Conspectus materiae tomi XXXV, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange / Address of the Editorial Board and of the exchange / Die Adresse der Schriftleitung und des Austausches / Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-01327-3   ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

'Easier' Waring problems for commutative rings

by

TED CHINBURG* (Cambridge, Mass.)

1. Introduction. Let R be a commutative ring with identity element and let k be a positive integer. Let $J(k, R)$ be the subring of R generated by its kth powers. If there is a non-negative integer v such that every f in $J(k, R)$ can be written in the form $\pm f_1^k \pm f_2^k \pm \ldots \pm f_v^k$ for some $f_1, \ldots, f_v$ in R, let $v(k, R)$ be the smallest such v. Otherwise, let $v(k, R) = \infty$. Let $V(k)$ be the supremum of $v(k, R)$ over all commutative rings with identity. As in [8], if p is a prime, then a number of the form $(p^{bc}-1)/(p^c-1)$ for some positive integers $b \geq 2$ and $c \geq 1$ is called a *p-power sum*. Call a prime q *exceptional* if it is a p-power sum for some prime p; otherwise, q is called *non-exceptional*. We will show that

$$V(k) \leq k^2(3\log k + 5.2) + 3[k\log(3k^2 - k)] + 3k + 4$$

if k is a non-exceptional prime. In [3] it is shown that $\sum \frac{1}{\sqrt{p_n}} < \infty$ as p_n ranges over the exceptional primes, where p_n is repeated if it is a q-power sum for more than one prime q. Thus $V(k)$ is finite for all non-exceptional primes, and 'almost all' primes are non-exceptional. This gives an affirmative answer to a question raised in [15] by J. R. Joly, who showed that $V(2) = 3$ and asked whether $V(k)$ is finite for some $k \geq 3$. In a later paper we will show that if $n \geq 2$ is an integer then $V(2^n) = \infty$.

The following related question was also raised in [15]. For n a positive integer, let $R[n]$ denote the polynomial ring $R[x_1, \ldots, x_n]$. It is shown in [15], Proposition 7.12, that $V(k) = \sup_{n \geq 1} v(k, Z[n])$. A natural question is hence whether $v(k, Z[n])$ is finite for $k \geq 3$ and $n \geq 1$. We will show that $v(k, Z[n])$ is always finite. Upper bounds will be produced which grow exponentially with n if k is composite, linearly with n if k is an exceptional prime, and which are independent of n if k is a non-exceptional

* NSF pre-doctoral fellow.

prime. Methods for obtaining sharper upper bounds are developed. These are illustrated in the appendix, in which the case $k = 4$ is considered.

In the course of obtaining these bounds, we will prove certain results concerning the structure of $J(k, Z[n])$. These results will provide, in particular, algorithms for determining whether $f \in Z[n]$ is in $J(k, Z[n])$, and for representing f as a (not necessarily minimal) sum $\pm f_1^k \pm f_2^k \pm \ldots \ldots \pm f_v^k$ if this is the case. Other related Waring problems are discussed in remarks throughout the text.

The author wishes to thank the referee and the editors of Acta Arithmetica for their assistance and patience during the preparation of this paper.

2. Upper bounds on $V(k)$ for non-exceptional primes. We first establish some notation. Unless otherwise specified, R will denote an arbitrary commutative ring with identity element. If A is a subset of R, let $H(k, R, A)$ denote the set of kth powers of elements of A. Let $J(k, R, A)$ be the additive subgroup of R generated by $H(k, R, A)$. Let $L(k, R, A)$ denote the set of sums of elements of $H(k, R, A)$, and let $L(k, R) = L(k, R, R)$. We will use p and q to denote primes, and n will denote a positive integer.

We adopt the conventions that the sum of an empty set of elements of R is 0, and that the zero ring has identity element 0. If there is a non-negative integer v such that every f in $A \cap J(k, R)$ equals $\pm f_1^k \pm f_2^k \pm \ldots \ldots \pm f_v^k$ for some $f_1, \ldots, f_v$ in R, then let $v(k, R, A)$ denote the smallest such v. Otherwise, let $v(k, R, A) = \infty$. Define $w(k, R, A)$ similarly for $A \cap L(k, R)$. Let $w(k, R) = w(k, R, R)$; customarily, $w(k, R)$ is called the 'harder' Waring constant of R. We will sometimes indicate how results concerning 'easier' Waring constants extend to cover 'harder' Waring constants.

We now make one basic observation. Suppose that I is an ideal of R, and that $a \in J(k, R)$. Then

$$v(k, R) \leqslant v(k, R/I) + v(k, R, I+a) \tag{1}$$

where $I + a = \{i + a;\ i \in I\}$. For if $f \in J(k, R)$, then

$$f - a = \sum_{i=1}^{v(k, R/I)} \pm f_i^k + b$$

for some $b \in I$ and some $f_i \in R$. Since $b + a \in (I+a) \cap J(k, R)$, (1) follows. Similarly, if $I \pm a \subseteq L(k, R)$ then

$$w(k, R) \leqslant w(k, R/I) + w(k, R, I+a). \tag{2}$$

Using only (1) and the results of [8] we can now show that $V(k)$ is finite if k is a non-exceptional prime. When referring to homomorphisms, we will always mean unitary homomorphisms.

THEOREM 1. *If k is a non-exceptional prime then*

$$V(k) \leqslant 1 + v(k, Z[x], \{kx\}) < \infty.$$

Proof. By (1),

$$v(k, R) \leqslant v(k, R/kR) + v(k, R, kR). \tag{3}$$

Since $(u \pm v)^k \equiv u^k \pm v^k \bmod kR$ if $u, v \in R$, $v(k, R/kR) \leqslant 1$. It follows from [8], Theorem 1, that $kx \in J(k, Z[x])$. If $u \in R$, consider the homomorphism $\Psi\colon Z[n] \to R$ induced by $x \to u$. It follows that

$$ku = \Psi(kx) \in \Psi\big(J(k, Z[x])\big) \subseteq J(k, R)$$

and that

$$v(k, R, kR) \leqslant v(k, Z[x], \{kx\}).$$

The theorem now results from (3).

As one consequence of Theorem 1, we have the following corollary from [15], Proposition 1.9.

COROLLARY. *If k is a non-exceptional prime, then the functor $R \to J(k, R)$ commutes over direct sums.*

We now consider explicit bounds on $V(k)$ when k is a non-exceptional prime. Parts (a) and (c) of the following lemma are contained in [15], Proposition 7.2. The proof of part (b) is left to the reader.

LEMMA 1. *If R is the direct sum $\bigoplus_{i=1}^{n} R_i$ of the rings R_i, then*

(a) (Joly) $v(k, R) = \sup_i v(k, R_i)$ *if k is odd;*

(b) $v(k, R) \leqslant \sup_{i,j} \left(1 - \frac{\delta_j^i}{2}\right)\big(v(k, R_i) + v(k, R_j)\big)$ *if k is even, where $\delta_i^i = 1$ and $\delta_j^i = 0$ if $i \neq j$;*

(c) (Joly) $w(k, R) = \sup_i w(k, R_i)$.

Define $v^*(k) = \inf_{d \in Z} v\big(k, Z, (d, \infty)\big)$. It is shown in [12] (p. 325–327) that $v(k, Z)$ is finite, so $v^*(k)$ is finite. Let ord_p denote the usual p-adic valuation on Z, so that $\mathrm{ord}_p(0) = \infty$ and $p^{\mathrm{ord}_p(a)} \| a$ if $0 \neq a \in Z$. To simplify notation, we supress indicating the dependence on k of the integers γ and γ_p now to be defined. Let

$$\gamma_p = \begin{cases} 1 & \text{if } p = k, \\ \mathrm{ord}_p(k) + 1 & \text{if } p \neq k \text{ and } p \text{ or } k \text{ is odd}, \\ \mathrm{ord}_p(k) + 2 & \text{if } p \neq k \text{ and } p = 2 \mid k \text{ and } k \neq 4, \\ 3 & \text{if } p = 2 \text{ and } k = 4. \end{cases}$$

$$\gamma = \prod_{p \leqslant k} p^{\gamma_p}.$$

LEMMA 2. *For all R and k,*

(a) $v(k, R) \leqslant v(k, R/k!\,R)+2^{k-1}$;

(b) $v(k, R) \leqslant v(k, R/\gamma R)+1+\min(2^{k-1}, kv^*(k))$;

(c) (Chen) $\min(2^{k-1}, kv^*(k)) = kv^*(k) \leqslant k^2(3\log k+5.2)$ *if* $k \geqslant 12$;

(d) (Rai) $\min(10v^*(10), 2^9) = 10v^*(10) \leqslant 300$ *and* $\min(11v^*(11), 2^{10}) = 11v^*(11) \leqslant 264$.

Proof. Let $a \in Z$ have image $\bar{a}$ in R under the homomorphism $Z \to R$. By (1),

$$v(k, R) \leqslant v(k, R/k!\,R)+v(k, R, k!\,R+\bar{a}). \tag{4}$$

In the standard identity (cf. [12], p. 325)

$$k!\,x+\frac{(k-1)\,k!}{2} = \sum_{i=0}^{k-1}\binom{k-1}{i}(x+i)^k(-1)^{k-1-i} \tag{5}$$

we have $\sum_{i=0}^{k-1}\binom{k-1}{i} = 2^{k-1}$. Then if $x \in R$ and $a = \frac{(k-1)\,k!}{2}$, it follows that $v(k, R, k!\,R+\bar{a}) \leqslant 2^{k-1}$. This and (4) prove (a).

Part (b) follows from (a) if $k \leqslant 2$, so suppose $k > 2$.

By (1),

$$v(k, R) \leqslant v(k, R/\gamma R)+v(k, R, \gamma R+\bar{a}). \tag{6}$$

Let b be a non-negative integer. By a standard application of Hensel's lemma, if $z \in R$ then there is a $w \in R$ such that

$$w^k \equiv 1+\gamma z \bmod 2^b k!\,R.$$

Hence

$$v(k, R, \gamma R+\bar{a}) \leqslant v(k, R, 2^b k!\,R+\bar{a}-1)+1. \tag{7}$$

Letting $b = 0$ and $\bar{a}-1 = (k-1)k!/2$, we have

$$\begin{aligned} v(k, R) &\leqslant v(k, R/\gamma R)+v(k, R, \gamma R+\bar{a}) \\ &\leqslant v(k, R/\gamma R)+v(k, R, k!\,R+\bar{a}-1)+1 \\ &\leqslant v(k, R/\gamma R)+2^{k-1}+1. \end{aligned}$$

If b is sufficiently large, then

$$v\left(k, Z, \binom{k-i}{i}(-1)^i 2^b\right) \leqslant v^*(k) \quad \text{for} \quad i = 1, \ldots, k-1.$$

Now multiplying (5) on both sides by 2^b and letting $a-1 = 2^{b-1}(k-1)k!$ shows that

$$v(k, R, 2^b k!\,R+\bar{a}-1) \leqslant kv^*(k).$$

Then

$$\begin{aligned} v(k, R) &\leqslant v(k, R/\gamma R)+v(k, R, \gamma R+\bar{a}) \\ &\leqslant v(k, R/\gamma R)+v(k, R, 2^b k!\,R+\bar{a}-1)+1 \\ &\leqslant v(k, R/\gamma R)+kv^*(k)+1 \end{aligned}$$

so (b) is proved.

The asymptotic 'harder' Waring constant of Z is defined to be $G(k) = \inf_{a \in Z} w(k, Z, (a, \infty))$. Clearly $v^*(k) \leqslant G(k)$. Part (c) now follows from bounds on $G(k)$ given by J. Chen in [7]. T. Rai has shown in [19] that $v(10, Z) \leqslant 30$ and $v(11, Z) \leqslant 24$, from which (d) follows.

