INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7 (2007), #A41

ON DIVISIBILITY OF SOME POWER SUMS

Tamás Lengyel
Department of Mathematics, Occidental College, 1600 Campus Road, Los Angeles, USA
lengyel@oxy.edu

Received: 5/4/07, Accepted: 9/17/07, Published: 9/19/07

Abstract

We determine the exact power of a prime p which divides the power sum $1^n+2^n+\cdots+(b^m-1)^n$ provided that m and b are positive integers, p divides b, and m is large enough.

1. Introduction

Let n and k be positive integers, p be a prime, and let $d_2(k)$ and $\rho_p(k)$ denote the number of ones in the binary representation of k and the highest power of p dividing k, respectively. The latter one is often referred to as the p-adic order of k. For rational n/k we set $\rho_p(n/k) = \rho_p(n) - \rho_p(k)$.

Let b and m be positive integers. In this paper we determine the p-adic order of $1^n + 2^n + \cdots + (b^m - 1)^n$ for any positive integer n in the exponent, provided that p divides b.

Our original motivation was to find the 2-adic order of the power sum $O_n(2^m - 1) = 1^n + 3^n + \cdots + (2^m - 1)^n$ in order to prove the congruence $S(c2^n, 2^m - 1) \equiv 3 \cdot 2^{m-1} \bmod 2^{m+1}$ for Stirling numbers of the second kind, with integer c so that $c2^n > 2^m - 1$ and $m \geq 2$. Thus we first consider the case with $p = 2$. We observe that $\rho_2(O_n(2^m - 1)) \geq m - 1$ by an easy induction proof on m. In fact, more can be said. For $n \geq 2$ even, the same proof yields $\rho_2(O_n(2^m - 1)) = m - 1$, too. Clearly, $O_1(2^m - 1) = 2^{2(m-1)}$ but in general, the odd case seems more difficult.

We set

$$S_n(x) = \sum_{k=0}^{x} k^n$$

and determine the exact 2-adic order of $S_n(2^m - 1)$ by using Bernoulli polynomials in Theorem 1 in Section 3.

We generalize Theorem 1 and its proof in Theorem 3 in Section 4 for any prime p. We also obtain Theorem 4 in order to get a lower bound on the p-adic order of $S_n(b^m-1)$ and Theorem 5 to determine the exact order for any large enough m.

2. An Odd Divisibility Property

There is a general divisibility property that we can apply here to prove that $S_1(b^m-1) \mid S_n(b^m-1)$ for $n \geq 1$ odd. Of course, this already implies that $\rho_p(S_n(b^m-1)) \geq m$.

So, in general, we write $S_n = S_n(c)$ where c is an arbitrary odd positive integer. We can easily prove that S_n is divisible by S_1. Note that $S_1 = \binom{c+1}{2}$. Then, by two different grouping of the terms in S_n we get

$$c \mid (1^n + (c-1)^n) + (2^n + (c-2)^n) + \cdots + \left(\left(\frac{c-1}{2}\right)^n + \left(\frac{c+1}{2}\right)^n\right) + c^n, \text{ and}$$

$$\frac{c+1}{2} \mid (1^n + c^n) + (2^n + (c-1)^n) + \cdots + \left(\left(\frac{c-1}{2}\right)^n + \left(\frac{c+3}{2}\right)^n\right) + \left(\frac{c+1}{2}\right)^n,$$

and the proof is complete since c and $c+1$ are relatively prime.

We note that Faulhaber had already known in 1631 (cf. [2]) that $S_n(c)$ can be expressed as a polynomial in $S_1(c)$ and $S_2(c)$, although with fractional coefficients. In fact, $S_n(c)$ can be written as a polynomial in $c(c+1)$ or $\big(c(c+1)\big)^2$, if n is even or odd, respectively. This gives rise to the appearance of factors such as b^m and b^{2m} in $S_n(b^m-1)$, depending on whether n is even or odd.

3. The Exact 2-adic Order

Now we discuss the case with $p = 2$.

Theorem 1 *For $m \geq 1$ and $n \geq 1$, we have that*

$$\rho_2(S_n(2^m-1)) = \begin{cases} m-1, & \text{if } n \text{ is even or } n = 1, \\ 2(m-1), & \text{if } n \geq 3 \text{ odd.} \end{cases}$$

We note that clearly, $S_1(2^m-1) = 2^{m-1}(2^m-1)$. For $m = 1$, we have $O_n(1) = S_n(1) = 1$, and in general, for $n \geq 2$, the 2-adic order of $O_n(2^m-1)$ and $S_n(2^m-1)$ are the same, as it easily follows from $O_n(2^m-1) = S_n(2^m-1) - 2^n S_n(2^{m-1}-1)$; thus $\rho_2(O_n(2^m-1)) = \rho_2(S_n(2^m-1))$.

