and so for every $B > 2\sqrt{2/\log 2}$, we have that

$$V(x) = O\{\pi(x)\exp\{B\sqrt{\log\log x}\}\}.$$

This completes the proof.

References

[1] P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quart. Journ. Math. 6 (1935), pp. 205–213.

[2] H. L. Montgomery, *Zeros of L-functions*, Invent. Math. 8 (1969), pp. 346–354.

MATHEMATICAL INSTITUTE OF THE HUNGARIAN
ACADEMY OF SCIENCES, Budapest
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
Heslington, York

Received on 6. 12. 1971 (243)

ACTA ARITHMETICA
XXII (1973)

Waring's problem in GF[q, x]

by

William A. Webb (Pullman, Wash.)

I. Introduction. Throughout this paper $q = p^\gamma$, p a prime greater than k, γ a positive integer; GF(q) denotes the finite field of q elements; and GF[q, x] denotes the ring of polynomials over GF(q).

Waring's problem is that of expressing an element of an algebraic system as a fixed number of elements of that system which are kth powers. In [11] and [12] Schwarz and Tornheim deal with Waring's problem for systems including GF(q). In [10] Paley treats Waring's problem in GF[q, x], and in [2], [3], [4], [5], [6] and [7], Carlitz and Cohen consider several problems where the powers are restricted to squares.

In Paley's work, the degree of the summands is not restricted, while in the work of Carlitz and Cohen it is. This makes the problem quite different. Also, Carlitz and Cohen obtain formulas for the number of ways a polynomial in GF[q, x] may be written as a sum of squares, whereas Paley's method yields only existence.

In this paper we wish to show that $K = A_1^k + \ldots + A_s^k$ always has a solution for a fixed s and all K, where $\deg A_i^k = \deg K$. It is convenient to restrict the A_i to be primary (i.e. have leading coefficient of 1), so we will actually treat the following slightly more restrictive problem.

Let $R_s(K)$ denote the number of solutions of

$$K = \delta_1 A_1^k + \ldots + \delta_s A_s^k \tag{1}$$

where $\deg K = nk$; $\deg A_i = n$; A_i primary; $\delta_i \in \mathrm{GF}(q)$, $\delta_i \neq 0$, and δ_i a kth power in GF(q); and $\delta_1 + \ldots + \delta_s = \mathrm{signum}\, K$ (signum K = leading coefficients of K). (By [11] if $s \geqslant k$ it is possible to pick the δ_i to be kth powers and have $\delta_1 + \ldots + \delta_s = \mathrm{signum}\, K$. It is then possible to absorb the δ_i into the A_i^k to get a solution of the original problem.) We will obtain an asymptotic formula for $R_s(K)$ and in doing so show that $R_s(K) > 0$ for s of a certain magnitude.

Although there are many possible analogs of Waring's problem for GF[q, x], the above is one of the most natural and closest to Waring's problem for the rational integers. It should be noted that allowing the

degree of the summands to be greater than the degree of the element expressed in an additive problem in $GF[q, x]$ often makes the problem significantly different and much easier, as can be seen by comparing [8] and [9].

Actually the method we will use in this paper is quite general. That many other problems with different restrictions on the A_i can be handled similarly should be obvious. It should also be noted that this method can deal with problems where we use polynomial functions of the A_i other than just kth powers.

II. Preliminary results. The method we will use to solve Waring's problem in $GF[q, x]$ is an analog of the Hardy–Littlewood method. This type of Hardy–Littlewood method was first used by Hayes [9], where he treats the Goldbach three prime problem for $GF[q, x]$.

We will adopt the following notation used in the Hayes paper.

$GF(q, x)$ denotes the field of rational functions over $GF(q)$. If $A/B \in GF(q, x)$ and we define $v(A/B) = \deg B - \deg A$, then v is a valuation on $GF(q, x)$. The completion of $GF(q, x)$ with respect to this valuation, denoted $K_{1/x}$, consists of all elements of the form:

$$a = \sum_{j=t}^{\infty} a_j \left(\frac{1}{x}\right)^j$$

where t is any integer and $a_j \in GF(q)$. $v(a) = t$ and the related absolute value is $|a|_v = q^{-v(a)}$.

If we define $\delta(a, b) = |a-b|_v$, then δ is an ultra-metric on $K_{1/x}$. We let

$$\mathscr{V}_m(a) = \{t \in K_{1/x} : v(t-a) > m\}.$$

The $\mathscr{V}_m(a)$ are the open balls of $K_{1/x}$. They are also closed and have the property that whenever two balls intersect, one must be contained in the other.

