ACTA ARITHMETICA
XXIX (1976)

Sums of k-th powers in the ring of polynomials with integer coefficients

by

TED CHINBURG and MELVIN HENRIKSEN (Claremont, Cal.)

1. Introduction. Suppose R is a ring with identity element 1 and k is a positive integer. Let $H(k, R)$ denote the set of kth powers of elements of R, and let $J(k, R)$ denote the additive subgroup of R generated by $H(k, R)$. If Z denotes the ring of integers, then

$$G(k, R) = \{a \in Z\colon \; aR \subseteq J(k, R)\}$$

is an ideal of Z.

Let $Z[x]$ denote the ring of polynomials over Z and suppose $a \in R$. Since the map $p(x) \to p(a)$ is a homomorphism of $Z[x]$ into R, the well known identity (see [8], p. 325)

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

in $Z[x]$ tells us that $k! \in G(k, Z[x]) \subseteq G(k, R)$. Since Z is a cyclic under addition, this shows that $G(k, R)$ is generated by its minimal positive element, which we denote by $m(k, R)$. Abbreviating $m(k, Z[x])$ by $m(k)$, we then have

$$m(k, R) \mid m(k) \quad \text{and} \quad m(k) \mid k!.$$

Let H denote an ideal of R, f an element of R and $\hat{f}$ the image of f under the homomorphism $R \to R/H$. Suppose n is a positive integer and that $a_i \in Z$ and $g_i \in R$ for $i = 1, \ldots, n$. If

$$f \equiv \sum_{i=1}^{n} a_i g_i^k \mod H \tag{2}$$

then we call the ordered set $W = \langle (a_i, g_i) \rangle_{i=1}^{n}$ a (k, R) *set for* f mod H, and if $H = \{0\}$, *for* f. Clearly $\hat{f} \in J(k, R/H)$ if and only if there is a (k, R) set for f mod H.

Suppose that $\langle (a_i, g_i)\rangle_{i=1}^n$ is a $(k, Z[x])$ set for $f = m(k)x$, so that (2) holds with $H = \{0\}$. Then on differentiating (2) with respect to x we have that $k|m(k)$. Thus, if R is any ring with identity,

$$(3) \qquad k|m(k), \quad m(k, R)|m(k) \quad \text{and} \quad m(k)|k!.$$

The main purpose of this paper is to give a readily computed formula for $m(k)$ as a function of k. Our proofs also provide (albeit not efficiently) a $(k, Z[x])$ set for $m(k)x$.

Before giving our results we introduce some notation and terminology. Let Z^+ denote the set of positive integers. If $k \in Z^+$, let $\mathscr{P}(k)$ denote the set of primes $\leqslant k$,

$$\mathscr{P}_1(k) = \{p \in \mathscr{P}(k)\colon p < k \text{ and } p|k\} \quad \text{and} \quad \mathscr{P}_2(k) = \{p \in \mathscr{P}(k)\colon p \nmid k\}.$$

Suppose p is a prime, r and m are positive integers, and $m > 1$. A number of the form $\dfrac{p^{mr}-1}{p^r-1}$ is called a *p-power-sum* and mr is called its *index*. We adopt the convention that the product of an empty set of integers is 1.

THEOREM 1. *If k is a positive integer then*

$$m(k) = k\prod \{p^{\alpha_k(p)}\colon p \in \mathscr{P}_1(k)\} \prod \{p^{\beta_k(p)}\colon p \in \mathscr{P}_2(k)\}$$

where

(a) $$\alpha_k(p) = 1 \quad \textit{if} \quad p \textit{ is odd};$$

(b) $$\alpha_k(2) = \begin{cases} 2 & \textit{if } (2^j-1)|k \textit{ for some } j \geqslant 2, \\ 1 & \textit{otherwise}; \end{cases}$$

(c) $$\beta_k(p) = \begin{cases} 1 & \textit{if some } p\textit{-power-sum divides } k, \\ 0 & \textit{otherwise}. \end{cases}$$

Sections 2, 3, and 4 are devoted to the proof of Theorem 1. In the course of the proof we indicate how $(k, Z[x])$ set for $m(k)x$ may be constructed.

In Section 5, we discuss briefly the behavior of the function $m(k)/k$ and indicate the relation of its behavior to some outstanding unsolved problems in the theory of numbers.

In Section 6, after noting that $J(k; R) = R$ if $m(k)$ is a unit in a ring R with an identity element, we apply some of our results to obtain conditions that guarantee that certain kinds of rings are commutative.

In an appendix, we give a table of values of $m(k)/k$ for $1 \leqslant k \leqslant 150$.

The techniques used are elementary and we make use of properties of finite fields and results due to Bhaskaran [3], [4], Bateman and Stemmler [2] and Joly [11].

2. A reduction of the problem of determining $m(k, R)$. For any prime p and non-zero $a, b \in Z$ let $v_p\left(\dfrac{a}{b}\right) = \alpha$ if $\dfrac{a}{b} = \dfrac{r}{s}p^\alpha$, where $(r, p) = (s, p) = 1$, and let $v_p(0) = \infty$. Then v_p is the usual p-adic valuation on the field Q of rational numbers, and as is readily verified

$$(4) \qquad v_p(ab) = v_p(a) + v_p(b) \quad \text{and} \quad v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}$$

if $a, b \in Q$.

If R is a ring and $mR = \{0\}$ for some $m \in Z^+$, then the smallest such m is called the *characteristic* of R. If no such m exists, R is said to have *characteristic* 0.

If $0 \leqslant m \leqslant n$ and $m, n \in Z$, we let, as usual, $\dbinom{n}{m} = \dfrac{n!}{m!(n-m)!} \in Z^+$.

If $W' = \langle (a_i', g_i')\rangle_{i=1}^{n'}$, define

$$W + W' = \langle (a_i'', g_i'')\rangle_{i=1}^{n+n'},$$

where $(a_i'', g_i'') = (a_i, g_i)$ if $1 \leqslant i \leqslant n$ and $(a_i'', g_i'') = (a_i', g_i')$ if $n+1 \leqslant i \leqslant n+n'$.

The following two lemmas will be used frequently.

LEMMA 2. *Suppose b, r, k and n are positive integers, R is a ring with identity element, f and f' are elements of R and $H, H', H(1), \ldots, H(n)$ are ideals of R. Let W and W' denote (k, R) sets for $f \bmod H$ and $f' \bmod H'$, respectively, and suppose $W = \langle (a_i, g_i)\rangle_{i=1}^r$.*

(a) *$W + W'$ is a (k, R) set for $f + f' \bmod H + H'$. If $f' = f - \sum_{i=1}^r a_i g_i^k$, then $W + W'$ is a (k, R) set for $f \bmod H'$.*

(b) *If $\hat{g}$ denotes the image of $g \in R$ under the homomorphism $R \to R/H$, then W is a (k, R) set for $g \bmod H$ if and only if $\hat{W} = \langle (a_i, \hat{g}_i)\rangle_{i=1}^r$ is a $(k, R/H)$ set for $\hat{g}$.*

(c) *If $H' \subset H$, then $m(k, R/H)|m(k, R/H')$, and if also $H \subset J(k, R) + H'$, then $m(k, R/H') = m(k, R/H)$.*

(d) *Suppose $\dbinom{k}{j}(H(i))^j \subset kH(i+1) \subset kH(i)$ for $i = 1, \ldots, n-1$, and $k \geqslant j \geqslant 2$. Then*

$$kH(1) \subset J(k, R) + kH(n), \quad m\big(k, R/kH(1)\big) = m\big(k, R/kH(n)\big),$$

and if $H = kH(1)$ then from W we may construct a (k, R) set for $f \bmod kH(n)$.

(e) *If R has characteristic b then $m(k, R) = \big(m(k, R), b\big)$. If b is prime to k then*

$$H \subset J(k, R) + H^n, \quad m(k, R/H) = m(k, R/H^n)$$

and from W we may construct a (k, R) set for $f \bmod H^n$.

(f) *If* $R = H(1)\oplus H(2)\oplus\ldots\oplus H(n)$ *is the direct sum of the ideals* $H(i)$, *then* $m(k, R)$ *is the least common multiple of* $\{m(k, H(i))\mid i = 1,\ldots,n\}$. *If* $f_i\in H(i)$ *and* $W(i)$ *is a* $(k, H(i))$ *set for* f_i, *for* $i = 1,\ldots,n$, *then* $W(1)+\ldots+W(n)$ *is a* (k, R) *set for* $f_1+\ldots+f_n$.

Proof. The proofs of (a), (b) and (c) are left as exercises.

In (d), suppose $f_1\in kH(1)$, so that $f_1 = kh_1$ for some $h_1\in H(1)$. If $h_i\in H(i)$ and f_i have been defined for $1\leqslant i\leqslant m<n$, let $f_{m+1} = -\sum_{j=2}^{k}\binom{k}{j}h_m^j$. Then $f_{m+1}\in kH(m+1)$ since $\binom{k}{j}(H(m))^j\subset kH(m+1)$ if $k\geqslant j\geqslant 2$. Hence there is some $h_{m+1}\in H(m+1)$ for which $f_{m+1} = kh_{m+1}$. By the binomial theorem,

$$f_{m+1} = kh_m-(1+h_m)^k+1^k = f_m-(1+h_m)^k+1^k \quad \text{if} \quad 1\leqslant m<n.$$

Hence $f_1 = f_n+1-n+\sum_{i=1}^{n-1}(1+h_i)^k$, so since $f_n\in kH(n)$,

$$kH(1)\subseteq J(k, R)+kH(n).$$

Since $kH(n)\subset kH(1)$, $m(k, R/kH(1)) = m(k, R/k(H(n)))$ now follows from (c). If $H = kH(1)$ and $f-\sum_{i=1}^{r}a_ig_i^k = f_1\in kH(1)$ then

$$W+\langle(1-n, 1)\rangle+\langle(1, 1+h_m)\rangle_{m=1}^{n-1}$$

is a (k, R) set for $f \bmod kH(n)$.

