MATHEMATICS OF COMPUTATION
Volume 73, Number 248, Page 2109
S 0025-5718(04)01691-6
Article electronically published on May 17, 2004

ADDENDUM TO "FACTORING POLYNOMIALS OVER FINITE FIELDS WITH DRINFELD MODULES"

G. J. VAN DER HEIDEN

After my paper [2] was electronically published by Mathematics of Computation, I came across the PhD thesis of professor I. Y. Potemine [6].

In Section 4.3 of his thesis, an algorithm for factoring polynomials is proposed which is equivalent to the algorithm discussed in my paper. Potemine's algorithm is acknowledged in my PhD thesis [1].

Our algorithms were found independently, both as analogues of H. W. Lenstra's well-known Elliptic Curve Method for factoring integers; cf. [3].

Professor Potemine informed me that there are two even earlier publications in which his algorithm is described; namely [5] and [4]. Nevertheless, a complexity analysis and a comparison with the well-known Cantor–Zassenhaus algorithm can only be found in [2] and [1].

References

[1] G. J. van der Heiden, *Weil Pairing and the Drinfeld Modular Curve*, PhD thesis, University of Groningen, 2003.

[2] ———, Factoring polynomials over finite fields with Drinfeld modules, *Math. Comp.*, **73**:317–322, 2004.

[3] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Ann. of Math.* (2), 126(3):649–673, 1987. MR 89g:11125

[4] A. Panchishkin, Algorithmes rapides pour factorisation des nombres et des polynômes, test de primalité, courbes elliptiques et modules de Drinfeld, *Séminaire de Théorie des Nombres*, Université de Caen, Fascicule de l'année 1992–1993, pp. 1–7, 1993.

[5] A. Panchishkin and I. Potemine, An algorithm for the factorization of polynomials using elliptic modules, In *Proceedings of the Conference "Constructive methods and algorithms in number theory"*, p. 117. Mathematical Institute of AN BSSR, Minsk, 1989 (Russian).

[6] I. Y. Potemine, *Arithmétique des corps globaux de fonctions et géométrie des schémas modulaires de Drinfeld*, PhD thesis, l'Université Joseph Fourier, Grenoble, 1997.

Department of Philosophy, University of Nijmegen, P.O. Box 9103, 6500 HD Nijmegen, The Netherlands

E-mail address: g.vdheiden@phil.kun.nl

Received by the editor December 13, 2003.

2000 *Mathematics Subject Classification.* Primary 11G09, 13P05.