We let $\mathscr{P}_j = \mathscr{V}_j(0)$, and $\mathscr{P}_0 = \mathscr{P}$. $\mathscr{P}$ is called the unit interval and is a compact topological group under addition. Hence, there is a Haar integral on $\mathscr{P}$ which we denote $\int d\varrho$. We then have

$$\int_{t \in \mathscr{P}_j} 1 \, d\varrho = q^{-j}.$$

Let λ be a fixed non-principal character on the additive group of $GF(q)$. If $a \in K_{1/x}$ and a is the coefficient of $1/x$ in the expansion of a, define $E_\lambda(a) = E(a) = \lambda(a)$. Then E is a character on the additive topological group $K_{1/x}$.

The following results concerning the character E may also be found in the paper by Hayes [9] (Theorems 3.6 and 3.7).

LEMMA 1. *If* $b \in \mathscr{P}$, $j \geqslant 0$ *and* $\mathscr{B} = \{t \in \mathscr{P} : v(t-b) > j\}$ *then*

$$\int_{\mathscr{B}} E(at)\, d\varrho = \begin{cases} q^{-j} E(ab) & \text{if} \quad v(a) > -j, \\ 0 & \text{otherwise.} \end{cases}$$

LEMMA 2. *If* $a \in \mathscr{P}$ *and* $n \geqslant 0$ *then*

$$\sum_{\deg B = n}{}' E(aB) = \begin{cases} q^n E(x^n a) & \text{if} \quad v(a) > n, \\ 0 & \text{otherwise} \end{cases}$$

(*where* $\sum'$ *will denote a summation over primary polynomials*).

We also have that $E(A/H) = E(B/H)$ if $A \equiv B (\mathrm{mod} H)$.

As in the usual Hardy–Littlewood method, the unit interval must be divided into small arcs. In order to do this for $\mathscr{P}$ we make the following

DEFINITION. If $G, H \in GF[q, x]$, we say G/H is *primordial with respect to* $2(k-1)n$ if

(i) $\deg G < \deg H$,

(ii) $(G, H) = 1$; (G, H) denotes the greatest common divisor of G and H,

(iii) H is primary,

(iv) $h = \deg H \leqslant (k-1)n$.

Subsets of $\mathscr{P}$ of the form

$$\mathscr{U}_{G/H} = \{t \in \mathscr{P} : v(t - G/H) > h + (k-1)n\}$$

are called *primordial subsets*, and the collection of all primordial subsets with respect to $2(k-1)n$ forms an open disjoint covering of $\mathscr{P}$ ([9], Theorem 4.3).

III. The Hardy-Littlewood method. In this section we develop an analog of the Hardy–Littlewood method.

Let

$$g(t) = \sum_{\deg A = n}{}' E(A^k t).$$

Then

$$\int_{\mathscr{P}} g(\delta_1 t) g(\delta_2 t) \dots g(\delta_s t) E(-Kt)\, d\varrho = \sum_{\deg A_1 = n}{}' \dots \sum_{\deg A_s = n}{}' \int_{\mathscr{P}} E\big((\delta_1 A_1^k + \delta_2 A_2^k + \dots + \delta_s A_s^k - K)t\big)\, d\varrho.$$

Now

$$v(\delta_1 A_1^k + \dots + \delta_s A_s^k - K) = -\deg(\delta_1 A_1^k + \dots + \delta_s A_s^k - K) > 0$$

if and only if $\delta_1 A_1^k + \dots + \delta_s A_s^k - K = 0$. Thus by Lemma 1 the above integral is 1 or 0 according as $\delta_1 A_1^k + \dots + \delta_s A_s^k$ is or is not equal to K.

Hence, the above expression counts the number of solutions of (1) and so

$$R_s(K) = \int_{\mathscr{P}} g(\delta_1 t)g(\delta_2 t)\dots g(\delta_s t)E(-Kt)d\varrho. \tag{2}$$

We now divide $\mathscr{P}$ into major and minor arcs as follows:

DEFINITION. $\mathscr{U}_{G/H}$ is a *major arc* if $\deg H = h < n$. $\mathscr{U}_{G/H}$ is a *minor arc* if $n \leqslant h \leqslant (k-1)n$.

IV. Contribution of the major arcs. Let $\mathscr{U}_{G/H}$ be a major arc and $t \in \mathscr{U}_{G/H}$. Thus $t = G/H + y$ where $v(y) > h+(k-1)n$. Let $v(y) = h+ +(k-1)n+\theta$, where $\theta > 0$.

