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 $k$th 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

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

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 [8], p. 325)

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

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

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

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

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

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 $f \in J(k, R/H)$ if and only if there is a $(k, R)$ set for $f \mod H$. 

2 — Acta Arithmetica XXIX.3
Suppose that $\langle (a_i, g_i) \rangle_{i=1}^n$ is a $(k, \mathbb{Z}[x])$ 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,

\[ k|m(k), \quad m(k, R)|m(k) \quad \text{and} \quad m(k, R)|k! . \]

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 $(k, \mathbb{Z}[x])$ set for $m(k)x$.

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

\[ \mathcal{P}_1(k) = \{ p \in \mathcal{P}(k) : p < k \text{ and } p|k \} \quad \text{and} \quad \mathcal{P}_2(k) = \{ p \in \mathcal{P}(k) : p \nmid k \} . \]

Suppose $p$ is prime, $r$ and $m$ are positive integers, and $m > 1$. A number of the form $p^{mr-1}$ 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

\[ m(k) = k \prod (p^{\alpha(p)} : p \in \mathcal{P}_1(k)) \prod (p^{\beta(p)} : p \in \mathcal{P}_2(k)) \]

where

(a) $\alpha_p(p) = 1$, if $p$ is odd;

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

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

Sections 2, 3, and 4 are devoted to the proof of Theorem 1. In the course of the proof we indicate how $(k, \mathbb{Z}[x])$ 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 $1 \leq k \leq 150$.

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 $a, b \in \mathbb{Z}$ let $v_p\left(\frac{a}{b}\right) = a$ if $\frac{a}{b} = p^m$, where $(r, p) = (a, p) = 1$, and let $v_p(0) = \infty$. Then $v_p$ is the usual $p$-adic valuation on the field $\mathbb{Q}$ of rational numbers, and as is readily verified

\[ v_p(ab) = v_p(a) + v_p(b) \quad \text{and} \quad v_p(a+b) \geq \min\{v_p(a), v_p(b)\} \]

if $a, b \in \mathbb{Q}$.

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

If $0 \leq m \leq n$ and $m, n \in \mathbb{Z}$, we let, as usual, $m! = \prod_{i=1}^{m} i$. If $W = \langle (a_i, g_i) \rangle_{i=1}^{n}$, define

\[ W + W' = \langle (a'_i, g'_i) \rangle_{i=1}^{n} \]

where $(a'_i, g'_i) = (a_i, g_i)$ if $1 \leq i \leq n$ and $(a'_i, g'_i) = (a_i, g_i)$ if $n+1 \leq i \leq n+n'$.

The following two lemmas will be used frequently.

**Lemma 2.** Suppose $b, r, k, a$ and $n$ are positive integers, $R$ is a ring with identity element, $f$ and $f'$ elements of $B$ 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 $W = \langle (a_i, g_i) \rangle_{i=1}^{n}$.

(a) If $W + W'$ is a $(k, R)$ set for $f + f' \bmod H + H'$, then $W + W'$ is a $(k, R)$ set for $f \bmod H$.

(b) If $\overline{g}$ denotes the image of $g \bmod R$ under the homomorphism $R \to R/\mathbb{Z}$, then $W + R(\overline{g})$ is a $(k, R)$ set for $g \bmod H$, and if only if $W = \langle (a_i, g_i) \rangle_{i=1}^{n}$ is a $(k, R)$ set for $\overline{g}$.

(c) If $H' \leq H$, then $m(k, R/\mathbb{Z})|m(k, R/H')$, and if also $H \leq J(k, R) + H'$, then $m(k, R/H') = m(k, R/H)$.

(d) Suppose $\langle a_i \rangle_{i=1}^{n} \subset H(1 + 1) \subset kH(1)$ for $i = 1, \ldots, n-1$, and $k \geq 2$. Then

\[ kH(1) \subset J(k, R) + kH(n), \quad m(k, R/kH(1)) = m(k, R/kH(n)) \quad \text{and} \quad \text{if } H = kH(1) \text{ then from } W \text{ we may construct a } (k, R) \text{ set for } f \bmod kH(n). \]

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

\[ H = J(k, R) + H^n, \quad m(k, R/\mathbb{Z}) = m(k, R/H^n) \quad \text{and from } W \text{ we may construct a } (k, R) \text{ set for } f \bmod H^n. \]
LEMMA 3. Suppose \( j, n \) and \( k \) are positive integers, \( 2 \leq j \leq k \) and \( p \in \mathcal{P}(k) \). 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 \( v_p(j) < p^{\binom{j}{2}} \leq j \) since \( p \geq 2 \), so \( j - 1 - v_p(j) \geq 0 \).

By (4), \( v_p(j) \geq v_p\left(\binom{k}{j}\right) - v_p\left(\binom{k}{j - 1}\right) = v_p\left(\frac{k}{j}\right) = v_p(k) - v_p(j) \).

