Journal of Number Theory 131 (2011) 1054–1061

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On stronger conjectures that imply the Erdős–Moser conjecture

B.C. Kellner

Mathematisches Institut, Universität Göttingen, Bunsenstr. 3-5, 37073 Göttingen, Germany

ARTICLE INFO

Article history:
Received 16 March 2010
Revised 29 November 2010
Accepted 3 January 2011
Available online 12 February 2011
Communicated by David Goss

MSC:
primary 11B83
secondary 11A05, 11B68

Keywords:
Erdős–Moser equation
Consecutive values of polynomials

ABSTRACT

The Erdős–Moser conjecture states that the Diophantine equation $S_k(m) = m^k$, where $S_k(m) = 1^k + 2^k + \cdots + (m-1)^k$, has no solution for positive integers k and m with $k \geqslant 2$. We show that stronger conjectures about consecutive values of the function S_k, that seem to be more naturally, imply the Erdős–Moser conjecture.

1. Introduction

Let k and m be positive integers throughout this paper. Define

$$S_k(m) = 1^k + 2^k + \cdots + (m-1)^k.$$

Conjecture 1 *(Erdős–Moser). The Diophantine equation*

$$S_k(m) = m^k \tag{1}$$

has only the trivial solution $(k, m) = (1, 3)$ for positive integers k, m.

E-mail address: bk@bernoulli.org.

doi:10.1016/j.jnt.2011.01.004

In 1953 Moser [7] showed that if a solution of (1) exists for $k \geqslant 2$, then k must be even and $m > 10^{10^6}$. Recently, this bound has been greatly increased to $m > 10^{10^9}$ by Gallot, Moree, and Zudilin [2]. So it is widely believed that non-trivial solutions do not exist. Comparing S_k with the integral $\int x^k\,dx$, see [2], one gets an easy estimate that

$$k < m < 2k. \tag{2}$$

A general result of the author [5, Prop. 8.5, p. 436] states that

$$m^{r+1} \mid S_k(m) \quad \Longleftrightarrow \quad m^r \mid B_k \tag{3}$$

for $r = 1, 2$ and even k, where B_k denotes the k-th Bernoulli number. Thus a non-trivial solution (k, m) of (1) has the property that m^2 must divide the numerator of B_k for $k \geqslant 4$; this result concerning (1) was also shown in [6] in a different form.

Because the Erdős–Moser equation is very special, one can consider properties of consecutive values of the function S_k in general. This leads to two stronger conjectures, described in the next sections, that imply the conjecture of Erdős–Moser.

2. Preliminaries

We use the following notation. We write $p^r \,\|\, m$ when $p^r \mid m$ but $p^{r+1} \nmid m$, i.e., $r = \operatorname{ord}_p m$ where p always denotes a prime. Next we recall some properties of the Bernoulli numbers and the function S_k. The Bernoulli numbers B_n are defined by

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}, \quad |z| < 2\pi.$$

These numbers are rational where $B_n = 0$ for odd $n > 1$ and $(-1)^{\frac{n}{2}+1} B_n > 0$ for even $n > 0$. A table of the Bernoulli numbers up to index 20 is given in [5, p. 437]. The denominator of B_n for even n is described by the von Staudt–Clausen theorem, see [4, p. 233], that

$$\operatorname{denom}(B_n) = \prod_{p-1 \mid n} p. \tag{4}$$

The function S_k is closely related to the Bernoulli numbers and is given by the well-known formula, cf. [4, p. 234]:

$$S_k(m) = \sum_{\nu=0}^{k} \binom{k}{\nu} B_{k-\nu} \frac{m^{\nu+1}}{\nu+1}. \tag{5}$$

3. Stronger conjecture — Part I

The strictly increasing function S_k is a polynomial of degree $k+1$ as a result of (5). One may not expect that consecutive values of S_k have highly common prime factors, such that $S_k(m+1)/S_k(m)$ is an integer for sufficiently large m.

