REDUCING THE ERDŐS-MOSER EQUATION $1^n + 2^n + \cdots + k^n = (k+1)^n$ MODULO k AND k^2

Jonathan Sondow
209 West 97th Street, New York, New York
jsondow@alumni.princeton.edu

Kieren MacMillan
55 Lessard Avenue, Toronto, Ontario, Canada
kieren@alumni.rice.edu

Received: 2/13/11, Accepted: 4/4/11, Published: 5/27/11

Abstract

An open conjecture of Erdős and Moser is that the only solution of the Diophantine equation in the title is the trivial solution $1+2=3$. Reducing the equation modulo k and k^2, we give necessary and sufficient conditions on solutions to the resulting congruence and supercongruence. A corollary is a new proof of Moser's result that the conjecture is true for odd exponents n. The proofs use divisibility properties of power sums as well as Lerch's relation between Fermat and Wilson quotients. Examples are provided using primary pseudoperfect numbers.

1. Introduction

Around 1953, Erdős and Moser made the following conjecture.

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

$$1^n + 2^n + \cdots + k^n = (k+1)^n \tag{1}$$

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

Using prime number theory, Moser [10] proved the statement for odd exponents n. By considering (1) modulo k, $k+2$, $2k+1$, and $2k+3$, and combining the information so obtained, Moser also showed that if a solution with even n exists, then both n and k must exceed 10^{10^6}. This bound was later improved by several authors—the current record is 10^{10^9}, obtained by Gallot, Moree, and Zudilin [3] using continued fractions. On the other hand, it has not even been proved that the *Erdős-Moser equation* (1) has only finitely many solutions. For surveys of work on this and related problems, see Butske, Jaje, and Mayernik [1], Guy [4, D7], and Moree [8, 9].

The next section gives necessary and sufficient conditions on solutions of the congruence

$$1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k} \tag{2}$$

in Theorem 3, which was proved implicitly by Moser in [10]. An application is a new proof of his result that Conjecture 1 is true for odd exponents n. We also connect Theorem 3 with primary pseudoperfect numbers.

In Section 3, we extend the theorem by giving necessary and sufficient conditions on solutions to the supercongruence modulo a square

$$1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k^2} \tag{3}$$

in Theorem 10. Here the conditions involve the Wilson quotient, and the proof uses Lerch's formula relating Fermat and Wilson quotients.

In the final section, we consider two supercongruences modulo a cube, and make a conjecture about one of them.

2. Congruences

We will use a well-known congruence for power sums.

Lemma 2. *If n is a positive integer and p is a prime, then*

$$1^n + 2^n + \cdots + p^n \equiv \begin{cases} -1 \pmod{p}, & (p-1) \mid n, \\ 0 \pmod{p}, & (p-1) \nmid n. \end{cases}$$

Proof. See Hardy and Wright [5, Theorem 119] for the standard proof using primitive roots, or MacMillan and Sondow [7] for a recent elementary proof. □

We now give necessary and sufficient conditions on solutions to (2).

Theorem 3. *Given positive integers n and k, the congruence*

$$1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k} \tag{4}$$

holds if and only if prime $p \mid k$ implies

(i) $n \equiv 0 \pmod{(p-1)}$, *and*

(ii) $\dfrac{k}{p} + 1 \equiv 0 \pmod{p}$.

In that case, k is square-free, and if n is odd, then $k = 1$ or 2.

Proof. Note first that if n, k and p are *any* positive integers with $p \mid k$, then

$$S_n(k) := 1^n + 2^n + \cdots + k^n = \sum_{h=1}^{k/p} \sum_{j=1}^{p} ((h-1)p + j)^n \equiv \frac{k}{p}\, S_n(p) \pmod{p}. \quad (5)$$

Now assume (i) and (ii) hold when prime $p \mid k$. Then, using Lemma 2, both $S_n(p)$ and k/p are congruent to -1 modulo p, and (5) gives $S_n(k) \equiv 1 \pmod{p}$. Thus, as (ii) implies k is square-free, k is a product of distinct primes each of which divides $S_n(k) - 1$. It follows that $S_n(k) \equiv 1 \pmod{k}$, implying (4).

