Wan, Daqing

Permutation polynomials and resolution of singularities over finite fields. (English)

Zbl 0711.11050
Proc. Am. Math. Soc. 110, No. 2, 303-309 (1990).

Let F_q denote the finite field of order q. In 1966 L. Carlitz conjectured that for each positive integer n, there is a constant C_n such that for each finite field of odd order $q > C_n$, there does not exist a permutation polynomial of degree n over F_q. The conjecture is quite easily shown to be true for n a power of two but is only known to be true for the additional values $n = 6, 10, 12$, and 14. The author verifies the truth of the Carlitz conjecture for $n = 2\ell$ where ℓ is an odd prime. This is accomplished by relating the conjecture to the study of the resolution of singularities of a plane algebraic curve over a finite field.

It should also be pointed out that, independently, *S. D. Cohen* has obtained the same result and has shown the conjecture to be true for all $n < 1000$ as well. Cohen's method is based on exceptional polynomials over finite fields and on the theory of primitive permutation groups. His paper is to appear in Arch. Math. While both methods certainly have merit, it is not clear to the reviewer which method has the greater probability of leading to a solution of the entire conjecture. A complete proof of the conjecture would indeed be a major result.

Reviewer: G.L.Mullen

MSC:

11T06 Polynomials over finite fields
11G20 Curves over finite and local fields
14H20 Singularities of curves, local rings

Keywords:
permutation polynomial; singularities of a plane algebraic curve over a finite field

Full Text: DOI

References:

[1] Stephen D. Cohen, Permutation polynomials and primitive permutation groups, Arch. Math. (Basel) 57 (1991), no. 5, 417 – 423. · Zbl 0766.11047 · doi:10.1007/BF01246737

[2] L. E. Dickson, The analytic representation of substitutions on a prime power of letters with a discussion of the linear group, Ann. of Math. 11 (1897), 65-120, 161-183. · Zbl 28.0135.03

[3] Robin Hartshorne, Algebraic geometry, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. · Zbl 0367.14001

[4] D. R. Hayes, A geometric approach to permutation polynomials over a finite field, Duke Math. J. 34 (1967), 293 – 305. · Zbl 0163.05202

[5] Rudolf Lidl and Gary L. Mullen, Unsolved Problems: When Does a Polynomial Over a Finite Field Permute the Elements of the Field?, Amer. Math. Monthly 95 (1988), no. 3, 243 – 246. · Zbl 0653.12010 · doi:10.2307/2323626

[6] R. Lidl and H. Niderreiter, Finite fields, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, MA, 1983.

[7] Wolfgang M. Schmidt, Equations over finite fields. An elementary approach, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976. · Zbl 0329.12001

[8] Beniamino Segre, Arithmetische Eigenschaften von Galois-Räumen. I, Math. Ann. 154 (1964), 195 – 256 (German). · Zbl 0126.17002 · doi:10.1007/BF01362097

[9] Da Qing Wan, On a conjecture of Carlitz, J. Austral. Math. Soc. Ser. A 43 (1987), no. 3, 375 – 384. · Zbl 0635.12011