Conjecture 2. *Let k, m be positive integers with $m \geqslant 3$. Then*

$$\frac{S_k(m+1)}{S_k(m)} \in \mathbb{N} \quad \Longleftrightarrow \quad (k, m) \in \{(1,3), (3,3)\}. \tag{6}$$

Note that we have to require $m \geqslant 3$, since $S_k(1) = 0$ and $S_k(2) = 1$ for all $k \geqslant 1$. Due to the well-known identity $S_1(m)^2 = S_3(m)$, a solution for $k = 1$ implies a solution for $k = 3$. Hereby we have the only known solutions

$$\frac{1+2+3}{1+2} = 2 \quad \text{and} \quad \frac{1^3+2^3+3^3}{1^3+2^3} = 4 \tag{7}$$

based on some computer search. Since $S_k(m+1)/S_k(m) \to 1$ as $m \to \infty$, it is clear that we can only have a finite number of solutions for a fixed k. By $S_k(m+1) = S_k(m) + m^k$, one easily observes that (6) is equivalent to

$$aS_k(m) = m^k \quad \Longleftrightarrow \quad (a, k, m) \in \bigl\{(1, 1, 3), (3, 3, 3)\bigr\},$$

where a is a positive integer. This gives a generalization of (1).

Proposition 1. *Conjecture* 2 *implies Conjecture* 1.

Proof. Eq. (1) can be rewritten as $2S_k(m) = S_k(m+1)$ after adding $S_k(m)$ on both sides. Conjecture 2 states that $S_k(m+1)/S_k(m)$ is not a positive integer except for the cases $(k, m) = (1, 3)$ and $(k, m) = (3, 3)$ as given in (7). This implies Conjecture 1, which predicts $S_k(m+1)/S_k(m) \neq 2$ for $k \geqslant 2$. □

4. Stronger conjecture — Part II

The connection between the function S_k and the Bernoulli numbers leads to the following theorem, which we will prove later. In the following we always write $B_k = N_k/D_k$ in lowest terms with $D_k > 0$ for even k. For now we write (a, b) for $\gcd(a, b)$.

Theorem 1. *Let k, m be positive integers with even k. Define*

$$g_k(m) = \frac{(S_k(m), S_k(m+1))}{m}.$$

Then

$$\min_{m \geqslant 1} g_k(m) = \frac{1}{D_k} \quad \text{and} \quad \max_{m \geqslant 1} g_k(m) \geqslant |N_k|.$$

Generally

$$g_k(m) = 1 \quad \Longleftrightarrow \quad (D_k N_k, m) = 1$$

and special values are given by

$$g_k(D_k) = \frac{1}{D_k}, \qquad g_k\bigl(|N_k|\bigr) = |N_k|, \quad \text{and} \quad g_k\bigl(D_k|N_k|\bigr) = |B_k|.$$

More generally,

$$g_k(m) = |N_k|, \quad \text{if } (D_k, m) = 1 \text{ and } |N_k| \mid m.$$

In particular if N_k is square-free, then

$$g_k(m) = \frac{(N_k, m)}{(D_k, m)} \quad \textit{and} \quad \max_{m \geqslant 1} g_k(m) = |N_k|.$$

Remark 1. It is well known that $|N_k| = 1$ exactly for $k \in \{2, 4, 6, 8\}$. Known indices k, where $|N_k|$ is prime, are recorded as sequence A092132 in [8]: 10, 12, 14, 16, 18, 36, 42. Sequence A090997 in [8] gives the indices k, where N_k is not square-free: 50, 98, 150, 196, 228, ... By this, all N_k are square-free for $2 \leqslant k \leqslant 48$.

Since $S_k(m+1) = S_k(m) + m^k$, we have

$$\bigl(S_k(m), S_k(m+1)\bigr) = \bigl(S_k(m), m^k\bigr), \tag{8}$$

giving a connection with (1). The function g_k heavily depends on the Bernoulli number B_k. For $2 \leqslant k \leqslant 48$ and some higher indices k we even have

$$\min_{m \geqslant 1} g_k(m) \cdot \max_{m \geqslant 1} g_k(m) = |B_k|.$$

The problem is to find an accurate upper bound of g_k to solve (1). This relation is demonstrated by Theorem 2 below and we raise the following conjecture based on Theorem 1 and some computations.

Conjecture 3. *The function g_k has an upper bound as given in Theorem 2.*

Theorem 2. *Let k, m, r be positive integers with even $k \geqslant 10$. If*

$$\max_{m \geqslant 1} g_k(m) < |N_k| \log^r |N_k| \quad \textit{for } k \geqslant C_r$$

and (1) has no solution for $k < C_r$, where C_r is an effectively computable constant, then Conjecture 1 is true. In particular, one can choose $C_r = 10$ for $r = 1, \ldots, 6$.

