Université Bordeaux 1 — **MHT911 – Algorithmique**
Mathématiques — Année 2012–2013

Partiel, 12 novembre 2008 (14:00 – 16:00)
Durée 2 heures. Notes de cours et programmes GP autorisés.

La clarté des programmes et la pertinence des commentaires est un élément important d'appréciation.

- Pour rendre votre copie, taper `~kbelabas/copie` dans un terminal, depuis le répertoire où se trouvent vos fichiers. (Vous pouvez rendre plusieurs fois votre copie : seule la dernière fait foi, les précédentes sont détruites.)

Autour du crible d'Ératosthène.

On désire obtenir le plus rapidement possibles la liste des premiers compris entre 0 et B, par des variantes optimisées du crible d'Ératosthène.

1) Implanter et comparer les algorithmes du document ci-joint [1].

a) À partir de quelle valeur de B l'algorithme d'Atkin devient-il supérieur à l'algorithme naïf ? Quelle est la complexité pratique de vos implantations ?

b) On s'intéresse maintenant aux premiers compris entre L et $L + B$, pour un certain $L \geqslant 0$; la valeur de L joue-t-elle un rôle important ?

2) Remplacer la congruence modulo 30 dans l'Algorithme 2.1 par une congruence modulo $P_k := p_1 p_2 \dots p_k$, où les p_i désignent les premiers consécutifs ; ainsi $P_0 = 1$; $P_1 = 2$, $P_2 = 6$, $P_3 = 30$, etc. Quelle valeur de k est la plus efficace en pratique, suivant les valeurs de B ?

3) On désire la liste des entiers sans facteur carré dans $[0, B]$; adapter l'algorithme d'Érathostène naïf (avec $k = 0$, donc sans congruence) à ce cadre en supprimant les entiers dans les progressions arithmétiques mod p^2 pour les premiers p consécutifs $p \leqslant B^{1/2}$. Quelle est la complexité théorique de cet algorithme ? Sa complexité pratique ?

Références

[1] A. O. L. Atkin & D. J. Bernstein, Prime sieves using binary quadratic forms, *Math. Comp.* **73** (2004), no. 246, pp. 1023–1030 (electronic).