Lecturas Matemáticas
Volumen **45** (1) (2024), páginas 75-78
ISSN 0120-1980

A note on “A counterexample to a proposition of R. Mathews”

Una nota acerca de “A counterexample to a proposition of R. Mathews”

Zhiguo Ding and Michael E. Zieve

University of Michigan, U.S.A.

ABSTRACT. We show that some published “counterexamples” to a theorem of R. Matthews are in fact not counterexamples, and the relevant theorem is true. We also provide a survey of known results and examples that are related to Matthews’ result.

***Key words*:** Dickson polynomials, finite fields, permutation polynomials.

RESUMEN. Mostramos que algunos “contraejemplos” a un teorema de R. Matthews que han sido publicados en realidad no son contraejemplos, y que el teorema relevante es válido. También incluimos un resumen de resultados y ejemplos conocidos relacionados con el resultado de Matthews.

***Palabras clave*:** Polinomios de Dickson, campos finitos, polinomios de permutación.

2010 AMS Mathematics Subject Classification. Primary 11T06.

For any positive integer n, write

$$E_n(X) := \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-1)^i X^{n-2i}.$$

This polynomial $E_n(X)$ is called the Dickson polynomial of the second kind, and is closely related to the classical Chebyshev polynomial of the second kind [15]. Crucially, $E_n(X)$ has integer coefficients, so for any prime power q the function $c \mapsto E_n(c)$ maps $\mathbb{F}_q \to \mathbb{F}_q$. Several authors have studied when this function is bijective. The first result on this topic is as follows [16, Thm. 2.5].

Proposition 1. *If q is a power of an odd prime p, and n is a positive integer satisfying the three congruences*

$$n+1 \equiv \pm 2 \pmod{p}$$
$$n+1 \equiv \pm 2 \left(\bmod \frac{q-1}{2}\right)$$
$$n+1 \equiv \pm 2 \left(\bmod \frac{q+1}{2}\right),$$

then $E_n(X)$ permutes each set $\{a, -a\}$ with $a \in \mathbb{F}_q$, so that in addition $E_n(X)$ permutes $\mathbb{F}_q$.

The paper [1] purports to give two counterexamples to Proposition 1. In order to help future readers avoid confusion, we show here that those “counterexamples” are not actually counterexamples. In fact, Proposition 1 is true, and its proof is quite simple; this proof appears in each of [6, 9, 13, 16].

The paper [1] claims that the pairs $(q, n) = (5, 11)$ and $(q, n) = (9, 17)$ are counterexamples to Proposition 1. However, if $(q, n) = (5, 11)$ then $n + 1 \not\equiv \pm 2 \pmod{(q+1)/2}$, and if $(q, n) = (9, 17)$ then $n + 1 \not\equiv \pm 2 \pmod{p}$. Thus the pairs $(q, n) = (5, 11)$ and $(q, n) = (9, 17)$ do not satisfy the hypotheses of Proposition 1, so they are not counterexamples to Proposition 1.

The mistake in [1] appears to be that its author interpreted the hypothesis of Proposition 1 to be that at least one of the three congruences holds, rather than that all three congruences hold. However, we note that there is no ambiguity on this issue, since the requirement that all three congruences hold is stated clearly in both [16] and in many subsequent references, including [2–15, 17–19].

It has been conjectured repeatedly that, if $E_n(X)$ permutes $\mathbb{F}_q$ where $q = p^k$ for some prime $p > 5$, then the three congruences in Proposition 1 must hold [2, 11, 12, 14, 17, 18]. This conjecture was proved in [4] when $k \leq 2$ (building on and correcting [3, 5, 6]). It remains open when $k > 2$. Examples in [9] show that the condition $p > 5$ is crucial in this conjecture.

Acknowledgments

The first author was supported in part by the Natural Science Foundation of Hunan Province of China (No. 2020JJ4164).

References

[1] P. A. Acosta Solarte, *A counterexample to a proposition of R. Mathews*, Lect. Mat., 27 (2006), 19-20.

[2] V. Albis, *Polinomios de permutación Algunos problemas de interés*, Lect. Mat., 22 (2001), 35-58.

[3] M. Cipu, *Dickson polynomials that are permutations*, Serdica Math. J., 30 (2004), 177-194.

[4] M. Cipu and S. D. Cohen, *Dickson polynomial permutations*, Finite fields and applications, Amer. Math. Soc., Providence (2008), 79-90.

[5] S. D. Cohen, *Dickson polynomials of the second kind that are permutations*, Canad. J. Math., 46 (1994), 225-238.

[6] S. D. Cohen, *Dickson permutations*, Number-theoretic and algebraic methods in computer science (Moscow, 1993), World Sci. Publ., River Edge (1995), 29-51.

[7] R. S. Coulter and R. W. Matthews, *On the permutation behaviour of Dickson polynomials of the second kind*, Finite Fields Appl., 8 (2002), 519-530.

[8] M. Fried and R. Lidl, *On Dickson polynomials and Rédei functions*, Contributions to general algebra, 5 (Salzburg, 1986), Hölder-Pichler-Tempsky, Vienna (1987), 139-149.

[9] M. Henderson and R. Matthews, *Permutation properties of Chebyshev polynomials of the second kind over a finite field*, Finite Fields Appl., 1 (1995), 115-125.

[10] M. Henderson and R. Matthews, *Dickson polynomials of the second kind which are permutation polynomials over a finite field*, New Zealand J. Math., 27 (1998), 227-244.

[11] X.-d. Hou, *Permutation polynomials over finite fields-a survey of recent advances*, Finite Fields Appl., 32 (2015), 82-119.

[12] N. S. James and R. Lidl, *Permutation polynomials on matrices*, Linear Algebra Appl., 96 (1987), 181-190.

[13] R. Lidl, *On cryptosystems based on polynomials and finite fields*, Advances in cryptology (Paris, 1984), Springer, Berlin (1985), 10-15.

[14] R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly, 95 (1988), 243-246.

[15] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Longman Sci. & Tech., 1993.

[16] R. W. Matthews, *Permutation polynomials in one and several variables*, Ph.D. thesis, University of Tasmania, 1982. Available at
`https://figshare.utas.edu.au/articles/thesis/Permutation_polynomials_in_one_and_several_variables/23232068`

[17] G. L. Mullen, *Dickson polynomials over finite fields*, Algebraic structures and number theory; proceedings of the first international symposium, Hong Kong, August 8-13, 1988, World Scientific, Teaneck (1990), 190-207.

[18] G. L. Mullen, *Dickson polynomials over finite fields*, Adv. in Math. (China), 20 (1991), 24-32.

[19] G. L. Mullen, *Permutation polynomials: a matrix analogue of Schur’s conjecture and a survey of recent results*, Finite Fields Appl., 1 (1995), 242-258.

Recibido en junio 2023. Aceptado para publicación en febrero de 2024.

Zhiguo Ding
Department of Mathematics
University of Michigan
Ann Arbor, USA
e-mail: dingz@umich.edu

Michael Zieve
Department of Mathematics
University of Michigan
Ann Arbor, USA
e-mail: zieve@umich.edu