Proof. Considering Theorem 1 and (8), a possible solution of (1) must trivially satisfy

$$m^k = \bigl(S_k(m), m^k\bigr) = m g_k(m). \tag{9}$$

For $k = 2, 4, 6, 8$ there is no solution of (1), since $|N_k| = 1$. Now let $k \geqslant 10$. Using the relation of B_k to the Riemann zeta function by Euler's formula, cf. [4, p. 231], we have

$$|B_k| = 2\zeta(k) \frac{k!}{(2\pi)^k}.$$

Since $\zeta(s) \to 1$ monotonically as $s \to \infty$ and $\zeta(2) = \pi^2/6$, we obtain

$$|N_k| < \frac{\pi^2}{3} \frac{k!}{(2\pi)^k} D_k < \frac{2\pi^2}{3} \frac{k!}{\pi^k},$$

using the fact that $D_k \mid 2(2^k - 1)$, see [1]. Stirling's series of the Gamma function, cf. [3, p. 481], states that $k! < \sqrt{2\pi k} k^k e^{-k+1/12k}$. Since $e^{1/12k} < \frac{11}{10}$, we deduce that

$$|N_k| < \eta k^{\frac{3}{2}} \left(\frac{k}{e\pi}\right)^{k-1} \quad \text{with } \eta = \frac{11}{15}\frac{\pi}{e}\sqrt{2\pi} \approx 2.12.$$

Further we conclude that $\log|N_k| < k\log(k/\pi)$. Finally, we achieve that

$$|N_k|\log^r|N_k| < f_r(k)\left(\frac{k}{e\pi}\right)^{k-1} \tag{10}$$

with

$$f_r(k) = \eta k^{\frac{3}{2}+r}\log^r(k/\pi).$$

For a fixed r we have $\sqrt[k-1]{f_r(k)} \to 1$ as $k \to \infty$. Define

$$I(r) = \min\left\{n \geqslant 10\colon\ \sqrt[k-1]{f_r(k)} < e\pi \text{ for all } k \geqslant n\right\},$$

which is an increasing function depending on r. A short computation shows that $I(r) = 10$ for $r = 1, \ldots, 6$. We set $C_r = I(r)$. Consequently (10) turns into

$$\sqrt[k-1]{|N_k|\log^r|N_k|} < k \quad \text{for } k \geqslant C_r. \tag{11}$$

Now, we assume that (1) has no solution for $k < C_r$ and that

$$\max_{m\geqslant 1} g_k(m) < |N_k|\log^r|N_k| \quad \text{for } k \geqslant C_r. \tag{12}$$

According to (9), (11), and (12), we then achieve that $m < k$ for $k \geqslant C_r$, which contradicts (2). Thus there is no solution of (1) for all $k \geqslant 2$ implying Conjecture 1. □

To prove Theorem 1, we shall need some preparations and a refinement of (3).

Theorem 3. *Let k, m be positive integers where k is even and $m \geqslant 2$. Then*

$$\begin{aligned} S_k(m) &\equiv B_k m \pmod{m}, && \text{if } k \geqslant 2,\\ S_k(m) &\equiv B_k m \pmod{m^2}, && \text{if } k \geqslant 4 \text{ and } (D_k, m) = 1,\\ S_k(m) &\equiv B_k m \pmod{m^3}, && \text{if } k \geqslant 6 \text{ and } m \mid N_k. \end{aligned}$$

More precisely for $p^r \,\|\, m$:

$$\begin{aligned} S_k(m) &\equiv B_k m \pmod{p^{2r}}, && \text{if } k \geqslant 4 \text{ and } p \nmid D_k,\\ S_k(m) &\equiv B_k m \pmod{p^{3r}}, && \text{if } k \geqslant 6 \text{ and } p \mid N_k. \end{aligned}$$

Proof. This follows by exploiting the proof of [5, Prop. 8.5, pp. 436–437]. □

Lemma 1. *Let a, b be positive integers. The sequence $\{(a, b^\nu)\}_{\nu\geqslant 1}$ is increasing and eventually constant. If $(a, b^r) = (a, b^{r+1})$ for some $r \geqslant 1$, then $\{(a, b^\nu)\}_{\nu\geqslant r}$ is constant. Especially if $\operatorname{ord}_p a \leqslant s \operatorname{ord}_p b$, then $\operatorname{ord}_p(a, b^\nu) = \operatorname{ord}_p a$ for $\nu \geqslant s$.*

