Elem. Math. 67 (2012) 182 – 186
0013-6018/12/040182-5
DOI 10.4171/EM/208

Elemente der Mathematik

Divisibility of power sums and the generalized Erdős-Moser equation

Kieren MacMillan and Jonathan Sondow

Kieren MacMillan is a professional composer and amateur number theorist. In 1987, he attended the University of Waterloo on a mathematics scholarship, subsequently transferring to the University of British Columbia where he graduated with a Bachelor of Music in 1993. He obtained his Master of Music in Composition from the Shepherd School of Music at Rice University in 1997. He currently lives in Toronto.

Jonathan Sondow is a mathematician living in New York City. He attended the University of Wisconsin at Madison and received in 1965 at the age of 22 a Ph.D. in mathematics from Princeton University, where he wrote a thesis in differential topology under John Milnor. Sondow has held numerous academic posts and currently maintains a home page devoted to research in number theory.

1 Introduction

For p a prime and k an integer, $v_p(k)$ *denotes the highest exponent* v *such that* $p^v \mid k$. (Here $a \mid b$ means a divides b.) For example, $v_2(k) = 0$ if and only if k is odd, and $v_2(40) = 3$.

Die Potenzsummen $S_n(m) = 1^n + 2^n + \cdots + m^n$ haben immer wieder Anlass zu mathematischer Forschung gegeben. Die Formel $S_1(m) = m(m+1)/2$ lässt sich bis in die griechische Antike nachweisen. Fermat zählte die Aufgabe, Formeln für die Potenzsummen zu finden, gar zu den schönsten Problemen der Mathematik. Der Ulmer Rechenmeister Johannes Faulhaber legte 1631 den Grundstein zur heute nach ihm benannten Formel für Potenzsummen. Carl Ludwig Siegel kommentierte gegenüber André Weil den Moment, als erstmals der einfachste Fall der Faulhaberschen Formel entdeckt wurde, mit den Worten "Es gefiel dem lieben Gott". In der vorliegenden Arbeit bestimmen die Autoren die höchste Potenz von 2, welche $S_n(m)$ teilt und verallgemeinern somit Tamás Lengyels Formel die den Spezialfall abdeckt, wo m eine Zweierpotenz ist. Als Anwendung resultiert ein neuer Beweis von Pieter Morees Resultat über die Lösungen der verallgemeinerten Erdős-Moser-Gleichung.

For any *power sum*

$$S_n(m) := \sum_{j=1}^{m} j^n = 1^n + 2^n + \cdots + m^n \qquad (m > 0,\ n > 0),$$

we determine $v_2(S_n(m))$. As motivation, we first give a classical extension of the fact that $S_1(m) = m(m+1)/2$, a formula known to the ancient Greeks [1, Ch. 1] and famously [4] derived by Gauss at age seven to calculate the sum

$$1 + 2 + \cdots + 99 + 100 = (1 + 100) + (2 + 99) + \cdots + (50 + 51) = 5050.$$

Proposition 1. *If $n > 0$ is odd and $m > 0$, then $m(m+1)/2$ divides $S_n(m)$.*

The proof is a modification of Lengyel's arguments in [5] and [6].

Proof of Proposition 1. *Case* 1: *both n and m odd*. Since m is odd we may group the terms of $S_n(m)$ as follows, and as n is also odd we see by expanding the binomial that

$$S_n(m) = m^n + \sum_{j=1}^{(m-1)/2} \left(j^n + (m-j)^n\right) \quad \Longrightarrow \quad m \mid S_n(m).$$

Similarly, grouping the terms in another way shows that

$$S_n(m) = \frac{1}{2}\sum_{j=1}^{m}\left(j^n + ((m+1)-j)^n\right) \quad \Longrightarrow \quad \frac{m+1}{2} \mid S_n(m).$$

As m and $m+1$ are relatively prime, it follows that $m(m+1)/2 \mid S_n(m)$.

Case 2: *n odd and m even*. Here

$$S_n(m) = \sum_{j=1}^{m/2}\left(j^n + ((m+1)-j)^n\right) \quad \Longrightarrow \quad (m+1) \mid S_n(m)$$

and

$$S_n(m) = \frac{1}{2}\sum_{j=0}^{m}\left(j^n + (m-j)^n\right) \quad \Longrightarrow \quad \frac{m}{2} \mid S_n(m).$$

Thus $m(m+1)/2 \mid S_n(m)$ in this case, too. □

Here is a paraphrase of Lengyel's comments [5] on Proposition 1:

> We note that Faulhaber had already known in 1631 (cf. [2]) that $S_n(m)$ can be expressed as a polynomial in $S_1(m)$ and $S_2(m)$, although with fractional coefficients. In fact, $S_n(m)/(2m+1)$ or $S_n(m)$ can be written as a polynomial in $m(m+1)$ or $(m(m+1))^2$, if n is even or $n \geq 3$ is odd, respectively.

