MOSER'S MATHEMAGICAL WORK ON THE EQUATION $1^k + 2^k + \ldots + (m-1)^k = m^k$

PIETER MOREE

Abstract. If the equation of the title has an integer solution with $k \geq 2$, then $m > 10^{10^6}$. Leo Moser showed this in 1953 by amazingly elementary methods. With the hindsight of more than 50 years his proof can be somewhat simplified. Also we give a further proof showing that Moser's result can be derived from a Von Staudt-Clausen type theorem. Finally we discuss more recent developments concerning this equation and derive a new result using the divisibility properties of numbers in the sequence $\{2^{2e+1}+1\}_{e=0}^{\infty}$.

1. Introduction

In this paper we are interested in non-trivial solutions, that is, solutions with $k \geq 2$, of the equation

$$1^k + 2^k + \ldots + (m-2)^k + (m-1)^k = m^k. \tag{1}$$

Conjecturally such solutions do not exist (this conjecture was formulated around 1950 by Paul Erdős in a letter to Leo Moser). For $k = 1$ one has clearly the solution $1 + 2 = 3$ (and no further ones). From now on we will assume that $k \geq 2$. Leo Moser [19] established the following theorem in 1953.

Theorem 1. (Leo Moser, 1953). *If (m, k) is a solution of (1), then $m > 10^{10^6}$.*

His result has since then been improved on. Butske et al. [4] have shown, by computing rather than estimating certain quantities in Moser's original proof, that $m > 1.485 \cdot 10^{9321155}$. By proceeding along these lines this bound cannot be improved on substantially. Butske et al. [4, p. 411] expressed the hope that new insights will eventually make it possible to reach the more natural benchmark 10^{10^7}.

The main purpose of this paper is to make Moser's remarkable proof of Theorem 1 better known. Indeed, with the hindsight of more than 50 years and given the recent computer possibilities an even cleaner version of Moser's proof can be given. This is what we do in Section 2. We obtain the following variant of Moser's result.

Theorem 2. *Suppose that (m, k) is a solution of (1), then*
1) $m > 1.485 \cdot 10^{9321155}$.
2) *k is even, $m \equiv 3 \pmod 8$, $m \equiv \pm 1 \pmod 3$;*
3) *$m - 1$, $(m + 1)/2$, $2m - 1$ and $2m + 1$ are all square-free.*
4) *If p divides at least one of the above four integers, then $p - 1 | k$.*

Date: October 16, 2009.
2000 *Mathematics Subject Classification.* 11D61, 11A07.

5) *The number* $(m^2-1)(4m^2-1)/12$ *is square-free and has at least* 4990906 *prime factors.*

In fact, Moser proved that k is even, $m \equiv 0 \pmod 8$ or $m \equiv 3 \pmod 8$, part 3 and 4 of this result and a weaker version of part 5

The reader only interested in the cleanest proof of Theorem 2 presently known, we refer to Moree [17].

In Section 3 we compare our alternative proof with Moser's proof.

In Section 4 we a give a more systematic proof of Moser's result, which uses a variant of the Von Staudt-Clausen theorem. The relevance of this result for the study of the Erdős-Moser equation was first pointed out in 1996 by Moree [13]. He used the result to show that the Moser approach can also be used to study the equation $1^k + 2^k + \ldots + (m-1)^k = am^k$ and $a \geq 1$ an integer. The main result of his paper will be improved on in Section 8.

In Section 6 we discuss some recent developments and in particular how very recently the benchmark 10^{10^7} was achieved by Gallot, Moree and Zudilin [8].

This paper is partly scholarly and partly of a research nature. A large part of the material in Section 2 is copied verbatim from Moser's paper. The proof given in Section 4 is implicit in Moree's [13] on setting $a = 1$ there. The proof given in Section 5 of the Carlitz-von Staudt theorem is easier than those in the literature and the deepest fact it uses is the existence of a primitive root modulo p. Section 7 is the most original part of the paper. In the final section a straightforward improvement of the main result on the generalized Erdős-Moser equation is given.

Leo Moser (1921-1970) was a mathematician of the problem solver type. For bibliographic information the reader is referred to the MacTutor History of Mathematics archive [20].

2. Moser's proof revisited

Let $S_r(n) = \sum_{j=0}^{n-1} j^r$. In what follows we assume that

$$S_k(m) = m^k, \ m > 1, \tag{2}$$

that is we are interested in non-trivial solutions of (1).

Lemma 1. *Let p be a prime. We have*

$$S_r(p) \equiv \epsilon_r(p) \pmod p,$$

where

$$\epsilon_r(p) = \begin{cases} -1 & if\ p-1|r; \\ 0 & otherwise. \end{cases}$$

Proof. Let g be a primitive root modulo p. In case $p-1 \nmid r$ we have

$$S_r(p) \equiv \sum_{j=0}^{p-2} (g^j)^r \equiv \frac{g^{r(p-1)}-1}{g^r-1} \pmod p,$$

and the numerator is divisible by p. In case $(p-1)|r$, we find by Fermat's Little Theorem that $S_r(p) = p - 1 \equiv -1 (\text{mod } p)$ as desired. □

Also a proof of this not using the existence of a primitive root can be given, see Moree [17].

Lemma 2. *In case p is odd and in case $p = 2$ and r is even, we have* $S_r(p^{\lambda+1}) \equiv pS_r(p^\lambda)(\text{mod } p^{\lambda+1})$.