Now as Q runs over all primary polynomials of degree $n-h$ and R runs over all polynomials of degree less than h (so R runs over a complete system of residues modulo H), $QH+R$ runs over all primary polynomials of degree n. Thus

$$g(t) = \sum_{\deg A=n}{}' E(A^k t) = \sum_{\deg R<h} \sum_{\deg Q=n-h}{}' E\big((QH+R)^k(G/H+y)\big)$$
$$= \sum_{\deg R<h} E(R^k G/H) \sum_{\deg Q=n-h}{}' E\big((QH+R)^k y\big)$$

since $E(B) = 1$ for any polynomial B. Also, $(QH+R)^k = (QH)^k + B$ where $v(B) > -n(k-1) - \deg R$ and so $v(By) > -n(k-1) - \deg R + h + (k-1)n + +\theta \geqslant 1+\theta \geqslant 2$. Therefore $E(By) = \lambda(0) = 1$, and so $E\big((QH+R)^k y\big) = E\big((QH)^k y\big)$. Hence

$$g(t) = \sum_{\deg R<h} E(R^k G/H) \sum_{\deg Q=n-h}{}' E(Q^k y_1). \tag{3}$$

Let

$$S_1 = \sum_{\deg Q=n-h}{}' E\big((QH)^k y\big) = \sum_{\deg Q=n-h}{}' E(Q^k y_1) \tag{4}$$

where $y_1 = H^k y$, $v(y_1) = h+(k-1)n+\theta-hk = (k-1)(n-h)+\theta$.

LEMMA 3. *Let $F(Q) = Q^k + B_1 Q^{k-1} + \dots + B_k$ be a polynomial in Q such that $\deg B_i Q^{k-i} < \deg Q^k$, and let $v(y) = (k-1)m+\theta$, $1 \leqslant \theta \leqslant m$. Then*

$$\sum_{\deg Q=m}{}' E\big(F(Q)y\big) = 0.$$

Proof. We use induction on k. If $k = 1$, $F(Q) = Q + B_1$ where $\deg B_1 < m$. Then

$$\sum_{\deg Q=m}{}' E\big((Q+B_1)y\big) = E(B_1 y) \sum_{\deg Q=m}{}' E(Qy)$$

where $1 \leqslant v(y) = \theta \leqslant m$. Thus $y \in \mathscr{P}$ and by Lemma 2

$$\sum_{\deg Q=m}{}' E(Qy) = 0.$$

Hence, the lemma is true for $k = 1$. Now assume the result is true for all positive integers less than k. Then, if

$$S = \sum_{\deg Q=m}{}' E\big(F(Q)y\big),$$

$$|S|^2 = S\bar{S} = \sum_{\deg Q_1=m}{}' \sum_{\deg Q_2=m}{}' E\Big(\big(F(Q_1)-F(Q_2)\big)y\Big) \tag{5}$$
$$= \sum_{\deg M<m} \sum_{\deg Q=m}{}' E\Big(\big(F(Q+M)-F(Q)\big)y\Big)$$

since $Q+M$ runs over all primary polynomials of degree m as M runs over all polynomials of degree less than m.

Now

$$F(Q+M)-F(Q) = (Q+M)^k + B_1(Q+M)^{k-1} + \dots + B_k - \\ -(Q^k + B_1 Q^{k-1} + \dots + B_k) \\ = kQ^{k-1}M + C_1 Q^{k-2} + \dots + C_{k-1}$$

where $\deg C_i Q^{k-i-1} < \deg Q^{k-1}M$ and $M | C_i$ for $1 \leqslant i \leqslant k-1$.

Therefore

$$\big(F(Q+M)-F(Q)\big)y = F_1(Q)y'$$

where $y' = kMy$ and

$$F_1(Q) = Q^{k-1} + B_1' Q^{k-2} + \dots + B_{k-1}'$$

and

$$\deg B_i Q^{k-i-1} = \deg(Q^{k-i-1}C_i/M) < \deg Q^{k-1}.$$

Also,

$$v(y') = v(y) - \deg M = (k-1)m + \theta - \deg M.$$

Now if $\deg M \geqslant \theta$

$$(k-2)m + \theta < v(y') \leqslant (k-1)m,$$

i.e.

$$v(y') = (k-2)m + \theta' \quad \text{where} \quad 1 \leqslant \theta' \leqslant m.$$

Therefore

$$\sum_{\deg Q=m}{}' E\big(F_1(Q)y'\big)$$

satisfies all the conditions of the lemma and degree of F_1 is less than k, and so the sum is zero by the induction hypothesis. Thus by (5)

$$|S^2| = \sum_{\deg M<0} \sum_{\deg Q=m}' E\big(F_1(Q)y'\big). \tag{6}$$

Also,

$$\begin{aligned}\nu\big((B_1'Q^{k-2}+\ldots+B_{k-1}')y'\big) &> -(k-1)m+\nu(y)\\ &= -(k-1)m+(k-1)m+\theta-\deg M\\ &= \theta-\deg M \geqslant 1 \quad \text{for } \deg M<\theta.\end{aligned}$$

Therefore

$$E\big((B_1'Q^{k-2}+\ldots+B_{k-1}')y'\big) = 1$$

and so

$$E\big(F_1(Q)y'\big) = E(Q^{k-1}y').$$

Now, since

$$\nu(Q^{k-1}y') = -(k-1)m+(k-1)m+\theta-\deg M = \theta-\deg M,$$

$$E(Q^{k-1}y') = \begin{cases} E(x^{(k-1)m}y') & \text{if } \deg M = \theta-1,\\ 1 & \text{if } \deg M<\theta-1.\end{cases} \tag{7}$$

