ON STRONGER CONJECTURES THAT IMPLY THE ERDŐS-MOSER CONJECTURE

BERND C. KELLNER

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 $k \geq 2$. 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.

In 1953 Moser [6] showed that if a solution of (1) exists for $k \geq 2$, 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 [4, 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 $k \geq 4$; this result concerning (1) was also shown in [5] 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.

2000 *Mathematics Subject Classification.* Primary 11B83; Secondary 11A05, 11B68.

Key words and phrases. Erdős-Moser equation, consecutive values of polynomials.

2. Preliminaries

We use the following notation. We write $p^r \mid\mid m$ 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 are given in [4, p. 437]. The denominator of B_n for even n is described by the von Staudt-Clausen theorem, see [3, 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. [3, 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 strongly monotonically 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 $m \geq 3$. Then*

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

Note that we have to require $m \geq 3$, since $S_k(1) = 0$ and $S_k(2) = 1$ for all $k \geq 1$. 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

$$\frac{1+2+3}{1+2} = 2 \quad \text{and} \quad \frac{1^3+2^3+3^3}{1^3+2^3} = 4 \tag{6}$$

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.

Proposition 1. *Conjecture 2 implies Conjecture 1 as a special case.*

Proof. The equation $S_k(m) = m^k$ 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 (6). This implies Conjecture 1, which predicts $S_k(m+1)/S_k(m) \neq 2$ for $k \geq 2$. $\square$

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.

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

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

Then

$$\min_{m \geq 2} g_k(m) = \frac{1}{D_k} \quad \text{and} \quad \max_{m \geq 2} g_k(m) \geq |N_k|.$$

Generally

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

and special values are given by

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

Moreover, if N_k is square free, then

$$\max_{m \geq 2} g_k(m) = |N_k|.$$

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 [7]: $10, 12, 14, 16, 18, 36, 42$. Sequence A090997 in [7] gives the indices k, where N_k is not square free: 50, 98, 150, 196, 228, $\ldots$. By this, all N_k are square free for $2 \leq k \leq 48$.

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

$$\gcd(S_k(m), S_k(m+1)) = \gcd(S_k(m), m^k), \tag{7}$$

giving a connection with (1). The function g_k heavily depends on the Bernoulli number B_k. One may speculate that this happens in a suitable form for all even k, which results in the following conjecture being true for $2 \leq k \leq 48$ and some higher indices k.

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

$$\min_{m \geq 2} g_k(m) \cdot \max_{m \geq 2} g_k(m) = |B_k|.$$

Proposition 2. *Conjecture 3 implies Conjecture 1.*

Proof. Let k, m be positive integers with even k. In view of Theorem 1, Conjecture 3 states in fact that

$$\max_{m \geq 2} g_k(m) = |N_k|. \tag{8}$$

According to Remark 1, we have for $k = 2, 4, 6, 8$ that $\max_{m \geq 2} g_k(m) = 1$. For those m, where $g_k(m) = 1$, we obtain by (7) that

$$\gcd(S_k(m), m^k) = m.$$

This implies that $m^2 \nmid S_k(m)$ and consequently that there is no solution of (1) for these cases. For now on we can assume that $k \geq 10$. Combining (7) and (8), there exist some m such that

$$\gcd(S_k(m), m^k) = m\, c_m$$

with integers c_m depending on m where $1 \leq c_m \leq |N_k|$. A possible solution of (1) must trivially satisfy

$$m^k = \gcd(S_k(m), m^k).$$

We then obtain the equation

$$m^k = m\, c_m.$$

Our goal is to show an estimate on an upper bound of m. Therefore we can assume that $c_m = |N_k|$ is maximal. Thus

$$m \leq \sqrt[k-1]{|N_k|}. \tag{9}$$

Using the relation of B_k to the Riemann zeta function by Euler's formula, cf. [3, 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

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

Due to the fact that $D_k \mid 2(2^k - 1)$, see [1], we have $D_k < 2^{k+1}$. Furthermore, it is easy to see that $k! < k^{k-1}$ for $k \geq 4$. Putting all together, we derive that

$$|N_k| < \frac{2\pi}{3}\left(\frac{k}{\pi}\right)^{k-1}.$$

Using (9) we finally deduce that

$$m \leq \sqrt[k-1]{|N_k|} < \frac{2}{\pi}k.$$

Hence $m < k$, which contradicts (2) requiring $k < m$. Consequently, there is no solution of (1) for $k \geq 10$. □

To prove Theorem 1, we shall need some preparations. Recall Eq. (3). Since we need a refinement of this result, we give a revised reprint of the proof here. The following proposition plays a crucial role, which gives a statement about the common prime factors of numerators and denominators of Bernoulli numbers having indices close to each other.

