Existence theorems for r-primitive elements in finite fields

Stephen D. Cohen

Abstract

Let $r|q-1$. An element of $\mathbb{F}_q$ is r-primitive if it has order $(q-1)/r$. Thus, a primitive element is 1-primitive and an r-primitive element is the rth power of a primitive element of $\mathbb{F}_q$. We describe some existence theorems for general r-primitive elements and, in particular, analogues for 2-primitive elements of the following *complete* existence theorems for primitive elements.

Theorem A (1990). For any $n \geq 2$ and $a \in \mathbb{F}_q$ (necessarily with $a \neq 0$ if $n = 2$) there exists a primitive $\alpha \in \mathbb{F}_{q^n}$ with trace a over $\mathbb{F}_q$, except when $a = 0, n = 3, q = 4$.

Theorem B (1983). Every line in $\mathbb{F}_{q^2}$ contains a primitive element. (A line in $\mathbb{F}_{q^2}$ is a set of the form $\{\beta(\gamma + a) : a \in \mathbb{F}_q\}$, for some nonzero $\beta \in \mathbb{F}_{q^2}, \gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.)

Joint work with Giorgos Kapetanakis.