By (6) and (7)

$$\begin{aligned}|S|^2 &= \Big(\sum_{\deg M<\theta-1}+\sum_{\deg M=\theta-1}\Big)\sum_{\deg Q=m}' E(Q^{k-1}kMy)\\ &= \sum_{\deg M<\theta-1} q^m + \sum_{\deg M=\theta-1} q^m\lambda(\alpha\beta)\end{aligned} \tag{8}$$

where $\alpha = \operatorname{signum} M$, $\beta = \operatorname{signum} ky$ (here, signum indicates the coefficient of the highest power of x appearing). Now

$$\sum_{\deg M=\theta-1}\lambda(\alpha\beta) = \sum_{\substack{\alpha\in GF(q)\\ \alpha\neq 0}}\sum_{\deg M=\theta-1}'\lambda(\alpha\beta) = q^{\theta-1}\sum_{\substack{\alpha\in GF(q)\\ \alpha\neq 0}}\lambda(\alpha\beta) = -q^{\theta-1}$$

since $\sum_{\substack{\gamma\in GF(q)\\ \gamma\neq 0}}\lambda(\gamma) = -1$ and $\alpha\beta$ runs over all nonzero elements of $GF(q)$ as α does. (β cannot be zero since it is the coefficient of a power of x which actually appears.)

Hence, from (8) we get

$$|S|^2 = q^m\sum_{\deg M<\theta-1} 1+q^m(-q^{\theta-1}) = q^{m+\theta-1}-q^{m+\theta-1} = 0. \tag{9}$$

Since $|S|^2 = 0$, $S = 0$ which completes the proof of the lemma.

Applying Lemma 3 to S_1, we have

$$S_1 = 0 \quad \text{if} \quad \theta \leqslant n-h, \text{ that is, if } \nu(y) \leqslant kn. \tag{10}$$

If $\nu(y) > kn$, $E\big((QH)^k y\big) = E(x^{kn}y)$ since $\nu\big((QH)^k y\big) \geqslant 1$ and QH is monic. Therefore

$$S_1 = \sum_{\deg Q=n-h} E(x^{kn}y) = q^{n-h}E(x^{kn}y).$$

Combining the results for S_1 we get

$$S_1 = \begin{cases} 0 & \text{if } \nu(y) \leqslant kn,\\ q^{n-h}E(x^{nk}y) & \text{if } \nu(y) > kn.\end{cases} \tag{11}$$

Now by (3), (4) and (11) we have

$$g(\delta t) = \begin{cases} 0 & \text{if } \nu(y) \leqslant kn,\\ q^{n-h}E(x^{nk}\delta y)\sum_{\deg R<h} E(\delta R^k G/H) & \text{if } \nu(y) > kn.\end{cases} \tag{12}$$

Note that (12) holds for all $t \in \mathfrak{A}_{G/H}$ where $\mathfrak{A}_{G/H}$ is a major arc.

Now by (12)

$$\begin{aligned}&\int_{\mathfrak{A}_{G/H}} g(\delta_1 t)g(\delta_2 t)\ldots g(\delta_s t)E(-Kt)\,d\varrho\\ &= q^{(n-h)s}\sum_{\deg R_1<h}\ldots\sum_{\deg R_s<h} E(\delta_1 R_1^k G/H)\ldots E(\delta_s R_s^k G/H)E(-KG/H)\times\\ &\qquad\times\int_{\{t=G/H+y:\,\nu(y)<kn\}} E(\delta_1 y x^{kn})\ldots E(\delta_s y x^{kn})E(-Ky)\,d\varrho.\end{aligned} \tag{13}$$

Since $\delta_1+\ldots+\delta_s = \operatorname{signum} K$, $\deg\big((\delta_1+\ldots+\delta_s)x^{kn}-K\big) < nk$, and so

$$\nu\big(\big((\delta_1+\ldots+\delta_s)x^{kn}-K\big)y\big) > 1, \quad E\big(\big((\delta_1+\ldots+\delta_s)x^{kn}-K\big)y\big) = 1$$

and hence

$$\int_{\{t=G/H+y:\,\nu(y)<kn\}} E\big(\big((\delta_1+\ldots+\delta_s)x^{kn}-K\big)y\big) = q^{-kn}.$$

Therefore (13) becomes

$$\begin{aligned}&\int_{\mathfrak{A}_{G/H}} g(\delta_1 t)\ldots g(\delta_s t)E(-Kt)\,d\varrho\\ &= q^{(n-h)s-kn}\sum_{\deg R_1<h}\ldots\sum_{\deg R_s<h} E(\delta_1 R_1^k G/H)\ldots E(\delta_s R_s^k G/H)E(-KG/H).\end{aligned} \tag{14}$$

Let

$$S(G,H)=\sum_{\deg R<h}E(R^kG/H) \tag{15}$$

and

$$A(H)=q^{-hs}\sum_{(G,H)=1}S(\delta_1G,H)\dots S(\delta_sG,H)E(-KG/H) \tag{16}$$

where the sum is over a reduced residue system modulo H.

