

Number Theory

Finite Fields

11Txx

- [1] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang. A trace conjecture and flag-transitive affine planes. *J. Combin. Theory Ser. A*, 95(1):158–168, 2001.
- [2] Aart Blokhuis, Robert S. Coulter, Marie Henderson, and Christine M. O’Keefe. Permutations amongst the Dembowski-Ostrom polynomials. In *Finite fields and applications (Augsburg, 1999)*, pages 37–42. Springer, Berlin, 2001.
- [3] Mihai Cipu. Dickson polynomials that are permutations. *Serdica Math. J.*, 30(2-3):177–194, 2004.
- [4] Stephen D. Cohen. Finite field elements with specified order and traces. *Des. Codes Cryptogr.*, 36(3):331–340, 2005.
- [5] Robert S. Coulter, George Havas, and Marie Henderson. Giesbrecht’s algorithm, the HFE cryptosystem and Ore’s p^s -polynomials. In *Computer Mathematics (Matsuyama, 2001)*, volume 9 of *Lecture Notes Ser. Comput.*, pages 36–45. World Sci. Publ., River Edge, NJ, 2001.
- [6] Robert S. Coulter, George Havas, and Marie Henderson. On decomposition of sub-linearised polynomials. *J. Aust. Math. Soc.*, 76(3):317–328, 2004.
- [7] Robert S. Coulter and Marie Henderson. The compositional inverse of a class of permutation polynomials over a finite field. *Bull. Austral. Math. Soc.*, 65(3):521–526, 2002.
- [8] Ronald Evans, Henk D. L. Hollmann, Christian Krattenthaler, and Qing Xiang. Gauss sums, Jacobi sums, and p -ranks of cyclic difference sets. *J. Combin. Theory Ser. A*, 87(1):74–119, 1999.
- [9] Marko Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. [arXiv:0706.2112](https://arxiv.org/abs/0706.2112), 19 pages, 2007.

- [10] Ferruh Özbudak. Elements of prescribed order, prescribed traces and systems of rational functions over finite fields. *Des. Codes Cryptogr.*, 34(1):35–54, 2005.
- [11] B. V. Petrenko. On the product of two primitive elements of maximal subfields of a finite field. *J. Pure Appl. Algebra*, 178(3):297–306, 2003.
- [12] B. V. Petrenko. On the sum of two primitive elements of maximal subfields of a finite field. *Finite Fields Appl.*, 9(1):102–116, 2003.