Proposition 3 ([4, Prop. 8.4, p. 435]). *Let $\mathcal{S} = \{2, 4, 6, 8, 10, 14\}$. Let k, s be even positive integers with $s \in \mathcal{S}$ and $k - s \geq 2$. Then*

$$C = \gcd(N_k, D_{k-s}) \quad \textit{implies} \quad C \mid k.$$

Moreover, if $C > 1$ then $C = p_1 \cdots p_r$ with some $r \geq 1$. The primes $p_1, \ldots, p_r$ are pairwise different and $p_\nu \nmid D_s$, $p_\nu \nmid B_k/k$ for $\nu = 1, \ldots, r$.

Proposition 4 ([4, Prop. 8.5, pp. 436–437]). *Let m, k be positive integers with even k. For $r = 1, 2$ we have*

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

Proof. We can assume that $m > 1$, since $m = 1$ is trivial. The case $k = 2$ follows by $B_2 = \frac{1}{6}$ and that

$$m^2 \nmid \frac{1}{6} m(m-1)(2m-1) = S_2(m) \tag{10}$$

for $m > 1$. For now we assume that $k \geq 4$. From (5) we have

$$S_k(m) = B_k\, m + \binom{k}{2} B_{k-2} \frac{m^3}{3} + \sum_{\nu=3}^{k} \binom{k}{\nu} B_{k-\nu} \frac{m^{\nu+1}}{\nu+1}. \tag{11}$$

By von Staudt-Clausen (4) and the cases $B_0 = 1$ and $B_1 = -\frac{1}{2}$ the denominator of all nonzero Bernoulli numbers is squarefree. For each prime power factor $p^s \mid\mid m$ and ν where $B_{k-\nu} \neq 0$ $(2 \leq \nu \leq k)$ we have the estimate

$$\operatorname{ord}_p \left(\binom{k}{\nu} B_{k-\nu} \frac{m^{\nu+1}}{\nu+1} \right) \geq s(\nu+1) - 1 - \operatorname{ord}_p(\nu+1) \geq \lambda\, s \tag{12}$$

with the following cases:

(1) $\lambda = 1$ for $\nu \geq 2$, $p \geq 2$;
(2) $\lambda = 2$ for $\nu \geq 2$, $p \geq 5$;
(3) $\lambda = 3$ for $\nu \geq 4$, $p \geq 5$.

The critical cases to consider are $p = 2, 3, 5$ and $s = 1$, which follow by a simple counting argument. Now, we are ready to evaluate (11) $\pmod{m^r}$ for $r = 1, 2$.

Case $r = 1$: By (12) (case $\nu \geq 2$, $p \geq 2$) we obtain

$$S_k(m) \equiv B_k\, m \pmod{m}. \tag{13}$$

Assume that $\gcd(m, D_k) > 1$. Then

$$S_k(m) \equiv B_k\, m \equiv \frac{N_k}{D_k} m \not\equiv 0 \pmod{m}.$$

Therefore, $\gcd(m, D_k) = 1$ must hold, which implies that $2 \nmid m$, $3 \nmid m$, and $p \geq 5$. Hence, by (12) (case $\nu \geq 2$, $p \geq 5$), we can write

$$S_k(m) \equiv B_k\, m \pmod{m^2}. \tag{14}$$

This yields

$$m^2 \mid S_k(m) \iff m \mid B_k. \tag{15}$$

Case $r = 2$: We have $m \mid B_k$ and $(m, 6) = 1$, because either $m^2 \mid B_k$ or $m^3 \mid S_k(m)$ is assumed. The latter case implies $m^2 \mid S_k(m)$ and therefore $m \mid B_k$ by (15). Since $|N_4| = 1$, we can assume that $k \geq 6$. We then have $B_{k-3} = 0$ and we can apply (12) (case $\nu \geq 4$, $p \geq 5$) to obtain

$$S_k(m) \equiv B_k\, m + \frac{k(k-1) N_{k-2}}{6 D_{k-2}} m^3 \pmod{m^3}. \tag{16}$$