Also, let

$$\mathscr{S}=\sum_{H}{}'A(H) \tag{17}$$

where the sum is over all primary polynomials.

We will need the following two results:

LEMMA 4. *If* $s\geqslant 2k+1$

$$\sum_{\deg H\geqslant m}{}'A(H)=O(q^{-m/k}). \tag{18}$$

THEOREM 1. $\mathscr{S}\geqslant C_0>0$ *where* C_0 *is a constant.*

The proofs of these results follow along the same lines as the proofs of the corresponding statements about the rational integers [1], with occasional modifications, and will be omitted.

V. Contribution of the minor arcs. Let $\mathscr{U}_{G/H}$ be a minor arc and let $t\in\mathscr{U}_{G/H}$. Thus $t=G/H+y$ where $\nu(y)>h+(k-1)n$ and $h=\deg H\geqslant n$.

Now

$$g(t)=\sum_{\deg A=n}{}'E\big(A^k(G/H+y)\big)$$

but $\nu(A^ky)=-kn+\nu(y)>-kn+(k-1)n+h\geqslant 0$, so $E(A^ky)=E(x^{kn}y)$. Therefore

$$g(t)=E(x^{kn}y)\sum_{\deg A=n}{}'E(A^kG/H). \tag{19}$$

Let

$$S=S(n;G,H)=\sum_{\deg A=n}{}'E(A^kG/H). \tag{20}$$

Although $S(n;G,H)$ is similar to $S(G,H)$, the sum is no longer over a complete system (mod H).

LEMMA 5. *Given any* $\varepsilon>0$

$$S(n;G,H)=O(q^{n\left(1-\frac{1}{2^{k-1}}\right)+\varepsilon}).$$

Proof. Proceeding as in Lemma 3, we have,

$$|S|^2=\sum_{M_i}\sum_{A}{}'E\big((kA^{k-1}M_1+\dots)G/H\big)$$

where it is understood that the summation on A is always over all primary polynomials of degree n, and summations on M_i are over all polynomials of degree $<n$.

By Cauchy's inequality

$$|S|^4\leqslant\Big(\sum_{M_1}\Big)\sum_{M_1}\sum_{M_2}\sum_{A}{}'E\big(\big(k(k-1)A^{k-2}M_1M_2+\dots\big)G/H\big).$$

Continuing in this way we get

$$\begin{aligned}|S|^{2^{k-1}}&\leqslant(q^n)^{2^{k-3}}(q^{2n})^{2^{k-4}}\dots(q^{(k-2)n})^{2^0}\times\\ &\times\sum_{M_1}\dots\sum_{M_{k-1}}\sum_{A}{}'E\big(\big(k!AM_1M_2\dots M_{k-1}+P(M_1,\dots,M_{k-1})G/H\big)\big)\\ &\leqslant q^{n(2^{k-1}-k)}\sum_{M_1}\dots\sum_{M_{k-1}}\Big|\sum_{A}{}'E\big((k!AM_1\dots M_{k-1})G/H\big)\Big|\end{aligned} \tag{21}$$

where $P(M_1,\dots,M_{k-1})$ is a polynomial in $M_1,\dots,M_{k-1}$.

Let

$$G^*\equiv k!\,M_1\dots M_{k-1}G(\bmod H)$$

and $\deg G^*<\deg H$. By Lemma 2

$$\Big|\sum_{\deg A=n}{}'E(AG^*/H)\Big|=\begin{cases}q^n & \text{if}\quad \nu(G^*/H)>n,\\ 0 & \text{otherwise.}\end{cases} \tag{22}$$

Now $\nu(G^*/H)>n$ if and only if $\deg G^*<h-n$.

Let r be the number of $(k-1)$-tuples $(M_1,\dots,M_{k-1})$ such that

$$M_1\dots M_{k-1}\equiv(k!G)^{-1}G^*(\bmod H)$$

where $\deg G^*<h-n$. Clearly $r\leqslant q^{h-n}r^*$ where

$$r^*=\max_{\deg T\leqslant h}\big(\text{number of solutions of } M_1\dots M_{k-1}\equiv T(\bmod H)\big).$$

Now $M_1\dots M_{k-1}\equiv T(\bmod H)$ if and only if

$$M_1\dots M_{k-1}=T+XH. \tag{23}$$

Since $\deg M_1\dots M_{k-1}\leqslant(k-1)(n-1)$, $\deg X\leqslant(k-1)(n-1)-h$.

Hence, there are at most $q^{(k-1)(n-1)-h+1}$ different X possible in (23).