THEOREM 2. *If k is a non-exceptional prime, then*

$$V(k) \leqslant k^2(3\log k+5.2)+3[k\log(3k^2-k)]+3k+4.$$

Proof. It is shown in [15] that $V(2) = 3$, so suppose $k > 2$. By Lemma 2(b), (c), (d) and Lemma 1(a),

$$\begin{aligned} v(k, R) &\leqslant v(k, R/\gamma R)+1+kv^*(k) \\ &\leqslant \sup_{p \leqslant k} v(k, R/pR)+1+k^2(3\log k+5.2). \end{aligned} \tag{8}$$

If $u, v \in R$ then $(u \pm v)^k \equiv u^k \pm v^k \bmod kR$, so $v(k, R/kR) \leqslant 1$. Since $kx \in J(k, Z[x])$ by the results of [8], it follows that $F_p[x] = J(k, F_p[x])$ if $p < k$, where F_p is the field with p elements. If now $z \in R/pR$, consider the homomorphism $\Psi_p\colon F_p[x] \to R/pR$ induced by $x \to z$. We conclude that $R/pR = J(k, R/pR)$ and that $v(k, R/pR) \leqslant v(k, F_p[x])$. It is shown in [16] that $v(k, F_p[x]) < 3k+3[k\log(3k^2-k)]+4$ if $p \nmid k$. The proof of the theorem is now completed by substituting these bounds on $v(k, R/pR)$ into (8).

Remark. The technique of Lemma 2 can be used to lower certain known bounds on other Waring constants. For example, suppose R is an algebra over a field of characteristic 0. It is shown in [15] that

$$w(k, R) \leqslant 2^{k-2}\left(1+w(k, R, \{-1\})\right). \tag{9}$$

Let b be a large positive integer, and note that every element of such an algebra is of the form $2^b k!\,x+2^{b-1}(k-1)k!$ for some $x \in R$. Then multiplying (5) by 2^b and bounding the number of summands on the right, we have

$$w(k, R) \leqslant G(k)\left[\frac{k+1}{2}\right]+v^*(k)\,w(k, R, \{-1\}). \tag{10}$$

Similarly,

$$w(k, R) \leqslant kv^*(k)\,w(k, R, \{-1\}). \tag{11}$$

From [7] and [19] we have that $v^*(k) \leqslant G(k) \leqslant k(3\log k+5.2)$ and $v^*(11) \leqslant 264$. Hence one of (10) or (11) improve (9) if $k \geqslant 11$.

3. Statement of bounds on $v(k, Z[n])$ and outline of the proofs. As mentioned in the introduction, it is shown in [15] that $V(k) = \sup_{n\geqslant 1} v(k, Z[n])$. If k is a non-exceptional prime, the bounds of Theorems 1 and 2 hold for $v(k, Z[n])$. We will show

THEOREM 3. *If k is an exceptional prime,*

(a) $v(k, Z[n]) \leqslant \big((k-2)^3+1\big)n+k+1+ \min\big(k^2(3\log k+5.2), 2^{k-1}\big)$ *if* $k>3$;

(b) $v(3, Z[n]) \leqslant 4n+5$;

(c) $v(k, Z[1]) \leqslant 3k+3[k\log(3k^2-k)]+4+ \min\big(k^2(3\log k+5.2), 2^{k-1}\big)$.

THEOREM 4. *If k is composite,*

(a) $v(k, Z[n]) \leqslant \exp\{(1+\varepsilon(k))n(\log k)^2/\log 2\} + n\exp\{(1+\varepsilon(k))2(\log k)^2/\log 2\}$

where $\varepsilon(k)$ is finite and $\varepsilon(k)\to 0$ as $k\to\infty$,

(b) $v(4, Z[n]) \leqslant 2(4^n-n)+34n+21$.

The first step towards proving these theorems is to reduce the consideration of $J(k, Z[n])$ and $v(k, Z[n])$ to that of $J(k, S_p[n])$ and $v(k, S_p[n])$ when p is a prime $\leqslant k$ and $S_p = Z/p^{\gamma_p}Z$.

In [8], the smallest positive integer $m(k)$ such that $m(k)Z[1] \subseteq J(k, Z[1])$ is computed. From [8], Theorem 1, it follows that $m(k)\,|\,\gamma$. Since $\gamma = \prod_{p\leqslant k} p^{\gamma_p}$, we have an exact sequence

$$0\to \gamma Z[n]\to J(k, Z[n])\to \bigoplus_{p\leqslant k} J(k, S_p[n])\to 0. \tag{12}$$

This shows that the structure of $J(k, Z[n])$ is determined by that of $J(k, S_p[n])$ for $p\leqslant k$. Similarly, Lemmas 2 and 1 show that upper bounds on $v(k, S_p[n])$ for $p\leqslant k$ will yield an upper bound on $v(k, Z[n])$.

We consider $J(k, S_p[n])$ and $v(k, S_p[n])$ when $p\nmid k$ in Section 4. In this case $S_p = F_p$. The method used involves first using [8] to determine whether there is a polynomial identity of the form

$$x \equiv \sum_i g_i(x)^k \tag{13}$$

in $F_p[x]$. If such an identity exists, it is shown that $J(k, F_p[n]) = F_p[n]$ and $v(k, F_p[n]) \leqslant v(k, F_p[1])$. Bounds on $v(k, F_p[n])$ then follow from known upper bounds on $v(k, F_p[1])$.

If no identity of the form (13) exists, then one constructs an identity of the form

$$(x_1^{p^b}-x_1)x_2+g_0(x_1) = \sum_{i=1}^{t} g_i(x_1, x_2)^k \tag{14}$$

in $F_p[x_1, x_2]$. From such an identity it follows that the ideal $I = \sum_{i=1}^{n}(x_i^{p^b}-x_i)F_p[n]$ is contained in $J(k, F_p[n])$, and that

$$v(k, F_p[n], I+h)\leqslant tn \quad \text{if} \quad h = \sum_{i=1}^{n} g_0(x_i).$$

Hence if $A = F_p[n]/I$, then

$$v(k, F_p[n]) \leqslant v(k, A)+v(k, F_p[n], I+h) \leqslant v(k, A)+tn.$$

If $\Phi\colon F_p[n]\to A$ is the quotient homomorphism, then $J(k, F_p[n]) = \Phi^{-1}(J(k, A))$. We are hence reduced to considering Waring problems for finite rings of the form $A = F_p[n]/I$.

Note that $pa = 0 = a^{p^b}-a$ if $a\in A$. By applying certain known structure theorems for rings A with these properties, one can bound $v(k, A)$ and determine the structure of $J(k, A)$. These results can then be lifted to $F_p[n]$, and in fact to any R such that $pR = \{0\}$.

In Section 5 we consider $J(k, S_p[n])$ and $v(k, S_p[n])$ when $p\,|\,k$. The case $p = k$ is very simple, since then $S_p = F_p$ and $f\to f^p$ is a homomorphism of $F_p[n]$ onto $J(p, F_p[n])$, so $v(p, F_p[n]) = 1$. Suppose now that $p\,|\,k$ and $p<k$. As in the case $p\nmid k$, one wishes to find polynomial identities which yield bounds on $v(k, S_p[n])$ as functions of $v(k, S_p[n]/I)$, where $S_p[n]/I$ is some finite quotient ring of $S_p[n]$. A major obstacle to achieving this is that in this case $S_p[n]/J(k, S_p[n])$ can be shown to be an infinite group. Hence there is no ideal I of $S_p[n]$ such that $S_p[n]/I$ is finite and $I\subseteq J(k, S_p[n])$.

The difficulty is resolved by considering the S_p-module

$$T^p = \sum_{i=0}^{\theta} p^{\theta-i} S_p[x_1^{p^i}, x_2^{p^i}, \ldots, x_n^{p^i}].$$

One first considers systems of polynomial identities in $S_p[x_1, x_2]$ satisfying certain conditions. These conditions depend on two integral parameters u and v, and the set of such identities is denoted by $F(u, v)$. One shows that given an element of $F(u, v)$ there exists an ideal I of $S_p[n]$ such that $S_p[n]/I$ is finite, $v(k, S_p[n]) \leqslant v(k, S_p[n]/I)+vn$ and $J(k, S_p[n]) = T^p\cap\Phi^{-1}(J(k, S_p[n]/I))$, where $\Phi\colon S_p[n]\to S_p[n]/I$ is the quotient homomorphism. The problem then becomes to construct an element of some $F(u, v)$, i.e. to find a system of identities of the required type, and to analyze $v(k, S_p[n]/I)$ and $J(k, S_p[n]/I)$.

The results of Sections 4 and 5 will be combined in Section 6 to prove the bounds on $v(k, Z[n])$ stated in Theorems 3 and 4. We will then summarize our results concerning the structure of $J(k, Z[n])$. We will also discuss the relation of $v(k, Z[n])$ to $v(k, R)$ as R ranges over finite Artin local rings which are homomorphic images of $Z[n]$.

4. The case $p \nmid k$. In this section we assume only that $p \nmid k$, without any restriction as to whether $p < k$ or $p > k$. By definition, $S_p = F_p$. As a typographical convenience, we will use F_m and $\mathrm{GF}(m)$ interchangably to denote the field with m elements when m is a power of p. If c is a positive integer, let c_p be the smallest divisor d of c such that $\left.\frac{p^c-1}{p^d-1}\right| k$.

PROPOSITION 1. *Suppose $p \nmid k$, $pR = \{0\}$ and $c = c_p$ for all positive integers c. Then $J(k, R) = R$ and*

(a) $v(k, R) \leqslant v(k, F_p[1]) \leqslant w(k, F_p[1])$;

(b) $w(k, R) \leqslant w(k, F_p[1])$;

(c) (Kubota) $w(k, F_p[1]) < 3k + 3[k\log(3k^2 - k)] + 4$;

(d) (Paley) *if $k = p^m + 1$ for some integer m,*

(i) $w(k, F_p[1]) \leqslant 5$ *if* $p = 2$,

(ii) $w(k, F_p[1]) \leqslant 6$ *if* $p > 2$;

(e) (Joly) $w(k, R) \leqslant k^2$ *if* $k < p$, *and* $v(2, R) \leqslant 3$.

Proof. It follows from [8], Theorem 1, that $p \nmid m(k)$ if $p \nmid k$ and $c_p = c$ for all c. Hence $F_p[x_1] = m(k) F_p[x_1] \subseteq J(k, F_p[x_1])$, so $F_p[x_1] = J(k, F_p[x_1])$. Suppose now that $z \in R$. Consider the homomorphism $F_p[x_1] \to R$ induced by $x_1 \to z$. It follows that $J(k, R) = R$, and that parts (a) and (b) of the proposition hold. Part (c) is shown in [16], Theorem 37. Part (d) is shown in [20], Theorems 5 and 6, and part (e) is shown in [15], Proposition 7.27 and Theorem 7.9.

We must now allow the possibility that $c_p < c$ for some c. We first produce a polynomial identity of the form

$$(15)\qquad (x_1^{p^b} - x_1)x_2 + g_0(x_1) = \sum_{i=1}^{t} g_i(x_1, x_2)^k$$

where b and t are positive integers, $g_0(x_1) \in F_p[x_1]$ and $g_i(x_1, x_2) \in F_p[x_1, x_2]$ for $i = 1, \ldots, t$.