If $bR = \{0\}$ then $m(k, R)|b$, so $m(k, R) = (b, m(k, R))$. If b is prime to k, then k is a unit of R. Hence if $H(i) = H^i$ for $i = 1,\ldots,n$ then $kH(i) = H(i)$ for all i since $H(i)$ is an ideal. Clearly

$$\binom{k}{j}H(i)^j\subset H(i)^j = kH(i)^j\subset kH(i+1)\subset kH(i) \quad \text{if} \quad i = 1,\ldots,n-1 \text{ and } k\geqslant j\geqslant 2,$$

so (e) now follows from (d).

Proof of (f). Since $m(k, H(i))H(i)\subset J(k, H(i))\subset J(k, R)$ for $i = 1,\ldots,n$, and $R = H(1)\oplus\ldots\oplus H(n)$, we have

$$\overline{m}R\subset J(k, R), \quad \text{where} \quad \overline{m} = \text{l.c.m.}\ \{m(k, H(i))\mid i = 1, 2,\ldots,n\}.$$

Thus $m(k, R)|\overline{m}$.

Since R is the direct sum of the ideals $H(i)$, each $H(i)$ has an identity element e_i and $e_iH(j) = 0$ if $i\neq j$. Hence $J(k, R)e_i\subset J(k, H(i))$ and

$$m(k, R)H(i) = m(k, R)H(i)e_i\subset J(k, R)e_i\subset J(k, H(i)).$$

Thus $m(k, H(i))|m(k, R)$ for $i = 1,\ldots,n$, so $\overline{m}|m(k, R)$. It follows that $m(k, R) = \overline{m}$, so (f) holds.

LEMMA 3. *Suppose* j, n *and* k *are positive integers,* $2\leqslant j\leqslant k$ *and* $p\in\mathscr{P}(k)$. *Then*

$$v_p(k)+n < v_p\left(\binom{k}{j}\right)+jn$$

unless $p = j = 2|k$ *and* $n = 1$, *in which case* $v_2(k)+1 = v_2\left(\binom{k}{2}\right)+2$.

Proof. Clearly $v_p(j) < p^{v_p(j)}\leqslant j$ since $p\geqslant 2$, so $j-1-v_p(j)\geqslant 0$. By (4),

$$v_p\left(\binom{k}{j}\right) = v_p\left(\frac{k}{j}\binom{k-1}{j-1}\right)\geqslant v_p\left(\frac{k}{j}\right) = v_p(k)-v_p(j).$$

Then

$$v_p\left(\binom{k}{j}\right)+jn-\{v_p(k)+n\}\geqslant n(j-1)-v_p(j)\geqslant j-1-v_p(j)\geqslant 0.$$

Since $j-1-v_p(j) = v_p\left(\frac{p^{j-1}}{j}\right)$, strict inequality will hold if $j<p^{j-1}$. Note that $(i+1)/i<2\leqslant p$ if $i\geqslant 2$. Then if $2<p$ and $2\leqslant j$,

$$j = 2\prod_{i=2}^{j-1}\frac{i+1}{i}\leqslant 2^{j-1}<p^{j-1}.$$

If $p = 2$ and $3\leqslant j$, then

$$j = 3\prod_{i=3}^{j-1}\frac{i+1}{i}<2^2\cdot 2^{j-3} = p^{j-1}.$$

Hence strict inequality follows unless $j = p = 2$.

Now

$$v_2\left(\binom{k}{2}\right) = v_2(k)+v_2(k-1)-1,$$

so

$$v_2\left(\binom{k}{2}\right)+2n-\{v_2(k)+n\} = v_2(k-1)+n-1.$$

Then

$$v_2(k)+n<v_2\left(\binom{k}{2}\right)+2n$$

unless $v_2(k-1) = n-1 = 0$, that is unless $2|k$ and $n = 1$, in which case

$$v_2(k)+1 = v_2\left(\binom{k}{2}\right)+2,$$

which proves the lemma.

If p is a prime in $\mathscr{P}(k)$, let

$$\delta(k,p) = \begin{cases} 0 & \text{if} \quad p = k, \\ 1 & \text{if} \quad p < k \text{ and } p \text{ or } k \text{ is odd}, \\ 2 & \text{if} \quad p = 2 < k \text{ and } k \text{ is even}. \end{cases} \tag{5}$$

For any ring R, $k \in Z^+$ and $p \in \mathscr{P}(k)$, we abbreviate

$$R/p^{\{v_p(k)+\delta(k,p)\}}R \text{ by } R(k,p).$$

PROPOSITION 4. *Let R be a ring with identity element, k a positive integer and f an element of $J(k, R)$. If $p \in \mathscr{P}(k)$, let f_p denote the image of f under the homomorphism $R \to R(k,p)$, and let $W(f, k, p, R)$ be a $(k, R(k,p))$ set for f_p. Then*

(a) $m(k, R) = \prod\{m(k, R(k,p)): p \in \mathscr{P}(k)\}$.

(b) $v_p(m(k,R)) = v_p(m(k; R(k,p))) \leqslant v_p(k) + \delta(k,p)$.

(c) *From $\{W(f,k,p,R): p \in \mathscr{P}(k)\}$ one can construct a (k, R) set for f.*

Proof. By (3), $k!R \subset J(k,R)$. Now

$$R/k!R = \sum \oplus \{R/p^{v_p(k!)}R: p \in \mathscr{P}(k)\} \quad \text{and} \quad m(k, R/p^{v_p(k!)}R) | p^{v_p(k!)}.$$

So, by Lemma 2 ((c), (f)),

$$\begin{aligned} m(k,R) &= m(k, R/k!R) = \text{l.c.m. } \{m(k, R/p^{v_p(k!)}R): p \in \mathscr{P}(k)\} \\ &= \prod \{m(k, R/p^{v_p(k!)}R): p \in \mathscr{P}(k)\}. \end{aligned} \tag{6}$$

If $p \in \mathscr{P}(k)$, let $\hat{f}_p$ denote the image of f under the homomorphism $R \to R/p^{v_p(k!)}R$. By Lemma 2 ((f), (b), (a)) and (1), to construct a (k, R) set for f, it suffices to construct for each $p \in \mathscr{P}(k)$ a $(k, R/p^{v_p(k!)}R)$ set for $\hat{f}_p$.

Fixing $p \in \mathscr{P}(k)$, let $R' = R/p^{v_p(k!)}R$. If $\delta(k,p) = 0$, then $v_p(k) = v_p(k!) = 1$, so

$$m(k, R/p^{v_p(k!)}R) = m(k, R') = m(k, R(k,p)). \tag{7}$$

By Lemma 2 (c), $m(k, R(k,p)) | m(k, R)$. Then since $R' = R(k,p)$, from $W(f, k, p, R)$ we may construct a (k, R') set for $\hat{f}_p$.

If $\delta(k,p) > 0$, let $n = v_p(k!) - v_p(k) - \delta(k,p) + 1$ and $H(i) = p^{\delta(k,p)+i-1}R'$ for $i = 1, \ldots, n$ so that $kH(n) = \{0\}$. By Lemma 3, if $1 \leqslant i \leqslant n-1$ and $k \geqslant j \geqslant 2$ then

$$v_p(k) + \delta(k,p) + i - 1 < v_p\left(\binom{k}{j}\right) + j(\delta(k,p) + i - 1).$$

Hence

$$\binom{k}{j}(H(i))^j = p^{v_p(\binom{k}{j}) + j(\delta(k,p)+i-1)}R' \subset p^{v_p(k)+\delta(k,p)+i}R' = kH(i+1),$$

and clearly $kH(i+1) \subset kH(i)$. Then by Lemma 2 (d),

$$m(k, R') = m(k, R'/kH(n)) = m(k, R'/kH(1)).$$

Now $R(k,p)$ and $R'/kH(1)$ are isomorphic, so (7) holds in all cases, and (a) follows from (6) and (7).

We now apply Lemma 2 (b) to construct from $W(f,k,p,R)$ a (k, R') set for $\hat{f}_p \bmod kH(1)$. Since $kH(n) = 0$, we may apply Lemma 2 (d) to construct a (k, R') set for $\hat{f}_p$ as required to establish (c).

For any $p \in \mathscr{P}(k)$, $p^{v_p(k)+\delta(k,p)}R(k,p) = \{0\}$. Hence

$$m(k, R(k,p)) | p^{v_p(k)+\delta(k,p)},$$

so from (a) we have $v_p(m(k,R)) = v_p(m(k, R(k,p))) \leqslant v_p(k) + \delta(k,p)$ and thus (b) holds.

The next corollary follows immediately from Proposition 4 (b) and the definition of $\delta(k,p)$.

COROLLARY 5. *If k is a positive integer, and p is a prime less than k, then*

(a) *If p or k is odd, then* $v_p\left(\dfrac{m(k)}{k}\right) \leqslant 1$.