Then

\[
v_p\left(\binom{k}{j}\right) + jn - v_p(k + n) \geq n(j - 1) - v_p(j) \geq j - 1 - v_p(j) \geq 0.
\]

Since \( j - 1 - v_p(j) \geq 0 \), strict inequality will hold if \( j < p^{j - 1} \). Note that \( (i + 1)/i < 2 \leq p \) if \( i \geq 2 \). Then if \( 2 < p \) and \( 2 < j \),

\[
j = 2 \sum_{i=2}^{j-1} \frac{i+1}{i} < 2^{j-1} < p^{j-1}.
\]

If \( p = 2 \) and \( 3 \leq j \), then

\[
j = 3 \sum_{i=2}^{j-1} \frac{i+1}{i} < 2^j \frac{j}{j - 1} = p^{j-1}.
\]

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 \( \mathcal{P}(k) \), let
\[
\delta(k,p) = \begin{cases} 
0 & \text{if } p = k, \\
1 & \text{if } p < k \text{ and } p \text{ or } k \text{ is odd,} \\
2 & \text{if } p = 2 < k \text{ and } k \text{ is even.} 
\end{cases}
\]
\[(5)\]

For any ring \( R \), \( k \in \mathbb{Z}^+ \) and \( p \in \mathcal{P}(k) \), we abbreviate
\[R/p^{\delta(k,p)+2}\mathbb{Z}(k) \] 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 \( p \in \mathcal{P}(k) \), 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
\[
(a) \ m(k,R) = \prod \{ m(k,R(k,p)) : p \in \mathcal{P}(k) \}.
\]
\[\text{(b) } v_p(m(k,R)) = v_p(m(k,R(k,p))) \leq v_p(k) + \delta(k,p).\]
\[\text{(c) From } W(f,k,p,R) : p \in \mathcal{P}(k) \text{; one can construct a } (k,R) \text{ set for } f.\]

**Proof.** By \((3)\), \( k \mid R \subseteq J(k,R) \). Now
\[R/k \cdot R = \sum \{ R/p^{\delta(k,p)+2} \mathbb{Z}(k) : p \in \mathcal{P}(k) \} \text{ and } m(k,R/p^{\delta(k,p)+2} \mathbb{Z}(k)) = \prod \{ m(k,R/p^{\delta(k,p)+2} \mathbb{Z}(k)) : p \in \mathcal{P}(k) \}.
\]
So, by Lemma 2 \((c), (f)\),
\[(6)\]
\[m(k,R) = m(k,R/k \cdot R) \text{ is c.} \quad (m(k,R/p^{\delta(k,p)+2} \mathbb{Z}(k)) : p \in \mathcal{P}(k)) \]
\[= \prod \{ m(k,R/p^{\delta(k,p)+2} \mathbb{Z}(k)) : p \in \mathcal{P}(k) \}.
\]
If \( p \in \mathcal{P}(k) \), let \( f_p \) denote the image of \( f \) under the homomorphism \( R \to R/p^{\delta(k,p)+2} \mathbb{Z}(k) \). By Lemma 2 \((f), (a), (1)\), to construct a \((k,R)\) set for \( f \), it suffices to construct for each \( p \in \mathcal{P}(k) \) a \((k,R/p^{\delta(k,p)+2} \mathbb{Z}(k)) \) set for \( f_p \). Fixing \( p \in \mathcal{P}(k) \), let \( R' = R/p^{\delta(k,p)+2} \mathbb{Z}(k) \). If \( \delta(k,p) = 0 \), then \( v_p(k) = v_p(k!) = 1 \), so
\[(7)\]
\[m(k,R/p^{\delta(k,p)+2} \mathbb{Z}(k)) = m(k,R) = m(k,R(k,p)).\]
By Lemma 2 \((c), m(k,R(k,p)) \mid m(k,R) \). Then since \( R' = R(k,p) \), from \( W(f,k,p,R) \) we may construct a \((k',R')\) set for \( f_p \). If \( \delta(k,p) > 0 \), let \( * = v_p(k!) - v_p(k) - \delta(k,p) + 1 \) and \( H(i) = p^{\delta(k,p)+i+3} \mathbb{Z}(k) \) for \( i = 1, 2, \ldots, n \) so that \( kH(n) = \{0\} \). By Lemma 3, if \( 1 \leq i < n \) and \( k \geq 2 \) then
\[v_p(k) + \delta(k,p) + i - 1 < v_p(k!) + j(\delta(k,p) + i - 1).
\]
Hence
\[
J_{(i)}(H(i)) = p^{\delta(k,p)+i+2} \mathbb{Z}(k) \quad R' = p^{\delta(k,p)+2} \mathbb{Z}(k) + i R' = kH(i+1),
\]
and clearly \( kH(i+1) = kH(i) \). 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 \( f_p \) as required to establish \( (c) \).

For any \( p \in \mathcal{P}(k) , p^{\delta(k,p)+2} \mathbb{Z}(k) \) set for \( f_p \) as required to establish \( (c) \).

For any \( p \in \mathcal{P}(k) , p^{\delta(k,p)+2} \mathbb{Z}(k) \) set for \( f_p \) as required to establish \( (c) \).

**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 \( v_p(m(k,R)) = v_p(m(k,R(k,p))) \leq v_p(k) + \delta(k,p) \) 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 \( v_p(m(k,R)) = v_p(m(k,R(k,p))) \leq v_p(k) + \delta(k,p) \) and thus \( (b) \) holds.