Our goal is to show that the second term of the right side of (16) vanishes, but the denominator D_{k-2} could possibly remove prime factors from m. Proposition 3 asserts that $\gcd(N_k, D_{k-2}) \mid k$. We also have $\gcd(m, D_{k-2}) \mid k$ since $m \mid B_k$. This means that the factor k contains those primes which D_{k-2} possibly removes from m. Therefore the second term of (16) vanishes $\pmod{m^3}$. The rest follows by $S_k(m) \equiv B_k\, m \equiv 0 \pmod{m^3}$. □

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

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

More precisely for $p^r \mid\mid m$:

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

Proof. This follows by exploiting the proof of Proposition 4 and considering (13) (also valid for $k = 2$ by (10)), (14), and (16) for the several cases. □

Proposition 5. *Let k, m be positive integers with even k. Then*

$$\gcd(S_k(m), m) = \frac{m}{\gcd(D_k, m)}.$$

Proof. From Corollary 1 we have

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

For each prime power $p^{e_p} \mid\mid m$, we then infer that $p^{e_p} \mid S_k(m)$, if $p \nmid D_k$; otherwise $p^{e_p - 1} \mid S_k(m)$, since D_k is square free due to (4). □

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

$$\min_{m \geq 2} g_k(m) = \frac{1}{D_k}.$$

Proof. Using Proposition 5 and (7), we deduce the relation

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

If $m = D_k$, then we even have

$$\gcd(S_k(m), m^k) = \gcd(S_k(m), m) = 1,$$

giving the minimum with $g_k(m) = 1/D_k$. □

Proposition 6. *Let k, m be positive integers with even k. Then*

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

Proof. The case $k = 2$ follows by (10), $B_2 = \frac{1}{6}$, and $\gcd((m-1)(2m-1), m) = 1$. Now let $k \geq 4$ and assume that $\gcd(D_k, m) = 1$. Applying Corollary 1 for this case we then have

$$S_k(m) \equiv \frac{N_k}{D_k} m \pmod{m^2}. \tag{17}$$

Thus we deduce that

$$\gcd(S_k(m), m^2) = m \gcd(N_k, m).$$

Now let m be arbitrary. Using Proposition 5 we have the relation

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

with some integer $c_{k,m} \geq 1$. Since $\gcd(N_k, D_k) = 1$, those factors of $\gcd(N_k, m)$ can only give a contribution to the factor $c_{k,m}$; while other factors of m are reduced by $\gcd(D_k, m)$. To be more precise, we consider two cases of primes p where $p^r \mid\mid m$:

First, $p \mid D_k$. Assume to the contrary that

$$\operatorname{ord}_p \gcd(S_k(m), m^2) > \operatorname{ord}_p \gcd(S_k(m), m) = r - 1,$$

where the right side follows by Proposition 5. Thus $\operatorname{ord}_p \gcd(S_k(m), m^2) \geq r$. But this implies that we also have $\operatorname{ord}_p \gcd(S_k(m), m) = r$. Contradiction.

Second, $p \nmid D_k$. By Corollary 1 Eq. (17) remains valid (mod p^{2r}). Hence $c_{k,m} = \gcd(N_k, m)$, which yields the result. ☐

Corollary 3. *Let m be a positive integer. For $k = 2, 4, 6, 8$ we have*

$$\max_{m \geq 2} g_k(m) = 1.$$

Proof. For these k we know that $|N_k| = 1$. By Proposition 6 we then deduce that

