Journal de Théorie des Nombres
de Bordeaux **17** (2005), 721–725

Sharper ABC-based bounds for congruent polynomials

par Daniel J. BERNSTEIN

Résumé. Agrawal, Kayal, et Saxena ont récemment introduit une nouvelle méthode pour montrer qu'un entier est premier. La vitesse de cette méthode dépend des minorations prouvées pour la taille du semi-groupe multiplicatif engendré par plusieurs polynômes modulo un autre polynôme h. Voloch a trouvé une application du théoreme ABC de Stothers et Mason dans ce contexte: sous de petites hypothèses, des polynômes distincts A, B, C de degré au plus $1.2 \deg h - 0.2 \deg \operatorname{rad} ABC$ ne peuvent pas être tous congrus modulo h. Nous présentons deux améliorations de la partie combinatoire de l'argument de Voloch. La première amélioration augmente $1.2 \deg h - 0.2 \deg \operatorname{rad} ABC$ en $2 \deg h - \deg \operatorname{rad} ABC$. La deuxième amélioration est une généralisation à $A_1, \ldots, A_m$ de degré au plus $((3m-5)/(3m-7)) \deg h - (6/(3m-7)m) \deg \operatorname{rad} A_1 \cdots A_m$, avec $m \geq 3$.

Abstract. Agrawal, Kayal, and Saxena recently introduced a new method of proving that an integer is prime. The speed of the Agrawal-Kayal-Saxena method depends on proven lower bounds for the size of the multiplicative semigroup generated by several polynomials modulo another polynomial h. Voloch pointed out an application of the Stothers-Mason ABC theorem in this context: under mild assumptions, distinct polynomials A, B, C of degree at most $1.2 \deg h - 0.2 \deg \operatorname{rad} ABC$ cannot all be congruent modulo h. This paper presents two improvements in the combinatorial part of Voloch's argument. The first improvement moves the degree bound up to $2 \deg h - \deg \operatorname{rad} ABC$. The second improvement generalizes to $m \geq 3$ polynomials $A_1, \ldots, A_m$ of degree at most $((3m-5)/(3m-7)) \deg h - (6/(3m-7)m) \deg \operatorname{rad} A_1 \cdots A_m$.

Manuscrit reçu le 3 octobre 2003.

The author was supported by the National Science Foundation under grant DMS–0140542, and by the Alfred P. Sloan Foundation. He used the libraries at the Mathematical Sciences Research Institute and the University of California at Berkeley. Permanent ID of this document: 1d9e079cee20138de8e119a99044baa3.

Daniel J. Bernstein
Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
E-mail : djb@cr.yp.to