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 \( Z[x]/p \cdot Z[x] \). 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 \( \epsilon \in \mathbb{Z}^+ \) 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 \( GF(p^j) \). The map \( p(x) Z_p[X] \to GF(p^j) \) 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 \( GF(p^j) \) 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 \( f(x) = a \cdot \prod_{i=1}^{n} (p_i(x))^m_i \), where \( p_1(x), \ldots, p_n(x) \) are irreducible in \( Z_p[X] \), \( a \in Z_p \) and \( m_i \in \mathbb{Z}^+ \) for \( i = 1, 2, \ldots, n \), then \( Z_p[X]/I \) is isomorphic to the direct sum of the rings \( Z_p[X]/I_j \) \( Z_p[X]/I_j \), where \( I_j = (p_j(x)) Z_p[X] \).

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 \( j > 1 \), \( J(k GF(p^j)) = GF(p^j) \) 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
\[
v_p(m(k)) = \beta_p(p) = 1
\]
and \( W(m(k)x, k, p, Z[x]) = \langle \langle 0, 0 \rangle \rangle \) is a \( \langle k, Z[x](k, p) \rangle \) set for
\[
m(k, Z[x](k, p)) = \langle \langle 0, 0 \rangle \rangle.
\]
Proof. Since \( p \in \mathcal{P}_k(k) \), \( v_p(k) = 0 \) and \( v_p(m(k)) = v_p(m(k, Z_p[x])) = 1 \) by Proposition 4(b). Hence if \( v_p(m(k)) = 0 \), then \( \langle k, Z_p[x](k, p) \rangle \) is empty. So, \( m(k, Z_p[x]) = \langle \langle 0, 0 \rangle \rangle \) is a \( \langle k, Z_p[x](k, p) \rangle \) set for \( m(k, Z_p[x]) = 0 \) in \( Z_p[x] \).

The rest of this section is devoted to determining \( \beta_p(p) \) in case \( k \) has a \( p \)-power-sum divisor.

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

Lemma 8. Suppose \( p \) is a prime and \( r \) is a positive integer relatively prime to \( p \). Then \( \dim(Z_p[x]/J(r, Z_p[x])) \) for any vector space over \( Z_p \) does not exceed \( (r-1)^\beta \).

Proof. Theorem 7 follows from Proposition 4(b), \( m \in \mathcal{P}_k(k) \) and \( \langle k, Z_p[x](k, p) \rangle \) is empty. So, \( \langle k, Z_p[x](k, p) \rangle \) is a \( \langle k, Z_p[x](k, p) \rangle \) set for \( \langle k, Z_p[x](k, p) \rangle = 0 \) in \( Z_p[x] \).

The rest of this section is devoted to determining \( \beta_p(p) \) in case \( k \) has a \( p \)-power-sum divisor.

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

Lemma 8. Suppose \( p \) is a prime and \( r \) is a positive integer relatively prime to \( p \). Then \( \dim(Z_p[x]/J(r, Z_p[x])) \) for any vector space over \( Z_p \) does not exceed \( (r-1)^\beta \).

Proof. Theorem 7 follows from Proposition 4(b), \( m \in \mathcal{P}_k(k) \) and \( \langle k, Z_p[x](k, p) \rangle \) is empty. So, \( \langle k, Z_p[x](k, p) \rangle \) is a \( \langle k, Z_p[x](k, p) \rangle \) set for \( \langle k, Z_p[x](k, p) \rangle = 0 \) in \( Z_p[x] \).

The rest of this section is devoted to determining \( \beta_p(p) \) in case \( k \) has a \( p \)-power-sum divisor.

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

Lemma 8. Suppose \( p \) is a prime and \( r \) is a positive integer relatively prime to \( p \). Then \( \dim(Z_p[x]/J(r, Z_p[x])) \) for any vector space over \( Z_p \) does not exceed \( (r-1)^\beta \).

Proof. Theorem 7 follows from Proposition 4(b), \( m \in \mathcal{P}_k(k) \) and \( \langle k, Z_p[x](k, p) \rangle \) is empty. So, \( \langle k, Z_p[x](k, p) \rangle \) is a \( \langle k, Z_p[x](k, p) \rangle \) set for \( \langle k, Z_p[x](k, p) \rangle = 0 \) in \( Z_p[x] \).

The rest of this section is devoted to determining \( \beta_p(p) \) in case \( k \) has a \( p \)-power-sum divisor.

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

Lemma 8. Suppose \( p \) is a prime and \( r \) is a positive integer relatively prime to \( p \). Then \( \dim(Z_p[x]/J(r, Z_p[x])) \) for any vector space over \( Z_p \) does not exceed \( (r-1)^\beta \).

Proof. Theorem 7 follows from Proposition 4(b), \( m \in \mathcal{P}_k(k) \) and \( \langle k, Z_p[x](k, p) \rangle \) is empty. So, \( \langle k, Z_p[x](k, p) \rangle \) is a \( \langle k, Z_p[x](k, p) \rangle \) set for \( \langle k, Z_p[x](k, p) \rangle = 0 \) in \( Z_p[x] \).

The rest of this section is devoted to determining \( \beta_p(p) \) in case \( k \) has a \( p \)-power-sum divisor.

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

Lemma 8. Suppose \( p \) is a prime and \( r \) is a positive integer relatively prime to \( p \). Then \( \dim(Z_p[x]/J(r, Z_p[x])) \) for any vector space over \( Z_p \) does not exceed \( (r-1)^\beta \).

Proof. Theorem 7 follows from Proposition 4(b), \( m \in \mathcal{P}_k(k) \) and \( \langle k, Z_p[x](k, p) \rangle \) is empty. So, \( \langle k, Z_p[x](k, p) \rangle \) is a \( \langle k, Z_p[x](k, p) \rangle \) set for \( \langle k, Z_p[x](k, p) \rangle = 0 \) in \( Z_p[x] \).

