

Johnston, Anna M.

Trace formulae for irreducible polynomials over \mathbb{F}_P with minimal order roots in \mathbb{F}_{P^q} . (English)

[Zbl 1178.11074](#)

Finite Fields Appl. 14, No. 4, 1002-1009 (2008).

Let P be a prime of the form $P = q^n s + 1$ for a prime q . Then $P^q = q^{n+1} s K + 1$, where $\gcd(K, P - 1) = 1$. The author gives formulas involving values of the trace function $\text{Tr} : \mathbb{F}_{P^q} \rightarrow \mathbb{F}_P$ of elements $\alpha \in \mathbb{F}_{P^q}$ of order R for a prime divisor R of K . For instance $\text{Tr}(\alpha) + \text{Tr}(\alpha^{-1}) = -1$, $\text{Tr}(\alpha)\text{Tr}(\alpha^{-1}) = (q + 1)/2$ if $q > 2, R = 2q + 1$ (take e.g. $P = 401, q = 5, R = 11$).

Reviewer: [Wilfried Meidl \(Istanbul\)](#)

MSC:

[11T06](#) Polynomials over finite fields

Keywords:

[Trace-function](#); [minimal polynomial](#); [reciprocal polynomial](#)

Full Text: [DOI](#)

References:

- [1] Bach, Eric; Shallit, Jeffrey, Algorithmic number theory, vol. 1: efficient algorithms, (1997), MIT · [Zbl 0873.11070](#)
- [2] Beaver, Cheryl; Gemmell, Peter; Johnston, Anna; Newmann, William, On the cryptographic value of the $\{q\}$ th root problem, (), 135-142 · [Zbl 1014.94553](#)
- [3] Cipolla, M., Un metodo per la risoluzione Della congruenza di secondo grado, *Rend. accad. sci. fis. mat.*, 9, 154-163, (1903) · [Zbl 34.0219.02](#)
- [4] Johnston, Anna; Gemmell, Peter, Authenticated key exchange provably secure against the man-in-the-middle attack, *J. cryptology*, 15, 2, 139-148, (2002) · [Zbl 0994.94027](#)
- [5] Anna M. Johnston, thesis, On the difficulty of the $\{q\}$ th root problem in certain finite cyclic groups, University of London, Senate House, Malet Street, London, 2006
- [6] Lidl, Rudolf; Niederreiter, Harald, *Finite fields*, (1997), Cambridge University Press

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.