Proposition 1 implies that if n is odd, then

$$v_p(S_n(m)) \geq v_p(m(m+1)/2),$$

for any prime p. When $p = 2$, Theorem 1 shows that the inequality is strict for odd $n > 1$.

Theorem 1. *Given any positive integers m and n, the following divisibility formula holds:*

$$v_2(S_n(m)) = \begin{cases} v_2(m(m+1)/2) & \text{if } n = 1 \text{ or } n \text{ is even,} \\ 2v_2(m(m+1)/2) & \text{if } n \geq 3 \text{ is odd.} \end{cases} \tag{1}$$

The elementary proof given in Section 3 uses a lemma proved by induction.

In the special case where m is a power of 2, formula (1) is due to Lengyel [5, Theorem 1]. His complicated proof, which uses Stirling numbers of the second kind and von Staudt's theorem on Bernoulli numbers, is designed to be generalized. Indeed, for m a power of an odd prime p, Lengyel proves results [5, Theorems 3, 4, 5] towards a formula for $v_p(S_n(m))$.

In the next section, we apply formula (1) to a certain Diophantine equation.

2 Equations of Erdős-Moser type

As an application of Theorem 1, we give a simple proof of a special case of a result due to Moree. Before stating it, we discuss a conjecture made by Erdős and Moser [11] around 1953.

Conjecture 1 (Erdős-Moser)**.** *The only solution of the Diophantine equation*

$$1^n + 2^n + \cdots + (m-1)^n = m^n$$

is the trivial solution $1 + 2 = 3$.

Moser proved, among many other things, that *Conjecture* 1 *is true for odd exponents n*. (An alternate proof is given in [7, Corollary 1].) In 1987 Schinzel showed that *in any solution, m is odd* [10, p. 800]. For surveys of results on the problem, see [3, Section D7], [8], [9], and [10].

In 1996 Moree generalized Conjecture 1.

Conjecture 2 (Moree)**.** *The only solution of the generalized Erdős-Moser Diophantine equation*

$$1^n + 2^n + \cdots + (m-1)^n = am^n \tag{2}$$

is the trivial solution $1 + 2 + \cdots + 2a = a(2a+1)$.

Actually, Moree [8, p. 290] conjectured that *equation* (2) *has no integer solution with* $n > 1$. The equivalence to Conjecture 2 follows from the formula

$$1 + 2 + \cdots + k = \frac{1}{2}k(k+1) \tag{3}$$

with $k = m - 1$.

Generalizing Moser's result on Conjecture 1, Moree [8, Proposition 3] proved that *Conjecture* 2 *is true for odd exponents* n. He also proved a generalization of Schinzel's result.

Proposition 2 (Moree)**.** *If equation* (2) *holds, then* m *is odd.*

In fact, Moree [8, Proposition 9] (see also [9]) showed more generally that *if* (2) *holds and a prime* p *divides* m*, then* $p-1$ *does not divide* n. (The case $p=2$ is Proposition 2.) His proof uses a congruence which he says [8, p. 283] can be derived from either the von Staudt-Clausen theorem, the theory of finite differences, or the theory of primitive roots.

We apply Theorem 1 to give an elementary proof of Proposition 2.

Proof of Proposition 2. If $n=1$, then (2) and (3) show that $m=2a+1$ is odd.

If $n>1$ and m is even, set $d := v_2(m) = v_2(m(m+1))$. Theorem 1 implies $v_2(S_n(m)) \le 2(d-1)$, and (2) yields $S_n(m) = S_n(m-1)+m^n = (a+1)m^n$. But then $nd \le v_2(S_n(m)) \le 2(d-1)$, contradicting $n>1$. Hence m is odd. □

3 Proof of Theorem 1

The heart of the proof of the divisibility formula is the following lemma.

Lemma 1. *Given any positive integers* n*,* d*, and* q *with* q *odd, we have*

$$v_2(S_n(2^d q)) = \begin{cases} d-1 & \text{if } n=1 \text{ or } n \text{ is even,} \\ 2(d-1) & \text{if } n \ge 3 \text{ is odd.} \end{cases} \tag{4}$$

Proof. We induct on d. Since the power sum for $S_n(2q)$ has exactly q odd terms, we have $v_2(S_n(2q)) = 0$, and so (4) holds for $d=1$. By (3) with $k = 2^d q$, it also holds for all $d \ge 1$ when $n=1$. Now assume inductively that (4) is true for fixed $d \ge 1$.