The rest of this section is devoted to determining \( \beta_p(p) \) in case \( k \) has a \( p \)-power-sum divisor.
Proof. We may write \( g(x) = b_0 + b_1 x + a^2 h(x) \) for some \( b_0, b_1 \in \mathbb{Z} \) and \( h(x) \in \mathbb{Z}[x] \). We abbreviate \( b_0 + b_1 a \) by \( a(x) \). By the binomial theorem

\[
(g(x))^p = \sum_{j=0}^{k} \binom{k}{j} (a(x))^{k-j} (h(x))^j a^j.
\]

and

\[
(a(x))^p = \sum_{j=0}^{n} \binom{n}{j} b_0^{n-j} b_1^j a^j.
\]

Hence

\[
\begin{align*}
oc(1, g^p) &= oc(1, a^p) = h b_0^{n-1} b_1, \\
\end{align*}
\]

If

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

and

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

then \( \sigma(p, g^p) = \sigma(p, t) \). Since \( r(p) < p \) and \( v_p(k) = n \), if \( 0 < j \leq r(p) \) then \( \binom{k}{j} \equiv 0 \mod p^n \). Hence

\[
\sigma(p, g^p) = \sigma(p, t) = \sigma(p, a^p) = \binom{k}{p} b_0^{k-p} b_1^p \mod p^n
\]

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

\[
\sigma(p, g^p) = \binom{k}{p} b_0^{k-1} b_1 = \binom{k}{p} \frac{oc(1, g^p)}{k} \mod p^n
\]

by (10).

Proposition 11. If \( k \) is a positive integer, \( p \) is a prime, \( p < k \) and \( p | k \), then

\[
a_p(p) = v_p \left( \frac{m(k)}{k} \right) = 1.
\]

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

\[
\begin{align*}
0 &= \sum_{i=1}^{q} a_i \sigma(p, g^i) = \binom{k}{p} \sum_{i=1}^{q} a_i \frac{oc(1, g^i)}{k} = \binom{k}{p} \frac{m(k)}{k} \mod p^n.
\end{align*}
\]

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

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 \( a_p(p) = v_p \left( \frac{m(k)}{k} \right) = 1. \)

(b) If \( p = 2 \), then \( a_p(2) = 2. \)

In the remaining cases, \( k = 2^a r \), where \( r \) is odd.

Proposition 13. If \( k, n, r \) and \( j \) are positive integers, \( k = 2^r r \), \( j > 2 \), \( r \) is odd, and \( r \) is divisible by \( 2^{j-1} \), then

\[
v_k \left( \frac{m(k)}{k} \right) = a_k(2) = 2.
\]

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

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

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 \( 2^{j-1} r = 1 \). Hence if \( g(x) \in \mathbb{Z}[x] \), then there is an \( m(x) \in \mathbb{Z}[x] \) such that either

\[
[g(x)]^r = 1 + 2 m(x) \mod I
\]

or

\[
g(x) = 2 m(x) \mod I.
\]

If (11) holds, then

\[
[g(x)]^{2^r} = 1 + 2^{n+1} [m(x) + [m(x)]^2] \mod I,
\]

while if (12) holds,

\[
[g(x)]^{2^r} = 2^{n+1} [m(x)]^{2^r} \mod I
\]

since \( r > 2 \). Moreover,

\[
m(0) + [m(0)]^2 = m(1) + [m(1)]^2 \equiv 0 \mod 2Z[x]
\]

for any \( m(x) \in \mathbb{Z}[x] \), so, in either case,

\[
[g(0)]^r = [g(1)]^r \mod I.
\]

If \( 2^{n+1} x = \sum_{i=1}^{q} a_i [g(x)]^{i} \) is an identity for \( 2^{n+1} x \) in \( (k, Z[x]) \mod I \), then successively replacing \( x \) by 0 and 1 yields \( 2^{n+1} = 0 \mod I \). 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 \( GF(p^j) \) is \( (p^j - 1)/d \).

Recall that if \( R \) is a ring with identity, \( H(k, R) \) is the set of \( k \)-th powers of elements of \( R \). If \( n, r \in \mathbb{Z}^+ \) and \( m, n \) and \( a \in R \), define

\[
\Phi(h, m, a, 1, r) = h^m + m^2 + a + a^2,
\]

and

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

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

\[
\begin{align*}
&h \neq 0 \quad \text{and} \quad b = \Phi(h, m, a, n, r), \\
&j^n - 1 = \Phi(h, m, a, n, r) + [v(a)]^r \quad \text{mod } I_0.
\end{align*}
\]

Proof. By assumption, \((2^j - 1, r) < 2^j - 1 \), so by Lemma 14 there is an \( h = \tau \in H(\tau, GF(2^j)) \) other than 0 or 1. Since the multiplicative order of \( \tau \) divides \( 2^j - 1 \), \( \tau^{2^j - 1} \neq 0 \) or 1. Hence if \( j = \tau^{2^j - 1} \), then \( \tau^{2^j - 1} = \tau^{2^j - 1} \). Then

\[
\begin{align*}
&f = \tau^{2^j - 1} - \tau^{2^j - 1}m + \tau^{2^j - 1}m^2 + \tau^{2^j - 1}m^3 = \tau^{2^j - 1}m + \tau^{2^j - 1}m^2.
\end{align*}
\]

But \( f = \tau^{2^j - 1}m + \tau^{2^j - 1}m^2 \).

