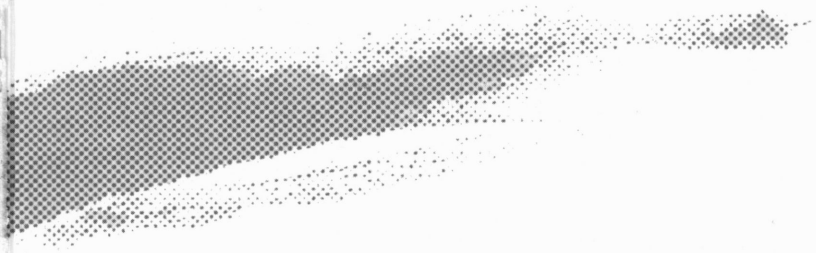
ISSN 1285-2783

ISBN 978-2-85629-279-2

Directeur de la publication : Stéphane JAFFARD

Séminaires & Congrès

COLLECTION SMF



ARITHMETICS, GEOMETRY, AND CODING THEORY (AGCT 2005)

Numéro 21

François Rodier, Serge Vladut, eds.

SOCIÉTE MATHÉMATIQUE DE FRANCE

François Rodier

Institut de Mathématiques de Luminy
Université Aix-Marseille II
Case Postale 907
163, Av. de Luminy
13288 Marseille cedex 9
France
rodier@iml.univ-mrs.fr

Serge Vladut

Institut de Mathématiques de Luminy
Université Aix-Marseille II
Case Postale 907
163, Av. de Luminy
13288 Marseille cedex 9
France
vladut@iml.univ-mrs.fr

Classification mathématique par sujets. — 11E10, 11F41, 11G**, 11R37, 11R42, 11T71, 14C22, 14F30,14G05,14G15,14G50,14H25, 14H40, 14H45, 14M15,14Q05, 15A63, 15A66, 84B27, 94B10 ; 05E15, 11H99, 11R47, 11R58, 14F40, 14G** , 14J20, 14K05, 94B05, 94B27, 94B65

Mots-clefs. — Addition de diviseurs, algorithmes de réduction, anneaux d'endomorphismes, arithmétique des corps globaux, borne de Gilbert Varshamov, borne de Hasse-Weil, codes algébriques géométriques, codes convolutionels, codes correcteur d'erreurs, codes de Grassmann, codes géometrique, cohomologie de de Rham, cohomologie p-adique, corps cyclotomique, corps totalement réel, courbes, courbes sur les corps finis, courbe hermitienne, courbe maximale, cycles de Schubert, complexité bilinéaire, corps de fonctions algébrique, corps fini, courbes C_{ab}, courbes de genre 2, descente des corps de fonctions, endomorphismes de variétés abéliennes, espace invariant, fibrés projectifs, fibrés vectoriels stables, fonctions zêta, forme modulaire de Hilbert, forme modulaire de Jacobi, groupe de Clifford-Weil, intersections dans l'espace projectif, Jacobiennes, Jacobiennes hyperelliptiques, multiplication complexe, nombre de Picard, polynômes de classe d'Igusa, rang d'un tenseur, représentations de Steinberg, revêtement non-ramifiés, surfaces, surfaces sur les corps finis, théorème chinois, théorie des codes, Variétés de Schubert.

ARITHMETICS, GEOMETRY, AND CODING THEORY

edited by François Rodier and Serge Vladut

Abstract. — The conference *Arithmetics, Geometry, and coding Theory* was held in Marseilles, in the International Center of Mathematical Meetings of Luminy (CIRM) from the 26 to 30 of September, 2005. Its topic was the interaction between number theory and algebraic geometry on the one hand, coding theory and cryptography on the other hand.

It dealt with such subjects as curves covered by the Hermitian curve, towers of function fields, bilinear complexity of the multiplication in the finite fields, codes on various varieties, estimate of the Picard number of surfaces via p-adic cohomology, minimal distance of codes on a surface, Euler-Kronecker constant on global fields.

Public key cryptography was an opportunity for talks on curves and their jacobians : jacobians of C_{ab} curves, a CRT algorithm to construct genus 2 curves over finite fields, hyperelliptic jacobians and the Steinberg representations.

Others talks are devoted to the relations between the enumerator polynomial of codes and modular forms and to a similar construction with construction A of lattices from binary codes to build convolutional codes starting from block codes.

***Résumé* (Arithmétique, Géométrie, et Théorie des codes).** — Le colloque *Arithmétique, Géométrie, et Théorie des codes* s'est tenu à Marseille, au Centre International de Rencontres Mathématiques de Luminy du 26 au 30 septembre 2005. Son thème était l'interaction entre la théorie des nombres et la géométrie algébrique d'une part, la théorie du codage et la cryptographie d'autre part.

Les sujets abordés sont les courbes admettant comme revêtement la courbe hermitienne, les tours de corps appliquées à la complexité bilinéaire de la multiplication dans les corps finis, les codes sur des variétés diverses, l'estimation du nombre de Picard des surfaces par la cohomologie p-adique, l'étude de la distance minimale des codes sur les surfaces, la constante d'Euler-Kronecker sur des corps globaux.

La cryptographie à clé publique a donné lieu à des exposés sur les courbes et leur jacobiennes : jacobiennes des courbes C_{ab}, un algorithme fondé sur le théorème chinois pour construire des courbes de genre 2 sur des corps finis, les jacobiennes hyperelliptiques et les représentations de Steinberg.