Journal of Symbolic Computation 66 (2015) 111–112

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Corrigendum to "A long note on Mulders' short product" [J. Symb. Comput. 37 (3) (2004) 391–401]

G. Hanrot [a], P. Zimmermann [b]

[a] CNRS, ENS de Lyon, Inria, UCBL, Université de Lyon; Laboratoire LIP, 46 allée d'Italie, F-69364 Lyon cedex 07, France
[b] Centre de recherche Inria Nancy – Grand Est, Équipe-projet CARAMEL – bâtiment A, 615 rue du jardin botanique, F-54600 Villers-lès-Nancy, France

ARTICLE INFO

Article history:
Received 17 February 2014
Accepted 17 February 2014
Available online 17 March 2014

Keywords:
Mulders' algorithm
Karatsuba model

ABSTRACT

We correct a minor mistake in the paper of Hanrot and Zimmermann (2004).

In Algorithm ShortProduct (Hanrot and Zimmermann, 2004, pp. 394–395), at the final step, read

$$\textbf{return } \left(\ell\left(x^2\right) + xm\left(x^2\right) + x^2h\left(x^2\right)\right) \bmod x^n.$$

In the printed version, the result might have degree n: if n is odd from the term $xm(x^2)$, or if n is even from $x^2h(x^2)$.

The proof of Theorem 2 actually only proves that the result of Algorithm ShortProduct is congruent to fg modulo x^n, not that it has degree $< n$. With the correction above, this is obvious. Note that it does not change the number of ring operations as it is merely a truncation step.

DOI of original article: http://dx.doi.org/10.1016/j.jsc.2003.03.001.
E-mail addresses: guillaume.hanrot@ens-lyon.fr (G. Hanrot), paul.zimmermann@inria.fr (P. Zimmermann).
URLs: http://perso.ens-lyon.fr/guillaume.hanrot (G. Hanrot), http://www.loria.fr/~zimmerma (P. Zimmermann).

http://dx.doi.org/10.1016/j.jsc.2014.02.002
0747-7171/

Acknowledgements

The authors would like to thank Bill Allombert and Karim Belabas for pointing this mistake.

References

Hanrot, G., Zimmermann, P., 2004. A long note on Mulders' short product. J. Symb. Comput. 37, 391–401.