In [18], a polynomial is called primary if its leading coefficient is 1. Suppose $m_2 > m_1 \geqslant 0$ and $l > 1$ are integers and that

$$(k-1)m_2 < p^l < km_2 \quad \text{and} \quad p^l - 1 = (k-1)m_2 + m_1.$$

In the course of proving Theorem III of [18], it is shown that

$$(16)\qquad \sum_{\substack{\text{degree } a = l\\ a \text{ primary}}} (a^{m_1}x_2 + a^{m_2})^k = \Gamma x_2 + \Delta$$

where the sum is over $a \in F_p[x_1]$, and $\Gamma \neq 0$ and Δ are in $F_p[x_1]$. Clearly

$$(17)\qquad \Gamma = \sum_{\substack{\text{degree } a = l\\ a \text{ primary}}} a^{p^l - 1}.$$

It is shown in [18] that if $r < p^l - 1$,

$$(18)\qquad \sum_{\substack{\text{degree } a = l\\ a \text{ primary}}} a^r = 0.$$

The familiar Vandermonde determinant is also stated:

$$(19)\qquad \begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{s-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & a_s & a_s^2 & \ldots & a_s^{s-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant s} (a_j - a_i).$$

Letting $s = p^l$ and $a_1, \ldots, a_s$ be the primary polynomials of degree l in (19), we replace the last row by the sum of all the rows (without changing the determinant). By equations (17) and (18), the only non-zero term in the bottom row is now Γ in the bottom right-hand corner. Expanding by minors along the bottom row and using the Vandermonde formula again, we derive

$$(20)\qquad \Gamma = \prod_{1 \leqslant i < j < p^l} (a_j - a_i) \Big/ \prod_{1 \leqslant i < j < p^l} (a_j - a_i)$$

$$= \prod_{1 \leqslant i < p^l} (a_{p^l} - a_i) = \prod_{\substack{\text{degree } a < l\\ a \neq 0}} a.$$

Let $b = \mathrm{L.C.M.}\{r < l\colon 0 < r \in Z\}$. Then

$$(21)\qquad (x_1^{p^b} - x_1) = \prod_{\substack{0 < \text{degree } a < l\\ a \text{ irreducible}}} a.$$

Hence from (20) and (21) we have $\Gamma | (x_1^{p^b} - x_1)^r$ for some positive integer r, and $\Gamma = x_1^{p^b} - x_1$ if $l = 1$. Thus if $l = 1$, (16) becomes

$$\sum_{\substack{\text{degree } a = 1\\ a \text{ primary}}} (a^{m_1}x_2 + a^{m_2})^k = (x_1^{p^b} - x_1)x_2 + \Delta$$

which is an identity of the form (15) with $t = p^l = p$. If $l > 1$, then by a standard refinement argument,

$$1 + (x_1^{p^b} - x_1)x_2 \equiv w^k \bmod (x_1^{p^b} - x_1)^r$$

for some $w \in F_p[x_1, x_2]$. Since $\Gamma | (x_1^{p^b} - x_1)^r$, we have

$$(x_1^{p^b} - x_1)x_2 = w^k - 1 + \Gamma g \quad \text{for some } g \in F_p[x_1, x_2].$$

Then (16) gives

$$\sum_{\substack{\text{degree } a = l\\ a \text{ primary}}} (a^{m_1}g + a^{m_2})^k + w^k = (x_1^{p^b} - x_1)x_2 + \Delta + 1$$

which is an identity of the form (15) with $t = p^l + 1$.

These identities exist on the condition that $m_2 > m_1 \geqslant 0$ and $l > 1$ are integers such that $(k-1)m_2 < p^l < km_2$ and $p^l - 1 = (k-1)m_2 + m_1$. These conditions lead to the following upper bounds on integers t for which identities of the form (15) exist.

LEMMA 3. *Suppose $p \nmid k$ and $p < k$. If $k \neq p^m+1$ for all integers m, then there exists an identity of the form*

$$(x_1^{p^b} - x_1)x_2 + g_0(x_1) = \sum_{i=1}^{t} g_i(x_1, x_2)^k$$

in $F_p[x_1, x_2]$ for some $b > 0$ and some $t \leqslant (k-2)^3+1$. If $k = p^m+1$, then

$$(x_1^{p^{2m}} - x_1)x_2 + x_1^{p^{2m}+p^m} - 1 = (x_2 + x_1^{p^m})^k - (x_2 x_1 + 1)^k - x_2^k + (x_1 x_2)^k$$

is such an identity with $t = 4$.

Proof. If $k = p^m+1$, then the above identity with $t = 4$ holds. Now suppose $k \neq p^m+1$ for all integers m. To prove the lemma, it will suffice to show there exist $m_2 > 0$ and $l > 1$ such that $(k-1)m_2 < p^l < km_2$ and $p^l+1 \leqslant (k-2)^3+1$. For then we may let $m_1 = p^l - 1 - (k-1)m_2$ in the previous construction, to have an identity with $t \leqslant p^l+1 \leqslant (k-2)^3 + +1$.

If $m_2 > k-1$, then the intervals $\big((k-1)m_2, km_2\big)$ and $\big((k-1)(m_2+1), k(m_2+1)\big)$ overlap. It is impossible that $p^l = k(k-1)$, since $p \nmid k$. Hence if $p^l > (k-1)^2$, then p^l is in some interval $\big((k-1)m_2, km_2\big)$. Thus it suffices to show that there is a prime power p^l such that $(k-1)^2 < p^l \leqslant (k-2)^3$.

Since $p < k$ and $k \neq p+1$, we have $p \leqslant k-2$. If $p > (k-1)^{2/3}$ then $(k-1)^2 < p^3 \leqslant (k-2)^3$ and we are finished. Now suppose $p \leqslant (k-1)^{2/3}$. Then if p^l is the smallest power of p greater than $(k-1)^2$, $p^l \leqslant (k-1)^{8/3}$. Hence the lemma holds if $k \geqslant 7$, since then $(k-2)^3 \geqslant (k-1)^{8/3}$. The hypotheses that $p \nmid k$, $p < k$ and $k \neq p^m+1$ for all m leave $k = 5$ and $p = 3$ as the only remaining case. This case is easily checked, so the lemma is proved.

Suppose now that we have an identity in $F_p[x_1, x_2]$ of the form

$$(x_1^{p^b} - x_1)x_2 + g_0(x_1) = \sum_{i=1}^{t} g_i(x_1, x_2)^k.$$

It follows that if $pR = \{0\}$, then the ideal I of R generated by $\{x^{p^b} - x\colon x \in R\}$ is contained in $J(k, R)$. Let $A = R/I$, and note that $pa = 0 = a^{p^b} - a$ if $a \in A$. We will first consider $J(k, A)$ and $v(k, A)$ for rings A with these properties. These results will then be lifted to rings R such that $pR = \{0\}$. The case $R = F_p[n]$ will then be considered.

LEMMA 4. *Let A be a ring such that $pa = 0$ and $a^{p^b} = a$ for all $a \in A$ and some fixed positive integer b. Suppose t and v are integers and $f_1, \ldots, f_t \in A[x_1, \ldots, x_v]$. Then there exists a solution $a = (a_1, \ldots, a_v) \in A^v$ of the equations $f_1(a) = \ldots = f_t(a) = 0$ if and only if for each maximal ideal M of A there is a solution $a_M \in A^v$ to $f_1(a_M) = \ldots = f_t(a_M) = 0 \bmod M$.*

Proof. The existence of a certainly implies the existence of the a_M, so we show the converse.

Let $B = A \otimes \mathrm{GF}(p^b)$. It is clear that every prime ideal of B is maximal. It is shown in [1], pp. 465–466, that there is a homeomorphism σ of $\mathrm{Spec}(B)$ of finite order such that A is isomorphic to the ring of all functions $f\colon \mathrm{Spec}(B) \to \mathrm{GF}(p^b)$ which are continuous in the Zariski topology, vanish outside a compact set, and satisfy $f(\sigma x) = f(x)^p$ for all $x \in B$. Since $1 \in B$, it follows from [13], [14] that $\mathrm{Spec}(B)$ is compact and zero-dimensional.

Since B is integral and finite dimensional over A, $x \cap A$ is a maximal ideal of A whenever $x \in \mathrm{Spec}(B)$. Hence for each such x there is an $a_x = (a_x^{(1)}, a_x^{(2)}, \ldots, a_x^{(v)})$ such that $f_1(a_x)(x) = \ldots = f_t(a_x)(x) = 0$, where $f_1(a_x), \ldots, f_t(a_x)$ are considered as functions on $\mathrm{Spec}(B)$. Since the elements of A are continuous functions on $\mathrm{Spec}(B)$, there is a compact, open and closed set U_x around x such that $f_1(a_x)(y) = \ldots = f_t(a_x)(y) = 0$ for $y \in U_x$. We can furthermore take U_x to be invariant under σ, since $f_j(a_x)(\sigma y) = \big(f_j(a_x)(y)\big)^p = 0$ for $y \in U_x$.

Since $\mathrm{Spec}(B)$ is compact, finitely many of the U_x, say $U_{x_1}, \ldots, U_{x_n}$, cover $\mathrm{Spec}(B)$. By taking appropriate complements and intersections, we may assume that $U_{x_1}, \ldots, U_{x_n}$ are disjoint. Now each U_{x_i} is compact, open and closed and is invariant under σ. Hence the characteristic function χ_i of U_i is an element of A. If now $a = \sum_i \chi_i a_{x_i}$, then $f_1(a) = \ldots = f_t(a) = 0$ and the lemma is proved.

To apply Lemma 4 to the Waring problems for A, define

$$\delta(b) = \sup_{c|b} w\big(k, \mathrm{GF}(p^c)\big) \quad \text{and} \quad \varepsilon(b) = \inf\Big(\delta(b), \sup_{c|b} 2v\big(k, \mathrm{GF}(p^c)\big)\Big)$$

when b is a positive integer. If $pR = \{0\}$, a maximal ideal M of R is said to be of degree c if R/M is isomorphic to $\mathrm{GF}(p^c)$. In the following proposition we do not need the hypothesis that $p \nmid k$.

PROPOSITION 2. *Let A be a ring such that $pa = 0$ and $a^{p^b} = a$ for all $a \in A$ and some fixed positive integer b. Then $a \in A$ is in $J(k, A)$ if and only if a is in $J(k, A) \bmod M$ for all maximal ideals M of A which have degree c for some $c > c_p$. Also, $w(k, A) \leqslant \delta(b) \leqslant k$ and $v(k, A) \leqslant \varepsilon(b) \leqslant k$.*

Proof. Suppose v is a positive integer and $a \in A$. Let

$$f = x_1^k + \ldots + x_v^k - a \in A[x_1, \ldots, x_v].$$

Every residue field of A must be isomorphic to $\mathrm{GF}(p^c)$ for some $c|b$. By Lemma 4, there is a solution $\bar{a} = (a_1, \ldots, a_v) \in A^v$ of $f(\bar{a}) = 0$ iff there is a solution mod M for all maximal ideals M of A. Since it is shown in [3] and [4] that $J\big(k, \mathrm{GF}(p^c)\big) = \mathrm{GF}(p^{c_p})$, we need only consider M of degree $c > c_p$. The stated condition in order that a be in $J(k, A)$ follows, as does the bound $w(k, A) \leqslant \delta(b)$. It is shown in [22] that $\delta(b) \leqslant k$. The bound $v(k, A) \leqslant \varepsilon(b) \leqslant k$ is proved similarly by considering polynomials of the form

$$f = x_1^k + \ldots + x_v^k - x_{v+1}^k - \ldots - x_{2v}^k - a.$$

Proposition 2 has the following two extensions to rings R such that $pR = \{0\}$.

PROPOSITION 3. *Suppose $pR = \{0\}$, $g \in J(k, R)$ and that I is an ideal of R containing $\{x^{p^b} - x \colon x \in R\}$ for some $b > 0$. Then*

(a) $v(k, R) \leqslant \varepsilon(b) + v(k, R, I+g) \leqslant k + v(k, R, I+g)$;

(b) $w(k, R) \leqslant \delta(b) + w(k, R, I+g) \leqslant k + w(k, R, I+g)$ *if* $I \pm g \subseteq J(k, R)$.

