УДК 512.624

ПРО ЕЛЕМЕНТИ ВЕЛИКОГО ПОРЯДУ В СКІНЧЕННИХ ПОЛЯХ, ЗАДАНИХ ДВОЧЛЕНОМ

Роман Попович

Національний університет «Львівська політехніка»

rombp07@gmail.com

Загальновідомо, що мультиплікативна група скінченного поля є циклічною. Твірну цієї групи називають примітивним елементом. На даний час в обчислювальній теорії скінченних полів немає поліноміального алгоритму побудови примітивного елемента для заданого скінченного поля. Ось чому розглядають менш обмежувальне питання: знайти елемент великого мультиплікативного порядку [2]. У цьому випадку не вимагається обчислити точний порядок елемента: достатньо отримати нижню межу для порядку. Елементи великого порядку потрібні для низки застосувань, які, зокрема, охоплюють криптографію та теорію кодування.

Як F_q позначимо поле з q елементів, де q – степінь простого числа. Розширення цього поля на основі двочлена має вигляд $F_q[x]/(x^m - a)$. Для таких полів два відомі найкращі результати виглядають так: нижняя межа для порядку $2^{\sqrt[3]{2m}}$ [3] та покращення цієї межі $5^{\sqrt[3]{m/2}}$ [1].

У цій роботі підсилюємо наведені відомі результати.

Теорема. *Нехай b – будь-який ненульовий елемент з F_q. Тоді $\theta + b$ має в розширеному полі, заданому двочленом, мультиплікативний порядок принаймні $2^{\sqrt{2m}}$.*

1. *Bovdi V., Diene A., Popovych R.* Elements of high order in finite fields specified by binomials // Carpathian Math. Publ. – 2022. – **14**, No. 1. – P. 238-246.
2. *Mullen L., Panario D.* Handbook of finite fields. – Boca Raton: CRC Press, 2013. – 1068 p.
3. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m-a)$ // Finite Fields Appl. – 2013. – **19**, No. 1. – P. 86-92.

ON ELEMENTS OF HIGH ORDER IN FINITE FIELDS, SPECIFIED BY BINOMIAL

We construct explicitly in any finite field, specified by a binomial, elements with the multiplicative order at least $2^{\sqrt{2m}}$.