SUMS OF \( k \)TH POWERS IN THE RING OF POLYNOMIALS WITH INTEGER COEFFICIENTS

BY TED CHINBURG AND MELVIN HENRIKSEN

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 \( k \)th powers. If \( Z \) denotes the ring of integers, then \( G(k, R) = \{ a \in Z : aR \subseteq J(k, R) \} \) is an ideal of \( Z \).

Let \( Z[x] \) denote the ring of polynomials over \( Z \) and suppose \( a \in R \). Since the map \( p(x) \mapsto p(a) \) is a homomorphism of \( Z[x] \) into \( R \), the well-known identity (see [3, p. 325])

\[
\sum_{i=0}^{k-1} (-1)^{k-1-i} \binom{k-1}{i} (x + i)^{k} - i^{k}
\]

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

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

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

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

\[
k|m(k), \ m(k, R)|m(k), \ and \ m(k)|k!.
\]

For any \( k \geq 1 \) 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 \( r \geq 1, m \geq 1 \) are integers, then a number

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

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

Copyright © 1975, American Mathematical Society
of the form \((p^m r - 1)/(p^r - 1)\) 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

\[
m(k) = k \Pi \{p^{\alpha_k(p)} : p \in \mathcal{P}_1(k)\} \Pi \{p^{\beta_k(p)} : p \in \mathcal{P}_2(k)\}
\]

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

A proof of this theorem will appear in [2]. Appropriate identities are developed in various homomorphic images of \(\mathbb{Z}[x]\) 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 \(1 \leq k \leq 20\). 

<table>
<thead>
<tr>
<th>(k)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m(k)/k)</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(k)</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m(k)/k)</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

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 \(\Gamma\) is any set of primes, let \(S(\Gamma)\) denote the multiplicative semigroup generated by \(\Gamma\). Let \(T(\Gamma)\) denote the set of \(a > 1\) in \(\mathbb{Z}\) for which there is a \(d > 1\) in \(\mathbb{Z}\) 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. \(p = 2 + 1\)) for some integer \(n > 1\).
THEOREM 2. Suppose $\Gamma$ is a finite set of primes.

(a) $T(\Gamma)$ is the union of a finite set and \{a $\in \mathbb{Z}$: 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 $p^r$ is a $q$-power sum for some prime $q$, where $p^r$ is repeated if it is a $q$-power sum for more than one prime $q$, then $\sum_{n=1}^{\infty} p^r < \infty$. Hence such primes are sparsely distributed. Indeed, they state that there are only 814 such primes less than $1.25 \times 10^9$, 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 $\Gamma$ is a finite set of odd primes, then there is a smallest positive integer $M(\Gamma)$ such that m(s)/s $\leq$ 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 $(11)^2 = (3^5 - 1)/(3 - 1)$, $M(\{11\}) > 33$. 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 $\mathbb{Z}[x]$, then m(k, R) = m(k). In particular, if \{x$\alpha$\} is any collection of indeterminates, then m(k, $\mathbb{Z}\{x$\}) = m(k).
REFERENCES


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