The number of solutions in $M_1, \dots, M_{k-1}$ of equation (23) is clearly less than $d(T+XH)^{k-1}$, where $d(B)$ denotes the number of divisors of B. But for any $\varepsilon > 0$,

$$d(T+XH) = O(|T+XH|^{\varepsilon})$$

just as for real numbers. Hence

$$d(T+XH) = O(q^{n\varepsilon})$$

and so

$$r^* = O(q^{(k-1)(n-1)-h+1} q^{n\varepsilon}).$$

Hence

$$r = O(q^{(k-2+\varepsilon)n}). \tag{24}$$

Thus by (21), (22) and (24)

$$|S|^{2^{k-1}} = O(q^{n(2^{k-1}-k)} q^n q^{(k-2+\varepsilon)n}) = O(q^{n(2^{k-1}-1+\varepsilon)})$$

which proves the lemma.

VI. Principal results. We are ready to prove:

THEOREM 2. *If $s \geqslant k2^k$ then*

$$|R_s(K) - \mathscr{S} q^{n(s-k)}| = O(q^{n(s-k)-n/k}). \tag{25}$$

Proof. By (2)

$$\begin{aligned} R_s(K) &= \int_{\mathscr{E}} g(\delta_1 t) \dots g(\delta_s t)\, E(-Kt)\, d\varrho \\ &= \sum_{\substack{G/H \text{ primordial} \\ \text{with respect to } 2(k-1)n}} \int_{\mathscr{U}_{G/H}} g(\delta_1 t) \dots g(\delta_s t) E(-Kt)\, d\varrho \\ &= \sum_{\deg H \leqslant (k-1)n}{}' \sum_{(G,H)=1} \int_{\mathscr{U}_{G/H}} g(\delta_1 t) \dots g(\delta_s t) E(-Kt)\, d\varrho \\ &= \sum_{\deg H < n}{}' \sum_{(G,H)=1} \int_{\mathscr{U}_{G/H}} g(\delta_1 t) \dots g(\delta_s t) E(-Kt)\, d\varrho + \\ &\quad + \sum_{n \leqslant \deg H \leqslant (k-1)n}{}' \sum_{(G,H)=1} \int_{\mathscr{U}_{G/H}} g(\delta_1 t) \dots g(\delta_s t) E(-Kt)\, d\varrho \\ &= S_1 + S_2'. \end{aligned} \tag{26}$$

By (14), (15), (16), (17) and (18)

$$\begin{aligned} S_1 &= q^{ns-kn} \sum_{\deg H < n}{}' A(H) = q^{n(s-k)} \Big\{ \mathscr{S} - \sum_{\deg H \geqslant n}{}' A(H) \Big\} \\ &= q^{n(s-k)} \mathscr{S} + O(q^{n(s-k)-n/k}). \end{aligned} \tag{27}$$

By Lemma 5 and (19)

$$\begin{aligned} S_2 &= \sum_{n \leqslant \deg H \leqslant (k-1)n}{}' \sum_{(G,H)=1} \int_{\mathscr{U}_{G/H}} g(\delta_1 t) \dots g(\delta_s t) E(-Kt)\, d\varrho \\ &= O\Big(\sum_{n \leqslant \deg H \leqslant (k-1)n}{}' \sum_{(G,H)=1} q^{ns\left(1-\frac{1}{2^{k-1}}+\varepsilon\right)} q^{-h-(k-1)n} \Big) \\ &= O\Big(\sum_{h=n}^{(k-1)n} (q^{2h} - q^{2h-1})\, q^{ns\left(1-\frac{1}{2^{k-1}}+\varepsilon\right)-h-(k-1)n} \Big) \\ &= O(q^{ns\left(1-\frac{1}{2^{k-1}}+\varepsilon\right)}) = O(q^{n(s-k)-n/k}) \end{aligned} \tag{28}$$

for $s \geqslant k2^k$. We have also used the fact that the number of primordial G/H with $\deg H = h$, is $q^{2h} - q^{2h-1}$, which may be found in [9].

The theorem now follows from (26), (27) and (28).

COROLLARY 1. *If $s \geqslant k2^k$, there exists a constant n_0 such that if $n \geqslant n_0$, $R_s(K) > 0$.*

Proof. This follows immediately from Theorems 1 and 2.

VII. Sums of squares. If $k = 2$, we use a primordial subdivision with respect to $2n$, which means that only polynomials H of degree $h \leqslant n$ appear in the subdivision, and so there are no minor arcs (see below). Hence, the results of Sections IV and VI lead to the following exact formula for the number of representations of K as a sum of squares:

$$R_s(K) = q^{n(s-2)} \sum_{\deg H \leqslant n}{}' A(H). \tag{29}$$

In the previous work neighborhoods of G/H for $\deg H = n$ were put in the minor arcs for convenience in some of the lemmas. However, they could easily have been put in the major arcs, since trivially

$$g(t) = \sum_{\deg R < n} E(R^k G/H) E(H^k y) = E(x^{nk} y) S(G, H).$$

Also, the function $S(G, H)$ is the same as the function appearing in Section IV and not the one in Section V since R does run through a complete system (mod H). Thus there is no need for minor arcs in the case of squares.