Since \( Z_4[2] \) is finite, \( h, m, a \), and \( v \) are effectively determined. Because \( h(2^j - 1)^{r} \) is a unit \( \text{mod } I_0 \), \( I_0 = I_0 \text{mod } I_0 \) and \( 2^j - 1 \text{ mod } I_0 \), we know that \( h(2^j - 1)^{r} \) is a unit \( \text{mod } I_0 \).

Proof. Since \( Z_4[2] \) is isomorphic, it suffices to prove the lemma in case \( g = 1 \) and \( I_1 = I_0 \). Now, \( Z_4[2] \) is isomorphic for some \( j > 1 \). If \( j = 1 \) and \( I_0 = (x + 1)Z_4[2] \), we may take \( h(x) = v(x) = 1 \) and \( a(x) = m(x) = 0 \). Otherwise \( I_0 = xZ_4[2] \). Now, \( h(x) = v(x) = 1 \) 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 \( x = \Phi(h(x), m(x), a(x), n, r) \) and \( v(x) = 0 \), so the Corollary holds.

**Proposition 17.** If \( k = 2^nr \geq 2 \) for some positive integers \( r \) and \( n \) such that \((2^j - 1)^{r} \) for any \( j \geq 2 \) and \( r \) is odd, then

\[
\alpha_k(2) = \nu_k\left(\frac{m(2)}{k}\right) = 1.
\]

A \((k, Z_4[2](k, 2))\) set for \( m(k, Z_4[2](k, 2)) \) can be effectively constructed.
so summing (17) and (18) and substituting in (15) gives

\[ 2^{n+1}x = g^k - h^k + (1 + 2\alpha)^k - 1^k + 2^{n+1}v \in J(k, R) + 2^{n+1}J(r, R) \mod 2^{n+1}I_0. \]

Hence (16) holds for all cases.

If \( j = \max(a_1, \ldots, a_n) \), then by Lemma 2 (e), \( I_0 = J(r, Z_1[x]) + I_j \).

Since \( I_j \subseteq I \subseteq J(r, Z_1[x]) \), we have \( I_0 \subseteq J(r, Z_1[x]) \).

Now \( I_0 = I \) and \( J(r, Z_1[x]) = J(r, R) \mod 2R \), so \( I_0 \subseteq J(r, R) \mod 2R \).

Thus, since \( 2^{n+1}R = \{0\} \),

\[ 2^{n+1}I_0 \subseteq 2^{n+1}J(k, R) \mod 2R. \]

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

\[ \sum_{\nu=0}^{n-1} (1 + 2f)^n \nu = n + 2^{n+1}(f^n + f^n). \]

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

\[ 2^{n+1}J(r, R) \subseteq J(k, R). \]

We now apply (20) and (21) sequentially to (16) to have \( 2^{n+1}x \in J(k, R) \).

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 do this, it is convenient to introduce some auxiliary number-theoretic functions.

If \( k \in \mathbb{Z}^+ \), let

\[ a(k) = \prod \{ p^{\nu(a)} : p \in \mathcal{P}_1(k) \}, \quad b(k) = \prod \{ p^{\nu(b)} : p \in \mathcal{P}_1(k) \}, \]

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

\[ m(k)/k = a(k)b(k) \]

and

\[ a(k) = \begin{cases} 1 & \text{if } k \text{ is prime,} \\ s(k) & \text{if } k \text{ is composite and } 2(2^j-1)|k \text{ for all } j \geq 2, \\ 2s(k) & \text{otherwise.} \end{cases} \]

To compute \( b(k) \) it suffices to determine when a divisor \( d \) of \( k \) is a \( p \)-power sum for some \( p \in \mathcal{P}_1(k) \); that is to determine if the exponential diophantine equation

\[ d = \frac{p^{a}-1}{p-1} = 1 + p^a + \ldots + p^{a(n-1)} \]

has a solution when \( d \) and \( p \) are relatively prime to \( a \).

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

Proposition 15. Suppose \( a, \gamma, \delta, \varepsilon, b \) are positive integers, \( \varepsilon > 1 \), \( p \) is a prime, \( \gamma = \frac{p^{\delta}-1}{p-1} \), and \( d \) is as in (24).

(a) \( a = \frac{a_p}{d} \).

(b) \( b = p^\varepsilon d + \varepsilon \) is a \( p \)-power sum of index \( \varepsilon \).

(c) If \( \varepsilon > \delta - 1 \), then \( d = 0 \mod \varepsilon \).

(d) If \( \varphi(\varepsilon) = 0 \) and \( \varphi(\delta) = 0 \) or \( \varphi(\varepsilon) = 0 \) and \( \varphi(\delta) = 0 \), then \( d = 0 \mod \varepsilon \).

(e) \( e \) if and only if \( \delta \).

(f) If \( d \) and \( p \) are odd, then \( p^\varepsilon(p^\delta - 1)(p^\delta - 1) \).

(g) If \( d \) is even, then \( (1 + p^\delta)^d \).

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

Suppose that \( d = 0 \mod b \) and that \( \gamma \) is the multiplicative order of \( p^\delta \mod b \). By Fermat’s theorem ([8], Chapter 6), \( \gamma|p \). Since \( p^\delta - 1 = (p^\delta - 1) \delta = 0 \mod b \), we have that \( \gamma \) is and so \( \gamma \).