Proof. Since $v(k, R) \leqslant v(k, R/I) + v(k, R, I+g)$ and $A = R/I$ satisfies the hypotheses of Proposition 2, part (a) holds. Part (b) is proved similarly.

PROPOSITION 4. *Suppose $p \nmid k$, $pR = \{0\}$ and that $f \in R$. Then $f \in J(k, R)$ if and only if $f \in J(k, R)$ mod M for all maximal ideals M of R which are of degree c for some $c > c_p$.*

Proof. If $p > k$, then $c_p = c$ for all c, and the proposition holds by Proposition 1. Now suppose $p < k$. By Lemma 3, there is a $b \geqslant 1$ such that the ideal I generated by $\{x^{p^b} - x \colon x \in R\}$ is contained in $J(k, R)$. The proposition now follows on applying Proposition 2 to $A = R/I$.

Remark. Let $\mathfrak{I}$ be the set of maximal ideals M of R which are of degree c for some $c > c_p$. Then

$$J(k, R) = \Phi^{-1}\Big(\prod_{M \in \mathfrak{I}} J(k, R/M)\Big)$$

where $\Phi \colon R \to \prod_{M \in \mathfrak{I}} R/M$ is the projection into the direct product of the R/M. If $\mathfrak{I}$ is finite (e.g. when $R = F_p[n]$), then this gives an exact sequence

$$0 \to \bigcap \mathfrak{I} \to J(k, R) \to \bigoplus_{M \in \mathfrak{I}} J(k, R/M) \to 0.$$

In the case $R = F_p[n]$, let

$$(x_1^{p^b} - x_1)x_2 + g_0(x_1) = \sum_{i=1}^{t} g_i(x_1, x_2)^k$$

be an identity of the type described in Lemma 3. Let

$$g = \sum_{i=1}^{n} g_0(x_i) \quad \text{and} \quad I = \sum_{i=1}^{n} (x_i^{p^b} - x_i) F_p[n].$$

Then $w(k, F_p[n], I+g) \leqslant tn$ and $I \pm g \subseteq J(k, F_p[n])$ by Lemma 3. Hence

$$\begin{aligned} w(k, F_p[n]) &\leqslant w(k, F_p[n]/I) + w(k, F_p[n], I+g) \\ &\leqslant \delta(b) + tn \leqslant k + tn \end{aligned}$$

by Proposition 3. Similarly,

$$v(k, F_p[n]) \leqslant \varepsilon(b) + tn \leqslant k + tn.$$

We now have the following results from the bounds on t given in Lemma 3.

PROPOSITION 5. *Suppose $p \nmid k$. Then*

(a) *the bounds of Proposition 1 hold if $c = c_p$ for all positive integers c; otherwise, $p < k$;*

(b) $v(k, F_p[n]) \leqslant w(k, F_p[n]) \leqslant ((k-2)^3+1)n + k$ *if* $p < k$ *and* $k \neq p^m + 1$ *for all integers* m.

(c) $w(k, F_p[n]) \leqslant 4n + \delta(2m) \leqslant 4n + k$ *and* $v(k, F_p[n]) \leqslant 4n + \varepsilon(2m) \leqslant 4n + k$ *if* $k = p^m + 1$;

(d) (Kubota) $w(k, F_p[1]) < 3k + 3[k \log(3k^2 - k)] + 4$.

From Proposition 4 we get the following simple condition in order that $f \in F_p[n]$ be in $J(k, F_p[n])$.

PROPOSITION 6. *Suppose $p \nmid k$ and $f = f(x_1, \ldots, x_n) \in F_p[n]$. Then f is in $J(k, F_p[n])$ if and only if*

$$f(a_1, a_2, \ldots, a_n) \in J(k, \mathrm{GF}(p^c)) = \mathrm{GF}(p^{c_p})$$

for all $c > c_p$ and all $a_1, \ldots, a_n \in \mathrm{GF}(p^c)$.

As one further application of Proposition 4, we compute

$$\varphi(k, p, n) = \dim_{F_p} F_p[n]/J(k, F_p[n])$$

when $p \nmid k$ (cf. [15], Proposition 3.6, and [16], Theorem 40).

PROPOSITION 7. *If $p \nmid k$ then*

$$\varphi(k, p, n) = \sum_{c=1}^{\infty} \Big(1 - \frac{c_p}{c}\Big)\Big(\sum_{d|c} \mu\Big(\frac{c}{d}\Big) p^{dn}\Big)$$

where μ is the Möbius function, and the right-hand sum is finite.

Proof. Let $\mathfrak{I}$ be the set of maximal ideals M of $F_p[n]$ which are of degree c for some $c > c_p$. By the remark following Proposition 4, $F_p[n]/J(k, F_p[n])$ is isomorphic to $\bigoplus_{M \in \mathfrak{I}} F[M]/J(k, F[M])$, where $F[M]$ is the residue field of M. Now $J(k, \mathrm{GF}(p^c)) = \mathrm{GF}(p^{c_p})$, so it follows that

$$\varphi(k, p, n) = \sum_{c=1}^{\infty} (c - c_p) g(c)$$

where $g(c)$ is the number of maximal ideals $M \in \mathfrak{I}$ which are of degree c.

To compute $g(c)$, let $R = F_p[n]$. Let I be the ideal generated by $\{x^{p^c} - x \colon x \in R\}$, and let $A = R/I$. Then A is the direct sum of its residue fields, each of which has degree d for some $d | c$. The map $M \to M/I$ sets up a one-to-one correspondence between the maximal ideals M of R which are of degree dividing c and the maximal ideals of A. Counting the order of A in two different ways,

$$p^{\mu cn} = \prod_{d|c} (p^d)^{g(d)}.$$

Hence $p^{cn} = \sum_{d|c} dg(d)$, so by Möbius inversion we have $g(c) = (1/c) \sum_{d|c} \mu(c/d) p^{dn}$. The proposition now follows from $\varphi(k, p, n) = \sum_{c=1}^{\infty} (c - c_p) g(c)$.

Remark. R. M. Kubota has shown in [16] that $\varphi(k, p, n) = (k^2 - 3k + 2)/2 = (p^{2h} - p^h)/2$ if $k = p^h + 1$ for some h. Using Proposition 7, this result can be extended as follows. Let q be a prime $\leqslant p$, and suppose $k = 1 + p^h + \ldots + p^{(q-1)h}$ for some h. Then $\varphi(k, p, n) = (q-1)(p^{hqn} - p^{hn})/q$. The main part of the proof is to show that $c = c_p$ unless $c = qd$ for some $d|h$ such that $(h/d, q) = 1$, and that $c_p = d$ for such c. The result then follows on simplifying the expressions which result from Proposition 7. The details are left to the reader.

Remark. If m is a positive integer and $p \nmid k$, define

$$\varphi(k, p^m, n) = \dim_{F_p} \mathrm{GF}(p^m)[n] / J(k, \mathrm{GF}(p^m)[n]).$$

Then the same arguments used in proving Proposition 7 will show

$$\varphi(k, p^m, n) = m \sum_{\substack{c=1 \\ m|c}}^{\infty} \left(1 - \frac{c_p}{c}\right) \left(\sum_{e|\frac{c}{m}} \mu\left(\frac{c}{me}\right) p^{mec} \right)$$

(cf. [16], Theorem 40).

5. The case $p|k$. If $p = k$ then $S_p = F_p$. As remarked in Section 3, the map $f \to f^p$ is a homomorphism of $F_p[n]$ onto $J(p, F_p[n])$. Hence

$$(21) \qquad v(p, F_p[n]) = 1 \quad \text{and} \quad J(p, F_p[n]) = F_p[x_1^p, \ldots, x_n^p].$$

Unless otherwise specified, for the rest of this section p will denote a fixed prime such that $p|k$ and $p < k$. Let $\theta = \mathrm{ord}_p(k)$ and $S = S_p = Z/p^{\gamma_p}Z$. Define

$$T = \sum_{i=0}^{\theta} p^{\theta - i} S[x_1^{p^i}, \ldots, x_n^{p^i}].$$

We now define the systems of polynomial identities which will be used in analyzing $J(k, S[n])$.

Definition 1. *Suppose u and v are non-negative integers. Let $F(u, v)$ be the set of $(\theta+2)$-tuples $(f(x_1), g_0(x_1), \ldots, g_\theta(x_1))$ of polynomials in $S[x_1]$ such that*

(a) $0 \neq f(x_1) \in S[x_1^{p^\theta}, \ldots, x_n^{p^\theta}]$, *$f(x_1)$ has degree u and leading coefficient prime to p;*

(b) $f(x_1) p^{\theta - i} x_2^{p^i} + g_i(x_1) \in J(k, S[x_1, x_2])$ *for* $i = 0, \ldots, \theta$.

(c) $\sum_{i=0}^{\theta} v(k, S[x_1, x_2], \{f(x_1) p^{\theta - i} x_2^{p^i} + g_i(x_1)\}) \leqslant v$.

In terms of the parameters of Definition 1, we have the following information about $v(k, S[n])$ and $J(k, S[n])$.

Proposition 8. *Suppose $(f, g_0, \ldots, g_\theta) \in F(u, v)$. Let $I = \sum_{i=1}^{n} f(x_i) S[n]$, $I' = \sum_{i=1}^{n} f(x_i) T$ and $h = \sum_{i=0}^{\theta} \sum_{j=1}^{n} g_i(x_j)$. Let $\Phi \colon S[n] \to S[n]/I$ be the quotient homomorphism. Then*

(a) $v(k, S[n]) \leqslant v(k, S[n]/I) + v(k, S[n], I' + h) \leqslant v(k, S[n]/I) + vn$.

(b) $J(k, S[n]) = T \cap \Phi^{-1}(J(k, S[n]/I))$.

Proof. Since $f(x_1)$ is a polynomial $x_1^{p^\theta}$ whose leading coefficient is prime to p, and the degree of $f(x_1)$ is u, the following is true. For every $g \in S[n]$ (respectively T) there is a unique $g' \in S[n]$ (respectively T) such that $g - g' \in I$ (respectively I') and g' is of degree $\leqslant u - 1$ in each of the variables $x_1, \ldots, x_n$. From this it follows that $T \cap I = I'$.

Clearly if $r = r(x_1, \ldots, x_n) \in S[n]$ then $r^p - r(x_1^p, \ldots, x_n^p) \in pS[n]$. A simple induction now shows that

$$(22) \qquad T = \{f_0^{p^\theta} + p f_1^{p^{\theta-1}} + \ldots + p^\theta f_\theta \colon f_0, \ldots, f_\theta \in S[n]\}.$$

Hence $J(k, S[n]) \subseteq T$, since T is an additive group and contains f^{p^θ} for $f \in S[n]$.

We conclude from (22) and Definition 1 (b), (c) that $I' + h \subseteq J(k, S[n])$ and $v(k, S[n], I' + h) \leqslant vn$. Since $h \in J(k, S[n]) \subseteq T$ and $I \cap T = I'$, we have $v(k, S[n], I + h) = v(k, S[n], I' + h)$. Part (a) of Proposition 8 now follows from the bound

$$v(k, S[n]) \leqslant v(k, S[n]/I) + v(k, S[n], I + h).$$

Since $I = \ker \Phi$ and $T \cap I = I' \subseteq J(k, S[n]) \subseteq T$, part (b) holds.

Remark. Given an element of $F(u, v)$ and a polynomial g in $S[n]$, a finite procedure exists for computing $\Phi(g)$ and for determining whether g is in T. Since $S[n]/I$ is finite, Proposition 8(b) thus gives an algorithm for determining if g is in $J(k, S[n])/I$. Similarly, the final upper bound of Proposition 8(a) is constructive.

