BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 6, November 1973

ADDITIVE GROUP THEORY—A PROGRESS REPORT

BY HENRY MANN

The first theorem in additive group theory was proved by Cauchy [2] in 1813.

THEOREM OF CAUCHY. *If A and B are residues* mod p *and* $A + B = \{x : x = a + b, a \in A, b \in B\}$ *then either* $A + B = G$ *or*

$$|A + B| \geqq |A| + |B| - 1. \tag{1}$$

(*Here $|S|$ denotes the cardinal of the set S.*)

This theorem was rediscovered by Davenport [5], [6] and is now known as [21] the Cauchy-Davenport theorem. Cauchy used it to show that every residue mod (p) is a sum of two squares i.e. the congruence

$$x^2 + y^2 \equiv r\,(p) \tag{2}$$

is solvable for every r. One easily obtains this result by setting $A = B = \{x : x \equiv a^2(p)\}$. We then have $|A| = |B| = (p + 1)/2$ and (2) follows from (1). Applying the C.-D. theorem to the representation of residues by sums of kth powers one may without loss of generality restrict k to divisors of $(p - 1)$. The C.-D. theorem then gives the result that every residue is a sum of not more than k kth powers. A considerable improvement is possible if one excludes the value $k = (p - 1)/2$. G. A. Vosper [30], [31], [21] refined the C.-D. theorem by completely characterizing those pairs A, B for which

$$|A + B| = |A| + |B| - 1.$$

Using Vosper's result one can show [4], [21]: If $a_1, \ldots, a_n$ are non-0 residues mod p and if $n \geqq (k + 1)/2$ then the congruence

$$a_1x_1^k + \cdots + a_nx_n^k \equiv r\,(p) \tag{3}$$

is solvable for every r provided that $k < (p - 1)/2$.

This result was extended to finite fields of order $q = p^d$ by Tietäväinen [29] under the assumptions $k < (q - 1)/2$, $(q - 1)/k \not| p^v - 1$ for $0 < v < d$. Tietäväinen's proof requires a result of Kempermann [13] on

---

An address delivered before the Annual Meeting of the Society in Dallas, Texas on January 26, 1973 by invitation of the Committee to Select Hour Speakers for Annual and Summer Meetings; received by the editors April 27, 1973.

AMS(MOS) subject classifications (1970). Primary 20F50, 05A05 22A99.

Key words and phrases. Elementary group theory, combinatorial mathematics, additive group theory.