Proof. Every $0 \le j < p^{\lambda+1}$ can be uniquely written as $j = \alpha p^\lambda + \beta$ with $0 \le \alpha < p$ and $0 \le \beta < p^\lambda$. Hence we obtain on invoking the binomial theorem

$$S_r(p^{\lambda+1}) = \sum_{\alpha=0}^{p-1} \sum_{\beta=0}^{p^\lambda-1} (\alpha p^\lambda + \beta)^r \equiv p \sum_{\beta=0}^{p^\lambda-1} \beta^r + rp^\lambda \sum_{\alpha=0}^{p-1} \alpha \sum_{\beta=0}^{p^\lambda-1} \beta^{r-1} (\text{mod } p^{2\lambda}).$$

Since the first sum equals $S_r(p^\lambda)$ and $2\sum_{\alpha=0}^{p-1} \alpha = p(p-1) \equiv 0(\text{mod } p)$, the result follows. □

Proof of Theorem 2. Suppose that $p|(m-1)$, then using Lemma 1 we infer that

$$S_k(m) = \sum_{i=0}^{(m-1)/p-1} \sum_{j=1}^{p} (j+ip)^k \equiv \frac{m-1}{p} \epsilon_k(p)(\text{mod } p).$$

On the other hand $m \equiv 1(\text{mod } p)$ so that by (2) we must have

$$\frac{m-1}{p} \cdot \epsilon_k(p) \equiv 1(\text{mod } p). \tag{3}$$

Hence $\epsilon_k(p) \not\equiv 0(\text{mod } p)$, so that from the definition of $\epsilon_k(p)$ it follows that $\epsilon_k(p) = -1$ and

$$p|(m-1) \text{ implies } (p-1)|k. \tag{4}$$

Thus (3) can be put in the form

$$\frac{m-1}{p} + 1 \equiv 0(\text{mod } p), \tag{5}$$

or

$$m - 1 \equiv -p(\text{mod } p^2). \tag{6}$$

We claim that $m-1$ must have an odd prime divisor p and that hence, by (4), k must be even. It is easy to see that $m-1 > 2$. If $m-1$ does not have an odd prime divisor, then $m-1 = 2^e$ for some $e \ge 2$. However, by (6) we see that $m-1$ is square-free. This contradiction shows that $m-1$ has indeed an odd prime factor p.

We now multiply together all congruences of the type (5), that is one for each prime p dividing $m-1$. Since $m-1$ is square-free, the resulting modulus is $m-1$. Furthermore, products containing two or more distinct prime factors of the form $(m-1)/p$ will be divisible by $m-1$. Thus we obtain

$$(m-1) \sum_{p|(m-1)} \frac{1}{p} + 1 \equiv 0(\text{mod } m-1), \tag{7}$$

or

$$\sum_{p|(m-1)} \frac{1}{p} + \frac{1}{m-1} \equiv 0(\text{mod } 1). \tag{8}$$

We proceed to develop three more congruences, similar to (8), which when combined with (8) lead to the proof of part 1. Equation (2) can be written in the form

$$S_k(m+2) = 2m^k + (m+1)^k. \tag{9}$$

Using Lemma 1 and the fact that k is even, we obtain as before

$$p|(m+1) \text{ implies } (p-1)|k. \tag{10}$$

and

$$\frac{m+1}{p} + 2 \equiv 0(\text{mod } p), \tag{11}$$

From (11) it follows that no odd prime appears with exponent greater than one in $m+1$. The prime 2 (according to H. Zassenhaus 'the oddest of primes'), requires special attention. If we inspect (1) with modulus 4, and use the fact that k is even, then we find that $m+1 \equiv 1$ or $4(\text{mod } 8)$. Now let us assume that we are in the first case and we let $2^f||m$ (that is $2^f|m$ and $2^{f+1} \nmid m$). Note that $f \geq 3$. Using Lemma 2 we find that $S_k(m+1) \equiv \frac{m}{2^f} S_k(2^f) \equiv 2^{f-1}(\text{mod } 2^f)$, contradicting $S_k(m+1) = 2m^k \equiv 0(\text{mod } 2^f)$. Thus $m+1$ contains 2 exactly to the second power and hence (11) can be put in the form

$$\frac{m+1}{2p} + 1 \equiv 0(\text{mod } p), \tag{12}$$

We multiply together all congruences of type (12). The modulus then becomes $(m+1)/2$. Further, any term involving two or more distinct factors $\frac{m+1}{2p}$ will be divisible by $\frac{m+1}{2}$ so that on simplification we obtain

$$\sum_{p|(m+1)} \frac{1}{p} + \frac{2}{m+1} \equiv 0(\text{mod } 1). \tag{13}$$

We proceed to find two similar equations to (13). Suppose that $p|(2m-1)$ and let $t = \frac{1}{2}(\frac{2m-1}{p} - 1)$. Clearly t is an integer and $m - 1 = tp + \frac{p-1}{2}$. We have $a^k = (-a)^k$ since k is even so that $2S_k(\frac{p+1}{2}) \equiv S_k(p)(\text{mod } p)$ and hence, by Lemma 1,

$$S_k(\frac{p+1}{2}) \equiv \frac{\epsilon_k(p)}{2}(\text{mod } p).$$

It follows that

$$S_k(m) \equiv \sum_{i=0}^{t-1} \sum_{j=1}^{p-1} (j+ip)^k + \sum_{i=1}^{(p-1)/2} i^k \equiv (t + \frac{1}{2})\epsilon_k(p)(\text{mod } p). \tag{14}$$