Conversely, assume that (4) holds, so that $S_n(k) \equiv 1 \pmod{k}$. If prime $p \mid k$, then (5) gives $(k/p)\, S_n(p) \equiv 1 \pmod{p}$, and so $S_n(p) \not\equiv 0 \pmod{p}$. Now Lemma 2 yields both $(p-1) \mid n$, proving (i), and $S_n(p) \equiv -1 \pmod{p}$, implying (ii).

If n is odd, then by (i) no odd prime divides k. As k is square-free, $k = 1$ or 2. □

Here is an easy consequence, due to Moser.

Corollary 4. *The only solution of the Erdős-Moser equation with odd exponent n is $1 + 2 = 3$.*

Proof. Given a solution with n odd, Theorem 3 implies $k = 1$ or 2. But $k = 1$ is clearly impossible, and $k = 2$ evidently forces $n = 1$. □

Solutions to (4) are related to the notion of a *primary pseudoperfect number*, defined by Butske, Jaje, and Mayernik [1] as an integer $K > 1$ that satisfies the Egyptian fraction equation

$$\frac{1}{K} + \sum_{p \mid K} \frac{1}{p} = 1,$$

where the summation is over all primes p dividing K. In particular, K is square-free. By computation, they found all such numbers K with eight or fewer prime factors (see [1, Table 1]). The first few are $K = 2, 6, 42, 1806, 47058, \ldots$.

Here is the connection between such numbers and solutions of the congruence (4). (Recall that for real numbers, $x \equiv y \pmod{1}$ means that $x - y$ is an integer.)

Corollary 5. *The positive integers n and k satisfy the congruence (4) if and only if n is divisible by the least common multiple $\mathrm{LCM}\{p-1 : \text{prime } p \mid k\}$ and k satisfies the Egyptian fraction congruence*

$$\frac{1}{k} + \sum_{p \mid k} \frac{1}{p} \equiv 1 \pmod{1}. \quad (6)$$

In particular, every primary pseudoperfect number K gives a solution $k = K$ to (4), for some exponent n.

Proof. Condition (6) is equivalent to the congruence

$$1 + \sum_{p|k} \frac{k}{p} \equiv 0 \pmod{k}, \tag{7}$$

which in turn is equivalent to condition (ii) in Theorem 3, since each implies k is square-free. The theorem now implies the corollary. □

Example 6. Since $47058 = 2 \cdot 3 \cdot 11 \cdot 23 \cdot 31$ and

$$\frac{1}{47058} + \frac{1}{2} + \frac{1}{3} + \frac{1}{11} + \frac{1}{23} + \frac{1}{31} = 1,$$

we see by computing $\mathrm{LCM}(1, 2, 10, 22, 30) = 330$ that one solution of (4) is

$$1^{330} + 2^{330} + \cdots + 47058^{330} \equiv 47059^{330} \pmod{47058}.$$

Examples 11 and 14 give a fortiori two other cases of the congruence (4) with $k = K$ a primary pseudoperfect number. We explore this relation more thoroughly in a paper in preparation.

3. Two Supercongruences Modulo a Square

If the conditions in Theorem 3 are satisfied, the following corollary shows that the congruence (5) can be replaced with a "supercongruence."

Corollary 7. *If* $1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k}$ *and prime* $p \mid k$*, then*

$$1^n + 2^n + \cdots + k^n \equiv \frac{k}{p}\left(1^n + 2^n + \cdots + p^n\right) \pmod{p^2}. \tag{8}$$

Proof. By Theorem 3, it suffices to prove the more general statement that, if prime $p \mid k$ and $(p-1) \mid n$, and if either $k = 2$ or n is even, then (8) holds. Set $a = k/p$ in the equation (5). Expanding and summing, we see that

$$S_n(k) \equiv aS_n(p) + \frac{1}{2}\,a(a-1)npS_{n-1}(p) \pmod{p^2}.$$

If $p > 2$, then $(p-1) \mid n$ implies $(p-1) \nmid (n-1)$, and Lemma 2 gives $p \mid S_{n-1}(p)$. In case $p = 2$, either $a = k/2 = 1$ or $2 \mid n$, and each implies $2 \mid (1/2)a(a-1)n$. In all cases, (8) follows. □

For an extension of Theorem 3 itself to a supercongruence, we need a definition and a lemma.

Definition 8. By Fermat's and Wilson's theorems, for any prime p the *Fermat quotient*

$$q_p(j) := \frac{j^{p-1}-1}{p} \qquad (p \nmid j), \tag{9}$$

and the *Wilson quotient*

$$w_p := \frac{(p-1)!+1}{p}$$

are integers.