(b) *If k is even, then* $v_2\left(\dfrac{m(k)}{k}\right) \leqslant 2$.

3. Computation of the exponents $\beta_k(p)$. If p is a prime let Z_p denote the ring of integers mod p and $Z_p[x]$ the ring $Z[x]/pZ[x]$. We now make use of some known properties of $Z_p[X]$ and of finite fields (for general background, see [1], Chapter 5). For every prime p and $j \in Z^+$ there is a monic irreducible $p(x) \in Z_p[x]$ of degree j and a unique finite field of p^j elements, which we denote by $\mathrm{GF}[p^j]$. The map $p(x)Z_p[x] \leftrightarrow p(x)$ is a one-one correspondence between the non-zero prime ideals $I = p(x)Z_p[x]$ of $Z_p[x]$ and the irreducible monic polynomials $p(x) \in Z_p[x]$. If $p(x)$ is of degree j, then $\mathrm{GF}[p^j]$ and $Z_p[x]/I$ are isomorphic, and I is said to be of degree j. Every ideal of $Z_p[x]$ is principal, and $Z_p[x]$ is a unique factorization domain. If $I = f(x)Z_p[x]$ is a non-zero proper ideal of $Z_p[x]$ and $f(x) = a\prod_{i=1}^{n}[p_i(x)]^{m_i}$, where $p_1(x), \ldots, p_n(x)$ are irreducible in $Z_p[x]$, $a \in Z_p$, and $m_i \in Z^+$ for $i = 1, 2, \ldots, n$, then $Z_p[x]/I$ is isomorphic to the direct sum of the rings $Z_p[x]/I_i^{m_i}$, where $I_i = [p_i(x)]Z_p[x]$.

The next lemma is proved by M. Bhaskaran in [3], [4]. See also [11].

LEMMA 6 (Bhaskaran). *If p is a prime less than a positive integer k, then for any positive integer $j > 1$, $J(k, \mathrm{GF}(p^j)) = \mathrm{GF}(p^j)$ if and only if k has no p-power-sum divisor of index j.*

Proposition 7. *Suppose p is a prime less than a positive integer k that does not divide k, and that k has a p-power-sum divisor. Then*

$$v_p(m(k)) = \beta_k(p) = 1$$

and $W(m(k)x, k, p, Z[x]) = \langle(0,0)\rangle$ is a $(k, Z[x](k,p))$ set for

$$m(k, Z[x](k,p))x.$$

Proof. Since $p \in \mathscr{P}_2(k)$, $v_p(k) = 0$ and $v_p(m(k)) = v_p(m(k, Z_p[x])) \leqslant 1$ by Proposition 4(b). Hence if $v_p(m(k)) = 0$, then $(p, m(k, Z_p[x])) = 1$. So, $m(k, Z_p[x]) = 1$ and $J(k, Z_p[x]) = Z_p[x]$ by Lemma 2 (e). By assumption, k has a p-power-sum divisor of some index $j > 1$. So by Lemma 6, $J(k, \mathrm{GF}[p^j])$ is contained properly in $\mathrm{GF}[p^j]$, which contradicts the above since $\mathrm{GF}[p^j]$ is a homomorphic image of $Z_p[x]$. Hence $v_p(m(k)) = \beta_k(p) = 1$. Clearly $\langle(0,0)\rangle$ is a $(k, Z_p[x])$ set for $m(k, Z_p[x])x$ since $m(k, Z_p[x])x = 0$ in $Z_p[x]$.

The rest of this section is devoted to determining $\beta_k(p)$ in case k has no p-power-sum divisor.

The first part of the next lemma is proved by J. Joly in [11], pp. 52–53.

Lemma 8. *Suppose p is a prime and r is a positive integer prime to p.*

(a) (Joly) *The dimension of $Z_p[x]/J(r, Z_p[x])$ as a vector space over Z_p does not exceed $(r-1)^2$. If $C = \{x^i\colon i = 1, \ldots, r^2-r-1$ and $i \not\equiv 0 \bmod k\}$ and D denotes the span of C, then given any $f(x) \in Z_p[x]$, there is a finite procedure for finding an $h(x) \in D$ and $g(x) \in J(r, Z_p[x])$ such that $f(x) = h(x) + g(x)$.*

(b) *There are integers $t > s > 0$ such that*

$$x^{rt+m} - x^{rs+m} \in J(r, Z_p[x])$$

for all nonnegative integers m.

(c) *There is a non-zero proper ideal I contained in $J(r, Z_p[x])$. Given any $g(x) \in I$, one may effectively determine a $(k, Z_p[x])$ set for $g(x)$.*

Proof of (b). Let $A = Z_p[x]/J(r, Z_p[x])$ and B be the direct sum of r copies of A. For each $s > 0$ let

$$G(s) = (x^{rs}, x^{rs+1}, \ldots, x^{rs+r-1}) \in B.$$

Since $\dim A \leqslant (r-1)^2$, we have

$$|A| \leqslant p^{(r-1)^2} \quad \text{and} \quad |B| \leqslant p^{r(r-1)^2}.$$

Hence there exist $0 < s < t \leqslant p^{r(r-1)^2}+1$ for which $G(t) - G(s) = 0$ in B. Moreover, if for each j, $0 < j \leqslant p^{r(r-1)^2}+1$, we use part (a) to express the components of $G(j)$ as elements of $D + J(r, Z_p[x])$, then we may effectively determine s, t and a set of $g_i(x) \in J(r, Z_p[x])$ for which $x^{tr+i} - x^{sr+i} = g_i(x)$ for $i = 0, 1, \ldots, r-1$. Hence if $m = rn + i$ for some $n \geqslant 0$ and $i = 0, \ldots, r-1$, we have

$$x^{tr+m} - x^{sr+m} = x^{rn} g_i(x) \in J(r, Z_p[x]).$$

Proof of (c). If $g(x) = \sum_{m=0}^{n} a_m x^m \in Z_p[x]$ and t and s are as in (b), then

$$g(x)(x^{rt} - x^{rs}) = \sum_{m=0}^{n} a_m (x^{rt+m} - x^{rs+m}) \in J(r, Z_p[x]).$$

Hence we may let $I = (x^{rt} - x^{rs})Z_p[x] \neq 0$.

Proposition 9. *If p is a prime less than a positive integer k, p does not divide k, and k has no p-power-sum divisor, then $v_p(m(k)) = \beta_k(p) = 0$. A $(k, Z[x](k,p))$ set for $m(k, Z[x](k,p))x$ can be effectively determined.*

Proof. By Lemma 6, $J(k, \mathrm{GF}(p^j)) = \mathrm{GF}(p^j)$ for all $j \geqslant 1$, so $m(k, Z_p[x]/P) = 1$ for any non-zero prime ideal P of $Z_p[x]$. Since $p \nmid k$, we have by Lemma 2 (e) that

$$1 = m(k, Z_p[x]/P) = m(k, Z_p[x]/P^m)$$

whenever P is a non-zero prime ideal of $Z_p[x]$ and $m \in Z^+$.

By Lemma 8 (c), there is a non-zero proper ideal $I \subset J(k, Z_p[x])$. Moreover, as noted at the beginning of this section, there are prime ideals $P_1, \ldots, P_n$ and $m_1, \ldots, m_n \in Z^+$ such that

$$Z_p[x]/I = \sum_{i=1}^{n} \oplus Z_p[x]/P_i^{m_i}.$$

Hence by Lemma 2 (c), (f),

$$m(k, Z_p[x]) = m(k, Z_p[x]/I) = \text{l.c.m.}\{m(k, Z_p[x])/P_i^{m_i}\colon i = 1, \ldots, n\} = 1.$$

So, by Proposition 4,

$$\beta_k(p) = v_p(m(k)) = v_p(m(k, Z_p[x])) = 0.$$

By Lemma 2 (b), (a) and Lemma 8 (c), to determine a $(k, Z_p[x])$ set for x it suffices to find a $(k, Z_p[x]/I)$ set for x. Then by Lemma 2 (f), (e), (b) it suffices to find a $(k, Z_p[x]/P_i)$ set for x for each of the prime ideals P_i, $i = 1, \ldots, n$. Since each $Z_p[x]/P_i$ is finite, we conclude that a $(k, Z_p[x])$ set for x can be effectively determined.

Propositions 7 and 9 establish (c) of Theorem 1.

4. Computation of the exponents $a_k(p)$. If $f(x) \in Z[x]$ and $i \geqslant 0$, let $c(i, f)$ denote the coefficient of x^i in $f(x)$.