On the other hand $1 \equiv (2m-1+1)^k \equiv (2m)^k(\text{mod } p)$, hence $m^k \not\equiv 0(\text{mod } p)$ so that (2) and (14) imply $\epsilon_k(p) \neq 0$. Hence $p-1|k$ and by Fermat's little theorem

$m^k \equiv 1 (\mathrm{mod}\ p)$. Thus (2) and (14) yield $-(t+\frac{1}{2}) \equiv 1 (\mathrm{mod}\ p)$. Replacing t by its value and simplifying we obtain

$$\frac{2m-1}{p} + 2 \equiv 0 (\mathrm{mod}\ p). \tag{15}$$

Since $2m-1$ is odd, (15) implies that $2m-1$ is square-free. Multiplying congruences of the type (15), one for each of the r prime diviosrs of $2m-1$, yields

$$2^{r-1}\Big((2m-1)\sum_{p|(2m-1)}\frac{1}{p} + 2\Big) \equiv 0 (\mathrm{mod}\ 2m-1).$$

Since the modulus $2m-1$ is odd this gives

$$\sum_{p|(2m-1)}\frac{1}{p} + \frac{2}{2m-1} \equiv 0 (\mathrm{mod}\ 1). \tag{16}$$

Finally we obtain a corresponding congruence for primes p dividing $2m+1$, namely (18) below. For this purpose we write (2) in the form

$$S_k(m+1) = 2m^k. \tag{17}$$

Suppose $p|(2m+1)$. Set $v = \frac{1}{2}(\frac{2m+1}{p} - 1)$. Clearly v is an integer. We have $m = pv + \frac{p-1}{2}$ and find $S_k(m+1) \equiv (v+\frac{1}{2})\epsilon_k(p) (\mathrm{mod}\ p)$. From this and (17) it is easy to infer that $v + \frac{1}{2} \equiv -2 (\mathrm{mod}\ p)$. Replacing v by its value and simplifying we obtain

$$\frac{2m+1}{p} + 4 \equiv 0 (\mathrm{mod}\ p).$$

Reasoning as before we obtain

$$\sum_{p|(2m+1)}\frac{1}{p} + \frac{4}{2m+1} \equiv 0 (\mathrm{mod}\ 1). \tag{18}$$

If we now add the left hand sides of (8), (13), (16) and (18), we get an integer, at least 4. By an argument similar to that showing $2 \nmid m$, we show that $3 \nmid m$ (but in this case we use Lemma 2 with $p = 3$ and $3^\lambda || m$ and the fact that k must be even). No prime $p > 3$ can divide more than one of the integers $m-1$, $m+1$, $2m-1$ and $2m+1$. Further, since $m \equiv 3 (\mathrm{mod}\ 8)$ and $3 \nmid m$, 2 and 3 divide precisely two of these integers. We infer that $M = (m-1)(m+1)(2m-1)(2m+1)/12$ is a square-free integer. We deduce that

$$\sum_{p|M}\frac{1}{p} + \frac{1}{m-1} + \frac{2}{m+1} + \frac{2}{2m-1} + \frac{4}{2m+1} \geq 4 - \frac{1}{2} - \frac{1}{3} = 3\frac{1}{6} \tag{19}$$

One checks that (16) has no solutions with $m \leq 1000$. Thus (19) yields (with $\alpha = 3.16$) $\sum_{p|M}\frac{1}{p} > \alpha$. From this it follows that if

$$\sum_{p \leq x}\frac{1}{p} < \alpha, \tag{20}$$

then $m^4/3 > M > \prod_{p\le x} p$ and hence

$$m > 3^{1/4} e^{\theta(x)/4}, \tag{21}$$

with $\theta(x) = \sum_{p\le x} \log p$, the Chebyshev θ-function. Since for example (20) is satisfied with $x = 1000$, we find that $m > 10^{103}$ and infer from (19) that we can take $\alpha = 3\frac{1}{6} - 10^{-100}$ in (20). Next one computes (using a computer algebra package, say PARI) the largest prime p_k such that $\sum_{p\le p_k} \frac{1}{p} < 3\frac{1}{6}$, with $p_1, p_2, \ldots$ the consecutive primes. Here one finds that $k = 4990906$ and

$$\sum_{i=1}^{4990906} \frac{1}{p_i} = 3.1666666588101728584 < 3\frac{1}{6} - 10^{-9}.$$

Using this part 1 of the Theorem is proved.

Notice that along our way towards proving part 1, the other parts of the Theorem have also been proved. □

`Remark`. Since for a solution of (1), $(m^2-1)(4m^2-1)/12$ has at least 4990906 distinct prime factors, it is perhaps reasonable to expect that each of the factors $m-1$, $m+1$, $2m-1$ and $2m+1$ must have many distinct prime factors. Brenton and Vasiliu [3], using the bound given in condition 1 of Theorem 2, showed that $m-1$ has at least 26 prime factors. Gallot et al. [8] increased this, using Theorem 5, to 33.

3. Comparison of the proof with Moser's

In this section it is explained to what extent the proof of Theorem 2 is different from Moser's of Theorem 1.