The formula (29) is essentially the same as that obtained by Carlitz and Cohen in their papers.

VIII. Polynomials of small degree. In Section VI we found that all polynomials of degree $\geqslant n_0$ are expressible as a sum of kth powers. In this section we treat polynomials of degree $< n_0$.

In doing Waring's problem for the rational integers, it is trivial to

get all integers less than some bound as a sum of a fixed number of kth power—just use all ones. It is not as trivial in GF$[q, x]$.

THEOREM 3. *If* $\deg K = nk$, $n \geqslant 1$, *then* K *may be written in the form*

$$K = \delta_1 A_1^k + \ldots + \delta_s A_s^k \tag{30}$$

where $\delta_i \in \mathrm{GF}(q)$ *is a* k*-th power, provided* $s \geqslant nk^2 + k$.

Proof. We first obtain (30) with arbitrary elements of GF(q) and $s = nk+1$. Then since every element of GF(q) can be written as a sum of k or fewer kth powers [11], our result follows.

For the A_i we use polynomials of the form $x^n + x^m + \alpha x^{m-1}$ for $m = 1, 2, \ldots, n$ and $\alpha = 1, 2, \ldots, k$; where it is understood that when $m = n$, we use the polynomials $x^n + \alpha x^{n-1}$. Since $p > k$, the numbers $1, 2, \ldots, k$ are distinct elements of GF(q).

The kth power of $x^n + x^m + \alpha x^{m-1}$ contains only powers of x greater than $k(m-1)-1$. Thus our procedure will be the pick the δ's which are coefficients of the polynomials with $m = 1$, so as to make the two sides of (30) agree for all powers of x less than k. Then pick the δ's which are coefficients of the polynomials with $m = 2$, so as to make the next k powers of x agree, and so on. At each stage, none of the smaller powers of x are changed.

Thus it suffices to show that we can find $\delta_\alpha \in \mathrm{GF}(q)$, such that the coefficients of $x^{km-1}, x^{km-2}, \ldots, x^{km-k}$ in the expression

$$\sum_{\alpha=1}^{k} \delta_\alpha (x^n + x^m + \alpha x^{m-1})^k \tag{31}$$

are equal to any given set $\{\beta_1, \ldots, \beta_k\}$ of elements of GF(q).

The coefficient of x^{km-j} in $(x^n + x^m + \alpha x^{m-1})^k$ is:

$$F_j(\alpha) = \binom{k}{j}\alpha^j + h_1 \alpha^{j-1} + \ldots + h_{j-1}\alpha \tag{32}$$

where the h_i are elements of GF(q), not depending on α. Thus F_j is a polynomial depending only on j. Hence, the problem is now reduced to solving the system:

$$\sum_{\alpha=1}^{k} \delta_\alpha F_j(\alpha) = \beta_j, \quad j = 1, 2, \ldots, k, \tag{33}$$

for $\delta_1, \ldots, \delta_k$.

If all of the $\beta_j = 0$, take all the $\delta_i = 0$. If not all of the $\beta_j = 0$, then (33) has a solution provided

$$\begin{vmatrix} F_1(1) & F_1(2) \ldots F_1(k) \\ F_2(1) & \ldots\ldots F_2(k) \\ \ldots\ldots\ldots\ldots \\ F_k(1) & \ldots\ldots F_k(k) \end{vmatrix} \neq 0. \tag{34}$$

But the determinent in (34) is equal to

$$\begin{vmatrix} \binom{k}{1} & 0 & \ldots & 0 \\ * & \binom{k}{2} & \ldots & \\ \ldots & & & 0 \\ * & \ldots\ldots & * & \binom{k}{k} \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 & \ldots & k \\ 1^2 & 2^2 & \ldots & k^2 \\ \ldots & & & \\ 1^k & 2^k & \ldots & k^k \end{vmatrix}$$

$$= \binom{k}{1}\binom{k}{2}\ldots\binom{k}{k} 1\cdot 2 \cdot \ldots \cdot k \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & k \\ 1 & 2^2 & \ldots & k^2 \\ \ldots & & & \\ 1 & 2^{k-1} & \ldots & k^{k-1} \end{vmatrix} \neq 0$$

since the last factor is a Vandermonde determinant which is not zero since the elements $1, 2, \ldots, k$ are distinct in GF(q).

The above procedure provides δ_i and A_i which make all coefficients of powers of x less than nk in (30) equal. Now just add $(\mathrm{sgn}\, K - \delta_1 + \ldots + \delta_{nk})x^{nk}$ to the sum $\sum \delta_i A_i$, and (30) is now satisfied.

