Elementos primitivos 2-normais sobre Corpos Finitos

Victor Gonzalo Lopez Neumann*
Faculdade de Matemática
Universidade Federal de Uberlândia
Uberlândia, Brasil

Abstract

Um elemento $\alpha \in \mathbb{F}_{q^n}$ é normal sobre $\mathbb{F}_q$ se $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ como espaço vetorial sobre $\mathbb{F}_q$. Sabe-se que $\alpha \in \mathbb{F}_{q^n}$ é normal sobre $\mathbb{F}_q$ se, e somente se, $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ e $x^n - 1$ são primos entre si em $\mathbb{F}_{q^n}[x]$. Usando esta equivalência, Huczynska et al. (ver [2]) introduziram a noção de elemento k-normal: um elemento $\alpha \in \mathbb{F}_{q^n}$ é k-normal sobre $\mathbb{F}_q$ se o maior divisor comum dos polinômios $g_\alpha(x)$ e $x^n - 1$ em $\mathbb{F}_{q^n}[x]$ é de grau k; assim, um elemento normal no sentido usual é 0-normal.

No mesmo artigo Huczynska et al. propuseram vários problemas, um deles foi: determinar os pares (n, k) para os quais existem elementos primitivos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Eles mesmos resolveram parcialmente o problema no caso $k = 1$. Alguns anos depois, Reis e Thomson (ver [4]) resolveram esse caso completamente. O Teorema da Base Normal Primitiva (ver [3] e [1]) resolve o caso $k = 0$. Na presente palestra mostramos a solução completa do caso $k = 2$. Este é um trabalho em conjunto com Josimar J. R. Aguirre.

References

[1] S.D. Cohen and S. Huczynska, The primitive normal basis theorem without a computer, *Journal of London Mathematical Society* 67(1) (2003), 41-56.

[2] S. Huczynska; G.L. Mullen; D. Panario and D. Thomson, Existence and properties of k-normal elements over finite fields, *Finite Fields and Their Applications* 24 (2013), 170-183.

[3] H.W. Lenstra and R. Schoof, Primitive normal bases for finite fields, *Mathematics of Computation* 48 (1987), 217-231.

[4] L. Reis and D. Thompson, Existence of primitive 1-normal elements in finite fields, *Finite Fields and Their Applications* 51 (2018), 238-269.

*Partially supported by FAPEMIG, e-mail: victor.neumann@ufu.br