Moser in his proof only uses Lemma 1, not Lemma 2. Not using Lemma 2, he can only conclude that either $m \equiv 3 \pmod 8$ or $m \equiv 0 \pmod 8$. In the first case he proceeds as above, in the latter case one has to note that we cannot use (13). Letting $N = (m-1)(2m-1)(2m+1)$ we get from (8), (16), (18)

$$\sum_{p|N} \frac{1}{p} + \frac{1}{m-1} + \frac{2}{2m-1} + \frac{4}{2m+1} > 3 - \frac{1}{3} \tag{22}$$

However, since $2 \nmid N$, (22) is actually a stronger condition on m than is (19).

The idea to use $3 \nmid m$, leading to a slight improvement for the bound on m, is taken from Butske et al. [4] and not there in Moser's proof. (Actually they consider the case $3 \nmid m$ and $3|m$ separately. We show that only $3 \nmid m$ can occur.)

By using some prime number estimates from Rosser, Moser deduces that (20) holds with $x = 10^7$ and $\alpha = 3.16$. In his argument he claims that by direct computation one see that (20) holds with $x = 1000$ and $\alpha = 2.18$. This is not true (as pointed out to me by Buciumas and Havarneanu). However, replacing 2.18 by 2.2 in Moser's equation (21) one sees that his proof still remains valid. The present day possibilities of computers allow us to proceed by direct computation, rather than to resort to prime number estimates as Moser was forced to do.

The advantage of the proof given in Section 2 is that it shows, in contrast to

Moser's proof and Butske et al.'s variation thereof, that *every* non-trivial solution satisfies the crucial inequality (19).

4. A second proof using a von Staudt-Clausen type theorem

In this section we show that Moser's four formulae (8), (13), (16) and (18) can be easily derived from the following lemma. Indeed using it, even a fifth formula can be derived, namely (25) below.

Theorem 3. (Carlitz-von Staudt, 1961). *Let r, y be positive integers. Then*

$$S_r(y) = \sum_{j=1}^{y-1} j^r = \begin{cases} 0 \pmod{\frac{y(y-1)}{2}} & \text{if } r \text{ is odd;} \\ -\sum_{p-1|r,\ p|y} \frac{y}{p} \pmod{y} & \text{otherwise.} \end{cases} \tag{23}$$

This result will be discussed and proved in Section 5.

Proof of Theorem 2. We will apply Theorem 3 with $r = k$.

In case k is odd, we find on combining (23) (with $y = m$) with (1) on using the coprimality of m and $m-1$ that $m = 2$ or $m = 3$, but these cases are easily excluded. Therefore k must be even.

Take $y = m - 1$. Then using (1) the left hand side of (23) simplifies to

$$S_k(m-1) = 1^k + 2^k + \ldots + (m-2)^k = m^k - (m-1)^k \equiv 1(\text{mod } m-1).$$

We get from (23) that

$$\sum_{p|m-1,\ p-1|k} \frac{m-1}{p} + 1 \equiv 0(\text{mod } m-1). \tag{24}$$

Suppose there exists $p|m-1$ such that $p - 1 \nmid k$. Then on reducing both sides modulo p we get $1 \equiv 0(\text{mod } p)$. This contradiction shows that in (24) the condition $p - 1|k$ can be dropped and thus we obtain (7). From (7) we see that $m - 1$ must be square-free and also we obtain (8).

Take $y = m$. Then using (1) and $2|k$ we infer from (23) that

$$\sum_{p-1|k,\ p|m} \frac{1}{p} \equiv 0(\text{mod } 1). \tag{25}$$

Since a sum of reciprocals of distinct primes can never be a positive integer, we infer that the sum in (25) equals zero and hence conclude that if $p-1|k$, then $p \nmid m$. We conclude for example that $(6, m) = 1$. Now on considering (1) with modulus 4 we see that $m \equiv 3(\text{mod } 8)$.

Take $y = m + 1$. Then using (1) and the fact that k is even, the left hand side of (23) simplifies to

$$S_k(m+1) = S_k(m) + m^k = 2m^k \equiv 2(\text{mod } m+1).$$

We obtain

$$\sum_{p|(m+1),\ p-1|k} \frac{(m+1)}{p} + 2 \equiv 0(\text{mod } m+1),$$

but by reasoning as in the case $y = m - 1$, it is seen that $p|m+1$ implies $p-1|k$ and thus (13) is obtained. From (13) and $m \equiv 3(\text{mod } 8)$, we derive that $(m+1)/2$ is square-free.

Take $y = 2m - 1$. On noting that

$$S_k(2m-1) = \sum_{j=1}^{m-1}(j^k + (2m-1-j)^k) \equiv 2S_k(m) \equiv 2m^k (\text{mod } 2m-1),$$

we infer that

$$(2m-1)\sum_{p|2m-1,\ p-1|k}\frac{1}{p} + 2m^k \equiv 0(\text{mod } 2m-1). \tag{26}$$

Since m and $2m-1$ are coprime we infer that if $p|2m-1$, then $p-1|k$, $m^k \equiv 1(\text{mod } p)$ and furthermore that $2m-1$ is square-free. It follows by the Chinese Remainder Theorem that $2m^k \equiv 2(\text{mod } 2m-1)$ and hence from (26) we obtain (16).

