Summary: Computing square, cube and \( n \)-th roots in general, in finite fields, are important computational problems with significant applications to cryptography. One interesting approach to computational problems is by using polynomial representations. Agou, Deléglise and Nicolas [Zbl 1023.12002] proved results concerning the lower bounds for the length of polynomials representing square roots modulo a prime \( p \). We generalize the results by considering \( n \)-th roots over finite fields for arbitrary \( n > 2 \).

Keywords: cube roots; \( n \)-th roots; finite fields

http://www.mathnet.or.kr/mathnet/kms_content.php?no=412309