Lercier, Reynald; **Lubicz, David**

A quasi quadratic time algorithm for hyperelliptic curve point counting. (English)

Zbl 1166.11021
Ramanujan J. 12, No. 3, 399-423 (2006).

Summary: We describe an algorithm to compute the cardinality of Jacobians of ordinary hyperelliptic curves of small genus over finite fields $\mathcal{F}_{2^n}$ with cost $O(n^{2+o(1)})$. This algorithm is derived from ideas due to Mestre. More precisely, we state the mathematical background behind Mestre's algorithm and develop from it a variant with quasi-quadratic time complexity. Among others, we present an algorithm to find roots of a system of generalized Artin-Schreier equations and give results that we obtain with an efficient implementation. Especially, we were able to obtain the cardinality of curves of genus one, two or three in finite fields of huge size.

MSC:

11G20 Curves over finite and local fields
11S40 Zeta functions and L-functions
14G50 Applications to coding theory and cryptography of arithmetic geometry

Keywords:

Point counting algorithms; Finite fields; Cryptography; Hyperelliptic curves; AGM

Software:

gmp; Magma; ZEN

Full Text: DOI

References:

[1] Bosma, W., Cannon, J., Playoust, C.: The Magma Algebra System I: The User Language. J. Symbolic Comp. 24(3), 235–265 (1997) · Zbl 0898.68039 · doi:10.1006/jsco.1996.0125

[2] Cantor, D.G.: Computing in the Jacobian of a hyperelliptic curve. Math. Comp. 48(177), 95–101 (1987) · Zbl 0613.14022 · doi:10.1090/S0025-5718-1987-0866101-0

[3] Carls, R.: Generalized AGM sequences and approximation of canonical lifts (2003). Available at http://www.math.leidenuniv.nl/\(\sim\)carls

[4] Chabaud, F., Lercier, R.: ZEN, User Manual (1996)

[5] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptology 10(4), 233–260 (1997) · Zbl 0912.11056 · doi:10.1007/s001459900030

[6] Denef, J., Vercauteren F.: An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In: Fieker C. Kohel D.R. (eds.) Algorithmic Number Theory, 5th International Symposium, ANTS-V, pp 369-384. Springer (2002) · Zbl 1058.11040

[7] Fay, J.D.: Theta functions on Riemann surfaces. Lecture Notes in Mathematics, vol. 352. Springer-Verlag, Berlin (1973) · Zbl 0281.30013

[8] Gaudry, P.: Algorithmique des courbes hyperelliptiques et applications à la cryptologie. PhD thesis, École Polytechnique (2000)

[9] Gaudry, P.: Cardinality of a genus 2 hyperelliptic curve over GF(5é1024+41). Email at the Number Theory List, (September, 2002)

[10] Free Software Foundation GNU. GMP library (2002). Available at http://www.swox.com/gmp/

[11] Griffiths, P., Harris, J.: Principles of algebraic geometry. Wiley Classics Library. Reprint of the 1978 original. John Wiley \& Sons Inc., New York (1994)

[12] Harley, R.: Asymptotically optimal p-adic point-counting. E-mail to the NMBRTHRY mailing list (December 2002)

[13] Kedlaya, K.S.: Counting points on hyperelliptic curves using Monsky Washnitzer cohomology. J. Ramanujan Math. Soc. 16, 323–328 (2001) · Zbl 1066.14024

[14] Kim, H.Y., Park, J.Y., Cheon, J.H., Park, J.H., Kim, J.H., Hahn. S.G.: Fast Elliptic Curve Point Counting Using Gaussian Normal Basis. In: Fieker C., Kohel D.R. (eds.) Algorithmic Number Theory, 5th International Symposium, ANTS-V, pp.

