Previous | Up | Next Article

Citations
From References: 1
From Reviews: 0

**MR2554042 (2010j:11172)** 11T06 (11T55)

**Koepf, Wolfram** (D-UKSL); **Kim, Ryul**

**The parity of the number of irreducible factors for some pentanomials. (English summary)**

*Finite Fields Appl.* **15** (2009), *no. 5,* 585–603.

The objective of the paper is to characterize the parity of the number of irreducible factors of some pentanomials over the binary field $\mathbb{F}_2$. More precisely, the authors cleverly use the classical theorem of Swan (first proved by Stickelberger), to prove several results of which the following is typical:

Let $m, n$ be positive numbers such that $m \equiv 2 \pmod 4$ and $n \equiv 1 \pmod 2$. Assume that $m \geq 2n + 2 + \delta$ where $\delta = 0$, $m$ is even and $\delta = 1$ otherwise. Then the pentanomial

$$x^m + x^{n+2} + x^{n+1} + x^n + 1$$

has an even number of prime (irreducible) factors over $\mathbb{F}_2$ if and only if $x = m, y = n$ or $x = -m, y = -n$ satisfies the condition

$$x \equiv 2 \pmod 8 \text{ and } y \in \{3, -1\} \pmod 8.$$

Reviewed by *Luis H. Gallardo*

## References

1. O. Ahmadi, A. Menezes, Irreducible polynomials of maximum weight, Util. Math. 72 (2007) 111–123. MR2306234 (2008e:11147)
2. O. Ahmadi, A. Menezes, On the number of trace-one elements in polynomial bases for $F_{2^n}$, Des. Codes Cryptogr. 37 (2005) 493–507. MR2177648 (2006m:11173)
3. 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)
4. A. Bluher, A Swan-like theorem, Finite Fields Appl. 12 (2006) 128–138. MR2190190 (2006h:11135)
5. A. Hales, D. Newhart, Swan's theorem for binary tetranomials, Finite Fields Appl. 12 (2006) 301–311. MR2206403 (2007d:11132)
6. R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1997. MR1294139 (95f:11098)
7. K.V. Mangipudi, R.S. Katti, Montgomery multiplier for a class of special irreducible pentanomials, preprint, http://www.ece.ndsu.nodak.edu/∼katti/pdf/jp04.pdf, 2004.
8. F. Rodriguez-Henriquez, Ç.K. Koç, Parallel multipliers based on special irreducible pentanomials, IEEE Trans. Comput. 52 (2003) 1535–1542.
9. B. Sunar, E. Savas, Ç.K. Koç, Constructing composite field representations for efficient conversion, IEEE Trans. Comput. 52 (2003) 1391–1398.
10. R.G. Swan, Factorization of polynomials over finite fields, Pacific J. Math. 12 (1962) 1099–

1106. MR0144891 (26 #2432)

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