Proof of Theorem 1. The statement is true for $n = 1$ or $m = 1$ so we assume that $n \geq 2$ and $m \geq 2$ from now on. The Bernoulli polynomials [3] are defined by

$$B_m(x) = \sum_{i=0}^{m} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} (x+k)^m. \tag{1}$$

It is well known [1] that

$$\sum_{k=0}^{x} k^n = \frac{B_{n+1}(x+1) - B_{n+1}(0)}{n+1}. \tag{2}$$

The usual Bernoulli numbers can be defined as $B_n = B_n(0)$, and the initial values are $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_3 = 0, B_4 = -1/30, B_5 = 0$, etc. Note that B_n=0 for every odd integer $n \geq 3$. We form the difference in the numerator of (2) and then, for $B_{n+1}(x+1)$, we use the binomial expansion of $(x+1+k)^{n+1}$ and focus on terms with $(x+1)^j$ with small exponents. We have

$$\begin{aligned} B_{n+1}(x+1) - B_{n+1}(0) &= \sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} \left(\sum_{j=0}^{n+1} \binom{n+1}{j} (x+1)^j k^{n+1-j} - k^{n+1} \right) \\ &= \sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} \Bigg((n+1)(x+1)k^n \\ &\qquad + \binom{n+1}{2} (x+1)^2 k^{n-1} + \sum_{j=3}^{n+1} \binom{n+1}{j} (x+1)^j k^{n+1-j} \Bigg), \end{aligned}$$

so that

$$\begin{aligned} \frac{B_{n+1}(x+1) - B_{n+1}(0)}{n+1} &= \sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} \Bigg((x+1)k^n + \frac{n}{2}(x+1)^2 k^{n-1} \\ &\qquad + \sum_{j=3}^{n+1} \frac{\binom{n}{j-1}}{j} (x+1)^j k^{n+1-j} \Bigg). \end{aligned}$$

Now we rewrite this with $x = 2^m - 1$ and get that

$$S_n(2^m - 1) = \sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} \left(2^m k^n + \frac{n}{2} 2^{2m} k^{n-1} + \sum_{j=3}^{n+1} \frac{\binom{n}{j-1}}{j} 2^{jm} k^{n+1-j} \right). \tag{3}$$

If $n \geq 2$ is even then we only need the first term in the last parenthetical expression, otherwise we need the first two terms.

Let $n \geq 2$ be even, then the term with $j = 1$ contributes

$$2^m \sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} k^n = 2^m B_n(0) = 2^m \sum_{i=0}^{n} \frac{1}{i+1} (-1)^i i! S(n,i) \tag{4}$$

by identity (1), a standard formula for the Stirling numbers of the second kind, and $S(n, n+1) = 0$. The other terms are all divisible by 2^m.

Clearly, $\rho_2\left(\frac{i!}{i+1}\right) \geq 0$ if $i \geq 4$. Indeed, in this case $i - d_2(i) - \rho_2(i+1) \geq 0$ since $i \geq 2\lfloor \log_2(i+1) \rfloor$. Therefore, we need only the 2-adic order of

$$\sum_{i=0}^{3} \frac{(-1)^i}{i+1} i! S(n,i) = -\frac{1}{2}S(n,1) + \frac{2}{3}S(n,2) - \frac{3}{2}S(n,3),$$

which yields $\rho_2(S_n(2^m-1)) = \rho_2\left(2^m \frac{1}{2}\left(3S(n,3)+7\right)\right) = \rho_2\left(2^m \frac{1}{2} \frac{3^{n+1}+23}{2}\right) = m-1$, by the identity $S(n,3) = \frac{1}{2}(3^{n-1} - 2^n + 1)$, $n \geq 1$. Note that $\rho_2(S_n(2^m-1)) = \rho_2(2^m B_n(0)) = m-1$ also follows by simply noting the well-known fact about the Bernoulli numbers that $\rho_2(B_n(0)) = -1$ for even $n \geq 2$ by a theorem by von Staudt [5]. □

Theorem 2 *(von Staudt, [5])* *For $n = 1$ and $n \geq 2$ even, we have* $-B_n \equiv \sum_{\substack{p \text{ prime} \\ p-1|n}} \frac{1}{p} \bmod 1.$

Proof. Clearly, for n even, the denominator of B_n is the product of the primes p with $(p-1) \mid n$, and thus, it must be square-free. It follows that $\rho_p(B_n) \geq -1$ for all primes p, and it is nonnegative unless $(p-1) \mid n$.

