ISSN 2590-9770
The Art of Discrete and Applied Mathematics 2 (2019) #P1.10
https://doi.org/10.26493/2590-9770.1330.993
(Also available at http://adam-journal.eu)

Polynomials of degree 4 over finite fields representing quadratic residues[*]

Shaofei Du [†]

Capital Normal University, School of Mathematical Sciences,
Bejing 100048, People's Republic of China

Klavdija Kutnar [‡]

University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia

Dragan Marušič [§]

University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia
IMFM, Jadranska 19, 1000 Ljubljana, Slovenia

Received 29 September 2019, accepted 13 October 2019, published online 30 December 2019

Abstract

It is proved that in a finite field F of prime order p, where p is not one of finitely many exceptions, for every polynomial $f(x) \in F[x]$ of degree 4 that has a nonzero constant term and is not of the form $\alpha g(x)^2$ there exists a primitive root $\beta \in F$ such that $f(\beta)$ is a quadratic residue in F. This refines a result of Madden and Vélez from 1982 about polynomials that represent quadratic residues at primitive roots.

Keywords: Finite field, polynomial, quadratic residues.

Math. Subj. Class.: 12E99

[*] The authors wish to thank Ademir Hujdurović and Kai Yuan for helpful conversations about the material of this paper.

[†] This work is supported in part by the National Natural Science Foundation of China (11671276).

[‡] Corresponding author. This work is supported in part by the Slovenian Research Agency (research program P1-0285 and research projects N1-0038, N1-0062, J1-6720, J1-6743, J1-7051, J1-9110, J1-1695, and J1-1715).

[§] This work is supported in part by the Slovenian Research Agency (I0-0035, research program P1-0285 and research projects N1-0038, N1-0062, J1-6720, J1-9108, and J1-1695), and in part by H2020 Teaming InnoRenew CoE (grant no. 739574).

E-mail addresses: dushf@mail.cnu.edu.cn (Shaofei Du), klavdija.kutnar@upr.si (Klavdija Kutnar), dragan.marusic@upr.si (Dragan Marušič)

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 2 (2019) #P1.10
https://doi.org/10.26493/2590-9770.1330.993
(Dostopno tudi na http://adam-journal.eu)

Polinomi stopnje 4 nad končnimi polji, ki predstavljajo kvadratne ostanke*

Shaofei Du †
*Capital Normal University, School of Mathematical Sciences,
Bejing 100048, People's Republic of China*

Klavdija Kutnar ‡
*University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia*

Dragan Marušič §
*University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia
IMFM, Jadranska 19, 1000 Ljubljana, Slovenia*

Prejeto 29. septembra 2019, sprejeto 13. oktobra 2019, objavljeno na spletu 30. decembra 2019

Povzetek

Dokažemo, da v končnem polju F reda p, kjer p ni eno izmed končno mnogih izjem, za vsak polinom $f(x) \in F[x]$ stopnje 4, ki nima neničelnega konstantnega člena in ki ni oblike $\alpha g(x)^2$, obstaja tak primitiven element $\beta \in F$, za katerega je $f(\beta)$ kvadratni ostanek v F. Ta rezultat predstavlja izboljšavo rezultata Maddena in Véleza iz leta 1982 o polinomih, ki predstavljajo kvadratne ostanke v primitivnih elementih.

Ključne besede: Končno polje, polinom, kvadratni ostanki.

Math. Subj. Class.: 12E99

*Avtorji se zahvaljujejo Ademirju Hujduroviću in Kaiu Yuanu za koristne pogovore o vsebini pričujočega članka.

†Delo je delno podprto s strani National Natural Science Foundation of China (11671276).

‡Kontaktni avtor. Delo je delno podprto s strani Javne agencije za raziskovalno dejavnost Republike Slovenije (raziskovalni program P1-0285 in raziskovalni projekti N1-0038, N1-0062, J1-6720, J1-6743, J1-7051, J1-9110, J1-1695 in J1-1715).

§Delo je delno podprto s strani Javne agencije za raziskovalno dejavnost Republike Slovenije (I0-0035, raziskovalni program P1-0285 in raziskovalni projekti N1-0038, N1-0062, J1-6720, J1-9108 in J1-1695) ter delno s strani H2020 Teaming InnoRenew CoE (dotacija št. 739574).

E-poštni naslovi: dushf@mail.cnu.edu.cn (Shaofei Du), klavdija.kutnar@upr.si (Klavdija Kutnar), dragan.marusic@upr.si (Dragan Marušič)