Proof. If $(a,b)=1$, then $(a,b^\nu)=1$ for $\nu \geqslant 1$. Assume that $(a,b)>1$. For each $p \mid (a,b)$, we have $\operatorname{ord}_p(a,b^\nu)=\min\{\operatorname{ord}_p a, \nu \operatorname{ord}_p b\}$, which is increasing and bounded as $\nu \to \infty$. It follows that if $\operatorname{ord}_p a \leqslant s \operatorname{ord}_p b$, then $\operatorname{ord}_p(a,b^\nu)=\operatorname{ord}_p a$ for $\nu \geqslant s$. Considering all primes $p \mid (a,b)$, we deduce that $(a,b^r)=(a,b^{r+1})$ for some $r \geqslant 1$ implies that (a,b^ν) is constant for $\nu \geqslant r$. □

Proposition 2. *Let k, m be positive integers with even k. Then*

$$\big(S_k(m),m\big)=\frac{m}{(D_k,m)} \quad \text{and} \quad \min_{m \geqslant 1} g_k(m)=\frac{1}{D_k}.$$

Proof. Let $m>1$, since the case $m=1$ is trivial. By Theorem 3 we have

$$S_k(m) \equiv \frac{N_k}{D_k} m \pmod{m}.$$

For each prime power $p^{e_p} \,\|\, m$, we then infer that $p^{e_p} \mid S_k(m)$, if $p \nmid D_k$; otherwise $p^{e_p-1} \,\|\, S_k(m)$, since D_k is square-free due to (4). This gives the first equation above. Using Lemma 1 and (8), we deduce the relation

$$g_k(m)=\frac{(S_k(m),m^k)}{m} \geqslant \frac{(S_k(m),m)}{m}=\frac{1}{(D_k,m)}.$$

If $m=D_k$, then we even have that $(S_k(m),m^\nu)=1$ for $\nu \geqslant 1$, giving the minimum with $g_k(m)=1/D_k$. □

Proposition 3. *Let k, m be positive integers with even k. Then*

$$\frac{(S_k(m),m^2)}{m}=\frac{(N_k,m)}{(D_k,m)}.$$

Proof. The case $k=2$ follows by (5), $B_2=\frac{1}{6}$, and $((m-1)(2m-1),m)=1$. Now let $k \geqslant 4$, $m \geqslant 2$, and assume that $(D_k,m)=1$. Applying Theorem 3 for this case we then have

$$S_k(m) \equiv \frac{N_k}{D_k} m \pmod{m^2}. \tag{13}$$

Thus we deduce that $(S_k(m),m^2)=m(N_k,m)$. Now let m be arbitrary. Using Proposition 2 we obtain the relation

$$\big(S_k(m),m^2\big)=c_{k,m}\big(S_k(m),m\big)=c_{k,m}\frac{m}{(D_k,m)}$$

with some integer $c_{k,m} \geqslant 1$. Since $(N_k,D_k)=1$, those factors of (N_k,m) can only give a contribution to the factor $c_{k,m}$; while other factors of m are reduced by (D_k,m). To be more precise, consider a prime p where $p^r \,\|\, m$: If $p \mid D_k$, then $\operatorname{ord}_p(S_k(m),m^\nu)=r-1$ for $\nu \geqslant 1$ by Proposition 2 and Lemma 1. Otherwise $p \nmid D_k$ and (13) remains valid (mod p^{2r}) by Theorem 3. Hence $c_{k,m}=(N_k,m)$, which yields the result. □