Now assume that $n \geq 3$ is odd. The first two terms in the parenthesis of (3) contribute

$$\begin{aligned}&2^m \textstyle\sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} k^n + 2^{2m} \frac{n}{2} \sum_{i=0}^{n+1} \frac{1}{i+1} \sum_{k=0}^{i} (-1)^k \binom{i}{k} k^{n-1} \\ &= 2^m B_n + 2^{2m} \frac{n}{2} \textstyle\sum_{i=0}^{n+1} \frac{(-1)^i}{i+1} i! S(n-1,i) = 2^m B_n + 2^{2m-1} n B_{n-1}.\end{aligned}$$

The 2-adic order is $2(m-1)$ since $B_n = 0$ and $\rho_2(B_{n-1}) = -1$ since $n \geq 3$ is odd. The other terms of (3) with $j \geq 3$ are all divisible by 2^{2m} since $jm - \rho_2(j) > 2m$ for $m \geq 2$, as $\frac{j-2}{\log_2 j} > \frac{1}{m}$ in this case. □

Remark 1. The above proof can be generalized to the case in which 2^m is replaced by $(2c)^m$ with any odd integer $c \geq 1$.

4. The General Case: The Exact p-adic Order

We note that $S_n(2^m-1) = \sum_{j=1}^{n+1} 2^{mj} B_{n+1-j} \frac{\binom{n}{j-1}}{j}$ by (3) with an observation similar to (4), and in general, for any positive integer b,

$$S_n(b^m-1) = \sum_{j=1}^{n+1} b^{mj} B_{n+1-j} \frac{\binom{n}{j-1}}{j}. \tag{5}$$

We now prove the generalized version of Theorem 1.

Theorem 3 *For $m, n,$ and b positive integers with $p \mid b$, p prime, and $m' = m\,\rho_p(b)$, we have that*

$$\rho_p(S_n(b^m-1)) = \begin{cases} m' + \rho_p(B_n), & \text{if } n = 1, \\ m' + \rho_p(B_n), & \text{if } n \text{ is even and } \rho_p(B_n) = 0 \text{ or } -1, \\ 2m' + \rho_p(B_{n-1}) + \rho_p(n/2), & \text{if } n \geq 3 \text{ odd and } \rho_p(B_{n-1}) = 0 \text{ or } -1. \end{cases} \tag{6}$$

Proof. We have already proved the statement for $p = 2$ in Theorem 1 and Remark 1. If $p \geq 3$ then the case with $n = 1$ is easy to check. Thus, we can also assume that $n \geq 2$. We now prove the theorem with $\rho_p(b) = 1$, i.e., if $m' = m$. The general case with $\rho_p(b) \geq 1$ easily follows by replacing m by m' in the proof below.

First, if n is even then all terms with $j \geq 5$ on the right hand side of (5) are divisible by p^{m+1} since $jm - 1 - \rho_p(j) \geq m + 1$ as $\frac{j-1}{2+\log_p j} \geq \frac{1}{m}$ for $m \geq 1$. If $j = 3$ and $p = 3$ then $3m + \rho_3(B_{n-2}) - \rho_3(3) \geq m + \rho_3(B_n) + 1$ for $m \geq 1$ and $n \geq 2$ even. If $j = 3$ and $p \geq 5$ then clearly $3m - 1 - \rho_p(3) \geq m + 1$. The term with $j = 2$ works since $B_{n-1} = 0$ except for $n = 2$ when $2m - \rho_p(2) \geq m + 1$. The term with $j = 4$ also works for $n \geq 4$ since $B_{n-3} = 0$ except for $n = 4$ when $4m - \rho_p(4) \geq m + 1$.

Next, if n is odd then we have two cases.

Case 1. If $n = 3$ then for $j = 3$ and 4 we have either $p = 3$ and thus, $jm + \rho_3(B_{4-j}) - 1 \geq 2m + \rho_3(B_2) + 1$, i.e., $jm - 1 \geq 2m$ for $m \geq 1$; or $p \geq 5$ and thus, $jm + \rho_p(B_{4-j}) \geq 2m + \rho_p(B_2) + 1$, i.e., $jm \geq 2m + 1$ again.

