The following full text is a publisher’s version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/60038

Please be advised that this information was generated on 2016-01-15 and may be subject to change.
ADDENDUM TO
“FACTORIZING POLYNOMIALS OVER FINITE FIELDS
WITH DRINFELD MODULES”

G. J. VAN DER HEIDEN


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

DEPARTMENT OF PHILOSOPHY, UNIVERSITY OF Nijmegen, P.O. BOX 9103, 6500 HD Nijmegen, THE NETHERLANDS

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

Received by the editor December 13, 2003.
2000 Mathematics Subject Classification. Primary 11G09, 13P05.

©2004 American Mathematical Society