The problem of bounding $v(k, S[n])$ now breaks into two parts:

(i) finding $u \geqslant 0$, $v \geqslant 1$ and $f, g_0, \ldots, g_\theta \in S[x_1]$ for which $(f, g_0, \ldots, g_\theta) \in F(u, v)$, and

(ii) bounding $v(k, S[n]/I)$ as a function of $(f, g_0, \ldots, g_\theta) \in F(u, v)$.

To accomplish (i) we make some further definitions. If $b \geqslant 0$, let

$S[n]_b$ be the additive group of polynomials $g \in S[n]$ which are of degree $\leqslant b$ in each of the variables $x_1, \ldots, x_n$. Let $T_b = T \cap S[n]_b$ and $J_b = J(k, S[n], S[n]_c)$, where $c = [b/k]$. Let U_b be the set of polynomials $g \in T_b$ which do not contain any monomial terms of the form $x_1^{ka_1} x_2^{ka_2} \ldots x_n^{ka_n}$, where $a_1, \ldots, a_n$ are non-negative integers. Here T_b, J_b and U_b depend implicitly on k, p and n.

We will first show that there exist integers λ and ζ such that $T_b \subseteq U_\lambda + J_{b+\zeta}$ for all $b \geqslant 0$. Then integers u and v such that $F(u, v) \neq \emptyset$ will be found as functions of λ and ζ.

Lemma 5. *If $h > 0$, $r \geqslant 0$ and $a \geqslant (h-1)(r+h)$ are integers, then there exist non-negative integers c and d such that*

(a) $a = c(h-1)+d$;

(b) $c-d > r \geqslant 0$;

(c) $hc \leqslant a+r+h$.

Proof. Choose $c', d' \in Z$ so that we have $a = (h-1)c'+d'$. Let $s = [(r-c'+d')/h]+1$, $c = c'+s$, $d = d'-(h-1)s$. Then (a) holds. Clearly $h+r-c'+d' \geqslant hs > r-c'+d'$, so $h+r \geqslant c'-d'+hs = c-d > r \geqslant 0$, which shows (b). Part (c) holds by part (a) and the inequality $h+r \geqslant c-d$. All that remains to be shown is that c and d are non-negative. Since $r+h+d \geqslant c$ and $a \geqslant (h-1)(r+h)$, we have $(h-1)(r+h+d)+d \geqslant (h-1)c+ +d = a \geqslant (h-1)(r+h)$. Rearranging the first and last terms in this inequality shows that $hd \geqslant 0$. Hence $d \geqslant 0$, and so $c \geqslant 0$ by (b).

Definition 2. Suppose $r \geqslant 0$ and $s \geqslant 1$ are integers and that $s|k$ Let

(a) $\sigma(s, r) = k(k/s-1)(r+k/s)+r+1-k$;

(b) $\zeta = k\Big(1+\sum_{i=0}^{\theta-1}\prod_{t=0}^{i}(1+p^t)\Big)$;

(c) $\lambda = \sigma(1, (\zeta-k)/2)$.

Lemma 6. *$T_b \subseteq U_\lambda + J_{b+\zeta}$ for all $b \geqslant 0$.*

Proof. For $w = 0, \ldots, \theta$ define

$$T_{b,w} = \sum_{i=0}^{w}\binom{k}{p^i}\big(S[x_1^{p^i}, \ldots, x_n^{p^i}] \cap S[n]_b\big).$$

Let $T_{b,-1} = \{0\}$. Since $\operatorname{ord}_p\Big(\binom{k}{p^i}\Big) = \theta - i$ for $i = 0, \ldots, \theta$, we have $T_{b,\theta} = T_b$.

Define $r_\theta = 0$, $\tau_\theta = k$ and $\sigma_\theta = \sigma(p^\theta, 0)$. If r_i, τ_i and σ_i have been defined for $-1 \leqslant w < i \leqslant \theta$, let $r_w = r_{w+1}+\tau_{w+1}$ and $\tau_w = p^w r_w + k$, and let $\sigma_w = \sigma(p^w, r_w)$ if $w \geqslant 0$. We will show that

(23) $T_{b,w} \subseteq J_{b+\tau_w} + T_{b+\tau_w, w-1} + T_{b-r_w-1}$ if $b \geqslant \sigma_w$ and $0 \leqslant w \leqslant \theta$.

We first show how the lemma follows from (23). It is readily verified that r_w, τ_w and σ_w are non-negative and nondecreasing as w decreases. Then induction on w in (23) shows that

(24) $$T_b = T_{b,\theta} \subseteq J_{b+r_{-1}} + T_{b-1} \quad \text{if} \quad b \geqslant \sigma_0.$$

The fact that $r_{-1} = \zeta$ is readily proved by induction on θ, so $\lambda = \sigma_0 - 1$. Hence by induction on b in (24), it follows that $T_b \subseteq J_{b+\zeta} + T_\lambda$ if $b \geqslant \lambda$. Since $T_\lambda \subseteq J_\lambda + U_\lambda$, this will show $T_b \subseteq U_\lambda + J_{b+\zeta}$. Hence to prove the lemma it will suffice to show (23).

By the definition of $T_{b,w}$, it will be enough to show that if $b \geqslant \sigma_w$ and $\binom{k}{p^w}(x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n})^{p^w} \in T_{b,w}$, then

$$\binom{k}{p^w}(x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n})^{p^w} \in J_{b+\tau_w} + T_{b+\tau_w, w-1} + T_{b-r_w-1}.$$

Let $N = \Big(\dfrac{k}{p^w}-1\Big)\Big(r_w + \dfrac{k}{p^w}\Big)$. If $a_1, \ldots, a_n < N$, then

$$p^w a_1, \ldots, p^w a_n \leqslant (k-p^w)\Big(r_w + \frac{k}{p^w}\Big) - p^w \leqslant \sigma(p^w, r_w) - r_w - 1 \leqslant b - r_w - 1$$

so (23) holds. Now suppose the a_i have been ordered so that $a_1, \ldots, a_t \geqslant N$ and $a_{t+1}, \ldots, a_n < N$. For $i = 1, \ldots, t$ let $h = k/p^w$ and $a = a_i$ in Lemma 5, and define $c_i = d$ and $d_i = d$, where c and d are as in the lemma. Define

$$y_1 = \prod_{i=1}^{t} x_i^{c_i}, \quad y_2 = \prod_{i=1}^{t} x_i^{d_i} \quad \text{and} \quad z = \prod_{i=t+1}^{n} x_i^{a_i}.$$

Now consider

(25) $$(y_1+y_2 z)^k = y_1^k + \sum_{0<i<p^w}\binom{k}{i} y_1^{k-i}(y_2 z)^i + \binom{k}{p^w} y_1^{k-p^w}(y_2 z)^{p^w} + \sum_{p^w < i \leqslant k}\binom{k}{i} y_1^{k-i}(y_2 z)^i.$$

We have $\binom{k}{p^w} y_1^{k-p^w}(y_2 z)^{p^w} = \binom{k}{p^w}(x_1^{a_1}\ldots x_n^{a_n})^{p^w}$. If $0 < i \leqslant k$ and $s = \operatorname{ord}_p(i)$ we have $\operatorname{ord}_p\Big(\binom{k}{i}\Big) \geqslant \theta - s = \operatorname{ord}_p\Big(\binom{k}{p^s}\Big)$. We also have the bound $k(N-1) \leqslant \sigma(p^w, r_w) - r_w - 1 \leqslant b - r_w - 1$. The following facts now follow from Lemma 3:

(25a) If $0 < i < p^w$ then $\binom{k}{i} y_1^{k-i}(y_2 z)^i \in T_{b+\tau_w, w-1}$.

(25b) If $p^w < i \leqslant k$ then $\binom{k}{i} y_1^{k-i}(y_2 z)^i \in T_{b-r_w-1}$.

(25c) y_1^k and $(y_1+y_2 z)^k$ are in $J_{b+\tau_w}$.

We may now rearrange (25) using (25a), (25b) and (25c) to have

$$\binom{k}{p^w}(x_1^{a_1}\dots x_n^{a_n})^{p^w} = \binom{k}{p^w} y_1^{k-p^w}(y_2z)^{p^w} \in J_{b+r_w}+T_{b+r_w,w-1}+T_{b-r_w-1}.$$

By our previous remarks, this shows that (23) holds, and the lemma is proved.

COROLLARY. *$T/J(k, S[n])$ is a finite p-group of order dividing that of U_λ.*

Proof. As shown by equation (22), $J(k, S[n]) \subseteq T$. Lemma 6 implies that $T \subseteq U_\lambda + J(k, S[n])$. Since U_λ is a finite p-group, the corollary follows.

In analogy to the case $p \nmid k$, we define $\varphi(k, p, n)$ for $p \mid k$ and $p < k$ so that $T/J(k, S[n])$ has order $p^{\varphi(k,p,n)}$. If $p = k$ then we define $\varphi(k, p, n) = 0$ in accordance with (21).

To now find u and v such that $F(u, v) \neq \emptyset$, and to later bound $V(k, S[n]/I)$ in Proposition 8(a), we need the following lemma. The proof sharpens an argument which goes back to C. L. Siegel (cf. [21], [20], p. 140–141, [22], Theorem 13). For all integers k and primes p, define

$$u(k, p) = \max\{w(k, Z/p^\delta Z)/\delta : 1 \leqslant \delta \in Z\}$$

and

$$\psi(k, p) = \max\{v(k, Z/p^\delta Z)/\delta : 1 \leqslant \delta \in Z\}.$$

LEMMA 7. *Let p be an arbitrary prime and let k be an arbitrary positive integer. Suppose $A \subseteq R$ is an additive subgroup of R of order p^a for some $a \in Z$. Suppose also that the subset B of A generates A. Then every $f \in A$ can be written in the forms*

(a) $f = \sum_{i=1}^{w} a_i^k f_i$,

(b) $f = \sum_{i=1}^{v} \pm b_i^k g_i$

for some $a_i, b_i \in Z$ and some $f_i, g_i \in B$, where $w = [u(k, p)a]$ and $v = [\psi(k, p)a]$.

Proof. We prove (a), (b) being similar.

Let $\{\eta_1, \dots, \eta_d\} \subseteq B$ be a minimal set of generators for A over Z, define p^{j_1} to be additive order of η_1. If $i \geqslant 1$, let $p^{j_{i+1}}$ be the index of the subgroup generated by $\{\eta_1, \dots, \eta_i\}$ in that generated by $\{\eta_1, \dots, \eta_{i+1}\}$. Then since $\{\eta_1, \dots, \eta_d\}$ is minimal,

(26) $$j_1, \dots, j_d \geqslant 1 \quad \text{and} \quad j_1 + \dots + j_d = a.$$

Furthermore, every $f \in A$ can be written as $f = x_1\eta_1 + \dots + x_d\eta_d$ for some $x_1, \dots, x_d \in Z$.

Let $z_d = w(k, Z/p^{j_d}Z)$. Then $x_d \equiv \sum_{i=1}^{z_d} a_i^k \bmod p^{j_d}$ for some $a_i \in Z$.

By the definition of j_d, this implies

(27) $$f - \sum_{i=1}^{z_d} a_i^k x_d = x_1'\eta_1 + \dots + x_{d-1}'\eta_{d-1}$$

for some $x_1', \dots, x_{d-1}' \in Z$. By induction on d in (27), we conclude that $f = \sum_{i=1}^{b} a_i^k f_i$ for some $a_i \in Z$ and $f_i \in B$ and

(28) $$b = \sum_{i=1}^{d} w(k, Z/p^{j_i}Z).$$

If $i \in Z$, $i \geqslant 1$, define m_i to be the number of j_t in equation (26) which equal i. Now (26) becomes

(29) $$\sum_{i=1}^{\infty} i m_i = a.$$

We may write (28) as

(30) $$b = \sum_{i=1}^{\infty} i m_i \{w(k, Z/p^i Z)/i\}.$$

It is now immediate from (29), (30) and the definition of $u(k, p)$ that $b \leqslant au(k, p)$, which proves the lemma, since b must be integral.