Lemma 10. *If k is a positive integer, p is a prime, $n = v_p(k) > 0$, and $g(x) \in Z[x]$, then*

$$c(p, g^k) \equiv \binom{k}{p} \frac{c(1, g^k)}{k} \bmod p^n.$$

Proof. We may write $g(x) = b_0+b_1x+x^2h(x)$ for some $b_0, b_1 \in Z$ and $h(x) \in Z[x]$. We abbreviate b_0+b_1x by $a(x)$. By the binomial theorem

$$(8)\qquad [g(x)]^k = \sum_{j=0}^{k}\binom{k}{j}[a(x)]^{k-j}[h(x)]^j x^{2j}$$

and

$$(9)\qquad [a(x)]^k = \sum_{j=0}^{k}\binom{k}{j} b_0^{k-j}b_1^j x^j.$$

Hence

$$(10)\qquad c(1, g^k) = c(1, a^k) = kb_0^{k-1}b_1.$$

If

$$r(p) = \begin{cases} N+1 & \text{if } p = 2N+1 \text{ is odd,}\\ 1 & \text{if } p = 2,\end{cases}$$

and

$$t(x) = \sum_{j=0}^{r(p)}\binom{k}{j}[a(x)]^{k-j}[h(x)]^j x^{2j},$$

then $c(p, g^k) = c(p, t)$. Since $r(p) < p$ and $v_p(k) = n$, if $0 < j \leqslant r(p)$ then $\binom{k}{j} \equiv 0 \bmod p^n$. Hence

$$c(p, g^k) = c(p, t) \equiv c(p, a^k) \equiv \binom{k}{p} b_0^{k-p}b_1^p \bmod p^n$$

by (9). Since $v_p(k) = n$, $\binom{k}{p} \equiv 0 \bmod p^{n-1}$, and by Fermat's Theorem ([7], p. 63), $b_0^{k-p}b_1^p \equiv b_0^{k-1}b_1 \bmod p$. Hence

$$c(p, g^k) \equiv \binom{k}{p} b_0^{k-1}b_1 \equiv \binom{k}{p}\frac{c(1, g^k)}{k} \bmod p^n$$

by (10).

PROPOSITION 11. *If k is a positive integer, p is a prime, $p < k$ and $p|k$, then*

$$a_k(p) = v_p\left(\frac{m(k)}{k}\right) \geqslant 1.$$

Proof. Suppose $m(k)x = \sum_{i=1}^{q} a_i[g_i(x)]^k$ is an identity for $m(k)x$ in $Z[x]$. Since $p|k$, $v_p(k) = n > 0$, so by Lemma 10,

$$0 = \sum_{i=1}^{q} a_i c(p, g_i^k) \equiv \binom{k}{p}\sum_{i=1}^{q} a_i\frac{c(1, g_i^k)}{k} \equiv \binom{k}{p}\frac{m(k)}{k} \bmod p^n.$$

Since $v_p\left(\binom{k}{p}\right) = n-1$, we have $a_k(p) = v_p\left(\frac{m(k)}{k}\right) \geqslant 1$.

Proposition 11 and Corollary 5 together imply

COROLLARY 12. *Suppose k is a positive integer, $p < k$ is a prime, and $p|k$.*

(a) *If p is odd, then* $a_k(p) = v_p\left(\frac{m(k)}{k}\right) = 1$.

(b) $1 \leqslant a_k(2) \leqslant 2$.

In the remaining cases, $k = 2^n r$, where r is odd.

PROPOSITION 13. *If k, n, r and j are positive integers, $k = 2^n r$, $j \geqslant 2$, r is odd, and r is divisible by 2^j-1, then*

$$v_2\left(\frac{m(k)}{k}\right) = a_k(2) = 2.$$

Proof. Let $p(x) \in Z[x]$ be an irreducible of degree $j \,(\bmod 2Z[x])$, so that $GF[2^j]$ and $Z[x]/\{p(x)Z[x]+2Z[x]\}$ are isomorphic. Let $I = p(x)Z[x]+2^{n+2}Z[x]$. If $v_2\left(\frac{m(k)}{k}\right) \leqslant 1$, then since $m(k, Z[x]/I)|m(k)$ and $m(k, Z[x]/I)|2^{n+2}$ we would have

$$m(k, Z[x]/I)|2^{n+1} \quad\text{and}\quad 2^{n+1}x \in J(k, Z[x]) \bmod I.$$

We will prove the proposition by showing that this cannot occur.

If $a \neq 0$ is in $GF[2^j]$, then $a^{2^j-1} = 1$. Since $(2^j-1)|r$, $a^r = 1$. Hence if $g(x) \in Z[x]$, then there is an $m(x) \in Z[x]$ such that either

$$(11)\qquad [g(x)]^r \equiv 1+2m(x) \bmod I$$

or

$$(12)\qquad g(x) \equiv 2m(x) \bmod I.$$

If (11) holds, then

$$[g(x)]^{r2^n} = 1+2^{n+1}\{m(x)+[m(x)]^2\} \bmod I,$$

while if (12) holds,

$$[g(x)]^{r2^n} \equiv 2^{r2^n}[m(x)]^{r2^n} \equiv 0 \bmod I$$

since $r > 2$. Moreover,

$$m(0)+[m(0)]^2 \equiv m(1)+[m(1)]^2 \equiv 0 \bmod 2Z[x]$$

for any $m(x) \in Z[x]$, so, in either case,

$$(13)\qquad [g(0)]^k \equiv [g(1)]^k \bmod I.$$

If $2^{n+1}x = \sum_{i=1}^{q} a_i[g_i(x)]^k$ is an identity for $2^{n+1}x$ in $J(k, Z[x]) \bmod I$, then successively replacing x by 0 and 1 yields $2^{n+1} \equiv 0 \bmod I$. The contradiction proves the proposition.

Next we consider the case when $k = 2^n r$, where r is odd and has no factor (2^j-1) for $j \geq 2$. We need a series of lemmas, the first of which is proved by L. Dickson in [5], p. 45.

LEMMA 14 (Dickson). *If p is a prime, j and r are positive integers and $d = (p^j-1, r)$ then the number of non-zero r-th powers of elements of* $\mathrm{GF}[p^j]$ *is* $(p^j-1)/d$.

Recall that if R is a ring with identity, $H(k, R)$ is the set of kth powers of elements of R. If $n, r \in Z^+$ and h, m and $a \in R$, define

$$\Phi(h, m, a, 1, r) = h^r m + m^2 + a + a^2, \quad \text{and}$$

$$\Phi(h, m, a, n, r) = (h^r)^{2^n-1} m + (h^r)^{2^n-2} m^2 + a + a^2 \quad \text{if } n > 1.$$

LEMMA 15. *If n, r, j are positive integers, $j > 1$, $(2^j-1) \nmid r$ and $b \in \mathrm{GF}[2^j]$, then there are h, m and $a \in \mathrm{GF}[2^j]$ such that*

$$h \neq 0 \quad \text{and} \quad b = \Phi(h, m, a, n, r).$$

Proof. By assumption, $(2^j-1, r) < 2^j-1$, so by Lemma 14 there is an $h^r = t \in H(r, \mathrm{GF}[2^j])$ other than 0 or 1. Since the multiplicative order of t divides 2^j-1, $t^{2^n-1} \neq 0$ or 1. Hence if $f = t^{2^n-1} - t^{2^{n-1}-1}$, then $f \neq 0$. Let $m = f^{-1} b$ and $a = t^{2^{n-1}-1} m$. Then

$$fm + a + a^2 = (t^{2^n-1} m - t^{2^{n-1}-1} m) + t^{2^{n-1}-1} m + t^{2^n-2} m^2 = t^{2^n-1} m + t^{2^n-2} m^2.$$

But $fm = b$, so $b = \Phi(h, m, a, n, r)$. Since $h^r = t \neq 0$ implies $h \neq 0$, the lemma follows.

COROLLARY 16. *If q, n, r are positive integers, $(2^j-1) \nmid r$ for any $j \geq 2$, and $I_1, \ldots, I_q$ are distinct non-zero proper prime ideals of $Z_2[x]$, and $I_0 = \prod_{i=1}^{q} I_i$, then there exist $v(x), h(x), m(x), a(x)$ in $Z_2[x]$ such that $h(x)$ is a unit* $\operatorname{mod} I_0$, *and* $x \equiv \Phi(h(x), m(x), a(x), n, r) + [v(x)]^r \operatorname{mod} I_0$.

Proof. Since $Z_2[x]/I_0$ and $\sum_{i=1}^{q} \oplus Z_2[x]/I_i$ are isomorphic, it suffices to prove the lemma in case $q = 1$ and $I_1 = I_0$. Now $Z_2[x]/I_0$ and $\mathrm{GF}(2^j)$ are isomorphic for some $j \geq 1$. If $j = 1$ and $I_0 = (x+1) Z_2[x]$, we may take $h(x) = v(x) = 1$ and $a(x) = m(x) = 0$. Otherwise $I_0 = x Z_2[x]$ and we may take $h(x) = 1$ and $a(x) = m(x) = v(x) = 0$. If $j > 1$, then by Lemma 15, there are $h(x), m(x), a(x)$ such that $x \equiv \Phi(h(x), m(x), a(x), n, r) \operatorname{mod} I_0$, and we may take $v(x) = 0$, so the Corollary holds.

PROPOSITION 17. *If $k = 2^n r > 2$ for some positive integers r and n such that $(2^j-1) \nmid r$ for any $j \geq 2$ and r is odd, then*

$$a_k(2) = v_2\left(\frac{m(k)}{k}\right) = 1.$$

A $(k, Z[x](k, 2))$ set for $m(k, Z[x](k, 2))x$ can be effectively constructed.

Proof. By Proposition 4 (b) and Corollary 12 (b), it suffices to show that $m(k, R) | 2^{n+1}$, where $R = Z[x]/2^{n+2} Z[x]$. We will show that $2^{n+1} x \in J(k, R)$ by constructing a (k, R) set for $2^{n+1} x$. To simplify notation, h, g, m, a, v, and s will denote elements of R. Recall that $Z_2[x] = Z[x]/2Z[x]$, so that $Z_2[x]$ and $R/2R$ are isomorphic.