If \( \gamma = 1 \), then by (24), \( s = d = 0 \mod b \). Otherwise \( \varphi(b) \).

Suppose \( \varepsilon = \delta + \varepsilon \) for some integers \( \varepsilon > 0 \) and \( \delta > 0 \).

Clearly

\[ (p^\delta - 1)(p^\delta - 1) \quad \text{so} \quad \frac{p^\delta - 1}{p - 1}. \]

Then since

\[ d = \left( \frac{p^\delta - 1}{p - 1} \right)^{p^\delta} + \frac{p^\delta - 1}{p - 1}, \]

\( e \) if and only if \( e \).

Suppose \( d \) and \( p \) are odd, so that \( \varepsilon > 2 \). Then by (a) and (c), \( (d-1)/p^\varepsilon \) is a \( p \)-power sum of index \( \varepsilon - 1 \).

Since \( (d-1)/p^\varepsilon \) is even and \( \varphi(2) = 1 \), part (d) implies that \( \varepsilon = 0 \mod 2 \).

Hence by (e), \( (d-1)/p^\varepsilon \) is divisible
by \((p^n - 1) / (p^2 - 1) = 1 + p^n\). Hence \(p^n(\mathbf{2}^p - 1) / (\mathbf{2}^p - 1) = 1 + p^n\), and by (e), 
\(p^n / (\mathbf{2}^p - 1) = 1 + p^n\), so (f) is established.

If \(d = 0\) then by (d), \(e = 0 \mod 2\), so by (e) \(d\) is divisible by 
\((p^n - 1) / (p^2 - 1) = 1 + p^n\), so (g) holds.

In Section 7, we present a table of values of \(a(k), b(k),\) and \(m(k)/k\) for \(1 \leq k \leq 150\). 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 \(p \leq 150\). Such a list is given at the end of the table. Note that in this range, they all take the form \(p^1 + 1\), \(p \geq 11\). Observe that if \(d = 1\), 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 for \(k\) 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 \(k = 567 = 3^2 \cdot 7\). By (23), \(a(3) = 3^2 = 21\). The divisors of 567 are 1, 3, 9, 27, 81, 7, 21, 63, 169, 57, and 567, and 567 is a prime number. By the table in Section 7, the prime divisors of \(b(k) = 2\) and those primes \(p 

(iii) if \(k = 372 = 2^3 \cdot 3^2 \cdot 11\), then the divisors of \(k\) are 1, 2, 3, 4, 6, 12, 3, 21, 63, 124, 196, and 372. By (23), \(a(3) = 2^3 \cdot 3^2 = 444\). The table in Section 7 shows that the prime divisors of \(b(k)\) are 5, 11, 61, and those \(p = 2, 3, 5, 11, 31, 61\) and where \(p = 5, 11, 31, 61\) 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 prime of this latter type. Hence \(b(372) = (5 \cdot 11 \cdot 61 = 3355\) and \(m(372)/372 = a(372)/b(372) = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 61 = 2, 496, 120\).

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 \(\{m(k^n)/k^n\}\) is bounded.

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

Lemma 20. If \(P\) is any set of primes and \(a \in T(P)\), then there is a prime \(p\) such that \((a^p - 1)/(a - 1) \in S(P)\).

Proof. Suppose \(a \in T(P)\). Then \(a = 1\mod m\), and \(a = 1\mod m\) for some \(p\). Thus \(p^q - 1\) for all \(q \in P\), then \(f_a(p) = p^q\) for some \(n \geq 1\). Since \(a^p - 1 = (a - 1)f_a(p) = 0\mod p\), Fermat's theorem implies \(a = 1\mod p\).

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

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

Lemma 21 (Polya). If \(f(a)z \mod a\) has more than one zero and all of its zeros are distinct, then \(\lim_{n \to \infty} f(n) = \infty\).

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

Theorem 23. Suppose \(P\) is a finite set of primes.

(a) \(I(P)\) is the union of a finite set and \(a \in T(P)\).

(b) If \(a \in T(P)\) then \(a \in T(P)\).

(c) If \(a \in T(P)\), then \(a \in T(P)\).

(d) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(e) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(f) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(g) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(h) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(i) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(j) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(k) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(l) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(m) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(n) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(o) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(p) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(q) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(r) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(s) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(t) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(u) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(v) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(w) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(x) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(y) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

(z) If \(a \in T(P)\), then \(m(k)/k \in T(P)\).

The proof of Lemma 20 follows immediately from (a).

If \(a \in T(P)\), then \(b(k) = 2^k \leq 2^k \mod p\), and by (b), \(b(k) = 2^k \mod p\) is bounded. Hence (e) holds by (22).

If \(a \in T(P)\) then, by Proposition 18 (a), (g), \((1 + p^n)\mod p\) for some \(n \geq 1\). Hence \(2^n = 1 + p^n\) for some \(n \in Z^+\) where \(1 \leq n\).
The numbers \( \frac{p^r - 1}{p^s - 1} \) 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 \( E \) is a ring with identity element, \( k \in \mathbb{Z}^+ \) and \( m(k) \) is a unit of \( E \) then \( E = m(k)E \leq J(k, E) \leq E \) so \( J(k, E) = E \).

