MR2610704 (2011d:11280) 11T06
Kim, Ryul; **Koepf, Wolfram** (D-UKSL)
Parity of the number of irreducible factors for composite polynomials. (English summary)
Finite Fields Appl. **16** (2010), *no. 3,* 137–143.

Using Stickelberger's theorem (later rediscovered by Swan) one can determine the parity of the number of irreducible factors of a given square-free univariate polynomial over a finite field. This is done by examining either the discriminant of the given polynomial or the discriminant of its lift to the integers. The authors of the paper under review prove some results about the discriminants of composition of some family of polynomials and use them to obtain some results about the parity of the number of irreducible factors of some polynomials over finite fields.

Reviewed by *Omran Ahmadi Darvishvand*

References

1. O. Ahmadi, A. Menezes, Irreducible polynomials of maximum weight, Util. Math. 72 (2007) 111–123. MR2306234 (2008e:11147)
2. O. Ahmadi, G. Vega, On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields, Finite Fields Appl. 14 (2008) 124–131. MR2381481 (2008k:12003)
3. A. Bluher, A Swan-like theorem, Finite Fields Appl. 12 (2006) 128–138. MR2190190 (2006h:11135)
4. K. Dilcher, K.B. Stolarsky, Resultants and discriminants of Chebyshev and related polynomials, Trans. Amer. Math. Soc. 357 (2004) 965–981. MR2110427 (2005k:13054)
5. S. Fan, W. Han, Primitive polynomials over finite fields of characteristic two, Appl. Algebra Engrg. Comm. Comput. 14 (2004) 381–395. MR2034920 (2004k:11186)
6. J. von zur Gathen, Irreducible trinomials over finite fields, Math. Comp. 72 (2003) 1987–2000. MR1986817 (2004c:11229)
7. A. Hales, D. Newhart, Swan's theorem for binary tetranomials, Finite Fields Appl. 12 (2006) 301–311. MR2206403 (2007d:11132)
8. W. Koepf, R. Kim, The parity of the number of irreducible factors for some pentanomials, Finite Fields Appl. 15 (2009) 585–603. MR2554042 (2010j:11172)
9. W. Koepf, Computeralgebra, Springer, Berlin, 2008.
10. R. Lidl, H. Niederreiter, Finite Fields, 2nd edition, Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1996. MR1429394 (97i:11115)
11. J.H. McKay, S. Sui-Sheng Wang, A chain rule for the resultant of two polynomials, Arch. Math. 53 (1989) 347–351. MR1015998 (90h:12006)
12. A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian, Applications of Finite Fields, Kluwer, 1993.
13. F. Rodriguez-Henriquez, C.K. Koc, Parallel multipliers based on special irreducible pentanomials, IEEE Trans. Comput. 52 (2003) 1535–1542.

14. I.E. Shparlinski, Finding irreducible and primitive polynomials, Appl. Algebra Engrg. Comm. Comput. 4 (1993) 263–268. MR1235861 (94i:11098)
15. L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, in: Verh. I. Internat. Math.-Kongress Zürich, 1897, Leipzig, 1898, pp. 182–193.
16. R.G. Swan, Factorization of polynomials over finite fields, Pacific J. Math. 12 (1962) 1099–1106. MR0144891 (26 #2432)
17. R. Zippel, Effective Polynomial Computation, Springer, 1993.

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.