By Lemma 8 (c), there is a non-zero proper ideal I of $Z_2[x]$ contained in $J(r, Z_2[x])$. There are prime ideals $I_1, \ldots, I_q$ and positive integers $n_1, \ldots, n_q$ such that $I = \prod_{i=1}^{q} I_i^{n_i}$. Let $I_0 = \prod_{i=1}^{q} I_i$ and let $\hat{I}_0$ be an ideal of R containing $2R$ such that $\hat{I}_0 \equiv I_0 \operatorname{mod} 2R$.

By Corollary 16, there are $h(x), m(x), a(x), v(x)$ in $Z_2[x]$ such that

$$x \equiv \Phi(h(x), m(x), a(x), n, r) + [v(x)]^r \operatorname{mod} I_0,$$

and $h(x)$ is a unit $\operatorname{mod} I_0$. Choose $h, m, a, v \in R$ such that

$$h - h(x) \equiv m - m(x) \equiv a - a(x) \equiv v - v(x) \equiv 0 \operatorname{mod} 2R.$$

Since $Z_2[x]/I_0$ is finite, h, m, a, and v may be effectively determined. Because $h(x)$ is a unit $\operatorname{mod} I_0$, $\hat{I}_0 \equiv I_0 \operatorname{mod} 2R$ and $2R \subset \hat{I}_0$, we know that h is a unit $\operatorname{mod} \hat{I}_0$. Since

$$\Phi(h(x), m(x), a(x), n, r) + [v(x)]^r \equiv \Phi(h, m, a, n, r) + v^r \operatorname{mod} 2R,$$

$$x \equiv \Phi(h, m, a, n, r) + v^r \operatorname{mod} \hat{I}_0, \tag{14}$$

which on multiplying by 2^{n+1} yields

$$2^{n+1} x \equiv 2^{n+1} \Phi(h, m, a, n, r) + 2^{n+1} v^r \operatorname{mod} 2^{n+1} \hat{I}_0. \tag{15}$$

Now if $r = 1$, then clearly

$$2^{n+1} x \in J(k, R) + 2^{n+1} J(r, R) + 2^{n+1} \hat{I}_0. \tag{16}$$

If $r > 1$, then since r and h are units $\operatorname{mod} \hat{I}_0$, we can find an $s \in R$ such that $rsh^{r-1} \equiv m \operatorname{mod} \hat{I}_0$. Hence if $g = h + 2s$, we have

$$g^r \equiv h^r + 2rsh^{r-1} \equiv h^r + 2m \operatorname{mod} 2\hat{I}_0.$$

Expanding $g^k = (g^r)^{2^n}$ by the binomial theorem and using Lemma 3 shows that

$$g^k - h^k \equiv 2^{n+1} \{h^{r(2^n-1)} m + h^{r(2^n-2)} m^2\} \operatorname{mod} 2^{n+1} \hat{I}_0. \tag{17}$$

Since $2^{n+2} R = \{0\}$, we have from Lemma 3 that

$$(1+2a)^k - 1^k = 2^{n+1} \{a + a^2\}. \tag{18}$$

The sum of the right hand side of (17) and (18) is

$$2^{n+1} \Phi(h, m, a, n, r) \operatorname{mod} 2^{n+1} \hat{I}_0,$$

so summing (17) and (18) and substituting in (15) gives

$$(19)\qquad 2^{n+1}x \equiv g^k - h^k + (1+2a)^k - 1^k + 2^{n+1}v^r \epsilon J(k, R) + 2^{n+1}J(r, R) \mod 2^{n+1}\hat{I}_0 .$$

Hence (16) holds for all cases.

If $j = \max(n_1, \ldots, n_q)$, then by Lemma 2 (e), $I_0 \subset J(r, Z_2[x]) + I_0^j$. Since $I_0^j \subset I \subset J(r, Z_2[x])$, we have $I_0 \subset J(r, Z_2[x])$.

Now $I_0 \equiv \hat{I}_0$ and $J(r, Z_2[x]) \subset J(r, R) \mod 2R$, so $\hat{I}_0 \subset J(r, R) \mod 2R$. Thus, since $2^{n+2}R = \{0\}$,

$$(20)\qquad 2^{n+1}\hat{I}_0 \subset 2^{n+1}J(r, R).$$

If $f \epsilon R$, then by the binomial theorem and (18),

$$\sum_{i=0}^{n-1} (1+2f^{r2^i})^{2^n r} = n + 2^{n+1}\{f^r + f^k\}.$$

Hence $2^{n+1}f^r \epsilon J(k, R)$ and so

$$(21)\qquad 2^{n+1}J(r, R) \subset J(k, R).$$

We now apply (20) and (21) sequentially to (16) to have $2^{n+1}x \epsilon J(k, R)$. By our previous remarks, this establishes Proposition 17.

In summary, Theorem 1 follows from (3), Propositions 4, 7, 9, Corollary 12 (a), Proposition 13 and Proposition 17.

5. Arithmetical properties of $m(k)/k$. In this section, we give a number of results concerning the computation of and distribution of values $m(k)/k$. To describe them, it is convenient to introduce some auxiliary number-theoretic functions.

If $k \epsilon Z^+$, let

$$a(k) = \prod \{p^{a_k(p)} : p \epsilon \mathscr{P}_1(k)\}, \qquad b(k) = \prod \{p^{\beta_k(p)} : p \epsilon \mathscr{P}_2(k)\},$$

and let $s(k)$ denote the square free part of k. (That is, $s(1) = 1$, and if $k > 1$, and $k = \prod_{i=1}^{r} p_i^{r_i}$ is the prime power decomposition of k, then $s(k) = \prod_{i=1}^{r} p_i$.) By Theorem 1,

$$(22)\qquad m(k)/k = a(k)\,b(k)$$

and

$$(23)\qquad a(k) = \begin{cases} 1 & \text{if } k \text{ is prime,} \\ s(k) & \text{if } k \text{ is composite and } 2(2^j-1) \nmid k \text{ for all } j \geqslant 2, \\ 2s(k) & \text{otherwise.} \end{cases}$$

To compute $b(k)$ it suffices to determine when a divisor d of k is a p-power sum for some $p \epsilon \mathscr{P}_2(k)$; that is to determine if the exponential diophantine equation

$$(24)\qquad d = \frac{p^{a\varepsilon}-1}{p^a-1} = 1 + p^a + \ldots + p^{a(\varepsilon-1)}$$

has a solution when $d|k$ and $p \epsilon \mathscr{P}_2(k)$.

The following proposition helps to determine when (24) has a solution. Recall that if $x \epsilon Z^+$, then $\varphi(x)$ denotes the number of positive integers $\leqslant x$ that are relatively prime to x. For a discussion of the properties of φ, see [8], Chapter 5.

Proposition 18. *Suppose $a, \gamma, \delta, \varepsilon, b$ are positive integers, $\varepsilon > 1$, p is a prime, $c = \dfrac{p^{\delta a}-1}{p^a-1}$, and d is as in* (24).

(a) $a = v_p(d-1) > 0$.

(b) *$p^{a\delta}d + c$ is a p-power sum of index $(\varepsilon+\delta)a$.*

(c) *If $\varepsilon > \delta+1$, then $(d-c)/p^{a\delta}$ is a p-power sum of index $(\varepsilon-\delta)a$.*

(d) *If $b|d$, then $\varepsilon \equiv 0 \mod b$ or $(\varepsilon, \varphi(b)) > 1$.*

(e) *$c|d$ if and only if $\delta|\varepsilon$.*

(f) *If d and p are odd, then $p^a(p^a+1)|(d-1)$ and $p^{2a}|(d-1-p^a)$.*

(g) *If d is even (where p is odd), then $(1+p^a)|d$.*

Proof. Parts (a), (b), and (c) follow immediately from the definitions of p-power sum and index.

Suppose that $d \equiv 0 \mod b$ and that γ is the multiplicative order of $p^a \mod b$. By Fermat's theorem ([8], Chapter 6), $\gamma|\varphi(b)$. Since $p^{a\varepsilon}-1 = (p^a-1)d \equiv 0 \mod b$, we have that $\gamma|\varepsilon$ and so $\gamma|(\varphi(b), \varepsilon)$. If $\gamma = 1$, then by (24), $\varepsilon \equiv d \equiv 0 \mod b$. Otherwise $(\varphi(b), \varepsilon) \geqslant \gamma > 1$, and so (d) holds.

Suppose $\varepsilon = t\delta + s$ for some integers $t \geqslant 0$ and $\delta > s \geqslant 0$. Clearly $(p^{\delta a}-1)|(p^{t\delta a}-1)$ so $c \,\Big|\, \dfrac{p^{t\delta a}-1}{p^a-1}$. Then since

$$d = \left(\frac{p^{t\delta a}-1}{p^a-1}\right)p^{sa} + \frac{p^{sa}-1}{p^a-1},$$

$c|d$ if and only if $c \,\Big|\, \dfrac{p^{sa}-1}{p^a-1}$. Since $0 \leqslant s < \delta$, this holds if and only if $s = 0$, and so (e) follows.

Suppose d and p are odd, so that $\varepsilon > 2$. Then by (a) and (c), $(d-1)/p^a$ is a p-power sum of index $(\varepsilon-1)a$. Since $(d-1)/p^a$ is even and $\varphi(2) = 1$, part (d) implies that $\varepsilon \equiv 0 \mod 2$. Hence by (e), $(d-1)/p^a$ is divisible by $(p^{2a}-1)/(p^a-1) = 1+p^a$. Hence $p^a(p^a+1)|(d-1)$, and by (c), $p^{2a}|d-(1+p^a)$, so (f) is established.

