MATHEMATICS OF COMPUTATION, VOLUME 27, NUMBER 121, JANUARY, 1973

Numerical Results for Waring's Problem in GF[q, x]

By William A. Webb

Abstract. Let p be a prime and let K and A_i denote polynomials whose coefficients are elements of the finite field with p elements. Problems concerning the expression of an arbitrary polynomial K as sums of a small number of squares or cubes of polynomials A_i are discussed. In the problems treated the degrees of the A_i are restricted to be as small as possible. In particular, it is shown that at least five cubes are necessary and that three squares seem to suffice in all but one special case.

1. Introduction. Let p be a prime, q a power of p, and let GF[q, x] denote the ring of polynomials having coefficients in the finite field of q elements. Waring's problem in GF[q, x] is essentially the problem of solving the equation

$$K = A_1^k + A_2^k + \cdots + A_s^k$$

for all $K \in \mathrm{GF}[q, x]$, where $A_i \in \mathrm{GF}[q, x]$ and s is fixed, depending only on k.

The general Waring's problem has been considered by Paley [8] and Webb [9], while the case of sums of squares ($k = 2$) has been extensively studied by Carlitz ([1], [2], [3], [4]), Cohen ([5], [6]) and Leahey [7].

There are actually many possible versions of Waring's problem, depending on the conditions placed on the A_i. The most important condition appears to be whether we restrict the degree of the A_i. The version in which the degree of A_i^k is required to be at most the degree of K (or as close as possible) in many ways is the most natural (see [9]), the most difficult, and the most interesting computationally. Although there are still many possible versions of Waring's problem, we will consider the following two equations.

$$K = A_1^k + A_2^k + \cdots + A_s^k : \deg A_i \leqq \left[\frac{\deg K - 1}{k}\right] + 1. \tag{1.1}$$

The condition on the degree of the A_i is merely that they are as small as possible.

$$K = \delta_1 A_1^k + \cdots + \delta_s A_s^k : \deg K = nk, \deg A_i = n, \delta_i \in \mathrm{GF}(q), \delta_i \neq 0; \tag{1.2}$$

also the A_i must be primary (having leading coefficient of 1) and $\sum \delta_i = \operatorname{sgn} K$, where $\operatorname{sgn} K$ denotes the leading coefficient of K. The solution of (1.2) in general implies the solution of (1.1) by taking the δ_i to be kth powers of GF(q).

For a given k, it is known that the above equations are solvable for a fixed s, but it is not known what the smallest value of s is for which they are solvable. In this paper, we give some numerical results which suggest what the best value for s is, if $k = 2$, or 3.

Received March 13, 1972.

AMS (MOS) subject classifications (1970). Primary 10J05, 12C05.

Key words and phrases. Sums of squares, polynomials over finite fields, Waring's problem.

There is the further complication that we could ask for the smallest value of s, for which (1.1) and (1.2) are solvable for all K and all $q = p^\gamma$, or we insist that (1.1) and (1.2) be solvable only for K of sufficiently large degree, and/or for p sufficiently large. It should be noted that, if $k = 2$, it is clearly necessary to assume $p \neq 2$, and, if $k = 3$, that $p > 3$. Although the corresponding questions concerning Waring's problem for the rational integers yield very different values for s, it appears quite possible that over GF[q, x] the values of s may be equal most of the time. Hence, we define the following numbers.

$g(k)$ = minimum s for which (1.1) is solvable for all K and all $p > k$.

$\bar{g}(k)$ = minimum s for which (1.2) is solvable for all K, all choices of the δ_i, and all $p > k$.

Generally, we should expect the largest necessary value of s will occur when degree K is small, and q is small. Thus, we consider only $q = p$ where p will be a small prime, and degree $K \leqq k$, or deg $K \leqq 2k$.

2. Sums of Squares. We first prove a theorem which shows that both $g(2)$ and $\bar{g}(2)$ are at least 3. Our result is an immediate consequence of the following theorem of Cohen [5, Theorem 10].