Case 2. If $n \geq 5$ odd then we rewrite $\binom{n}{j-1}$ as $\frac{n}{j-1}\binom{n-1}{j-2}$ for $j \geq 2$. All terms with $j \geq 5$ on the right hand side of (5) are divisible by $p^{2m+\rho_p(n/2)+1}$ since $jm - 1 + \rho_p(n) - \rho_p(j(j-1)) \geq 2m + \rho_p(n/2) + 1$ as $\frac{j-2}{2+\rho_p(j(j-1))} \geq \frac{1}{m}$ for $m \geq 1$. If $p = 3$ then for the term with $j = 4$, we get that $4m + \rho_3(B_{n-3}) + \rho_3(n) - \rho_3(4 \cdot 3) \geq 2m + \rho_3(B_{n-1}) + \rho_3(n/2) + 1$ since $4m - 2 \geq 2m$ for $m \geq 1$ and $\rho_3(B_k) = -1$ for $k \geq 2$ even. If $p \geq 5$ then for the term with $j = 4$, we get that $4m - 1 + \rho_p(n) \geq 2m + \rho_p(n/2) + 1$ since $4m - 1 \geq 2m + 1$ for $m \geq 1$. The term with $j = 3$ makes no contribution to (5) as $B_{n-2} = 0$. $\square$

We obtain a lower bound and the exact p-adic order of $S_n(b^m - 1)$ in the next two theorems.

Theorem 4 *For $m, n,$ and b positive integers with $p \mid b$, p prime, and $m' = m\,\rho_p(b)$, we have that*

$$\rho_p(S_n(b^m-1)) \geq \begin{cases} m' - 1, & \text{if } n \text{ is even or } n = 1, \\ 2m' + \rho_p(n/2) - 1, & \text{if } n \geq 3 \text{ odd.} \end{cases}$$

Theorem 5 *For m, n, and b positive integers so that m is sufficiently large and $p \mid b$, p prime, and $m' = m\,\rho_p(b)$, we have that*

$$\rho_p(S_n(b^m-1)) = \begin{cases} m' + \rho_p(B_n), & \text{if } n \text{ is even or } n = 1, \\ 2m' + \rho_p(B_{n-1}) + \rho_p(n/2), & \text{if } n \geq 3 \text{ odd.} \end{cases}$$

The proof of Theorem 3 shows how to extend it to those of Theorems 4 and 5. A result by Andrews [6] implies that $\rho_p(B_n)$ can be arbitrary large. For example, if $(p-1) \nmid n$ and $\rho_p(n) = l > 0$ then $\rho_p(B_n) \geq l$, and this suggests that it might be difficult to get the exact order of $\rho_p(S_n(b^m-1))$ with a formula, similar to (6), which is uniformly valid in all m.

Remark 2. We intended to find the p-adic order of $S_n(x)$ for special integers of the form $x = b^m - 1$ with $p \mid b$, however, the above theorems remain true for $x = c\,b^m - 1$ with $p \mid b$ and $p \nmid c$, by adjusting identity (5). In this case, $S_n(c\,b^m + 1) \equiv 1 \bmod p$ also follows if m is sufficiently large.

We note that if p divides b for some prime p, and we calculate $B_{n+1-j}\binom{n}{j-1}/j$ in (5) p-adically, such as by using a theorem discovered independently by Anton, Stickelberger, and Hensel [4] on binomial coefficients modulo powers of p, then we can find further and more refined congruential properties of $S_n(b^m-1)$.

Acknowledgment The author wishes to thank Gregory Tollisen for making helpful suggestions and comments that improved the presentation of this paper.

References

[1] L. Comtet, *Advanced Combinatorics*, D. Reidel Publishing Co., Dordrecht, 1974.

[2] A. W. F. Edwards, A quick route to sums of powers, *Amer. Math. Monthly*, 93(6):451–455, 1986.

[3] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publishing Company, Reading, MA, second edition, 1994.

[4] A. Granville, Arithmetic properties of binomial coefficients I, Binomial coefficients modulo prime powers, In *Organic Mathematics (Burnaby, BC, 1995)*, volume 20 of *CMS Conf. Proc.*, pages 253–276. Amer. Math. Soc., Providence, RI, 1997. Electronic version (a dynamic survey): `http://www.dms.umontreal.ca/~andrew/Binomial/`.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[6] R. Thangadurai, Adams theorem on Bernoulli numbers revisited, *J. Number Theory*, 106(1):169–177, 2004.