If d is even, then by (d), $\varepsilon \equiv 0 \bmod 2$, so by (e) d is divisible by $(p^{2a}-1)/(p^a-1) = 1+p^a$, so (g) holds.

In Section 7, we present a table of values of $a(k)$, $b(k)$, and $m(k)/k$ for $1 \leqslant k \leqslant 150$. It was computed by the following "sieve-like" method. First, compute $a(k)$ over the indicated range. Next, make a list of all p-power sums for primes $p < 150$. Such a list is given at the end of the table. Note that in this range, they all take the form $p+1$ if $p > 11$. Observe that if d is a p-power sum, then for any positive integer n, $p|b(nd)$ unless $p|n$ (i.e., unless $p|a(nd)$). In this way, if $b(k')$ is computed for all $k' < k$, all of the prime factors of $b(k)$ can be recorded with the possible exception of those primes p for which k itself is a p-power sum, and using the table of p-power sums will supply these as well.

To extend the table, or to compute individual values of $b(k)$, Proposition 18 can be quite useful as is illustrated by the following example.

Example 19. (i) Suppose $k = 567 = 3^4\cdot 7$. By (23), $a(k) = 3\cdot 7 = 21$. The divisors of 567 are 1, 3, 9, 27, 81, 7, 21, 63, 189, and 567. By the table in Section 7, the prime divisors of $b(k)$ are 2, and those primes $p \neq 2, 3$, or 7 for which either 189 or 567 is a p-power sum. Now $189-1 = 188 = 2^2\cdot 47$, and $567-1 = 566 = 2\cdot 283$, so Proposition 18 (a), (f) eliminates the possibility that 189 or 567 is a p-power sum for any odd prime p. Hence $b(567) = 2$ and $m(567)/567 = 3\cdot 7\cdot 2 = 42$.

(ii) If $k = (97)^2 = 9409$, then $a(k) = 97$, and by the table in Section 7, $b(97) = 1$. Since $(97)^2-1 = 9408 = 2^6\cdot 3\cdot 7^2$, if 9409 is a p-power sum, then by Proposition 18(a), (f), $p = 2$ or 3. By Proposition 18(a), if k is a 3-power sum, then for some $\varepsilon \in Z^+$, $3^\varepsilon = (3-1)(9409)+1 = 18819 \not\equiv 0 \bmod 3^4$. Similarly, k is not a 2-power sum, so $b(9409) = 1$ and $m(9409)/9409 = 97$.

(iii) If $k = 372 = 2^2\cdot 3\cdot 31$, then the divisors of k are 1, 2, 3, 4, 6, 12, 31, 62, 93, 124, 186 and 372. By (23), $a(k) = 2^3\cdot 3\cdot 31 = 744$. The table in Section 7 shows that the prime divisors of $b(k)$ are 5, 11, 61 and those $p \neq 2, 3, 5, 11, 31$ and 61 for which 186 or 372 is a p-power sum. Now $186-1 = 185 = 5\cdot 37$ and $372-1 = 371 = 7\cdot 53$, so by Proposition 18(a), (g), there are no primes of this latter type. Hence $b(372) = 5\cdot 11\cdot 61 = 3355$ and $m(372)/372 = a(372)b(372) = 2^3\cdot 3\cdot 31\cdot 5\cdot 11\cdot 61 = 2{,}496{,}120$.

Next we will prove a result that will yield information about the exponential diophantine equation (24) and will imply that if $k > 1$ is odd, then the sequence $\left\{\frac{m(k^n)}{k^n}\right\}$ is bounded.

The next lemma is closely related to a result of D. Suryanarayana [15]. If Γ is a set of primes, let $S(\Gamma)$ denote the multiplicative semigroup of Z^+ generated by Γ and let $T(\Gamma)$ denote the set of $a > 1$ in Z for which there is a $d > 1$ in Z^+ such that $(a^d-1)/(a-1) \in S(\Gamma)$. If $a > 1$, $d \geqslant 1$ are in Z let $f_a(d) = (a^d-1)/(a-1)$.

Lemma 20. *If Γ is any set of primes and $a \in T(\Gamma)$, then there is a prime p such that $(a^p-1)/(a-1) \in S(\Gamma)$ and $p = 2$ or $p|q-1$ for some $q \in \Gamma$.*

Proof. Suppose $a \in T(\Gamma)$. If $d_1, d_2 \in Z^+$ and $d_1|d_2$ then $f_a(d_1)|f_a(d_2)$. Hence if $f_a(d) \in S(\Gamma)$ and p is a prime divisor of d, then $f_a(p) \in S(\Gamma)$. If $p = 2$, we are done, so assume p is odd.

If $q \in \Gamma$, $q|f_a(p)$, and $a \not\equiv 1 \bmod q$, then $a^p \equiv 1 \bmod q$. Hence $p|\varphi(q) = q-1$. If $a \equiv 1 \bmod q$, then $f_a(p) \equiv p \bmod q$, so $q = p$. Thus if $p \nmid q-1$ for all $q \in \Gamma$, then $f_a(p) = p^n$ for some $n \geqslant 1$. Since $a^p-1 = (a-1)f_a(p) \equiv 0 \bmod p$, Fermat's theorem implies $a \equiv 1 \bmod p$.

Now $f_a(p) = 1+a+\ldots+a^{p-1} \equiv p \bmod p^2$ so $n = 1$. But $a > 1$ so $p = f_a(p) > p$. This contradiction establishes the lemma.

Let $h(1) = 1$ and for $n > 1$ in Z^+, let $h(n)$ denote the largest prime factor of n. The following lemma is proved by G. Polya in [13].

Lemma 21 (Polya). *If $f(x) \in Z[x]$ has more than one complex zero and all of its zeros are distinct, then $\lim_{n\to\infty} h(f(n)) = \infty$.*

The next theorem yields some information about the distribution of values of $m(k)/k$. Recall that a prime is called a *Mersenne* (resp. *Fermat*) prime if $p = 2^n-1$ (resp. $p = 2^n+1$) for some integer $n \geqslant 1$.

Theorem 22. *Suppose Γ is a finite set of primes.*

(a) *$T(\Gamma)$ is the union of a finite set and $\{a \in Z\colon\ a > 1$ and $(a+1) \in S(\Gamma)\}$.*

(b) *If $2 \notin \Gamma$, then $\{a \in T(\Gamma)\colon\ a$ is odd$\}$ is finite.*

(c) *If $2 \notin \Gamma$, then $\{m(k)/k\colon\ k \in S(\Gamma)\}$ is bounded. In particular, if $k > 1$ is an odd integer, then $\{m(k^n)/k^n\}$ is a bounded sequence.*

(d) *If $n > 1$ is an integer, then $m(2^n)/2^{n+1}$ is the product of all the Mersenne primes less than 2^n.*

(e) *If p is a Fermat prime, then $m(p^n)/p^n = 2p$ for every integer $n > 1$.*

Proof. By Lemma 20, there is a finite set Γ_0 of primes such that if $a \in T(\Gamma)$, then

$$\frac{a^p-1}{a-1} = 1+a+\ldots+a^{p-1} \in S(\Gamma) \quad \text{for some } p \in \Gamma_0.$$

If $p = 2$, then $a+1 \in S(\Gamma)$. If p is odd, let $f(x) = 1+x+\ldots+x^{p-1}$ and note that $f(x)$ satisfies the hypothesis of Lemma 21. If $\{a \in Z\colon f(a) \in S(\Gamma)\}$ were infinite, then the sequence $\{h(f(n))\}$ would have a bounded subsequence contrary to the conclusion of Lemma 21. It follows that $\{a \in T(\Gamma)\colon\ a+1 \notin S(\Gamma)\}$ is finite, which establishes (a).

Clearly (b) follows immediately from (a).

If $k \in S(\Gamma)$, then by (23), $a(k) \leqslant 2s(k) \leqslant 2\prod\{p\colon\ p \in \Gamma\}$, and by (b), $\{b(k)\colon\ k \in S(\Gamma)\}$ is bounded. Hence (c) holds by (22).

If 2^n has a p-power sum divisor, then, by Proposition 18 (a), (g), $(1+p^a)|2^n$ for some $a \geqslant 1$. Hence $2^{n_1} = 1+p^a$ for some $n_1 \in Z$ where $1 \leqslant n_1$

$\leqslant n$. But as was noted by J. Cassels and W. LeVeque ([6], [12]), $2^{n_1} = 1+p^a$ implies $a = 1$, so p is a Mersenne prime, and hence (d) follows from (22) and (23).

Part (e) follows easily from (22), (23) and Lemma 20, so the theorem is proved.

We conclude this section with some remarks and unsolved problems.

(A) P. Bateman and R. M. Stemmler show in [2], p. 152, that if $\{p_n\}$ is the sequence of primes such that p_n is a q-power sum for some prime q, where p_n is repeated if it is a q-power sum for more than one prime q, then $\sum_{n=1}^{\infty} p_n^{-1/2} < \infty$. Hence such primes are sparsely distributed. Indeed they state that there are only 814 such primes less than 1.25×10^{10} and they exhibit the first 240 of them. In this range $31 = \dfrac{2^5-1}{2-1} = \dfrac{5^3-1}{5-1}$ is the only prime that is a q-power sum for more than one prime q. For any prime p, $m(p)/p$ is the product of all primes q such that p is a q-power sum. It does not seem to be known if there is a positive integer N such that $m(p)/p$ has no more than N prime factors for every prime p.