Together Theorems 2 and 3 give us the following result:

THEOREM 4. *If* $\deg K = nk$, $n \geqslant 1$, *then there exists a constant* $g(k)$ *depending only on* k, *such that if* $s \geqslant g(k)$ *then*

$$K = A_1^k + \ldots + A_s^k$$

is solvable with $\deg A_i = n$.

Remarks. (1) No attempt has been made here to make s as small as possible. Reducing the size of s and treating some related problems will be considered in a later paper.

(2) The condition that p must be greater than k is a necessary one in that if we allow $p \leqslant k$ there exist polynomials that cannot be written as the sum of any number of kth powers. Such examples are easily found if $k = p$. It may be possible however, to replace $p > k$ by a somewhat weaker condition.

(3) If $\deg K$ is not a multiple of k, it is clearly impossible to have $\deg K = \deg A_i^k$. The best we can do is to restrict $\deg A_i = \left[\frac{\deg K}{k}\right] + 1$. Our results can easily be carried through in this case. Also, we could allow $\deg A_i < n$ for some of the A_i. This will also be considered in a later paper.

(4) It is also possible to remove the condition that the δ_i be kth

powers. This requires modifications of some of the results leading to the estimate of the singular series $\mathfrak{S}$.

References

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Providence, Rhode Island, 1963.

[2] 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. 35 (1933), pp. 397–410.

[3] — *On the representation of a polynomial in a Galois field as the sum of an odd number of squares*, Duke Math. Journ. 1 (1935), pp. 298–315.

[4] — *Sums of squares of polynomials*, Duke Math. Journ. 3 (1937), pp. 1–7.

[5] — *The singular series for sums of squares of polynomials*, Duke Math. Journ. 14 (1947), pp. 1105–1120.

[6] Eckford Cohen, *Sums of an even number of squares in* GF$[p^n, x]$, Duke Math. Journ. 14 (1947), pp. 251–267.

[7] — *Sums of an even number of squares in* GF$[p^n, x]$, *II*, Duke Math. Journ. 14 (1947), pp. 543–557.

[8] D. R. Hayes, *A polynomial analog of the Goldbach conjecture*, Bull. Amer. Math. Soc. 69 (1963), pp. 115–116.

[9] — *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. 11 (1966), pp. 461–488.

[10] R. E. A. C. Paley, *Theorems on polynomials in a Galois field*, Quart. Journ. Math. 4 (1933), pp. 52–63.

[11] Stefan Schwarz, *On Waring's problem for finite fields*, Quart. Journ. Math. 19 (1948), pp. 123–128.

[12] L. Tornheim, *Sums of n^{th} powers in fields of prime characteristic*, Duke Math. Journ. 4 (1938), pp. 359–362.

WASHINGTON STATE UNIVERSITY

Received on 6. 12. 1971 (241)

ACTA ARITHMETICA
XXII (1973)

On a theorem of Bauer and some of its applications II

by

A. Schinzel (Warszawa)

The aim of this paper is to extend to polynomials in many variables the results of papers [1] and [6]. It is convenient to first restate these results in a concise form.

Let K be an algebraic number field, $|K|$ its degree, $\bar{K}$ its normal closure. We denote by $P(K)$ the set of primes which have in K at least one prime ideal factor of the first degree, and by $N_{K|Q}$ the norm from K to the rational field Q. We say that K *has property* (P) if for all but finitely many primes q and for every $\omega \in K$ $\left(\mathrm{ord}_q N_{K|Q}(\omega), |K|\right) = 1$ implies $q \in P(K)$. A field K is called *Bauerian* if for every Ω, $P(\Omega) \leqslant P(K)$ implies that Ω contains one of the conjugates of K ($P(\Omega) \leqslant P(K)$ means that $P(\Omega) \setminus P(K)$ is finite).

Several types of Bauerian fields have been described in [6], it happens so that all those fields have property (P). For some of them (cubic and quartic fields, solvable fields K with $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$) this has been established in the course of proof of Lemma 1 ([6]) for the others (certain solvable fields of degree p^2) it follows from Lemma 3 and Theorem 4 below. For normal fields the fact is obvious and for Bauerian fields of the types described in [4] (fields with property (N), fields $Q(\sqrt[n]{A})$ with $n \not\equiv 0 \bmod 8$) it is also true (see Corollary 2 and p. 230). In Theorem 5 I give a new class of Bauerian fields (normal extensions of quadratic fields) which need not have property (P).

Apart from the description of Bauerian fields, from Theorem 1 of [1] which has been generalized in [5] and various counterexamples the results of papers [1] and [6] can be summarized as follows.

Theorem A. *If K is a cyclic field or a solvable field such that $|K|$ is squarefree and $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$, $f(x) \in Q[x]$ and in every arithmetic progression there is an integer x such that*

$$f(x) = N_{K|Q}(\omega), \qquad \omega \in K,$$