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

Proposition 23. If \( E \) is a ring with identity element and there is a homomorphism \( \varphi \) of \( R \) onto \( \mathbb{Z}[x] \), then

\[
m(k, \mathbb{Z}[x]) = m(k)
\]

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

\[
m(k, \mathbb{Z}[\{a_n\}] = m(k).
\]

Proof. By (3) in Section 1,

\[
m(k, E)m(k).
\]

Since \( R\varphi = \mathbb{Z}[x] \),

\[
m(k, E)\mathbb{Z}[x] = m(k, E)E \varphi \leq J(k, E)\varphi = J(k, \mathbb{Z}[x]).
\]

Hence \( m(k)/m(k, E) \), so \( m(k) = m(k, E) \). Since there is a homomorphism \( \varphi \) from \( \mathbb{Z}[\{x_k\}] \) onto \( \mathbb{Z}[x] \), \( m(k) = m(k, \mathbb{Z}[\{x_k\}]) \).

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

I. Kaplansky has shown that if \( R \) is a ring such that for every \( a \in R \), there is an \( n(a) \in \mathbb{Z}^+ \) 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, \( k \geq 1 \) 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 $1 \leq k \leq 100$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$a(k)$</th>
<th>$b(k)$</th>
<th>$m(k)/k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>3 = 12</td>
<td>5</td>
<td>60</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>3 = 21</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2 - 5 = 10</td>
<td>3</td>
<td>30</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>3 = 12</td>
<td>5 - 11 = 55</td>
<td>680</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>4 - 7 = 28</td>
<td>13</td>
<td>306</td>
</tr>
<tr>
<td>15</td>
<td>3 - 3 = 15</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>3 - 7 = 21</td>
<td>42</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>3 = 12</td>
<td>5 - 17 = 55</td>
<td>1,020</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>2 - 5 = 10</td>
<td>3 - 19 = 57</td>
<td>570</td>
</tr>
<tr>
<td>21</td>
<td>3 - 7 = 21</td>
<td>2</td>
<td>42</td>
</tr>
<tr>
<td>22</td>
<td>2 - 11 = 22</td>
<td>1</td>
<td>22</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>4 - 3 = 12</td>
<td>5 - 7 - 11 = 23 = 8,856</td>
<td>106,260</td>
</tr>
<tr>
<td>25</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>26</td>
<td>2 - 13 = 26</td>
<td>3 - 5 = 15</td>
<td>309</td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>28</td>
<td>4 - 7 = 28</td>
<td>3 - 13 = 39</td>
<td>1,092</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>4 - 3 - 5 = 60</td>
<td>29</td>
<td>1,740</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>2 - 5 = 10</td>
<td>10</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>3 - 7 - 31 = 651</td>
<td>1,309</td>
</tr>
<tr>
<td>33</td>
<td>3 - 11 = 33</td>
<td>2</td>
<td>66</td>
</tr>
<tr>
<td>34</td>
<td>2 - 17 = 34</td>
<td>1</td>
<td>34</td>
</tr>
<tr>
<td>35</td>
<td>5 - 7 = 28</td>
<td>2</td>
<td>70</td>
</tr>
<tr>
<td>36</td>
<td>4 - 3 = 12</td>
<td>5 - 11 - 17 = 935</td>
<td>11,320</td>
</tr>
<tr>
<td>37</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>38</td>
<td>2 - 13 = 38</td>
<td>37</td>
<td>1,406</td>
</tr>
<tr>
<td>39</td>
<td>3 - 19 = 59</td>
<td>2</td>
<td>78</td>
</tr>
<tr>
<td>40</td>
<td>2 - 5 = 10</td>
<td>3 - 7 - 19 = 399</td>
<td>3,990</td>
</tr>
<tr>
<td>41</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>42</td>
<td>4 - 3 - 7 = 84</td>
<td>5 - 13 - 41 = 2,665</td>
<td>228,860</td>
</tr>
<tr>
<td>43</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>44</td>
<td>2 - 11 = 22</td>
<td>3 - 43 = 129</td>
<td>2,688</td>
</tr>
<tr>
<td>45</td>
<td>3 - 5 - 15</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>46</td>
<td>2 - 23 = 46</td>
<td>1</td>
<td>46</td>
</tr>
</tbody>
</table>
Table (continued)

