

1079-12-145

Sophie Huczynska, University of St. Andrews, **Gary L Mullen*** (mullen@math.psu.edu), Department of Mathematics, Pennsylvania State University, University Park, PA 16802, **Daniel Panario**, Carleton University, and **David Thomson**, Carleton University. *K-Normal Elements of Finite Fields*. Preliminary report.

The finite field F_{q^n} can be viewed as a vector space of dimension n over F_q . An element $\alpha \in F_{q^n}$ generates a *normal basis* if the powers $\alpha^{q^i}, i = 0, 1, \dots, n - 1$ form a basis. Such a basis is very useful in finite field arithmetic, in particular when q -th powering field elements.

It is known that an element α generates a normal basis if and only if the polynomial $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \dots + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime.

We call an element α *k-normal* if the gcd of $g_\alpha(x)$ and $x^n - 1$ has degree k . We will discuss various results concerning the existence and number of k -normal elements. We will also discuss the existence of primitive k -normal elements for small values of k . (Received January 09, 2012)