292–307. Springer Verlag, Berlin (2002) · Zbl 1058.11075

[15] Koblitz, N.: Hyperelliptic cryptosystems. J. Cryptology 1(3), 139–150 (1989) · Zbl 0674.94010 · doi:10.1007/BF02252872

[16] Lang, S.: Algebra. 3rd revised ed. Graduate Texts in Mathematics. 211. Springer, New York, NY (2002)

[17] Lauder, A.G.B., Wan, D.: Computing Zeta functions of Artin-Schreier curves over finite fields. LMS J. Comput. Math. 5, 34–55 (electronic) (2002) · Zbl 1067.11078

[18] Lenstra, A.K., Lenstra, H.W., Jr., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. 261, 513–534 (1982) · Zbl 0488.12001 · doi:10.1007/BF01457454

[19] Lercier, R., Lubicz, D.: Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In: Biham E (ed.) Advances in CryptologyÑEUROCRYPT 2003, Lecture Notes in Computer Science. Springer-Verlag (2003) · Zbl 1035.11067

[20] Lubin, J., Serre, J.-P., Tate, J.: Elliptic curves and formal groups. Available at http://ma.utexas.edu/users/voloch/lst.html (1964)

[21] Menezes, A.J., Blake, I.F., Gao, X., Mullin, R.C., Vanstone, S.A., Yaghoobian, T.: xi, 218, Applications of finite fields. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, Boston, p. (1993) · Zbl 0779.11059

[22] Mestre, J.-F.: Lettre à Gaudry et Harley (2001). Available at http://www.math.jussieu.fr/\(\sim\)mestre

[23] Mestre, J.-F.: Notes of a talk given at the seminar of cryptography of Rennes (2002). Available at http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps

[24] Mumford, D.: On the equations defining abelian varieties. I. Invent. Math. 1, 287–354 (1966) · Zbl 0219.14024 · doi:10.1007/BF01389737

[25] Mumford, D.: On the equations defining abelian varieties. II. Invent. Math. 3, 75–135 (1967) · doi:10.1007/BF01389741

[26] Mumford, D.: Tata lectures on theta I, volume 28 of Progress in Mathematics. Birkhäuser Boston Inc., Boston, MA (1983). With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman · Zbl 0509.14049

[27] Mumford, D.: Tata lectures on theta II, volume 43 of Progress in Mathematics. Birkhäuser Boston Inc., Boston, MA (1984). Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura · Zbl 0549.14014

[28] Neukirch, J.: Algebraic number theory, volume 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin (1999)

[29] Pila, J.: Frobenius maps of abelian varieties and finding roots of unity in finite fields. Math. Comp. 55(192), 745-763 (1990) · Zbl 0724.11070 · doi:10.1090/S0025-5718-1990-1035941-X

[30] Ritzenthaler, C.: Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis. PhD thesis, Université Paris 7-Denis Diderot (2003)

[31] Satoh, T.: The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J. Ramanujan Math. Soc. 15(4), 247–270 (2000) · Zbl 1009.11051

[32] Satoh, T., Skjernaa, B., Taguchi, Y.: Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields and Their Applications 9(1), 89–101 (2003) · Zbl 1106.14302 · doi:10.1016/S1071-5797(02)00013-8

[33] Schoof, R.: Counting points on elliptic curves over finite fields. J. Théorie des nombres de Bordeaux 7, 483–494 (1998) · Zbl 0579.14025

[34] Serre, J.-P.: Géométrie algébrique et géométrie analytique. Ann. Inst. Fourier, Grenoble 6, 1–42 (1955–1956)

[35] Shimura, G.: Abelian Varieties with Complex Multiplication and Modular Functions. Princ. Univ. Press, NJ (1998) · Zbl 0908.11023

[36] Silverman, J.H.: The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Corrected reprint of the 1986 original. Springer-Verlag, New York (1986)

[37] Tate, J.: Endomorphisms of abelian varieties over finite fields. Invent. Math. 2, 134–144 (1966) · Zbl 0147.20303 · doi:10.1007/BF01404549

[38] Vercauteren, F.: Computing zeta functions of curves over finite fields. PhD thesis, Katholieke Universiteit Leuven (2003). Preprint · Zbl 1023.14007