<table>
<thead>
<tr>
<th>$h$</th>
<th>$a(k)$</th>
<th>$b(k)$</th>
<th>$m(k)/h$</th>
</tr>
</thead>
<tbody>
<tr>
<td>94</td>
<td>2·47 = 94</td>
<td>1</td>
<td>94</td>
</tr>
<tr>
<td>95</td>
<td>5·19 = 95</td>
<td>2</td>
<td>190</td>
</tr>
<tr>
<td>96</td>
<td>4·3 = 12</td>
<td>3·7·11·23·31·47 = 12,901,735</td>
<td>154,820,820</td>
</tr>
<tr>
<td>97</td>
<td>4·7 = 28</td>
<td>13·97 = 1,261</td>
<td>35,308</td>
</tr>
<tr>
<td>99</td>
<td>3·11 = 33</td>
<td>2</td>
<td>66</td>
</tr>
<tr>
<td>100</td>
<td>2·5 = 10</td>
<td>3·7·19 = 3,990</td>
<td>36,900</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>102</td>
<td>4·3·17 = 204</td>
<td>5·101 = 506</td>
<td>150,020</td>
</tr>
<tr>
<td>103</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>104</td>
<td>2·13 = 26</td>
<td>3·5·7·103 = 10,815</td>
<td>281,190</td>
</tr>
<tr>
<td>105</td>
<td>3·5·7 = 105</td>
<td>2</td>
<td>210</td>
</tr>
<tr>
<td>106</td>
<td>2·53 = 106</td>
<td>1</td>
<td>106</td>
</tr>
<tr>
<td>107</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>108</td>
<td>4·3 = 12</td>
<td>5·11·17·31·107 = 5,302,385</td>
<td>63,629,620</td>
</tr>
<tr>
<td>109</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>110</td>
<td>2·3·11 = 66</td>
<td>3·109 = 327</td>
<td>35,970</td>
</tr>
<tr>
<td>111</td>
<td>3·37 = 111</td>
<td>2</td>
<td>233</td>
</tr>
<tr>
<td>112</td>
<td>4·7·29 = 29</td>
<td>3·13 = 39</td>
<td>1,092</td>
</tr>
<tr>
<td>113</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>114</td>
<td>4·3·19 = 228</td>
<td>5·7·37·113 = 146,435</td>
<td>33,364,380</td>
</tr>
<tr>
<td>115</td>
<td>5·23 = 115</td>
<td>2</td>
<td>230</td>
</tr>
<tr>
<td>116</td>
<td>2·29 = 58</td>
<td>3</td>
<td>174</td>
</tr>
<tr>
<td>117</td>
<td>3·13 = 39</td>
<td>2</td>
<td>78</td>
</tr>
<tr>
<td>118</td>
<td>2·59 = 118</td>
<td>1</td>
<td>118</td>
</tr>
<tr>
<td>119</td>
<td>7·17 = 119</td>
<td>2</td>
<td>238</td>
</tr>
<tr>
<td>120</td>
<td>4·3·5 = 60</td>
<td>5·7·11·19·23·29 = 37,578,480</td>
<td>3,454,404,940</td>
</tr>
<tr>
<td>121</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>122</td>
<td>2·61 = 122</td>
<td>11</td>
<td>1,342</td>
</tr>
<tr>
<td>123</td>
<td>3·41 = 123</td>
<td>2</td>
<td>246</td>
</tr>
<tr>
<td>124</td>
<td>4·31 = 124</td>
<td>3·5·61 = 915</td>
<td>113,460</td>
</tr>
<tr>
<td>125</td>
<td>5</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>126</td>
<td>4·3·7 = 84</td>
<td>5·13·17·41 = 46,305</td>
<td>3,805,360</td>
</tr>
<tr>
<td>127</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>128</td>
<td>2</td>
<td>2</td>
<td>1,016</td>
</tr>
<tr>
<td>129</td>
<td>3·43 = 129</td>
<td>2</td>
<td>258</td>
</tr>
<tr>
<td>130</td>
<td>2·5·13 = 130</td>
<td>1</td>
<td>130</td>
</tr>
<tr>
<td>131</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>132</td>
<td>4·3·11 = 132</td>
<td>5·43·131 = 28,165</td>
<td>3,717,778</td>
</tr>
<tr>
<td>133</td>
<td>7·19 = 153</td>
<td>2·11 = 22</td>
<td>2,926</td>
</tr>
<tr>
<td>134</td>
<td>2·67 = 154</td>
<td>1</td>
<td>134</td>
</tr>
<tr>
<td>135</td>
<td>3·5 = 15</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>136</td>
<td>2·17 = 34</td>
<td>3·7·67 = 1,407</td>
<td>47,833</td>
</tr>
<tr>
<td>137</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>138</td>
<td>4·3·23 = 276</td>
<td>5·137 = 685</td>
<td>189,090</td>
</tr>
<tr>
<td>139</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>140</td>
<td>4·5·7 = 140</td>
<td>3·13·19·139 = 103,999</td>
<td>14,409,860</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>$p$</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$-power sums</td>
<td>3,57,9,15,17,21,31,33,37,61,73,83,101,127,129</td>
<td>4,10,13,26,40,82,91,121</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$-power sums</td>
<td>6,26,31,126</td>
<td>8,50,57</td>
<td>15,122</td>
<td>14,18</td>
<td>20</td>
<td>24</td>
<td>30</td>
<td>32</td>
<td>38</td>
<td>42</td>
<td>44</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$-power sums</td>
<td>48</td>
<td>54</td>
<td>69</td>
<td>69</td>
<td>68</td>
<td>72</td>
<td>74</td>
<td>50</td>
<td>54</td>
<td>90</td>
<td>98</td>
<td>103</td>
</tr>
<tr>
<td>$p$-power sums</td>
<td>128</td>
<td>132</td>
<td>138</td>
<td>140</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
</tr>
</tbody>
</table>


**References**


A note on Fermat's conjecture

by

K. Inkeri (Tuikk)

Introduction. Recently Everett [3] has proved the following theorem.

Theorem 1. Let an odd prime $p \geq 3$ and an integer $e \geq 1$ 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 $\geq 3$. Then there exist at most a finite number of positive integer triples $(x, y, z)$ which satisfy the conditions

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

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 Hyryr [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 ($p+y+z$).

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. 53 in [3] is worth mentioning. According to this note, the proof of Theorem 2, excluding the case $x-y < M, p+y+z$, can be carried out elementary, 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