THEOREM 2.1. *If* deg $K = 2n$, deg $A \leqq n$, deg $B \leqq n$, *then the number of solutions of* $K = A^2 + B^2$ *is*

$$(q-1) \sum_{D \mid K;\ \deg D = n}{}' 1 \quad \text{if } p \equiv 1 \pmod 4, \tag{2.1}$$

$$(q+1) \sum_{j=0}^{2n} (-1)^j \sum_{D \mid K;\ \deg D = j}{}' 1 \quad \text{if } p \equiv 3 \pmod 4, \tag{2.2}$$

where $\sum'$ *denotes a sum over primary polynomials.*

THEOREM 2.2. *If* deg $K = 2n$, deg $A \leqq n$, deg $B \leqq n$, *then* $K = A^2 + B^2$ *has a solution if and only if*

(i) *K is divisible by some polynomial of degree n—if $p \equiv 1 \pmod 4$.*

(ii) *Every irreducible polynomial of odd degree which divides K appears in the factorization of K to an even power—if $p \equiv 3 \pmod 4$.*

Proof. (i) follows trivially from (2.1).

(ii) follows from (2.2) since $K = \alpha P_1^{a_1} \cdots P_r^{a_r}$ implies

$$\sum_{j=0}^{2n} (-1)^j \sum_{D \mid K;\ \deg D = j}{}' 1 = \prod_{P_i \mid K;\ \deg P_i \text{ even}} \left(\sum_{j=0}^{a_i} 1 \right) \prod_{P_i \mid K;\ \deg P_i \text{ odd}} \left(\sum_{j=0}^{a_i} (-1)^j \right).$$

Note that if $p \equiv 3 \pmod 4$ the conditions on the solvability of $K = A^2 + B^2$ are the same even if no restriction is placed on the degrees of A and B, while if $p \equiv 1 \pmod 4$ the results are different [7].

We also note that Theorem 13 of [5] implies both (1.1) and (1.2) have solutions for $k = 2$ if $s = 4$. Thus, $3 \leqq g(2) \leqq 4$ and $3 \leqq \bar{g}(2) \leqq 4$.

In what follows in this section, when we refer to Eqs. (1.1) and (1.2), we will assume $k = 2$ and $s = 3$. We conjecture that both equations are solvable, with one exception.

The exception is that (1.1) is in general not solvable in GF[3, x]. This exception is not too surprising since the sum of 3 nonzero squares in GF(3) must be zero making this a rather special case. The following result was established by generating all possible sums of squares of 3 polynomials of degree $\leqq 2$.

THEOREM 2.3. *There are exactly eight polynomials K of degree $\leqq 4$, for which* (1.1) *is unsolvable in* GF[3, x], $k = 2$, $s = 3$; *namely:* $x^3 + 2x + 1$, $2x^3 + x + 1$, $x^4 + x + 1$, $x^4 + 2x + 1$, $x^4 + x^3 + 1$, $x^4 + 2x^3 + 1$, $x^4 + 2x^3 + x$ *and* $x^4 + x^3 + 2x$.

It would be interesting to know whether there are polynomials K of arbitrarily high degree for which (1.1) is unsolvable in GF[3, x], or if (1.1) is always solvable if deg K is sufficiently large.

It appears that for $p \neq 3$, (1.1) is solvable in GF[p, x] for all K, and that the number of solutions grows quite rapidly. For example, (1.1) is solvable for all K such that degree $K \leqq 2$ in both GF[5, x] and GF[7, x]. In GF[7, x], every such K is expressible in the form (1.1) in at least 42 ways (counting different orderings).

It also appears that (1.2) is always solvable. In the case where all $\delta_i = 1$, we have

THEOREM 2.4. *If all $\delta_i = 1$, then Eq.* (1.2) *is solvable for all K of degree* 2 *having leading coefficient* 3 *in* GF[p, x] *for $p \leqq 83$, and for all K of degree* 4 *having leading coefficient* 3 *in* GF[5, x] *and* GF[7, x], $k = 2$, $s = 3$.

