Bauer, Mark L.

The arithmetic of certain cubic function fields. (English) Zbl 1053.11087

Math. Comput. 73, No. 245, 387-413 (2004).

Summary: We discuss the properties of curves of the form $y^3 = f(x)$ over a given field K of characteristic different from 3. If $f(x)$ satisfies certain properties, then the Jacobian of such a curve is isomorphic to the ideal class group of the maximal order in the corresponding function field. We seek to make this connection concrete and then use it to develop an explicit arithmetic for the Jacobian of such curves. From a purely mathematical perspective, this provides explicit and efficient techniques for performing arithmetic in certain ideal class groups which are of fundamental interest in algebraic number theory. At the same time, it provides another source of groups which are suitable for Diffie-Hellman type protocols in cryptographic applications.

MSC:

11R58 Arithmetic theory of algebraic function fields
94A60 Cryptography
14H05 Algebraic functions and function fields in algebraic geometry
11Y40 Algebraic number theory computations

Full Text: DOI

References:

[1] David G. Cantor, Computing in the Jacobian of a hyperelliptic curve, Math. Comp. 48 (1987), no. 177, 95 – 101. · Zbl 0613.14022 ·

[2] S. D. Galbraith, S. M. Paulus, and N. P. Smart, Arithmetic on superelliptic curves, Math. Comp. 71 (2002), no. 237, 393 – 405. · Zbl 1013.11026 ·

[3] Robin Hartshorne, Algebraic geometry, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. · Zbl 0367.14001

[4] A. K. Lenstra, Factoring multivariate polynomials over finite fields, J. Comput. System Sci. 30 (1985), no. 2, 235 – 248. · Zbl 0577.12013 · doi:10.1016/0022-0000(85)90016-9 · doi.org

[5] Renate Scheidler, Ideal arithmetic and infrastructure in purely cubic function fields, J. Théor. Nombres Bordeaux 13 (2001), no. 2, 609 – 631 (English, with English and French summaries). · Zbl 0995.11064

[6] Renate Scheidler and Andreas Stein, Unit computation in purely cubic function fields of unit rank 1, Algorithmic number theory (Portland, OR, 1998) Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 592 – 606. · Zbl 0935.11051 · doi:10.1007/BFb0054895 · doi.org

[7] Henning Stichtenoth, Algebraic function fields and codes, Universitext, Springer-Verlag, Berlin, 1993. · Zbl 0816.14011