Journal de Théorie des Nombres
de Bordeaux **18** (2006), 471–476

Small exponent point groups on elliptic curves

par Florian LUCA, James MCKEE et Igor E. SHPARLINSKI

Résumé. Soit $\mathbf{E}$ une courbe elliptique définie sur $\mathbb{F}_q$, le corps fini à q éléments. Nous montrons que pour une constante $\eta > 0$ dépendant seulement de q, il existe une infinité d'entiers positifs n tels que l'exposant de $\mathbf{E}(\mathbb{F}_{q^n})$, le groupe des points $\mathbb{F}_{q^n}$-rationnels sur $\mathbf{E}$, est au plus $q^n \exp\left(-n^{\eta/\log\log n}\right)$. Il s'agit d'un analogue d'un résultat de R. Schoof sur l'exposant du groupe $\mathbf{E}(\mathbb{F}_p)$ des points $\mathbb{F}_p$-rationnels, lorsqu'une courbe elliptique fixée $\mathbf{E}$ est définie sur $\mathbb{Q}$ et le nombre premier p tend vers l'infini.

Abstract. Let $\mathbf{E}$ be an elliptic curve defined over $\mathbb{F}_q$, the finite field of q elements. We show that for some constant $\eta > 0$ depending only on q, there are infinitely many positive integers n such that the exponent of $\mathbf{E}(\mathbb{F}_{q^n})$, the group of $\mathbb{F}_{q^n}$-rational points on $\mathbf{E}$, is at most $q^n \exp\left(-n^{\eta/\log\log n}\right)$. This is an analogue of a result of R. Schoof on the exponent of the group $\mathbf{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points, when a fixed elliptic curve $\mathbf{E}$ is defined over $\mathbb{Q}$ and the prime p tends to infinity.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
E-mail : fluca@matmor.unam.mx

James McKee
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey, TW20 0EX, UK
E-mail : james.mckee@rhul.ac.uk

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail : igor@ics.mq.edu.au

Manuscrit reçu le 1er janvier 2005.