Lemma 9. (Lerch [6]) *If p is an odd prime, then the Fermat and Wilson quotients are related by* Lerch's formula

$$\sum_{j=1}^{p-1} q_p(j) \equiv w_p \pmod{p}.$$

Proof. Given a and b with $p \nmid ab$, set $j = ab$ in (9). Substituting $a^{p-1} = pq_p(a)+1$ and $b^{p-1} = pq_p(b)+1$, we deduce Eisenstein's relation [2]

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p},$$

which implies

$$q_p((p-1)!) \equiv \sum_{j=1}^{p-1} q_p(j) \pmod{p}.$$

On the other hand, setting $j = (p-1)! = pw_p - 1$ in (9) and expanding leads, as $p-1$ is even, to $q_p((p-1)!) \equiv w_p \pmod{p}$. This proves the lemma. □

We now give necessary and sufficient conditions on solutions to (3).

Theorem 10. *For $n = 1$, the supercongruence*

$$1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k^2} \tag{10}$$

holds if and only if $k = 1$ or 2. For $n \geq 3$ odd, (10) *holds if and only if $k = 1$. Finally, for $n \geq 2$ even,* (10) *holds if and only if prime $p \mid k$ implies*

(i) $n \equiv 0 \pmod{(p-1)}$, *and*

(ii) $\dfrac{k}{p} + 1 \equiv p\,(n(w_p+1)-1) \pmod{p^2}$.

Proof. To prove the first two statements, use Theorem 3 together with the fact that the congruences $1^n + 2^n \equiv 1 \pmod 4$ and $3^n \equiv (-1)^n \equiv -1 \pmod 4$ all hold when $n \geq 3$ is odd.

Now assume $n \geq 2$ is even. Let p denote a prime. By Theorem 3, we may assume that (i) holds if $p \mid k$, and that k is square-free. It follows that the supercongruence (10) is equivalent to the system

$$S_n(k) \equiv (k+1)^n \pmod{p^2}, \qquad p \mid k.$$

Corollary 7 and expansion of $(k+1)^n$ allow us to write the system as

$$\frac{k}{p} S_n(p) \equiv 1 + nk \pmod{p^2}, \qquad p \mid k.$$

Since n is at least 2 and $(p-1) \mid n$, we have

$$\begin{aligned} S_n(p) &\equiv S_n(p-1) \pmod{p^2} \\ &= \sum_{j=1}^{p-1} (j^{p-1})^{n/(p-1)}. \end{aligned}$$

Substituting $j^{p-1} = 1 + pq_p(j)$ and expanding, the result is

$$S_n(p) \equiv \sum_{j=1}^{p-1} \left(1 + \frac{n}{p-1} pq_p(j)\right) \equiv p - 1 - np \sum_{j=1}^{p-1} q_p(j) \pmod{p^2}, \tag{11}$$

since $n/(p-1) \equiv -n \pmod p$. Now Lerch's formula (if p is odd), together with the equality $q_2(1) = 0$ and the evenness of n (if $p = 2$), yield

$$S_n(p) \equiv p - 1 - npw_p \pmod{p^2}.$$

Summarizing, the supercongruence (10) is equivalent to the system

$$\frac{k}{p}(p - 1 - npw_p) \equiv 1 + nk \pmod{p^2}, \qquad p \mid k.$$

It in turn can be written as

$$\frac{k}{p} + 1 \equiv -k\big(n(w_p + 1) - 1\big) \pmod{p^2}, \qquad p \mid k. \tag{12}$$

On the right-hand side, we substitute $k \equiv -p \pmod{p^2}$ (deduced from (12) multiplied by p), and arrive at (ii). This completes the proof. □

Example 11. Given any solution of (10) with $n > 1$ and k a primary pseudoperfect number having eight or fewer prime factors, one can show that $k = 2$ or 42 (see Corollary 5 in [11], an early version of the present paper). Example 14 illustrates the case $k = 2$. For $k = 42$, the simplest example is

$$1^{12} + 2^{12} + \cdots + 42^{12} \equiv 43^{12} \pmod{42^2}.$$

4. Two Supercongruences Modulo a Cube

In light of the extension of Theorem 3 to Theorem 10, it is natural to ask whether Corollary 7 extends as well. Numerical experiments suggest that it does.