Take $y = 2m + 1$. On noting that

$$S_k(2m+1) = \sum_{j=1}^{m}(j^k + (2m+1-j)^k) \equiv 2S_k(m+1) \equiv 4m^k (\text{mod } 2m+1)$$

and proceeding as in case $y = 2m - 1$ we obtain (18) and the square-freeness of $2m+1$. To finish the proof we proceed as in Section 2 just below (18). □

With some of the magic behind the four Moser identities revealed, the reader might be well tempted to derive further ones. A typical example would start from

$$4^k - 1^k - 2^k - 3^k \equiv -\sum_{\substack{p-1|k \\ p|(m-4)}}\frac{1}{p}(\text{mod } m-4). \tag{27}$$

For simplicity let us assume that $m \equiv 2(\text{mod } 3)$. We have $(6, m-4) = 1$. For this to result in a further equation, we need the left hand side to be a constant modulo $m-4$. If we could infer that $p|m-4$ implies $p-1|k$, then the left hand side would equal $-2(\text{mod } m-4)$ and we would be in business. (For the reader familiar with the Carmichael function λ, this can be more compactly formulated as $\lambda(m-4)|k$.) Unfortunately a problem is caused by the fact that the left hand side could be divisible by p. Thus all we seem to obtain is that if $m \equiv 2(\text{mod } 3)$, and $\lambda(m-4)|k$ or $4^k - 1^k - 2^k - 3^k$ and $m-4$ are coprime, then

$$\sum_{p|(m-4)}\frac{1}{p} - \frac{2}{m-4} \equiv 0(\text{mod } 1).$$

In Section 7 we will see that if we replace $m-4$ by $m+2$ we can do a little better, the reason being that in the left hand side in this case, $2^{k+1}+1$ appears and numbers of these form have only a rather restricted set of possible prime factors.

5. The Carlitz-von Staudt theorem

Carlitz [5] gave a proof of Theorem 3 using finite differences and states that the result is due to von Staudt. In the case r is odd, he claims that $S_r(y)/y$ is an integer, which is not always true (it is true though that $2S_r(y)/y$ is always an integer). The author [12] gave a reproof using the theory of primitive roots and Kellner [11] a reproof (in case r even only) using Stirling numbers of the second kind. Here we present an easier reproof than the ones above.

Proof of Theorem 3. First let us consider the case where r is odd. Assume $S_r(m)$ is a multiple of $m(m-1)/2$. We need to show that $S_r(m+1) = S_r(m) + m^r$ is a multiple of $m(m+1)/2$.

If m is even, we have that $m/2$ divides $S_r(m)$. But

$$S_r(m+1) = (1^r + m^r) + (2^r + (m-1)^r) + \ldots + ((\frac{m}{2})^r + (\frac{m}{2}+1)^r)$$

which is a multiple of $m+1$ as each pair above is. Thus, $S_r(m+1)$ is a multiple of $m/2$ as well as of $m+1$ which are coprime and hence a multiple of $m(m+1)/2$.

If m is odd, then $m|S_r(m)$. But

$$S_r(m+1) = (1^r + m^r) + (2^r + (m-1)^r) + \ldots + (\frac{m+1}{2})^r,$$

which is a multiple of $(m+1)/2$ as each pair as well as the last remaining term is. Thus $S_r(m+1)$ is a multiple of m as well as $(m+1)/2$ which are coprime and hence a multiple of $m(m+1)/2$.

Next we consider the case where r is even. Suppose that $p^f|y$, then

$$S_r(y) = \sum_{\alpha=0}^{yp^{-f}-1} \sum_{\beta=0}^{p^f-1} (\alpha p^f + \beta)^r \equiv \frac{y}{p^f} S_r(p^f) (\text{mod } p^f). \tag{28}$$

By the Chinese Remainder Theorem it is enough to show that

$$S_r(y) \equiv \frac{y}{p}\epsilon_r(p) (\text{mod } p^{e_p}),$$

where $y = \prod_p p^{e_p}$ is a factorization of y into prime powers p^{e_p}. By (28), Lemma 2 and Lemma 1, we then infer that

$$S_r(y) \equiv \frac{y}{p^{e_p}} S_r(p^{e_p}) \equiv \frac{y}{p} S_r(p) \equiv \frac{y}{p}\epsilon_r(p) (\text{mod } p^{e_p}),$$

thus concluding the proof. □

A further application of the Carlitz-von Staudt theorem is to show that Giuga's conjecture (1950) and Agoh's conjecture (1990) are equivalent, see Kellner [11]. Giuga's conjecture states that if $n \geq 2$, then $S_{n-1}(n) \equiv -1 (\text{mod } n)$ iff n is prime. Agoh's conjecture states that if $n \geq 2$, then $nB_{n-1} \equiv -1 (\text{mod } n)$ iff n is a prime, where B_r denotes the r-th Bernoulli number.

6. Recent developments

Moree et al. [18], using properties of the Bernoulli numbers and polynomials, showed that $N_1 = \mathrm{lcm}(1, 2, \dots, 200) \mid k$. Kellner [10] in 2002 showed that also all primes $200 < p < 1000$ have to divide k. Actually Moree et al. [18, p. 814] proved a slightly stronger result and on combining this with Kellner's, one obtains that $N_2 \mid k$ with

$$N_2 = 2^8 \cdot 3^5 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdots 997 > 5.7462 \cdot 10^{427}.$$

Gallot, Moree and Zudilin [8] study (1) using the theory of continued fractions. This approach was first explored in 1976 by Best and te Riele [2] in their attempt to solve a related conjecture of Erdős, see also Guy [9, D7]. Gallot et al. showed that if (m, k) is a solution of (1) with $k \geq 2$, then $2k/(2m-3)$ is a convergent p_j/q_j of $\log 2$. Their main result reads as follows, where given $N \geq 1$, we define

$$\mathcal{P}(N) = \{p : p - 1 \mid N\} \cup \{p : 3 \text{ is a primitive root modulo } p\},$$

and if $p^f || m$, we put $\nu_p(m) = f$.