Proposition 4. *Let k, m be positive integers with even k. Then*

$$\frac{(S_k(m),m^3)}{m}=\frac{(N_k,m^2)}{(D_k,m)}.$$

Proof. The cases $k = 2, 4, 6, 8$ are compatible with Proposition 3, since $|N_k| = 1$. Now let $k \geqslant 10$, $m \geqslant 2$, and assume that $m \mid N_k$. Using Theorem 3 we have for this case that

$$S_k(m) \equiv \frac{N_k}{D_k} m \pmod{m^3}. \tag{14}$$

This shows that $(S_k(m), m^3) = m(N_k, m^2)$. Now let m be arbitrary. With Proposition 3 we obtain the relation

$$\bigl(S_k(m), m^3\bigr) = d_{k,m}\bigl(S_k(m), m^2\bigr) = d_{k,m} m \frac{(N_k, m)}{(D_k, m)}$$

with some integer $d_{k,m} \geqslant 1$. Consider a prime p where $p^r \,\|\, m$: If $p \nmid N_k$, then

$$\operatorname{ord}_p\bigl(S_k(m), m^\nu\bigr) \leqslant r, \quad \nu \geqslant 1,$$

using Propositions 2 and 3 and Lemma 1. Thus p gives no contribution to $d_{k,m}$. If $p \mid N_k$, then (13) and (14) remain valid (mod p^{2r}) and (mod p^{3r}) by Theorem 3, respectively. So a power of p gives a contribution to $d_{k,m}$. Counting the prime powers, which fulfill both (13) and (14), we then finally deduce that $d_{k,m} = (N_k, m^2)/(N_k, m)$. □

Corollary 1. *Let k, m be positive integers with even k. Then*

$$\bigl(S_k(m), m^k\bigr) = e_{k,m}\bigl(S_k(m), m^3\bigr),$$

where $e_{k,m}$ is a positive integer with the property that $p \mid e_{k,m}$ implies that $p \mid N_k$.

Proof. As in the proof of Proposition 4, we can use the same arguments. A prime p with $p \nmid N_k$ cannot give a contribution to $e_{k,m}$ anymore. □

Proof of Theorem 1. The minimum of g_k is shown by Proposition 2. As a consequence of Proposition 4 and Corollary 1, it follows for arbitrary m that $g_k(m) = 1$ if and only if $(D_k N_k, m) = 1$. Combining Propositions 2–4 we have achieved that

$$\bigl(S_k(m), m^\nu\bigr) = m \frac{(N_k, m^{\nu-1})}{(D_k, m)}, \quad \nu = 1, 2, 3. \tag{15}$$

The values of $g_k(m)$ for $m = D_k, |N_k|, D_k|N_k|$ follow easily by (15) using Lemma 1, since $(S_k(m), m^\nu)$ is constant for $\nu \geqslant 2$ in these cases. If $(D_k, m) = 1$ and $|N_k| \mid m$, then $g_k(m) = |N_k|$ by the same arguments, which implies that

$$\max_{m \geqslant 1} g_k(m) \geqslant |N_k|. \tag{16}$$

It remains the case where N_k is square-free. By (15) and Lemma 1 we conclude that $(S_k(m), m^\nu)$ is constant for $\nu \geqslant 2$ for arbitrary m. Thus $g_k(m) = (N_k, m)/(D_k, m)$ in this case. Consequently (16) holds with equality. □

Acknowledgments

The author wishes to thank both the Max Planck Institute for Mathematics at Bonn for an invitation for a talk in February 2010 and especially Pieter Moree for the organization and discussions on the Erdős–Moser equation.

References

[1] S. Chowla, P. Hartung, An “exact” formula for the m-th Bernoulli number, Acta Arith. 22 (1972) 113–115.
[2] Y. Gallot, P. Moree, W. Zudilin, The Erdős–Moser equation $1^k + 2^k + \cdots + (m-1)^k = m^k$ revisited using continued fractions, Math. Comp. 80 (2011) 1221–1237.
[3] R.L. Graham, D.E. Knuth, O. Patashnik, Concrete Mathematics, Addison–Wesley, Reading, MA, USA, 1994.
[4] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd edition, Grad. Texts in Math., vol. 84, Springer-Verlag, 1990.
[5] B.C. Kellner, On irregular prime power divisors of the Bernoulli numbers, Math. Comp. 76 (2007) 405–441.
[6] P. Moree, H.J.J. te Riele, J. Urbanowicz, Divisibility properties of integers x and k satisfying $1^k + 2^k + \cdots + (x-1)^k = x^k$, CWI Reports and Notes, Numerical Mathematics, 1992.
[7] L. Moser, On the Diophantine equation $1^n + 2^n + 3^n + \cdots + (m-1)^n = m^n$, Scripta Math. 19 (1953) 84–88.
[8] N.J.A. Sloane, Online Encyclopedia of Integer Sequences (OEIS), electronically published at: http://www.research.att.com/~njas/sequences.