(B) Can the sequence $\left\{\dfrac{m(k^n)}{k^n}\right\}$ be bounded if k is even? By Theorem 22 (d), $\left\{\dfrac{m(2^n)}{2^n}\right\}$ is bounded if and only if there are only finitely many Mersenne primes. What if k is even and composite? By Theorem 22 (a), if we write $k = 2^r a$, where $r\geqslant 1$ and a is odd, this amounts to determining if there are infinitely many primes p such that $(p^y+1)|(2^r a)^x$ for some $x\in Z^+$.

(C) By Theorem 22 (c), if Γ is a finite set of odd primes, then there is a smallest positive integer $M(\Gamma)$ such that $\dfrac{m(s)}{s}\leqslant M(\Gamma)$ for every $s\in S(\Gamma)$. By Theorem 22 (e), $M(\Gamma) = 2p$ if $\Gamma = \{p\}$ and p is a Fermat prime, and since $(11)^2 = \dfrac{3^5-1}{3-1}$, $M(\{11\})\geqslant 33$. Is there a general method for computing $M(\Gamma)$? What if $|\Gamma| = 1$?

(D) The current state of knowledge about the exponential diophantine equation

$$p^n = \frac{q^{rd}-1}{q^r-1} \tag{25}$$

where p, q are primes and $r>1$, $d>1$ are integers is summarized by H. Edgar in [7]. If follows from Proposition 18(a) that p, n and q determine r and d uniquely. As is indicated in [7], there are many problems associated with (25) even if $r = 1$.

The numbers $\dfrac{p^{rd}-1}{p^r-1}$ are special cases of what are called *Lucas numbers* or *Lehmer* numbers; see [14] and the references therein where A. Schinzel shows that many positive integers of this form have a large number of factors.

In a subsequent note we expect to make a more extensive study of the distribution of values of $m(k)/k$.

6. Some applications to the theory of rings. Clearly if R is a ring with identity element, $k\in Z^+$ and $m(k)$ is a unit of R then $R = m(k)R \subseteq J(k, R)\subseteq R$ so $J(k, R) = R$.

The following proposition gives a sufficient condition on a ring R in order that $m(k, R) = m(k)$.

PROPOSITION 23. *If R is a ring with identity element and there is a homomorphism φ of R onto $Z[x]$, then*

$$m(k, R) = m(k)$$

for any positive integer k. In particular, if $\{x_a\}$ is any non-empty collection of indeterminates, then

$$m(k, Z[\{x_a\}]) = m(k).$$

Proof. By (3) in Section 1,

$$m(k, R)|m(k).$$

Since $R\varphi = Z[x]$,

$$m(k, R)Z[x] = m(k, R)R\varphi \subseteq J(k, R)\varphi = J(k, Z[x]).$$

Hence $m(k)|m(k, R)$, so $m(k) = m(k, R)$. Since there is a homomorphism φ from $Z[\{x_a\}]$ onto $Z[x]$, $m(k) = m(k, Z[\{x_a\}])$.

The ring S of "polynomials" over Z in a single indeterminate with non-negative rational exponents shows that the requirement in Proposition 23 that there be a homomorphism of R onto $Z[x]$ cannot be replaced by the assumption that the only units of R are $\{\pm 1\}$. For in this case, $m(k, S) = 1$ for every $k\in Z^+$.

I. Kaplansky has shown that if R is a ring such that for every $a\in R$, there is an $n(a)\in Z^+$ such that $a^{n(a)}$ is in the center of R, then there is a nil ideal I of R such that R/I is commutative. See [10], pp. 218–219.

The following proposition, which relies on more stringent assumptions, but eliminates the need to reduce modulo a nil ideal, follows immediately from the remarks at the beginning of this section.

PROPOSITION 24. *If R is a ring with identity element, $k>1$ is a positive integer such that y^k is in the center of R for every $y\in R$, and $m(k)$ is a unit of R, then R is commutative.*

7. Appendix.

Table of values of $a(k)$, $b(k)$, and $m(k)/k$ for $1 \leqslant k \leqslant 150$

k	$a(k)$	$b(k)$	$m(k)/k$
1	1	1	1
2	1	1	1
3	1	2	2
4	2	3	6
5	1	2	2
6	$4\cdot 3 = 12$	5	60
7	1	2	2
8	2	$3\cdot 7 = 21$	42
9	3	2	6
10	$2\cdot 5 = 10$	3	30
11	1	1	1
12	$4\cdot 3 = 12$	$5\cdot 11 = 55$	660
13	1	3	3
14	$4\cdot 7 = 28$	13	364
15	$3\cdot 5 = 15$	2	30
16	2	$3\cdot 7 = 21$	42
17	1	2	2
18	$4\cdot 3 = 12$	$5\cdot 17 = 85$	1,020
19	1	1	1
20	$2\cdot 5 = 10$	$3\cdot 19 = 57$	570
21	$3\cdot 7 = 21$	2	42
22	$2\cdot 11 = 22$	1	22
23	1	1	1
24	$4\cdot 3 = 12$	$5\cdot 7\cdot 11\cdot 23 = 8{,}855$	106,260
25	5	2	10
26	$2\cdot 13 = 26$	$3\cdot 5 = 15$	390
27	3	2	6
28	$4\cdot 7 = 28$	$3\cdot 13 = 39$	1,092
29	1	1	1
30	$4\cdot 3\cdot 5 = 60$	29	1,740
31	1	$2\cdot 5 = 10$	10
32	2	$3\cdot 7\cdot 31 = 651$	1,302
33	$3\cdot 11 = 33$	2	66
34	$2\cdot 17 = 34$	1	34
35	$5\cdot 7 = 35$	2	70
36	$4\cdot 3 = 12$	$5\cdot 11\cdot 17 = 935$	11,220
37	1	1	1
38	$2\cdot 19 = 38$	37	1,406
39	$3\cdot 13 = 39$	2	78
40	$2\cdot 5 = 10$	$3\cdot 7\cdot 19 = 399$	3,990
41	1	1	1
42	$4\cdot 3\cdot 7 = 84$	$5\cdot 13\cdot 41 = 2{,}665$	223,860
43	1	1	1
44	$2\cdot 11 = 22$	$3\cdot 43 = 129$	2,838
45	$3\cdot 5 = 15$	2	30
46	$2\cdot 23 = 46$	1	46

Table (continued)

k	$a(k)$	$b(k)$	$m(k)/k$
47	1	1	1
48	$4\cdot 3 = 12$	$5\cdot 7\cdot 11\cdot 23\cdot 47 = 416{,}185$	4,994,220
49	7	2	14
50	$2\cdot 5 = 10$	$3\cdot 7 = 21$	210
51	$3\cdot 17 = 51$	2	102
52	$2\cdot 13 = 26$	$3\cdot 5 = 15$	390
53	1	1	1
54	$4\cdot 3 = 12$	$5\cdot 17\cdot 53 = 4{,}505$	54,060
55	$5\cdot 11 = 55$	2	110
56	$4\cdot 7 = 28$	$3\cdot 13 = 39$	1,092
57	$3\cdot 19 = 57$	$2\cdot 7 = 14$	798
58	$2\cdot 29 = 58$	1	58
59	1	1	1
60	$4\cdot 3\cdot 5 = 60$	$11\cdot 19\cdot 29\cdot 59 = 357{,}599$	21,455,940
61	1	1	1
62	$4\cdot 31 = 124$	$5\cdot 61 = 305$	37,820
63	$3\cdot 7 = 21$	2	42
64	2	$3\cdot 7\cdot 31 = 651$	1,302
65	$5\cdot 13 = 65$	$2\cdot 3 = 6$	390
66	$4\cdot 3\cdot 11 = 132$	5	660
67	1	1	1
68	$2\cdot 17 = 34$	$3\cdot 67 = 201$	6,834
69	$3\cdot 23 = 69$	2	138
70	$4\cdot 5\cdot 7 = 140$	$3\cdot 13 = 39$	5,460
71	1	1	1
72	$4\cdot 3 = 12$	$5\cdot 7\cdot 11\cdot 17\cdot 23\cdot 71 = 10{,}687{,}985$	128,255,820
73	1	2	2
74	$2\cdot 37 = 74$	73	5,402
75	$3\cdot 5 = 15$	2	30
76	$2\cdot 19 = 38$	$3\cdot 37 = 111$	4,218
77	$7\cdot 11 = 77$	2	154
78	$4\cdot 3\cdot 13 = 156$	5	780
79	1	1	1
80	$2\cdot 5 = 10$	$3\cdot 7\cdot 19\cdot 79 = 31{,}521$	315,210
81	3	2	6
82	$2\cdot 41 = 82$	3	246
83	1	1	1
84	$4\cdot 3\cdot 7 = 84$	$5\cdot 11\cdot 13\cdot 41\cdot 83 = 2{,}433{,}145$	204,384,180
85	$5\cdot 17 = 85$	2	170
86	$2\cdot 43 = 86$	1	86
87	$3\cdot 29 = 87$	2	174
88	$2\cdot 11 = 22$	$3\cdot 7\cdot 43 = 903$	19,866
89	1	1	1
90	$4\cdot 3\cdot 5 = 60$	$17\cdot 29\cdot 89 = 43{,}877$	2,632,620
91	$7\cdot 13 = 91$	$2\cdot 3 = 6$	546
92	$2\cdot 23 = 46$	3	138
93	$3\cdot 31 = 93$	$2\cdot 5 = 10$	930