Theorem 4. *Let $N \geq 1$ be an arbitrary integer. Let*

$$\frac{\log 2}{2N} = [a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

be the (regular) continued fraction of $(\log 2)/(2N)$, with $p_i/q_i = [a_0, a_1, \dots, a_i]$ its i-th partial convergent.

Suppose that the integer pair (m, k) with $k \geq 2$ satisfies (1) with $N \mid k$. Let $j = j(N)$ be the smallest integer such that:
a) *j is even;*
b) *$a_{j+1} \geq 180N - 2$;*
c) *$(q_j, 6) = 1$;*
d) *$\nu_p(q_j) = \nu_p(3^{p-1} - 1) + \nu_p(N) + 1$ for all primes $p \in \mathcal{P}(N)$ dividing q_j.*
Then $m > q_j/2$.

Condition d is derived using the Moser method, namely by analyzing the equation

$$\frac{2(3^k - 1)(m-1)^k}{2m-3} \equiv - \sum_{\substack{p \mid 2m-3 \\ p-1 \mid k}} \frac{1}{p} \pmod 1, \tag{29}$$

that a solution (m, k) of (1) has to satisfy.

Applying Theorem 2 with $N = 2^8 \cdot 3^5 \cdot 5^3$ or $N = 2^8 \cdot 3^5 \cdot 5^4$, and using that $N|N_2|k$, they obtained the current world record:

Theorem 5. *If an integer pair (m, k) with $k \geq 2$ satisfies (1), then*

$$m > 2.7139 \cdot 10^{1\,667\,658\,416}.$$

7. A new result

The rest of the paper is the research part and here some familiarity with the theory of divisors of second order sequences is helpful, see e.g. Ballot [1] and Moree [16] for more introductory accounts.

Let S be an infinite sequence of positive integers. We say that a prime p divides the sequence if it divides at least one of its terms. Here we will be interested in the sequence $S_2 := \{2^{2e+1}+1\}_{e=0}^{\infty}$. It can be shown that $p > 3$ divides S_2 iff $\mathrm{ord}_2(p) \equiv 2 (\mathrm{mod}\ 4)$, with $\mathrm{ord}_g(p)$ (with $p \nmid g$) the smallest positive integer t such that $g^t \equiv 1 (\mathrm{mod}\ p)$. The set of these primes is known to have natural density $7/24$. Furthermore, if $\mathrm{ord}_2(p) \equiv 2 (\mathrm{mod}\ 4)$ then

$$p | 2^{2e+1} + 1 \text{ iff } 2e \equiv \frac{\mathrm{ord}_2(p)}{2} - 1 (\mathrm{mod}\ \mathrm{ord}_2(p)). \tag{30}$$

In coding theoretical work of Dicuangco and Solé [6] integers n coprime to the sequence S_2 play an important role. Likewise in the study of the Stufe of cyclotomic fields, see e.g. [7, 14].

If $m+2$ is coprime with S_2, then from (32) we can infer that a fifth identity of Moser type, (31), must hold true. This then leads to $m > 10^{10^{11}}$ for such m. We now consider the situation in greater detail.

Theorem 6. *Suppose that (m, k) is a solution of (1) with*

$$k > 1,\ 24|M|k \text{ and } m < 10^{10^{11}},$$

then $m+2$ has a prime divisor $p > 3$ such that:
1) $(\mathrm{ord}_2(p), M) = 2$;
2) $k \equiv \frac{\mathrm{ord}_2(p)}{2} - 1 (\mathrm{mod}\ \mathrm{ord}_2(p))$.
In case $m \equiv 2 (\mathrm{mod}\ 3)$, we can replace $10^{10^{11}}$ by $10^{10^{16}}$. In case $M = N_2$ we have $p \geq 2099$.

Corollary 1. *If every prime divisor $p > 3$ of $m+2$ satisfies $p \equiv 5, 7 (\mathrm{mod}\ 8)$, then $m \geq 10^{10^{11}}$ if $m \equiv 1 (\mathrm{mod}\ 3)$ and $m \geq 10^{10^{16}}$ otherwise. In particular, if every prime divisor p of $m+2$ satisfies $p \equiv 5, 7 (\mathrm{mod}\ 8)$, then $m \geq 10^{10^{16}}$.*

Proof. Using the supplementary law of quadratic reciprocity, $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$, one sees that if $p \equiv 5, 7 (\mathrm{mod}\ 8)$, then $\mathrm{ord}_2(p) \not\equiv 2 (\mathrm{mod}\ 4)$. thus condition 1 is not satisfied, as for this to be satisfied we must have $\mathrm{ord}_2(p) \equiv 2 (\mathrm{mod}\ 4)$. □

Put

$$P(M) = \{p > 3 : (\mathrm{ord}_2(p), M) = 2\}.$$

Thus if p is to be in $P(M)$, then $p \equiv 1 (\mathrm{mod}\ 8)$ or $p \equiv 3 (\mathrm{mod}\ 8)$. In the latter case we have $\mathrm{ord}_2(p) \equiv 2 (\mathrm{mod}\ 4)$. In the former case it is not necessarily so that $\mathrm{ord}_2(p) \equiv 2 (\mathrm{mod}\ 4)$ and numerically there is a strong preponderance of primes $p \equiv 3 (\mathrm{mod}\ 8)$ in $P(M)$. Indeed, we have the following result.

