

Wang, Luyan

On permutation polynomials. (English) Zbl 1044.11103
Finite Fields Appl. 8, No. 3, 311-322 (2002).

The author studies the question when a polynomial of the form $f(x) = x^u(x^v + 1)$ with positive integers u, v induces a permutation on the finite field \mathbb{F}_q . For $d = 3$ and $d = 5$ he gives sufficient and necessary conditions for f to be a permutation polynomial over \mathbb{F}_q where $d \mid q - 1$ and $\gcd(v, q - 1) = (q - 1)/d$. The proof is based on Hermite's criterion for permutation polynomials.

Remark: The numerous inductions in the proof of Lemma 4 can be evaded. Because of the symmetry of binomial coefficients, we have $M(2n, 3, c) = M(2n, 3, 2n - c)$ for all c and $M(2n, 3, c + 1) = M(2n, 3, c) + 1$ whenever $2n + c \equiv 2 \pmod{3}$. With $M(2n, 3, 0) + M(2n, 3, 1) + M(2n, 3, 2) = 2^{2n}$, this yields Lemma 4.

Reviewer: [Astrid Reifegerste \(Hannover\)](#)

MSC:

[11T06](#) Polynomials over finite fields

Cited in **1** Review
Cited in **7** Documents

Keywords:

[permutation polynomials over finite fields](#); [Hermite's criterion](#); [Lucas numbers](#)

Full Text: [DOI](#)

References:

- [1] Lidl, R.; Mullen, G.L., When does a polynomial over a finite field permute the elements of the field?, Amer. math. monthly, 95, 243-246, (1988) · [Zbl 0653.12010](#)
- [2] Lidl, R.; Niederreiter, H., Finite fields, (1983), Addison-Wesley Reading
- [3] Lidl, R.; Mullen, G.L., When does a polynomial over a finite field permute the elements of the field?, II, Amer. math. monthly, 100, 71-74, (1993) · [Zbl 0777.11054](#)
- [4] Mullen, G.L., Permutation polynomials over finite fields, Proceedings Las Vegas 1991, 141, (1993), Dekker New York, p. 131-151 · [Zbl 0808.11069](#)
- [5] Wan, D.; Lidl, R., Permutation polynomials of the form $x^{\text{rf}(x(q-1)/d)}$ and their group structure, Monatsh. math., 112, 149-163, (1991) · [Zbl 0737.11040](#)
- [6] Lee, J.B.; Park, Y.H., Some permuting trinomials over finite fields, Acta math. sci. (English ed.), 17, 250-254, (1997) · [Zbl 0921.11062](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.