Table (continued)

k	$a(k)$	$b(k)$	$m(k)/k$
94	$2\cdot 47 = 94$	1	94
95	$5\cdot 19 = 95$	2	190
96	$4\cdot 3 = 12$	$5\cdot 7\cdot 11\cdot 23\cdot 31\cdot 47 = 12{,}901{,}735$	154,820,820
97	1	1	1
98	$4\cdot 7 = 28$	$13\cdot 97 = 1{,}261$	35,308
99	$3\cdot 11 = 33$	2	66
100	$2\cdot 5 = 10$	$3\cdot 7\cdot 19 = 3{,}990$	39,900
101	1	1	1
102	$4\cdot 3\cdot 17 = 204$	$5\cdot 101 = 505$	103,020
103	1	1	1
104	$2\cdot 13 = 26$	$3\cdot 5\cdot 7\cdot 103 = 10{,}815$	281,190
105	$3\cdot 5\cdot 7 = 105$	2	210
106	$2\cdot 53 = 106$	1	106
107	1	1	1
108	$4\cdot 3 = 12$	$5\cdot 11\cdot 17\cdot 53\cdot 107 = 5{,}302{,}385$	63,629,620
109	1	1	1
110	$2\cdot 5\cdot 11 = 110$	$3\cdot 109 = 327$	35,970
111	$3\cdot 37 = 111$	2	222
112	$4\cdot 7 = 28$	$3\cdot 13 = 39$	1,092
113	1	1	1
114	$4\cdot 3\cdot 19 = 228$	$5\cdot 7\cdot 37\cdot 113 = 146{,}335$	33,364,380
115	$5\cdot 23 = 115$	2	230
116	$2\cdot 29 = 58$	3	174
117	$3\cdot 13 = 39$	2	78
118	$2\cdot 59 = 118$	1	118
119	$7\cdot 17 = 119$	2	238
120	$4\cdot 3\cdot 5 = 60$	$7\cdot 11\cdot 19\cdot 23\cdot 29\cdot 59 = 57{,}573{,}439$	3,454,406,340
121	11	3	33
122	$2\cdot 61 = 122$	11	1,342
123	$3\cdot 41 = 123$	2	246
124	$4\cdot 31 = 124$	$3\cdot 5\cdot 61 = 915$	113,460
125	5	2	10
126	$4\cdot 3\cdot 7 = 84$	$5\cdot 13\cdot 17\cdot 41 = 45{,}305$	3,805,260
127	1	2	2
128	2	$3\cdot 7\cdot 31\cdot 127 = 82{,}677$	16,354
129	$3\cdot 43 = 129$	2	258
130	$2\cdot 5\cdot 13 = 130$	1	130
131	1	1	1
132	$4\cdot 3\cdot 11 = 132$	$5\cdot 43\cdot 131 = 28{,}165$	3,717,780
133	$7\cdot 19 = 133$	$2\cdot 11 = 22$	2,926
134	$2\cdot 67 = 134$	1	134
135	$3\cdot 5 = 15$	2	30
136	$2\cdot 17 = 34$	$3\cdot 7\cdot 67 = 1{,}407$	47,838
137	1	1	1
138	$4\cdot 3\cdot 23 = 276$	$5\cdot 137 = 685$	189,060
139	1	1	1
140	$4\cdot 5\cdot 7 = 140$	$3\cdot 13\cdot 19\cdot 139 = 102{,}999$	14,419,860

Table (continued)

k	$a(k)$	$b(k)$	$m(k)/k$
141	$3\cdot 47 = 141$	2	282
142	$2\cdot 71 = 142$	1	142
143	$11\cdot 13 = 143$	3	429
144	$4\cdot 3 = 12$	$5\cdot 7\cdot 11\cdot 17\cdot 23\cdot 47\cdot 71 = 502{,}335{,}295$	6,028,023,540
145	$5\cdot 29 = 145$	2	290
146	$2\cdot 73 = 146$	1	146
147	$3\cdot 7 = 21$	2	42
148	$2\cdot 37 = 74$	$3\cdot 73 = 219$	16,206
149	1	1	1
150	$4\cdot 3\cdot 5 = 60$	$7\cdot 29\cdot 149 = 30{,}247$	1,814,820

Table of p-power sums for primes $p < 150$

p	2	3
p-power sums	3,5,7,9,15,17,21,31,33,63,65,73,85,127,129	4,10,13,28,40,82,91,121

p	5	7	11	13	17	19	23	29	31	37	41	43
p-power sums	6,26,31,126	8,50,57	12,122	14	18	20	24	30	32	38	42	44

p	47	53	59	61	67	71	73	79	83	89	97	101	103	107	109	113
p-power sums	48	54	60	62	68	72	74	80	84	90	98	102	104	108	110	114

p	127	131	137	139	149
p-power sums	128	132	138	140	150

Added in proof, June 20, 1975. Part (c) of Lemma 8 follows easily from Theorem III of R. Paley's paper, *Theorems on polynomials in a Galois field*, Quart. J. Math. 4 (1933), pp. 52–63.

Mention of Lemma 20 is made in papers of A. Rotkiewicz, *An elementary proof of the existence of a prime, primitive divisor of the number $a^n - b^n$* (Polish), Prace Matematyczne 4 (1960), pp. 21–27, and K. Szymiczek, *On the equation $a^x - b^x = (a-b)c^y$* (Polish), Wiadomości Matematyczne 7 (1964), pp. 233–236.

References

[1] A. A. Albert, *Fundamental Concepts of Higher Algebra*, University of Chicago Press, Chicago, Illinois, 1956.

[2] P. T. Bateman and R. M. Stemmler, *Warings problem for algebraic number fields and primes of the form $(p^r-1)/(p^d-1)$*, Illinois J. Math. 6 (1962), pp. 142–156.

[3] M. Bhaskaran, *Sums of m^{th} powers in algebraic and abelian number fields*, Archiv der Mathematik (Basel), 17 (1966).

[4] M. Bhaskaran, *Corrections to the paper "Sums of m^{th} powers"*, ibid. 22 (1971), pp. 370–371.
[5] L. E. Dickson, *Linear Groups with an Exposition of the Galois Theory*, Dover Publications, New York, N. Y., 1958.
[6] J. W. Cassels, *On the equation $a^x - b^y = 1$*, Amer. J. Math. 75 (1953), pp. 159–162.
[7] H. Edgar, *The exponential diophantine equation $1+a+a^2+\ldots+a^{x-1} = p^y$*, Amer. Math. Monthly 81 (1974), pp. 758–759.
[8] G. H. Hardy and E. M. Wright, *The Theory of Numbers*, Oxford University Press, Oxford 1946.
[9] K. Inkeri, *On the diophantine equation $a(x^n-1)/(x-1) = y^m$*, Acta Arith. 21 (1972), pp. 299–311.
[10] N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. 37, Providence, R. I., 1956.
[11] J. Joly, *Sommes de puissances d-iemes dans un anneaux commutatif*, Acta Arith. 17 (1970), pp. 37–114.
[12] W. LeVeque, *On the equation $a^x - b^y = 1$*, Amer. J. Math. 74 (1952), pp. 325–331.
[13] G. Polya, *Zur arithmetischen Untersuchung der Polynome*, Math. Zeitschr. 1 (1918), pp. 143–148.
[14] A. Schinzel, *On primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), pp. 213–233.
[15] D. Suryanarayana, *Certain diophantine equation*, Math. Student 35 (1967), pp. 197–199.

HARVEY MUDD COLLEGE
Claremont, California, USA

Received on 29. 6. 1974 (591)

ACTA ARITHMETICA
XXIX (1976)

A note on Fermat's conjecture

by

K. Inkeri (Turku)

Introduction. Recently Everett [2] has proved the following theorem.

Theorem 1. *Let an odd prime $p \geqslant 3$ and an integer $v \geqslant 1$ be fixed. Then there are at most a finite number of relatively prime, positive integer pairs (x, y) on the line $y = x+v$ such that x^p+y^p is the p-th power of an integer.*

The proof is based on Roth's famous theorem, stating that a real algebraic irrational is approximable to no order higher than 2. It is surprising in the proof that $2^{1/p}$ works as the irrational.

Some time ago, the author [3] stated the next theorem.

Theorem 2. *Let p be a prime $\geqslant 3$. Then there exist at most a finite number of positive integer triples (x, y, z) which satisfy the conditions*

$$x^p+y^p = z^p, \quad (x, y, z) = 1 \tag{1}$$

and for which some difference $|x-y|$, $z-x$, $z-y$ is less than a given positive number M.

Theorem 1 is contained in the case $|x-y| < M$. Theorem 2 can be proved most naturally by the general method given by Inkeri and Hyyrö [5]. Because they only discussed one case (albeit a typical one), we give a complete proof in Section 2. Further we will state a generalization of this theorem. The proof of Theorem 2 given in [3] is of interest for that part which concerns the so-called first case of Fermat's conjecture ($p \nmid xyz$). The method used is completely elementary, and yields also an upper bound in terms of p and M for each of the numbers x, y, z of every solution. On account of Theorem 1, a footnote on p. 52 in [3] is worth mentioning. According to this note, the proof of Theorem 2, excluding the case $z-y < M$, $p|yz$, can be carried out elementarily, using only Thue's theorem concerning (like Roth's), the approximability of an algebraic number by rational numbers. Since Roth's result is fairly deep, we will, in Section 1, prove Theorem 1 by means of Thue's theorem. Our proof is simpler and shorter than that of Everett. In Section 3 our results, and a result of