Remark. The bound of Lemma 7(a) is sharp if $A = R$ is the direct sum of $n\delta$ copies of $Z/p^\delta Z$, where $w(k, Z/p^\delta Z)/\delta = u(k, p)$ and B consists of those elements of A which equal the identity on one direct summand and are zero elsewhere. Similarly, the bounds of Lemma 7(b) are sharp if $v(k, Z/p^\delta Z)/\delta = \psi(k, p)$ in the above example.

Remark. It is shown in [23] that $w(k, Z/pZ) \leqslant k$ for all p and k. In [11], Theorem 4, it is shown that $w(k, Z/p^\delta Z) \leqslant 3k/2$ if $1 \leqslant \delta \in Z$, unless $k = 2^\delta = p^\delta$ for some $\delta > 1$, in which case $w(k, Z/p^\delta Z) \leqslant 4k$. It readily follows from these bounds and direct calculation when $k = 4$ or 8 that

(31) $$\psi(k, p) \leqslant u(k, p) \leqslant k \quad \text{for all } k \text{ and } p.$$

Equality holds in (31) if $k = (p-1)/2$ and p is odd. It is also clear that $u(k, p) = \max\{w(k, Z/p^\delta Z) : 1 \leqslant \delta \leqslant 4k\}$, so that $u(k, p)$ can be readily calculated given k and p. Similarly $\psi(k, p)$ may be easily computed.

We now find bounds on u and v for which $F(u, v) \neq \emptyset$. If $b \geqslant 0$, then T_b has order a power of p; let $p^{t(b)}$ be this order. Let $p^{u(b)}$ be the order of U_b. Then $t(b)$ and $u(b)$ depend implicitly on k, n and p. We let $t_2(b)$ and $u_2(b)$ denote $t(b)$ and $u(b)$ when $n = 2$.

LEMMA 8. *Suppose $n = 2$ and that $T_b \subseteq U_e + J_{b+d}$ for some fixed* *integers d and e and all $b \geqslant 0$. Let*

$$\varphi_2 = \varphi(k, p, 2), \quad w = (\theta+1)u_2(e)p^\theta + d \quad \text{and}$$
$$v = [\psi(k, p)(t_2(w) - \varphi_2)](\theta+1).$$

Then $F(u, v) \neq \emptyset$ for some $u \leqslant w-d$. In particular, this is true for $(d, e) = (\zeta, \lambda)$ as in Lemma 6.

Proof. Let b be a positive integer which we will later specify. Define

$$W(b) = \Big\{h = \sum_{j=0}^{b} t_j x_1^{jp^\theta} \in S[x_1, x_2]:\ t_j = 0, 1, \ldots, p-1\Big\}.$$

The order of $W(b)$ is p^{b+1}. Define

$$Y(b) = \{hp^{\theta-i}x_2^{p^i} \in S[x_1, x_2]:\ h \in W(b),\ i \in Z \text{ and } 0 \leqslant i \leqslant \theta\}.$$

Clearly $Y(b) \subseteq T_{bp^\theta}$. By assumption, $T_{bp^\theta} \subseteq U_e + J_{bp^\theta+d}$. Since U_e has order $p^{u_2(e)}$, there are hence at most $p^{u_2(e)}$ distinct elements of $Y(b)$ mod $J_{bp^\theta+d}$.

If A is an additive subgroup of $S[x_1, x_2]$, let $A^{\theta+1}$ denote the product of $\theta+1$ copies of A. By the preceding remarks, there are at most $p^{(\theta+1)u_2(d)}$ distinct elements of $Y(b)^{\theta+1}$ mod $(J_{bp^\theta+d})^{\theta+1}$.

Now let

$$X(b) = \{(hp^\theta x_2, hp^{\theta-1}x_2^p, \ldots, hx_2^{p^\theta}):\ h \in W(b)\}$$

so that $X(b) \subseteq Y(b)^{\theta+1}$. From our bound on the order of $Y(b)^{\theta+1}$ mod $(J_{bp^\theta+d})^{\theta+1}$, if

(32) $$\text{order } X(b) = p^{b+1} > p^{(\theta+1)u_2(e)}$$

then $z_1 = z_2 + f_1$ for some $z_1, z_2 \in X(b)$ and some $f_1 \in (J_{bp^\theta+d})^{\theta+1}$ such that $z_1 \neq z_2$.

Assume for the moment that (32) holds and that z_1 and z_2 are as above. Suppose $z_1 = (h_1p^\theta x_2, \ldots, h_1x_2^{p^\theta})$ and $z_2 = (h_2p^\theta x_2, \ldots, h_2x_2^{p^\theta})$ for some $h_1, h_2 \in W(b)$. Let $f = h_1 - h_2$, and let u be the degree of f. Then f is a nonzero polynomial in $x_1^{p^\theta}$, is of degree $u \leqslant bp^\theta$, has leading coefficient prime to p, and is such that $fp^{\theta-i}x_2^{p^i} \in J_{bp^\theta+d}$ for $i = 0, \ldots, \theta$. Hence $(f, 0, \ldots, 0)$ satisfies the first two conditions of Definition 1 in order that $(f, 0, \ldots, 0) \in F(u, v)$ for some v. We now show that it satisfies the third condition as well for v as in the statement of Lemma 8.

Let $R = S[x_1, x_2]$ and $A = J_{bp^\theta+d}$ in Lemma 7. By the inclusion $J(k, S[2]) \subseteq T$ and our assumption on d and e, we have

$$J(k, S[2]) \subseteq T \subseteq U_e + J(k, S[2]).$$

Assume $bp^\theta + d \geqslant e$; it follows that the canonical map $T_{bp^\theta+d} \to T/J(k, S[2])$ is onto. Hence p^{φ_2}, the order of $T/J(k, S[2])$, divides the order of $(T_{bp^\theta+d})/A$. Hence A must have order p^a for some $a \leqslant t_2(bp^\theta+d) - \varphi_2$, since $T_{bp^\theta+d}$ has order $p^{t_2(bp^\theta+d)}$. Let $B = \{g^k \in A\}$ in Lemma 7. We conclude from the lemma that

$$v(k, S[2], \{fp^{\theta-i}x_2^{p^i}\}) \leqslant [\psi(k, p)(t_2(bp^\theta+d) - \varphi_2)]$$

for $i = 0, \ldots, \theta$. Thus if $w = bp^\theta + d$ and $v = [\psi(k, p)(t_2(w) - \varphi_2)](\theta+1)$, we have that $(f, 0, \ldots, 0) \in F(u, v)$. This holds subject to the condition of equation (32) and the condition $bp^\theta + d \geqslant e$.

Let $b = (\theta+1)u_2(e)$; then (32) clearly holds. We now show that $bp^\theta + d \geqslant e$ for this b. Recall that $p^{u_2(e)}$ is the order of U_e. Since $0 \neq p^\theta x_1^i$, $p^\theta x_2^i \in U_e$ when $0 < i \leqslant e$ and $k \nmid i$, we have that $u_2(e) \geqslant 2\left(e - \left[\frac{e}{k}\right]\right)$. Hence $bp^\theta + d \geqslant b \geqslant u_2(e) \geqslant e$ if $k \geqslant 2$. But the lemma holds trivially if $k = 1$. We conclude that when $b = (\theta+1)u_2(e)$, there is an f such that $(f, 0, \ldots, 0) \in F(u, v)$ for some $u \leqslant bp^\theta$ and $v = [\psi(k, p)(t_2(bp^\theta+d) - \varphi_2)] \times (\theta+1)$. This completes the proof.

We now produce a bound on $v(k, S[n])$ as a function of integers u and v for which $F(u, v) \neq \emptyset$. Using Lemmas 6 and 8, the main terms of one such bound will then be computed.

LEMMA 9. *If $u \geqslant 0$, $v \geqslant 1$ and $F(u, v) \neq \emptyset$ then*

$$v(k, S[n]) \leqslant [\psi(k, p)(t(u-1) - \varphi(k, p, n))] + vn < \infty.$$

Proof. Suppose $(f, g_0, \ldots, g_\theta) \in F(u, v)$ and let $I = \sum_{i=1}^{n} f(x_i)S[n]$. By Proposition 8(a),

(33) $$v(k, S[n]) \leqslant v(k, S[n]/I) + vn.$$

Let $\Phi: S[n] \to S[n]/I$ be the quotient map. As in the proof of Proposition 8, for every $g \in T$ there is a unique $g' \in T_{u-1}$ such that $g - g' \in I$. Hence $\Phi(T)$ has the same order as T_{u-1}, namely $p^{t(u-1)}$. Now by Proposition 8(b), $T/J(k, S[n])$ is isomorphic to $\Phi(T)/\Phi(J(k, S[n]))$. Since $T/J(k, S[n])$ has order $p^{\varphi(k,p,n)}$, we conclude that $\Phi(J(k, S[n])) = J(k, S[n]/I)$ has order $p^{t(u-1)-\varphi(k,p,n)}$. We now apply Lemma 7 with $A = J(k, S[n]/I)$ and $B = \{g^k:\ g \in S[n]/I\}$. It follows that

$$v(k, S[n]/I) \leqslant [\psi(k, p)(t(u-1) - \varphi(k, p, n))]$$

so the lemma holds by (33).

Remark. The argument of Lemma 9 provides a means of computing $\varphi(k, p, n)$ if the order p^a of $J(k, S[n]/I)$ can be computed, since $a = t(u-1) - \varphi(k, p, n)$.

Remark. The functions $t(b)$, $t_2(b)$, $u(b)$ and $u_2(b)$ are computed to be

$$t(b) = (\gamma_p - \theta)(b+1)^n + \sum_{i=1}^{\theta}\left(\left[\frac{b}{p^i}\right]+1\right)^n, \tag{34}$$

$$t_2(b) = (\gamma_p - \theta)(b+1)^2 + \sum_{i=1}^{\theta}\left(\left[\frac{b}{p^i}\right]+1\right)^2, \tag{34a}$$

$$u(b) = t(b) - \gamma_p\left(\left[\frac{b}{k}\right]+1\right)^n, \tag{35}$$

$$u_2(b) = t_2(b) - \gamma_p\left(\left[\frac{b}{k}\right]+1\right)^2. \tag{35a}$$

An upper bound on $v(k, S[n])$ may now be computed from Lemmas 6, 8 and 9, the bound $\psi(k,p) \leqslant k$ of equation (31), and the trivial bound $\varphi(k,p,n) \geqslant 0$. Sharper bounds may result if better lower bounds on $\varphi(k,p,n)$ are used, or if more is known concerning the parameters d, e, u and v for which Lemmas 8 and 9 hold. Ultimately one can return to Proposition 8(a) and try to find better bounds on $v(k, S[n]/I)$. Note that $S[n]/I$ is Artinian, and so a finite product of Artin local rings, to which Lemma 1 applies.

We now compute, in terms of k, n and θ, the main terms of an upper bound on $v(k, S[n])$.

