Journal de Théorie des Nombres
de Bordeaux **13** (2001), 27–41

Signed bits and fast exponentiation

par Wieb BOSMA

Résumé. Nous donnons une analyse précise du gain obtenu en utilisant la représentation des entiers sous la forme non-adjacente, plutôt que la représentation binaire, lorsqu'il s'agit de calculer les puissances d'éléments dans un groupe dans lequel l'inversion est facile. En comptant le nombre de multiplications pour un exposant aléatoire ayant un nombre donné de bits dans son écriture binaire, nous obtenons une version précise du résultat asymptotique connu, selon lequel en moyenne, un parmi trois bits signés de la forme non-adjacente n'est pas nul. Cela montre que l'utilisation des bits signés réduit le coût de l'exponentiation d'un neuvième, par rapport à la méthode ordinaire consistant à des élevations au carré et à des multiplications répétées.

Abstract. An exact analysis is given of the benefits of using the non-adjacent form representation for integers (rather than the binary representation), when computing powers of elements in a group in which inverting is easy. By counting the number of multiplications for a random exponent requiring a given number of bits in its binary representation, we arrive at a precise version of the known asymptotic result that on average one in three signed bits in the non-adjacent form is non-zero. This shows that the use of signed bits (instead of bits for ordinary repeated squaring and multiplication) reduces the cost of exponentiation by one ninth.

Wieb Bosma
Vakgroep Wiskunde
Universiteit van Nijmegen
The Netherlands
E-mail : wieb@sci.kun.nl

Manuscrit reçu le 22 octobre 1999.
Thanks to Ruud Jeurissen for first versions of proofs and for helpful discussions.