World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:16, No:09, 2022

Open Science Index, Mathematical and Computational Sciences Vol:16, No:09, 2022 publications.waset.org/abstracts/149587.pdf

Existence of Rational Primitive Normal Pairs with Prescribed Norm and Trace

Authors : Soniya Takshak, R. K. Sharma

Abstract : Let q and n be positive integers, then F_{φ} denotes the finite field of q elements, and Fqn denotes the extension of F_{φ} of degree n. Also, F_{φ}* represents the multiplicative group of non-zero elements of F_{φ}, and the generators of F_{φ}* are called primitive elements. A normal element α of a finite field F_{φ}^n is such that $\{\alpha, \alpha^{\varphi}, . . . , \alpha^{\varphi n-1}\}$ forms a basis for F_{φ}^n over F_{φ}. Primitive normal elements have several applications in coding theory and cryptography. So, establishing the existence of primitive normal elements under certain conditions is both theoretically important and a natural issue. In this article, we provide a sufficient condition for the existence of a primitive normal element α in F_{φ}^n of a prescribed primitive norm and non-zero trace over F_{φ} such that f(α) is also primitive, where $f(x) \in F_{\varphi}^n(x)$ is a rational function of degree sum m. Particularly, we investigated the rational functions of degree sum 4 over F_{φ}^n, where $q = 11^k$ and demonstrated that there are only 3 exceptional pairs (q, n), $n \geq 7$ for which such kind of primitive normal elements may not exist. In general, we show that such elements always exist except for finitely many choices of (q, n). To arrive to our conclusion, we used additive and multiplicative character sums.

Keywords : finite field, primitive element, normal element, norm, trace, character
Conference Title : ICFFAC 2022 : International Conference on Finite Field Arithmetic and Cryptography
Conference Location : Lisbon, Portugal
Conference Dates : September 20-21, 2022