Journal de Théorie des Nombres
de Bordeaux **16** (2004), 233–239

On some subgroups of the multiplicative group of finite rings

par José Felipe VOLOCH

Résumé. Soit S un sous-ensemble de $\mathbf{F}_q$, le corps à q éléments et $h \in \mathbf{F}_q[x]$ un polynôme de degré $d > 1$ sans racines dans S. On considère le groupe généré par l'image de $\{x - s \mid s \in S\}$ dans le groupe des unités de l'anneau $\mathbf{F}_q[x]/(h)$. Dans cet article nous présentons les bornes inférieures pour le cardinal de ce groupe. Notre motivation principale est une application au nouvel algorithme polynomial pour tester la primalité [AKS]. Ces bornes ont également des applications à la théorie des graphes et pour majorer le nombre de points rationnels sur les revètement abeliens de la droite projective sur les corps finis.

Abstract. Let S be a subset of $\mathbf{F}_q$, the field of q elements and $h \in \mathbf{F}_q[x]$ a polynomial of degree $d > 1$ with no roots in S. Consider the group generated by the image of $\{x - s \mid s \in S\}$ in the group of units of the ring $\mathbf{F}_q[x]/(h)$. In this paper we present a number of lower bounds for the size of this group. Our main motivation is an application to the recent polynomial time primality testing algorithm [AKS]. The bounds have also applications to graph theory and to the bounding of the number of rational points on abelian covers of the projective line over finite fields.

José Felipe Voloch
Department of Mathematics
The University of Texas at Austin
1 University Station C1200
Austin, TX 78712-0257 USA
E-mail : voloch@math.utexas.edu

Manuscrit reçu le 25 septembre 2002.