ZMATH 2016e.00781

Aabrandt, Andreas; Hansen, Vagn Lundsgaard

A note on powers in finite fields.

Int. J. Math. Educ. Sci. Technol. 47, No. 6, 987-991 (2016).

Summary: The study of solutions to polynomial equations over finite fields has a long history in mathematics and is an interesting area of contemporary research. In recent years, the subject has found important applications in the modelling of problems from applied mathematical fields such as signal analysis, system theory, coding theory and cryptology. In this connection, it is of interest to know criteria for the existence of squares and other powers in arbitrary finite fields. Making good use of polynomial division in polynomial rings over finite fields, we have examined a classical criterion of Euler for squares in odd prime fields, giving it a formulation that is apt for generalization to arbitrary finite fields and powers. Our proof uses algebra rather than classical number theory, which makes it convenient when presenting basic methods of applied algebra in the classroom.

Classification: H40 F60
Keywords: finite fields; prime numbers; squares and powers in finite fields
doi:10.1080/0020739X.2015.1129076