The case $p = 3$ is of course not included in the above theorem since $1 + 1 + 1 = 0$ in GF(3), and the leading coefficient of K must be nonzero. Although the average number of solutions of (1.2) grows larger as p increases, there are polynomials for which (1.2) has an essentially unique solution (not counting order). Some of these polynomials occur when p is large, for example in GF[83, x], although none occur in GF[79, x] or GF[73, x].

Cases other than all $\delta_i = 1$ have also been considered and, in all examples so far, (1.2) has been solvable for all K, with $s = 3$.

3. Sums of Cubes. Although the results in [9] imply that both (1.1) and (1.2) are solvable for every k and for a fixed s depending only on k, the bounds obtained for s are clearly far from the best possible.

In this section, we will treat sums of cubes, and so, from now on, we assume $k = 3$ in (1.1) and (1.2). The amount of computation necessary to obtain a reasonable amount of numerical evidence for the cases $k \geqq 4$ appears to be excessive.

THEOREM 3.1. *There are* 336 *polynomials K of degree* 3 *for which* (1.1) *is not solvable with $k = 3$, $s = 4$ in* GF[7, x]. *However,* (1.1) *is solvable for all K of degree* 3 *with $k = 3$, $s = 4$ in* GF[5, x].

Theorem 3.1 implies that $g(3) \geqq 5$, and it would seem reasonable to conjecture that $g(3)$ may equal 5, although the evidence for this is still scanty.

THEOREM 3.2. *There are* 14 *polynomials of the form $K = 6x^3 + ax^2 + bx + c$ for which* (1.2) *is unsolvable with $k = 3$, $s = 6$, and all $\delta_i = 1$ in* GF[7, x]. *However,* (1.2) *is solvable for all such K, $k = 3$, $s = 6$, all $\delta_i = 1$ in* GF[p, x] *for $p = 5, 11, 13$.*

Theorem 3.2 implies that $\bar{g}(3) \geqq 7$ and it appears likely that $g(3) = 7$. Cases other than all $\delta_i = 1$ have been considered, and, in these examples, (1.2) was solvable with $s = 6$. It is possible that (1.2) may be solvable with $s = 6$ with only finitely many exceptions.

Department of Pure and Applied Mathematics
Washington State University
Pullman, Washington 99163

1. L. CARLITZ, "On the representation of a polynomial in a Galois field as the sum of an even number of squares," *Trans. Amer. Math. Soc.*, v. 35, 1933, pp. 397–410.

2. L. CARLITZ, "On the representation of a polynomial in a Galois field as the sum of an odd number of squares," *Duke Math. J.*, v. 1, 1935, pp. 298–315.

3. L. CARLITZ, "Sums of squares of polynomials," *Duke Math. J.*, v. 3, 1937, pp. 1–7.

4. L. CARLITZ, "The singular series for sums of squares of polynomials," *Duke Math. J.*, v. 14, 1947, pp. 1105–1120. MR **9**, 337.

5. ECKFORD COHEN, "Sums of an even number of squares in GF[p^n, x]," *Duke Math. J.*, v. 14, 1947, pp. 251–267. MR **9**, 81.

6. ECKFORD COHEN, "Sums of an even number of squares in GF[p^n, x]. II," *Duke Math. J.*, v. 14, 1947, pp. 543–557. MR **9**, 176.

7. WILLIAM LEAHEY, "Sums of squares of polynomials with coefficients in a finite field," *Amer. Math. Monthly*, v. 74, 1967, pp. 816–819.

8. R. E. A. C. PALEY, "Theorems on polynomials in a Galois field," *Quart. J. Math.*, v. 4, 1933, pp. 52–63.

9. WILLIAM WEBB, "Waring's problem in GF[q, x]," *Acta Arith.* (To appear.)