

# 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] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. [arXiv:0804.4799](https://arxiv.org/abs/0804.4799), 12 pages, 2008.
- [4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields Appl.*, 14(3):703–714, 2008.
- [5] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, 49(1-3):273–288, 2008.
- [6] Mihai Cipu. Dickson polynomials that are permutations. *Serdica Math. J.*, 30(2-3):177–194, 2004.
- [7] Mihai Cipu and Stephen D. Cohen. Dickson polynomial permutations. In *Finite Fields and Applications*, volume 461 of *Contemporary Mathematics*, 79–91 pages. 2008.
- [8] Stephen D. Cohen. Finite field elements with specified order and traces. *Des. Codes Cryptogr.*, 36(3):331–340, 2005.
- [9] Stephen D. Cohen. Primitive polynomials with a prescribed coefficient. *Finite Fields Appl.*, 12(3):425–491, 2006.

- [10] 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.
- [11] Robert S. Coulter, George Havas, and Marie Henderson. On decomposition of sub-linearised polynomials. *J. Aust. Math. Soc.*, 76(3):317–328, 2004.
- [12] 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.
- [13] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields and Their Applications*, 15(1):1 – 22, 2009.
- [14] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3(1):59–81, 2009.
- [15] 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.
- [16] Reza Rezaeian Farashahi and Ruud Pellikaan. The quadratic extension extractor for (hyper)elliptic curves in odd characteristic. In *Arithmetic of finite fields*, volume 4547 of *Lecture Notes in Comput. Sci.*, pages 219–236. Springer, Berlin, 2007.
- [17] Kseniya Garaschuk. *On Binary and Ternary Kloosterman Sums*. Ph D thesis, Simon Fraser University, 2007.
- [18] Lenwood S. Heath and Nicholas A. Loehr. New algorithms for generating Conway polynomials over finite fields. In *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999)*, pages 429–437, New York, 1999. ACM.
- [19] Dae San Kim. Codes associated with  $O^+(2n, 2^r)$  and power moments of Kloosterman sums. [arXiv:0807.4671](https://arxiv.org/abs/0807.4671), 9 pages, 2008.
- [20] Dae San Kim. Codes associated with orthogonal groups and power moments of Kloosterman sums. [arXiv:0808.3003](https://arxiv.org/abs/0808.3003), 2008.

- [21] Dae San Kim. Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums. *arXiv:0807.3991*, 7 pages, 2008.
- [22] Douglas A. Leonard. A weighted module view of integral closures of affine domains of type I. *Adv. Math. Commun.*, 3(1):1–11, 2009.
- [23] Marko Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Acta Arith.*, 132(4):329–350, 2008.
- [24] Ferruh Özbudak. Elements of prescribed order, prescribed traces and systems of rational functions over finite fields. *Des. Codes Cryptogr.*, 34(1):35–54, 2005.
- [25] 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.
- [26] 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.
- [27] Håvard Raddum and Igor Semaev. Solving multiple right hand sides linear equations. *Des. Codes Cryptogr.*, 49(1-3):147–160, 2008.