Lemma 3. *The relative density of primes $p \equiv 1 (\mathrm{mod}\ 8)$ satisfying $\mathrm{ord}_2(p) \equiv 2 (\mathrm{mod}\ 4)$ is $1/6$.*

Proof. We have seen that if $\mathrm{ord}_2(p) \equiv 2(\mathrm{mod}\ 4)$, then $p \equiv 1, 3(\mathrm{mod}\ 8)$. If $p \equiv 3(\mathrm{mod}\ 8)$, then $\mathrm{ord}_2(p) \equiv 2(\mathrm{mod}\ 4)$. From this and the fact that $\delta(\mathrm{ord}_2(p) \equiv 2(\mathrm{mod}\ 4)) = 7/24$ and the prime number theorem for primes in arithmetic progression, we infer that the density of primes $p \equiv 1(\mathrm{mod}\ 8)$ such that $\mathrm{ord}_2(p) \equiv 2(\mathrm{mod}\ 4)$ equals $\frac{7}{24} - \frac{1}{4} = \frac{1}{24}$. The sought for relative density is then $\frac{1}{24}/\frac{1}{4} = \frac{1}{6}$. □

Thus if $p \equiv 3(\mathrm{mod}\ 8)$, then $\mathrm{ord}_2(p) \equiv 2(\mathrm{mod}\ 4)$ and if $p \equiv 1(\mathrm{mod}\ 8)$, then $\mathrm{ord}_2(p) \equiv 2(\mathrm{mod}\ 4)$ in 1/6-th of the cases.

A further observation concerning the set $P(M)$ is related to Sophie Germain primes. A prime q such that $2q+1$ is a prime, is called a Sophie Germain prime.

Lemma 4. *Let q_M be the largest prime factor of M. If $q > q_M$, $q \equiv 1(\mathrm{mod}\ 4)$ and q is a Sophie Germain prime, then $p = 2q+1 \in P(M)$.*

Proof. The assumptions imply that $(\frac{2}{p}) = -1$ and since $p > 3$ we infer that $\mathrm{ord}_2(p) = 2q$. Since $(\mathrm{ord}_2(p), M) = (2q, M) = 2$ we are done. □

There are 42 primes p in $P(N_2)$ not exceeding 10.000. Of those 7 primes p are such that $(p-1)/2$ is not Sophie Germain, the smallest one being 7699. However, the Sophie Germain primes have natural density zero, whereas as we shall see $P(M)$ has positive natural density.

Given a rational number g such that $g \notin \{-1, 0, 1\}$, the natural density $\delta_g(d)$ of the set of primes p such that the order of $g(\mathrm{mod}\ p)$ is divisible by d is known to exist and can be computed, see e.g. Moree [15]. Using inclusion and exclusion one then finds that the set $P(M)$ has natural density

$$\delta(M) = \sum_{d|M_1} (\delta_2(2d) - \delta_2(4d))\mu(d),$$

where M_1 is the product of the odd prime divisors dividing M and μ denotes the Möbius function. By Moree [15, Theorem 2] we then find that

$$\delta(M) = \frac{7}{24} \prod_{p|M_1} \left(1 - \frac{p}{p^2-1}\right).$$

Taking $M = N_2$ one finds that

$$\delta(N_2) = \frac{7}{24} \prod_{2<p\le 1000} \left(1 - \frac{p}{p^2-1}\right) \approx 0.043578833\cdots$$

`Remark`. In [6] an asymptotic for the number of integers $n \le x$ that are coprime with S_2 is derived. Let us call an integer n *M-good* if none of its prime divisors p satisfy condition 1. By the same methods it can be shown, cf. [6, 14], that asymptotically the number of integers $n \le x$ that are M-good, $N_G(x)$, satisfies $N_G(x) \sim c_M x \log^{-\delta(M)} x$, where $c_M > 0$ is positive constant depending on M.

Proof of Theorem 6. The idea of the proof is to show if for every prime divisor $p > 3$ of $m + 2$ at least one the conditions 1 and 2 is not satisfied, then the identity

$$\sum_{p|(m+2)} \frac{1}{p} - \frac{3}{m+2} \equiv 0 (\text{mod } 1) \tag{31}$$

holds. Using this we then show that m is bigger than the bound in the theorem. A contradiction. As usual we make heavy use of the fact that k must be even.

We start with the equation

$$2^{k+1} + 1 \equiv - \sum_{p-1|k,\ p|m+2} \frac{m+2}{p} (\text{mod } m+2), \tag{32}$$

found on noting that $S_k(m+2) = 2m^k + (m+1)^k \equiv 2^{k+1} + 1 (\text{mod } m+2)$ and on invoking Theorem 3. Suppose that $p|m+2$. The idea is to reduce (32) modulo p (except if $p = 3$, then we reduce modulo 9).

If $p = 3$, then using $6|k$ we see that $2^{k+1} + 1 \equiv 3 (\text{mod } 9)$ and we infer that $3^2||(m+2)$, that is we must have $m \equiv 16 (\text{mod } 27)$. Next assume $p > 3$.