Let ζ and λ be as in Definition 2, and let $d_1 = \prod_{s=0}^{\infty}(1+2^{-s})$. Then

$$\zeta/k - 1 = \sum_{i=0}^{\theta-1}\prod_{s=0}^{i}(1+p^s) \leqslant p^{\theta(\theta-1)/2}\sum_{i=0}^{\theta-1}\Big(\prod_{s=0}^{i}1+p^{-s}\Big)\Big(\prod_{s=i+1}^{\theta-1}p^{-s}\Big)$$

$$\leqslant k^{(\theta-1)/2}d_1\Big(1+\sum_{s=\max(\theta-1,1)}^{\infty}p^{-s}\Big) = \big(d_1+O(2^{-\theta})\big)k^{(\theta-1)/2}.$$

Note $k^{-1} = O(2^{-\theta})$. Since $\theta > 0$ has been assumed, it follows that

$$\zeta \leqslant \big(d_1+O(2^{-\theta})\big)k^{(\theta+1)/2}.$$

From this and Definition 2,

$$\lambda \leqslant \big(d_1/2+O(2^{-\theta})\big)k^{(\theta+5)/2}.$$

It is shown in [9], Theorem 6, that $v(k, Z/p^\delta Z) \leqslant 2k$ for all positive k and δ. Now

$$\psi(k,p) = \max\{v(k, Z/p^\delta Z)/\delta\colon\ \delta \geqslant 1\},$$

and

$$v(k, Z/p^\delta Z)/\delta \leqslant p^\delta/\delta \leqslant p^\theta/\theta \leqslant k/\theta \quad \text{if} \quad \delta = 1, \ldots, \theta.$$

If $\delta > \theta$ then $v(k, Z/p^\delta Z) \leqslant 2k/(\theta+1)$, so for all k and p,

$$\psi(k,p) \leqslant 2k/(\theta+1).$$

Now for $b \geqslant 1$ we have from (34) and (35) that

$$u(b) \leqslant t(b) \leqslant 2(b+1)^n + \sum_{i=1}^{\theta}\left(\left[\frac{b}{p^i}\right]+1\right)^n \leqslant (b+k)^n(2^{n+1}-1)/(2^n-1).$$

We now bound the u, v and w in Lemma 8 when $(d, e) = (\zeta, \lambda)$. From the above,

$$w \leqslant \big(d_1^2\, 7/12 + O(2^{-\theta})\big)(\theta+1)k^{\theta+6}$$

and

$$v \leqslant \big(d_1^4\, 243/216 + O(2^{-\theta})\big)(\theta+1)^2 k^{2\theta+13}.$$

If $u \leqslant w - \zeta \leqslant w - k$, then

$$\psi(k,p)t(u-1) \leqslant \left(\frac{2k}{\theta+1}\right)\left(\frac{2^{n+1}-1}{2^n-1}\right)w^n.$$

There now results from Lemma 9 the following bound on $v(k, S[n])$.

PROPOSITION 10. *Suppose $p|k$ and $\theta = \mathrm{ord}_p(k)$. Let*

$$d_1 = \sum_{s=0}^{\infty}(1+2^{-s}) < 4.78, \qquad d_2 = (\theta+1)d_1^2\, 7/12 \quad \textit{and}$$
$$d_3 = (\theta+1)^2 d_1^4\, 243/216.$$

Then

$$v(k, S[n]) \leqslant \left(\frac{2k}{\theta+1}\right)\left(\frac{2^{n+1}-1}{2^n-1}\right)\exp\{n((\theta+6)\log k + \log d_2 + \varepsilon)\} +$$
$$+ n\exp\{(2\theta+13)\log k + \log d_3 + \varepsilon\}$$

where $\varepsilon = O(2^{-\theta})$, the implied constant being absolute.

6. End of the proofs. We now prove Theorems 3 and 4 of Section 3. Let $R = Z[n]$ in Lemma 2; we have

$$v(3, Z[n]) \leqslant v(3, Z[n]/6Z[n]) + 4 \tag{36}$$

and

$$v(k, Z[n]) \leqslant v(k, Z[n]/\gamma Z[n]) + 1 + \min(k^2(3\log k + 5.2), 2^{k-1}). \tag{37}$$

Since $Z[n]/\gamma Z[n]$ is isomorphic to $\bigoplus_{p \leqslant k} S_p[n]$, Lemma 1 implies

$$v(k, Z[n]/\gamma Z[n]) = \sup_{p \leqslant k} v(k, S_p[n]) \quad \text{if } k \text{ is odd}, \tag{38}$$

and

$$v(k, Z[n]/\gamma Z[n]) = \sup_{p,q \leqslant k}\left(1 - \frac{\delta_q^p}{2}\right)\big(v(k, S_p[n]) + v(k, S_q[n])\big) \quad \text{if } k \text{ is even}. \tag{39}$$

Theorem 3 now follows from (36)–(38) and the bounds on $v(k, S_p[n])$ given in Proposition 5 and equation (21) of Section 5. Similarly, Theorem 4(a) follows from (37)–(39), (21) and the bounds on $v(k, S_p[n])$ given in Propositions 5 and 10. (In Proposition 10, one makes straightforward estimates using the bound $\theta \leqslant \log k/\log p \leqslant \log k/\log 2$.) Theorem 4(b) is shown in the appendix.

We now summarize what has been shown concerning $J(k, Z[n])$. The exact sequence

$$0 \to \gamma Z[n] \to J(k, Z[n]) \to \bigoplus_{p \leqslant k} J(k, S_p[n]) \to 0$$

relates the structure of $J(k, Z[n])$ to that of $J(k, S_p[n])$ as p ranges over primes $\leqslant k$. Let $p \leqslant k$ be fixed, $\theta = \operatorname{ord}_p(k)$ and $S = S_p$. Define

$$T = \sum_{i=0}^{\theta} p^{\theta-i} S[x_1^{p^i}, \ldots, x_n^{p^i}].$$

Then $T/J(k, S[n])$ is a finite additive group of order $p^{\varphi(k,p,n)}$.

If $p \nmid k$, then $S = F_p$ and $T = F_p[n]$. Let $\mathfrak{J}$ be the set of maximal ideals M of $F_p[n]$ such that $J(k, F_p[n]/M) \neq F_p[n]/M$. These M are those of degree c for some $c > c_p$. Then we have an exact sequence

$$0 \to \bigcap \mathfrak{J} \to J(k, F_p[n]) \to \bigoplus_{M \in \mathfrak{J}} J(k, F_p[n]/M) \to 0.$$

If $F_p[n]/M = \mathrm{GF}(p^c)$, then

$$J(k, F_p[n]/M) = \mathrm{GF}(p^{c_p}).$$

If $p = k$, then $S = F_p$ and the Froebenius map $f \to f^p$ is a homomorphism of $F_p[n]$ onto $J(p, F_p[n])$. Hence

$$J(p, F_p[n]) = F_p[x_1^p, \ldots, x_n^p] = T.$$

If $p \neq k$ and $p \mid k$, then one can construct an ideal I of $S[n]$ such that $S[n]/I$ is a finite ring and

$$J(k, S[n]) = T \cap \Phi^{-1}(J(k, S[n]/I))$$

where $\Phi\colon S[n] \to S[n]/I$ is the quotient homomorphism. Here $S[n]/I$ is a finite direct sum $\bigoplus_i R_i$ of finite Artin local rings R_i, and

$$J(k, S[n]/I) = \bigoplus_i J(k, R_i).$$

Let $\bar{v}(k, n)$ denote the supremum of $v(k, R)$ over finite Artin local rings R such that (i) R is a homomorphic image of $Z[n]$, and (ii) $q^{\gamma_q} R = 0$ for some $q \neq k$ such that $q \mid k$. For each such R we have $v(k, R) \leqslant v(k, Z[n])$ since R is a homomorphic image of $Z[n]$. Hence $\bar{v}(k, n) \leqslant v(k, Z[n])$. If $q \neq k$ and $q \mid k$, then by Proposition 8 and Lemma 8,

$$v(k, S_q[n]) \leqslant v(k, S_q[n]/I) + \varepsilon_{k,q} n$$

for some $\varepsilon_{k,q} \in Z$ and some finite quotient ring $S_q[n]/I$ of $S_q[n]$. Writing $S_q[n]/I$ as the direct sum of finitely many finite Artin local rings, we have from Lemma 1 that

$$v(k, S_q[n]/I) \leqslant \bar{v}(k, n) \quad \text{if } k \text{ is odd},$$

and

$$v(k, S_q[n]/I) \leqslant 2\bar{v}(k, n) \quad \text{if } k \text{ is even}.$$

From Proposition 5,

$$v(k, S_p[n]) \leqslant \varepsilon_{k,p} n \quad \text{if} \quad p \nmid k,$$

and by (21),

$$v(p, S_p[n]) = 1 \quad \text{if} \quad p = k.$$

From these bounds and (37)–(39) we have

(40)
$$\begin{aligned} \bar{v}(k, n) &\leqslant v(k, Z[n]) \leqslant \bar{v}(k, n) + \varepsilon_k n \quad &\text{if } k \text{ is odd},\\ \bar{v}(k, n) &\leqslant v(k, Z[n]) \leqslant 4\bar{v}(k, n) + \varepsilon_k n \quad &\text{if } k \text{ is even} \end{aligned}$$

where ε_k is a constant which depends only on k. (Upper bounds for ε_k could in fact be given.) Thus for a fixed k, the rate of growth of $v(k, Z[n])$ with n is closely related to that of $\bar{v}(k, n)$. In a later paper we will consider the consequences of this to $V(k) = \sup_{n \geqslant 1} v(k, Z[n])$, one of which will be that $V(2^j) = \infty$ if $j \geqslant 2$.

Appendix. *The case* $k = 4$.

By Lemma 2(a) and Lemma 1(b) we have

(41)
$$v(4, Z[n]) \leqslant v(4, S[n]) + v(4, F_3[n]) + 8$$

where $S = Z/8Z$. By (12), there is an exact sequence

(42)
$$0 \to 24\, Z[n] \to J(4, Z[n]) \to J(4, S[n]) \oplus J(4, F_3[n]) \to 0.$$

We now consider $J(4, R)$ and $v(4, R)$ when $R = S[n]$ and $R = F_3[n]$.

Case 1. $R = S[n]$. The following identities hold mod 8:

(43)
$$\begin{aligned} 4(x^4 + x^2)y \equiv\ & 2(1 + x^2 + x^2y + xy)^4 - 2(x^2 + x^2y + xy)^4 -\\ & -(1 + x^2y)^4 + x^8y^4 + (1 + y + x^2y)^4 -\\ & -(x^2+1)^4y^4 - (1 + x^2 + x^2y)^4 + x^8(y+1)^4 +\\ & +(y + x^2 + x^2y)^4 - (x^2+1)^4(y+1)^4. \end{aligned}$$

(44)
$$\begin{aligned} 2(x^8 + x^4)y^2 - 1 - x^8 \equiv\ & 2x^8y^4 - (x^2 + x^2y)^4 - (1 + x^2y)^4 +\\ & + 4(x^4 + x^2)(x^4y^3 + x^4y + x^2y + y). \end{aligned}$$

(45)
$$(x^8 + x^4)y^4 \equiv (x^2y)^4 + (xy)^4.$$

Let $T = S[x_1^4, \ldots, x_n^4] + 2S[x_1^2, \ldots, x_n^2] + 4S[n]$, $I = \sum_{i=1}^{n} (x_i^8 + x_i^4) S[n]$, $D = S[n]/I$ and let $\Phi\colon S[n] \to D$ be the quotient homomorphism. Then from Proposition 8 and the identities (43)–(45) we have that

$$v(4, S[n]) \leqslant v(4, D)+30n, \tag{46}$$

$$J(4, S[n]) = T \cap \Phi^{-1}(J(4, D)). \tag{47}$$

Now D is the direct sum $\bigoplus_{\mathfrak{p}} D_{\mathfrak{p}}$ of its localizations at primes $\mathfrak{p}$ of D. Hence

$$J(4, D) = \bigoplus_{\mathfrak{p}} J(4, D_{\mathfrak{p}}) \tag{48}$$

and by Lemma 1(b),

$$v(4, D) \leqslant 2 \max_{\mathfrak{p}} v(4, D_{\mathfrak{p}}). \tag{49}$$

There are 2^n primes $\mathfrak{p}$, corresponding to the homomorphisms of D into F_2.