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

This implies for $\gcd(D_k, m) = 1$ that

$$m = \gcd(S_k(m), m^2) = \gcd(S_k(m), m^k).$$

By (7) this shows the result. ☐

Proposition 7. *Let k, m be positive integers with even k. Then*

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

Proof. For the cases $k = 2, 4, 6, 8$ this is compatible with Corollary 3, since $|N_k| = 1$. Now let $k \geq 10$ and assume that $m \mid N_k$. Using Corollary 1 we have for this case that

$$S_k(m) \equiv \frac{N_k}{D_k} m \pmod{m^3}. \tag{18}$$

This shows that

$$\gcd(S_k(m), m^3) = m \gcd(N_k, m^2).$$

Now let m be arbitrary. Using Proposition 6 we have the relation

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

with some integer $d_{k,m} \geq 1$. Again, we distinguish between two cases of primes p where $p^r \mid\mid m$. First case $p \nmid N_k$: We have

$$\operatorname{ord}_p \gcd(S_k(m), m^2) \leq r,$$

which also implies that

$$\operatorname{ord}_p \gcd(S_k(m), m^3) \leq r.$$

Otherwise we would get a contradiction. Thus this prime p gives no contribution to $d_{k,m}$. Second case $p \mid N_k$: For this prime p (17) and (18) remain valid $\pmod{p^{2r}}$ and $\pmod{p^{3r}}$, respectively, using Corollary 1. So a power of p gives a contribution to $d_{k,m}$. Counting the prime powers, which fulfill both (17) and (18), we then deduce that

$$d_{k,m} = \frac{\gcd(N_k, m^2)}{\gcd(N_k, m)}. \qquad \square$$

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

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

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 7, we can use the same arguments. A prime p with $p \nmid N_k$ cannot give a contribution to $e_{k,m}$ anymore. $\square$

Proof of Theorem 1. Let k, m be positive integers with even k. The first part, the minimum of g_k and that $g_k(D_k) = 1/D_k$, is already shown by Corollary 2. The cases $k = 2, 4, 6, 8$ are handled by Corollary 3. Now we show for $k \geq 10$ that

$$\max_{m \geq 2} g_k(m) \geq |N_k|. \tag{19}$$

We set $m = |N_k|$ and can apply Corollary 1 to obtain

$$S_k(m) \equiv B_k\, m \equiv \frac{\pm 1}{D_k} m^2 \pmod{m^3}.$$

Thus we derive that

$$m^2 = \gcd(S_k(m), m^3) = \gcd(S_k(m), m^k).$$

This finally shows with (7) that

$$g_k(m) = |N_k|,$$

also giving the estimate in (19). As a consequence of Proposition 7 and Corollary 4, it follows for arbitrary m that $g_k(m) = 1$ if and only if $\gcd(D_k N_k, m) = 1$.

It remains the case where N_k is squarefree. Then we have $\gcd(N_k, m^2) = \gcd(N_k, m)$ for arbitrary m. Combining Propositions 6 and 7, we deduce that

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

Hence

$$\max_{m \geq 2} g_k(m) = |N_k|. \qquad \square$$

Proposition 3 has played a key role to obtain a formula for $\gcd(S_k(m), m^3)/m$. The next milestone would be to show a formula for

$$\frac{\gcd(S_k(m), m^4)}{m},$$

which seems to need some new ideas.

Acknowledgement

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 and P. Hartung, *An "exact" formula for the m-th Bernoulli number*, Acta Arith. **22** (1972), 113-115.
2. Y. Gallot, P. Moree, and W. Zudilin, *The Erdős-Moser equation* $1^k + 2^k + \cdots + (m-1)^k = m^k$ *revisited using continued fractions*, to appear in Math. Comp., arXiv:0907.1356, 2009.
3. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, GTM **84**, Springer–Verlag, 2nd edition, 1990.
4. B. C. Kellner, *On irregular prime power divisors of the Bernoulli numbers*, Math. Comp. **76** (2007), 405-441.
5. P. Moree, H. J. J. te Riele, and 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.
6. L. Moser, *On the Diophantine equation* $1^n + 2^n + 3^n + \cdots + (m-1)^n = m^n$, Scripta Math. **19** (1953), 84–88.
7. N. J. A. Sloane, *Online Encyclopedia of Integer Sequences (OEIS)*, electronically published at: `http://www.research.att.com/~njas/sequences`.

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

E-mail address: `bk@bernoulli.org`