BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 81, Number 1, January 1975

SUMS OF kTH POWERS IN THE RING OF POLYNOMIALS WITH INTEGER COEFFICIENTS

BY TED CHINBURG AND MELVIN HENRIKSEN[1]

Communicated by Robert Fossum, August 1, 1974

Suppose R is a ring with identity element and k is a positive integer. Let $J(k, R)$ denote the subring of R generated by its kth powers. If Z denotes the ring of integers, then $G(k, R) = \{a \in Z: aR \subset J(k, R)\}$ is an ideal of Z.

Let $Z[x]$ denote the ring of polynomials over Z and suppose $a \in R$. Since the map $p(x) \longrightarrow p(a)$ is a homomorphism of $Z[x]$ into R, the well-known identity (see [3, 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 group 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 $m(k, R)|m(k)$ and $m(k)|k!$.

Thus $m(k)$ is the smallest positive integer a for which there is an identity of the form

$$ax = \sum_{i=1}^{n} a_i[g_i(x)]^k \tag{2}$$

where $a_1, \cdots, a_n \in Z$ and $g_1(x), \cdots, g_n(x) \in Z[x]$.

On differentiating (2) with respect to x we have $k|m(k)$. Thus if R is any ring with identity,

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

For any $k \geqslant 1$ in Z, let $P_1(k)$ denote the set of primes less than k that divide k, and let $P_2(k)$ denote the set of primes less than k that fail to divide k. If p is a prime and $r \geqslant 1$, $m > 1$ are integers, then a number

AMS (MOS) subject classifications (1970). Primary 10M05, 10B25, 12C15; Secondary 13F20.

[1]We are indebted to H. Edgar and W. LeVeque for valuable references.

of the form $(p^{mr} - 1)/(p^r - 1)$ is called a *p-power sum.* We adopt the convention that the product of an empty set of integers is 1. The main theorem of this paper is the following.

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

$$m(k) = k\Pi\{p^{\alpha_k(p)}: p \in P_1(k)\}\Pi\{p^{\beta_k(p)}: p \in P_2(k)\}$$

where

(a) $\alpha_k(p) = 1$ *if p is odd.*

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

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

A proof of this theorem will appear in [2]. Appropriate identities are developed in various homomorphic images of $Z[x]$ and lifted. Except for (b), these homomorphic images are Galois fields. A constructive but impractical algorithm is developed for obtaining identities of the form (2) with $a = m(k)$. The reader may easily verify the entries in the following table of values of $m(k)/k$ for $1 \leq k \leq 20$.

k	1	2	3	4	5	6	7
$m(k)/k$	1	1	2	$2\cdot 3 = 6$	2	$4\cdot 3\cdot 5 = 60$	2

k	8	9	10	11	12
$m(k)/k$	$2\cdot 3\cdot 7 = 42$	$2\cdot 3 = 6$	$2\cdot 3\cdot 5 = 30$	1	$4\cdot 3\cdot 5\cdot 11 = 660$

k	13	14	15	16	17	18
$m(k)/k$	3	$4\cdot 7\cdot 13 = 364$	$2\cdot 3\cdot 5 = 30$	$2\cdot 3\cdot 7 = 42$	2	$4\cdot 3\cdot 5\cdot 17 = 1,020$

k	19	20
$m(k)/k$	1	$2\cdot 3\cdot 5\cdot 19 = 570$

A table of values for $m(k)/k$ for $1 \leq k \leq 150$ is supplied in [2] together with an algorithm for computing values of $m(k)/k$ efficiently.

If Γ is any set of primes, let $S(\Gamma)$ denote the multiplicative semigroup generated by Γ. Let $T(\Gamma)$ denote the set of $a > 1$ in Z for which there is a $d > 1$ in Z such that $(a^d - 1)/(a - 1) \in S(\Gamma)$.

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. $p = 3$ or $p = 2^n + 1$) for some integer $n > 1$.

THEOREM 2. *Suppose* Γ *is a finite set of primes.*

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

(b) *If* $S(\Gamma)$ *contains no even integer, then* $\{a \in T(\Gamma): a$ *is odd*$\}$ *is finite.*

(c) *If* $2 \notin \Gamma$, *then* $\{m(k)/k: k \in S(\Gamma)\}$ *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* $m(2^n)/2^n$ *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* $n > 1$.

A proof of Theorem 2 is given in [2].

We conclude with some remarks and unsolved problems.

(A) P. Bateman and R. M. Stemmler show in [1, 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 $\Sigma_{n=1}^{\infty} p_n^{-1/2} < \infty$. 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 $31 = (2^6 - 1)/(2 - 1) = (5^3 - 1)/(5 - 1)$ 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 $\{m(k^n)/k^n\}$ be bounded if k is even? By Theorem 2 (d), $\{m(2^n)/2^n\}$ is bounded if and only if there are only finitely many Mersenne primes. What if k is even and composite?

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

(D) It is not difficult to prove that if R is a ring with identity for which there is a homomorphism of R onto $Z[x]$, then $m(k, R) = m(k)$. In particular, if $\{x_\alpha\}$ is any collection of indeterminates, then $m(k, Z[\{x_\alpha\}]) = m(k)$.

REFERENCES

1. 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), 142–156. MR **25** #2059.

2. T. Chinburg and M. Henriksen, *Sums of kth powers in the ring of polynomials with integer coefficients*, Acta Arith. (submitted).

3. G. H. Hardy and E. M. Wright, *The theory of numbers*, Oxford Univ. Press, London, 1946.

DEPARTMENT OF MATHEMATICS, HARVEY MUDD COLLEGE, CLAREMONT, CALIFORNIA 91711