SUMS OF POWERS IN LARGE FINITE FIELDS

CHARLES SMALL

Abstract. If \( k \) is a positive integer, then, in any finite field with more than \((k - 1)^4\) elements, every element is a sum of two \( k \)th powers.

In this note we prove an "outrageous conjecture" of Kaplansky [3]; for each fixed positive integer \( k \), every element of every sufficiently large finite field is a sum of two \( k \)th powers. More precisely, we show that every finite field with more than \((k - 1)^4\) elements is sufficiently large. The proof is a straightforward application of a basic inequality from the theory of diagonal equations over finite fields.

Theorem. Let \( k \) be a positive integer, let \( F \) be a finite field with, say, \( q \) elements, and put \( \delta = (q - 1, k) \). Assume \( q > (\delta - 1)^4 \). Then every element of \( F \) is a sum of two \( k \)th powers. (In particular, the conclusion holds if \( q > (k - 1)^4 \), since \( k > \delta \).

Proof. For \( b \in F \) let \( N(b) \) denote the number of solutions \((x, y) \in F \times F\) of \( x^k + y^k = b \). Then, by definition, \( N(b) > 0 \); we have to show that \( q > (\delta - 1)^4 \) implies \( N(b) > 0 \). We may assume \( b \neq 0 \), since 0 is certainly a sum of two \( k \)th powers. Then, by Corollary 1 on p. 57 of [2], we have \( |N(b) - q| < (\delta - 1)^2\sqrt{q} \). In particular, \( N(b) - q > -(\delta - 1)^2\sqrt{q} \), so that \( N(b) > \sqrt{q} \). Hence \( N(b) > 0 \), for all \( b \), provided \( \sqrt{q} > (\delta - 1)^2 \), or in other words \( q > (\delta - 1)^4 \).

The Theorem is best possible in the sense that there are arbitrarily large finite fields in which not everything is a single \( k \)th power, for instance the prime fields with \( p \) elements, \( p \equiv 1 \) (mod \( k \)).

It would be interesting to know if the bound \( (\delta - 1)^4 \) is anywhere near best possible. For \( k = 3, 4, 5 \) the Theorem implies that two \( k \)th powers suffice as soon as \( q > 16, 81, 256 \), respectively, whereas the largest prime fields requiring three \( k \)th powers have 7, 41, 101 elements, respectively. These computations, as well as the above Theorem in the prime-field case, were noted in [6] and [7].

For \( k < 3 \) the Theorem is not new. Nagell [4] showed that the field with seven elements is the only prime field containing elements which are not sums of two cubes. A different proof, based on a theorem of Vosper, appears in [6]. There is also an older proof due to Skolem [5], based on a result of Hurwitz [1]. For arbitrary finite fields \( F \) (not necessarily prime), John G. Thompson
proved (1975; unpublished) by an argument involving group characters that two cubes suffice provided $F$ has more than 25 elements.

References


Department of Mathematics, Queens University, Kingston, Ontario, Canada