Journal de Théorie des Nombres
de Bordeaux **14** (2002), 151–169

A fast algorithm for polynomial factorization over $\mathbb{Q}_p$

par David FORD*, Sebastian PAULI†
et Xavier-François ROBLOT*

Résumé. Dans cet article, nous présentons un algorithme qui retourne pour un polynôme $\Phi(x)$ à coefficients dans l'anneau $\mathbb{Z}_p$ des entiers p-adiques, soit un facteur propre de ce polynôme, soit, dans le cas où $\Phi(x)$ est irréductible, un élément générateur de l'anneau des entiers de $\mathbb{Q}_p[x]/\Phi(x)\mathbb{Q}_p[x]$. Cet algorithme se fonde sur l'algorithme Round Four pour le calcul de l'ordre maximal. Les expérimentations montrent que le nouvel algorithme est cependant beaucoup plus performant que l'algorithme Round Four.

Abstract. We present an algorithm that returns a proper factor of a polynomial $\Phi(x)$ over the p-adic integers $\mathbb{Z}_p$ (if $\Phi(x)$ is reducible over $\mathbb{Q}_p$) or returns a power basis of the ring of integers of $\mathbb{Q}_p[x]/\Phi(x)\mathbb{Q}_p[x]$ (if $\Phi(x)$ is irreducible over $\mathbb{Q}_p$). Our algorithm is based on the Round Four maximal order algorithm. Experimental results show that the new algorithm is considerably faster than the Round Four algorithm.

David Ford, Sebastian Pauli
Centre Interuniversitaire en Calcul Mathématique Algébrique
Department of Computer Science
Concordia University
Montréal, Québec
E-mail : `ford@cs.concordia.ca, pauli@mathstat.concordia.ca`

Xavier-François Roblot
Institut Girard Desargues
Université Claude Bernard (Lyon I)
43, boulevard du 11 Novembre 1918
69622 VILLEURBANNE cedex, France
E-mail : `roblot@desargues.univ-lyon1.fr`

Manuscrit reçu le 5 avril 2001.
*supported in part by NSERC (Canada) and FCAR/CICMA (Québec).
†supported in part by ISM and FCAR/CICMA (Québec).