Let $\mathfrak{p}$ be a fixed prime of D. If $x \in S[n]$, let x' denote $\Phi(x)$ and let $\bar{x}$ denote the image of x' under the map $D \to D\mathfrak{p}$. Since the residue field of $\mathfrak{p}$ is F_2, either $x' \in \mathfrak{p}$ or $x'-1 \in \mathfrak{p}$. Let Γ_1 be the set of $i = 1, \ldots, n$ such that $x_i' \in \mathfrak{p}$, and let Γ_2 be those i such that $x_i'-1 \in \mathfrak{p}$. If $i \in \Gamma_1$ then $\bar{x}_i$ is nilpotent, so $\bar{x}_i^8+\bar{x}_i^4 = 0$ implies $\bar{x}_i^4 = 0$. Similarly, $\bar{x}_i^4 = -1$ if $i \in \Gamma_2$. Since the map $D \to D_{\mathfrak{p}}$ is surjective, the order of $D_{\mathfrak{p}}$ is hence $\leqslant 8^{4^n}$. But D has order 8^{8^n} and there are 2^n prime ideals $\mathfrak{p}$, so $D_{\mathfrak{p}}$ has order 8^{4^n}. From this we have that

$$D_{\mathfrak{p}} = \bigotimes_{i \in \Gamma_1^S} R_1 \otimes \bigotimes_{i \in \Gamma_2^S} R_2 \tag{50}$$

where the tensor products are over S, R_1 is the ring $S[x]/x^4S[x]$ and R_2 is the ring $S[x]/(x^4+1)S[x]$. Note that R_1 and R_2 are not isomorphic, since $u^2 = 0$ for u in the maximal ideal of R_1, but $(1+x)^8 = 0 \neq (1+x)^4$ in R_2.

Let $T_{\mathfrak{p}}$ be the image of T under the map $S[n] \to D \to D_{\mathfrak{p}}$. By (47),

$$T/J(4, S[n]) \simeq \bigoplus_{\mathfrak{a}} T_{\mathfrak{a}}/J(4, D_{\mathfrak{a}}) \tag{51}$$

the sum being over the primes $\mathfrak{a}$ of D. We now consider $T_{\mathfrak{p}}/J(4, D_{\mathfrak{p}})$.

For $i \in \Gamma_1$, let $u_i = x_i$, and for $i \in \Gamma_2$ let $u_i = x_i-1$. Then each $\bar{u}_i$ is nilpotent, the $\bar{u}_i$ generate the maximal ideal of $D_{\mathfrak{p}}$, and $1, \bar{u}_1, \ldots, \bar{u}_n$ generate $D_{\mathfrak{p}}$. We also have

$$T = S[u_1^4, \ldots, u_n^4]+2S[u_1^2, \ldots, u_n^2]+4S[u_1, \ldots, u_n]. \tag{52}$$

Let I_1 be the ideal of $S[n]$ generated by $(u_1, \ldots, u_n)$. Consider the mod 8 identities

$$4xy+4x^3y+4xy^3+4x^3y^3 \equiv (x+y)^4-x^4-y^4-(1+xy)^4+1+(xy)^4, \tag{53}$$

$$6x^2y^2+4x^3y+4xy^3 \equiv (x+y)^4-x^4-y^4, \tag{54}$$

$$4x+6x^2+4x^3 \equiv (1+x)^4-1-x^4. \tag{55}$$

If x and y are nilpotent elements in $D_{\mathfrak{p}}$, then by induction on the nilpotency of x and y, (53) implies that $4xy \in J(4, D_{\mathfrak{p}})$. From (54) and (55) we now have that

$$4\bar{f}\bar{g},\ 2\bar{f}^2\bar{g}^2,\ 4\bar{f}+2\bar{f}^2 \in J(4, D_{\mathfrak{p}}) \quad \text{if} \quad f, g \in I_1. \tag{56}$$

From (52) and (56) we have that $4\bar{u}_1, \ldots, 4\bar{u}_n$ generate $T_{\mathfrak{p}}$ mod $J(4, D_{\mathfrak{p}})$. I claim that $\sum_{i=1}^{n} \bar{a}_i 4\bar{u}_i \in J(4, D_{\mathfrak{p}})$ and $a_i \in S$ imply $4a_i = 0$ for all i. For if say $4a_i \neq 0$, then $4\bar{u}_1 \in J(4, D_{\mathfrak{p}})$. Now (50) implies $4x \in J(4, R_1)$ or $4x \in J(4, R_2)$, which one shows directly not to hold. Hence $T_{\mathfrak{p}}/J(4, D_{\mathfrak{p}})$ is a vector space of dimension n over F_2, with basis $4\bar{u}_1, \ldots, 4\bar{u}_n$. From (51) it now follows that $T/J(4, S[n])$ is a vector space of dimension $n2^n$ over F_2. Hence

$$\varphi(4, 2, n) = n2^n.$$

We now bound $v(4, D_{\mathfrak{p}})$. We have

$$2T = 2S[x_1^4, \ldots, x_n^4]+4S[x_1^2, \ldots, x_n^2],$$

and if $f(x_1^2, \ldots, x_n^2) \in S[x_1^2, \ldots, x_n^2]$ then

$$4f(x_1^2, \ldots, x_n^2) = 2(1+f(x_1, \ldots, x_n))^4-2-2f(x_1, \ldots, x_n)^4.$$

Hence $2T_{\mathfrak{p}} \subseteq J(4, D_{\mathfrak{p}})$ and $v(4, D_{\mathfrak{p}}, 2T_{\mathfrak{p}}) \leqslant 6$. Now $T_{\mathfrak{p}}/2T_{\mathfrak{p}}$ is of dimension 4^n over F_2, so $J(4, D_{\mathfrak{p}})/2T_{\mathfrak{p}}$ is of dimension 4^n-n over F_2. Hence every $f \in J(4, D_{\mathfrak{p}})$ equals $\sum_{i=1}^{4^n-n} g_i^4+h$ for some $g_i \in D_{\mathfrak{p}}$ and some $h \in 2T_{\mathfrak{p}}$. It follows that

$$v(4, D_{\mathfrak{p}}) \leqslant 4^n-n+6. \tag{57}$$

In a later paper we will make a more detailed study of $v(4, D_{\mathfrak{p}})$.

Now from (46), (49) and (57) we have

$$v(4, S[n]) \leqslant 2(4^n-n)+12+30n. \tag{58}$$

Case 2. $R = F_3[n]$. In the notation of Proposition 5, we have $c_3 = c$ for all positive integers c except $c = 2$, in which case $c_3 = 1$. Let $\mathfrak{J}$ be the set of $(9^n-3^n)/2$ maximal ideals M of $F_3[n]$ such that R/M is isomorphic to F_9 (cf. the proof of Proposition 6). Then by the remarks following Proposition 4, we have an exact sequence

$$0 \to \bigcap \mathfrak{J} \to J(4, F_3[n]) \to \bigoplus_{M \in \mathfrak{J}} J(4, F_3[n]/M) \to 0 \tag{59}$$

where $J(4, F_3[n]/M) \cong F_3$ if $M \in \mathfrak{J}$.

By Propositions 7 and 5 we have

$$\varphi(4, 3, n) = \dim_{F_3} F_3[n]/J(4, F_3[n]) = (9^n-3^n)/2$$

and

$$v(4, F_3[n]) \leqslant 4n+1. \tag{60}$$

Summary. The analysis of $J(4, Z[n])$ is reduced by the exact sequence (43) to that of $J(4, S[n])$ and $J(4, F_3[n])$. By (47) and (48), the structure of $J(4, S[n])$ is determined by that of $J(4, D_p)$ when D_p is a finite local ring of the form (50). The structure of $J(4, F_3[n])$ is given by the exact sequence (59). We have $\varphi(4, 2, n) = n2^n$, $\varphi(4, 3, n) = (9^n - 3^n)/2$, and by (41), (58) and (59),

$$v(4, Z[n]) \leqslant 2(4^n - n) + 34n + 21.$$

References

[1] R. F. Arens and I. Kaplansky, *Topological representation of algebras*, Trans. Amer. Math. Soc. 63 (1948), pp. 457–481.
[2] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison Wesley, U. S. A., 1969.
[3] P. T. Bateman and R. M. Stemmler, *Waring's problem for algebraic number fields and primes of the form* $(p^r - 1)/(p^d - 1)$, Illinois J. Math. 6 (1962), pp. 142–156.
[4] M. Bhaskaran, *Sums of* m^{th} *powers in algebraic and abelian number fields*, Archiv der Mathematik (Basel), 17 (1966), pp. 497–504.
[5] — *Corrections to the paper 'Sums of* m^{th} *powers'*, ibid. 22 (1971), pp. 370–371.
[6] N. Borevich and I. Shafarevich, *Number theory*, Academic Press U. S. A. (1966).
[7] J. Chen, *On Waring's problem for* n^{th} *powers*, Acta Math. Sinica 8 (1958), pp. 253–257 (Chinese-English summary).
[8] T. Chinburg and M. Henriksen, *Sums of k-th powers in the ring of polynomials with integer coefficients*, Acta Arith. 29 (1976), pp. 227–250.
[9] W. H. J. Fuchs and E. M. Wright, *The 'easier' Waring problem*, Quart. J. Math. (Oxford) 10 (1939), pp. 190–209.
[10] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum' (IV) The singular series in Waring's problem and the value of the number* $G(k)$, Math. Zeitschr. 12 (1922), pp. 161–188.
[11] — *(VIII) The number* $\Gamma(k)$ *in Waring's problem*, Proc. London Math. Soc. (2), 28 (1928).
[12] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Great Britain (1938).
[13] N. Jacobson, *Theory of rings*, Mathematical Surveys, vol. 2, Amer. Math. Soc., New York, 1943.
[14] — *A topology for the set of primitive ideals in an arbitrary ring*, Proc. Nat. Acad. Sci. U. S. A. 31 (1945), pp. 333–338.
[15] J. R. Joly, *Sommes de puissances d-ièmes dans un anneau commutatif*, Acta Arith. 17 (1970), pp. 37–114.
[16] R. M. Kubota, *Waring's problem for* $F_q[x]$, Dissertationes Mathematicae, 117 (1974), pp. 1–60.
[17] W. J. LeVeque, *Topics in number theory*, Addison Wesley, U. S. A. (1956).
[18] R. E. A. C. Paley, *Theorems on polynomials in a Galois field*, Quart. J. Math (Oxford) 4 (1933), pp. 22–63.
[19] T. Rai, *Easier Waring problem*, J. Sci. Res. Benares Hindu Univ. 1 (1950–1951), pp. 5–12.

[20] C. P. Ramanujam, *Sums of* m^{th} *powers in p-adic rings*, Mathematika 10 (1963), pp. 137–146.
[21] C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. 66 (1944).
[22] R. M. Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arith. 6 (1961), pp. 447–468.
[23] L. Tornheim, *Sums of* n^{th} *powers in fields of prime characteristic*, Duke Math. J. 4 (1938), pp. 359–362.
[24] I. M. Vinogradov, *On an upper bound for* $G(n)$, Izw. Akad. Nauk SSSR, Ser. Mat. 23 (1959), pp. 637–642.

HARVARD UNIVERSITY
Cambridge, Mass., U.S.A.

Received on 29. 7. 1976
and in revised form on 18. 3. 1977 (865)