PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 65, Number 1, July 1977

# 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 kth powers.* (*In particular, the conclusion holds if $q > (k-1)^4$, since $k \geqslant \delta$.*)

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, $N(b) \geqslant 0$; 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 $|N(b) - q| \leqslant (\delta - 1)^2\sqrt{q}$. In particular, $N(b) - q \geqslant -(\delta - 1)^2\sqrt{q}$, so that $N(b) > \sqrt{q}\ (\sqrt{q} - (\delta - 1)^2)$. 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, $p \equiv 1 \pmod{k}$.

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 $k \leqslant 3$ 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

Received by the editors September 21, 1976.
*AMS (MOS) subject classifications* (1970). Primary 12C15; Secondary 14G15.

proved (1975; unpublished) by an argument involving group characters that two cubes suffice provided $F$ has more than 25 elements.

## References

1. A. Hurwitz, *Über die Kongruenz* $ax^e + by^e + cz^e \equiv 0 \pmod p$, J. Reine Angew. Math. **136** (1909), 272–292.

2. J.-R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseignement Math. **19** (1973), 1–117. MR **48** #6065.

3. I. Kaplansky, Private communications, October 7, 1975 and August 25, 1976.

4. T. Nagell, *On the solvability of some congruences*, Norske Vid. Selsk. Forh. Trondheim **27** (1954), 1–5. MR **16**, 220.

5. Th. Skolem, *Unlösbarkeit von Gleichungen, deren entsprechende Kogruenz für jeden Modul lösbar ist*, Avh. Norske Vid.-Akad. Oslo I **1942**, No. 4, 28 pp. MR **8**, 7.

6. C. Small, *Waring's problem* mod $n$, Amer. Math. Monthly **84** (1977), 12–25.

7. ———, *Solution of Waring's problem* mod $n$, Amer. Math. Monthly **84** (1977), 356–359.

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