Conjecture 12. *If* $1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k^2}$ *and prime* $p \mid k$, *then*

$$1^n + 2^n + \cdots + k^n \equiv \frac{k}{p}\left(1^n + 2^n + \cdots + p^n\right) \pmod{p^3}.$$

Example 13. For $p = 2, 3$, and 7, one can compute that

$$1^{12} + 2^{12} + \cdots + 42^{12} \equiv \frac{42}{p}\left(1^{12} + 2^{12} + \cdots + p^{12}\right) \pmod{p^3}.$$

In fact, for $p = 2, 3$, and 7 it appears that $S_n(42) \equiv (42/p)\, S_n(p) \pmod{p^3}$ holds true not only when $n \equiv 12 \pmod{42}$, but indeed for all $n \equiv 0 \pmod 6$. One reason may be that, for $p = 7$ (but not for $p = 2$ or 3), apparently $6 \mid n$ implies $p^2 \mid S_{n-1}(p)$. (Compare $p \mid S_{n-1}(p)$ in the proof of Corollary 7.)

Just as Corollary 7 helped in the proof of Theorem 10, a proof of Conjecture 12 might help in extending Theorem 10 to necessary and sufficient conditions on solutions to the supercongruence

$$1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k^3}.$$

Example 14. Given any solution with $n > 1$ and k a primary pseudoperfect number having eight or fewer prime factors, one can show that $k = 2$. The smallest case is

$$1^4 + 2^4 \equiv 3^4 \pmod{2^3}.$$

More generally, for any positive integers n and d we have

$$1^n + 2^n \equiv 3^n \pmod{2^d}, \quad \text{if } 2^{d-1} \mid n.$$

Acknowledgments We are very grateful to Wadim Zudilin for contributing the results in Section 3, and to the anonymous referee whose suggestions led to improvements in the exposition. The first author thanks both the Max Planck Institute for Mathematics for its hospitality during his visit in October 2008 when part of this work was done, and Pieter Moree for reprints and discussions of his articles on the Erdős-Moser equation. The second author thanks Angus MacMillan and Dr. Stanley K. Johannesen for supplying copies of hard-to-locate papers, and Drs. Jurij and Daria Darewych for underwriting part of the research.

References

[1] W. Butske, L. M. Jaje, and D. R. Mayernik, On the equation $\sum_{p|N} \frac{1}{p} + \frac{1}{N} = 1$, pseudoperfect numbers, and perfectly weighted graphs, *Math. Comp.* **69** (2000), 407–420; also available at `http://www.ams.org/journals/mcom/2000-69-229/S0025-5718-99-01088-1/`.

[2] F. G. Eisenstein, Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhaengen und durch gewisse lineare Funktional-Gleichungen definiert werden, *Verhandlungen der Koenigl. Preuss. Akademie der Wiss. zu Berlin* (1850), 36–42; reprinted in *Mathematische Werke*, vol. 2, 705–711, Chelsea, New York, 1975.

[3] 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, *Math. Comp.* **80** (2011), 1221–1237; also available at `http://arxiv.org/abs/0907.1356`.

[4] R. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, D. R. Heath-Brown and J. H. Silverman, eds., 6th ed., Oxford University Press, Oxford, 2008.

[6] M. Lerch, Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$, *Math. Ann.* **60** (1905), 471–490.

[7] K. MacMillan and J. Sondow, Proofs of power sum and binomial coefficient congruences via Pascal's identity, *Amer. Math. Monthly* **118** (2011), 549–551; also available at `http://arxiv.org/abs/1011.0076`.

[8] P. Moree, A top hat for Moser's four mathemagical rabbits, *Amer. Math. Monthly* **118** (2011), 364–370; also available at `http://arxiv.org/abs/1011.2956`.

[9] P. Moree, Moser's mathemagical work on the equation $1^k + 2^k + ... + (m-1)^k = m^k$, *Rocky Mountain J. Math.* (to appear); available at `http://arxiv.org/abs/1011.2940`.

[10] L. Moser, On the Diophantine equation $1^n + 2^n + \cdots + (m-1)^n = m^n$, *Scripta Math.* **19** (1953), 84–88.

[11] J. Sondow and K. MacMillan, Reducing the Erdős-Moser equation $1^n+2^n+\ldots+k^n = (k+1)^n$ modulo k and k^2 (2010, preprint); available at `http://arxiv.org/abs/1011.2154v1`.