Given a positive integer a, we can write the power sum $S_n(2a)$ as

$$\begin{aligned} S_n(2a) = a^n + \sum_{j=1}^{a} \left((a-j)^n + (a+j)^n\right) &= a^n + 2\sum_{j=1}^{a}\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} a^{n-2i} j^{2i} \\ &= a^n + 2\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} a^{n-2i} S_{2i}(a). \end{aligned}$$

If $n \ge 2$ is even, we extract the last term of the summation, set $a = 2^d q$, and write the result as

$$S_n(2^{d+1}q) = 2^{nd}q^n + 2^d \frac{S_n(2^d q)}{2^{d-1}} + 2^{2d+1} \sum_{i=0}^{(n-2)/2} \binom{n}{2i} 2^{d(n-2i-2)} q^{n-2i} S_{2i}(2^d q).$$

By the induction hypothesis, the fraction is actually an odd integer. Since $nd > d$, we conclude that $v_2(S_n(2^{d+1}q)) = d$, as desired.

Similarly, if $n \geq 3$ is odd, then

$$S_n(2^{d+1}q) = 2^{nd}q^n + 2^{2d}nq\frac{S_{n-1}(2^dq)}{2^{d-1}} + 2^{3d+1}\sum_{i=0}^{(n-3)/2}\binom{n}{2i}2^{d(n-2i-3)}q^{n-2i}S_{2i}(2^dq).$$

Again by induction, the fraction is an odd integer. Since $nd > 2d$, and n and q are odd, we see that $v_2(S_n(2^{d+1}q)) = 2d$, as required. This completes the proof of the lemma. □

Proof of Theorem 1. When m is even, write $m = 2^dq$, where $d \geq 1$ and q is odd. Then $v_2(m(m+1)/2) = d - 1$, and (4) implies (1).
If m is odd, set $m + 1 = 2^dq$, with $d \geq 1$ and q odd. Again we have $v_2(m(m+1)/2) = d - 1$. From (3) with $k = m$ we get $v_2(S_1(m)) = d - 1$, so that (1) holds for $n = 1$. If $n > 1$, then $nd > 2(d-1) \geq d - 1$, and so (4) and the relations

$$S_n(m) = S_n(m+1) - (m+1)^n \equiv S_n(m+1) \pmod{2^{nd}}$$

imply $v_2(S_n(m)) = v_2(S_n(m+1))$ and, hence, (1). This proves the theorem. □

Acknowledgments. The authors are grateful to Tamas Lengyel and Pieter Moree for valuable comments and suggestions.

References

[1] Dickson, L.E.: *History of the Theory of Numbers. Volume II: Diophantine Analysis*. Carnegie Institute, Washington, D.C., 1919; reprinted by Dover, New York 2005.
[2] Edwards, A.W.F.: A quick route to sums of powers. *Amer. Math. Monthly* 93 (1986), 451–455.
[3] Guy, R.K.: *Unsolved Problems in Number Theory*. 3rd ed. Springer, New York 2004.
[4] Hayes, B.: Gauss's day of reckoning. *Amer. Scientist* 94 (2006), 200–205; see `http://www.sigmaxi.org/amscionline/gauss-snippets.html`.
[5] Lengyel, T.: On divisibility of some power sums. *Integers* 7 (2007) A41, 1–6.
[6] Lengyel, T.: Personal communication. 4 November 2010.
[7] MacMillan, K.; Sondow, J.: Reducing the Erdős-Moser equation $1^n + 2^n + \cdots + k^n = (k+1)^n$ modulo k and k^2. *Integers* 11 (2011) A34, 1–8.
[8] Moree, P.: Diophantine equations of Erdős-Moser type. *Bull. Austral. Math. Soc.* 53 (1996), 281–292.
[9] Moree, P.: Moser's mathemagical work on the equation $1^k + 2^k + \cdots + (m-1)^k = m^k$. *Rocky Mountain J. Math.* (to appear); available at `http://arxiv.org/abs/1011.2940`
[10] Moree, P.; Te Riele, H.; Urbanowicz, J.: Divisibility properties of integers x, k satisfying $1^k + 2^k + \cdots + (x-1)^k = x^k$. *Math. Comp.* 63 (1994), 799–815.
[11] Moser, L.: On the Diophantine equation $1^n + 2^n + \cdots + (m-1)^n = m^n$. *Scripta Math.* 19 (1953), 84–88.

Kieren MacMillan
55 Lessard Avenue
Toronto, Ontario, Canada M6S 1X6
e-mail: `kieren@alumni.rice.edu`

Jonathan Sondow
209 West 97th Street
New York, NY 10025, USA
e-mail: `jsondow@alumni.princeton.edu`