First assume that $\text{ord}_2(p) \not\equiv 2 (\text{mod } 4)$, Then p does not divide S_2. Thus the right hand side of (32) is non-zero modulo p and this implies that $p-1|k$ and $p^2 \nmid (m+2)$ and hence $2^{k+1} + 1 \equiv 3 (\text{mod } p)$.

Next assume that $\text{ord}_2(p) \equiv 2 (\text{mod } 4)$ and condition 1 is not satisfied. Then $\text{ord}_2(p)$ and M have an odd prime factor in common and by (30) (with $e = k/2$) we get a contradiction with the assumption $M|k$.

Finally assume that condition 2 is not satisfied. Then also the right hand side of (32) is non-zero modulo p and the same conclusion as before holds. By the Chinese remainder theorem we then infer that $2^{k+1} + 1 \equiv 3 (\text{mod } m+2)$ and hence from (32) we see that (31) holds. It is easy to see that the left hand side of (31) must be strictly positive. Thus we infer that

$$\sum_{p|(m+2)} \frac{1}{p} > 1. \tag{33}$$

Put $N_3 = (m^2-1)(4m^2-1)(m+2)$. Note that amongst the numbers $m-1, m+1, m+2, 2m-1, 2m+1$, no prime $p \geq 7$ occurs more than once as divisor, the prime 2 occurs precisely twice, the prime 3 at most 3 times and the prime 5 at most two times. Using this, we obtain on adding Moser's equations (8), (13), (16) and (18) to (33):

$$\sum_{p|N_3} \frac{1}{p} + \frac{1}{m-1} + \frac{2}{m+1} + \frac{2}{2m-1} + \frac{4}{2m+1} \geq \frac{109}{30} = 3.63333333333\cdots, \tag{34}$$

where $\frac{109}{30} = 5 - \frac{1}{2} - \frac{2}{3} - \frac{1}{5}$. Using the estimate

$$\sum_{p \leq x} \frac{1}{p} < \log\log x + 0.2615 + \frac{1}{\log^2 x} \text{ for } x > 1,$$

due to Rosser and Schoenfeld [21, (3.20)], we find that $\sum_{p\le\beta} 1/p < 3.63332$ with $\beta = 4.33\cdot 10^{12}$. From another paper by the same authors [22] we have

$$|\theta(x)-x| < \frac{x}{40\log x},\ x \ge 678407.$$

Hence

$$\log(4m^5) > \log(N_3) > \log\prod_{p\le\beta} p = \theta(\beta) > .999\beta,$$

from which we infer that $m \ge 10^{10^{11}}$.

In case $m \equiv 2(\mathrm{mod}\ 3)$ there are precisely two of the five terms $m-1, m+1, 2m-1, 2m+1$ and $m+2$ divisible by 3, and in (34) we can replace 109/30 by $109/30 + 1/3 = 119/30$. In that case we can take $\beta = 4.425\cdot 10^{17}$ and this leads to $m \ge 10^{10^{16}}$.

The smallest two primes in $P(N_2)$ are 2027 and 2099. For $p = 2027$ we can actually show that condition 2 is not satisfied. To this end we must show that $k \not\equiv 1012(\mathrm{mod}\ 2026)$. Computation shows that $(1012, 6079)$ $(3038, 6079)$ and $(5064, 6079)$ are good pairs. If (r, p) is a good pair, then $k \not\equiv r(\mathrm{mod}\ p-1)$, see [18] for further details. The smallest prime that possibly satisfies both condition 1 and 2 is hence 2099.

8. The generalized Erdős-Moser conjecture

The Erdős-Moser conjecture has the following generalization.

Conjecture 1. *There are no integer solutions (m, k, a) of*

$$1^k + 2^k + \ldots + (m-1)^k = am^k \tag{35}$$

with $k \ge 2$, $m \ge 2$ and $a \ge 1$.

In this direction the author proved in 1996 [13] that (35) has no integer solutions (a, m, k) with $k > 1$ and $m < \max(10^{10^6}, a\cdot 10^{22})$. With the hindsight of more than 10 years this can be improved.

Theorem 7. *The equation (35) has no integer solutions (a, m, k) with*

$$k > 1,\ m < \max\left(10^{9\cdot 10^6}, a\cdot 10^{28}\right).$$

Proof. (In this proof references to propositions and lemmas are exclusively to those in [13].) The Moser method yields that $2|k$ and gives the following four inequalities

$$\sum_{\substack{p-1|k\\ p|m-1}} \frac{1}{p} + \frac{a}{m-1} \ge 1,\quad \sum_{\substack{p-1|k\\ p|m+1}} \frac{1}{p} + \frac{a+1}{m+1} \ge 1. \tag{36}$$

$$\sum_{\substack{p-1|k\\ p|2m-1}} \frac{1}{p} + \frac{2a}{2m-1} \ge 1,\quad \sum_{\substack{p-1|k\\ p|2m+1}} \frac{1}{p} + \frac{2(a+1)}{2m+1} \ge 1. \tag{37}$$

Since $p|m$ implies $p-1 \nmid k$ (Proposition 9), we infer that $(6, m) = 1$. Using this we see that $G = (m^2-1)(4m^2-1)/12$ is an even integer. Since no prime > 3 can divide more than one of the numbers $m-1, m+1, 2m-1$ and $2m+1$, and since 2 and 3 divide two of these numbers, we find on adding the inequalities that

$$\sum_{p-1|k,\ p|G} \frac{1}{p} + \frac{a}{m-1} + \frac{a+1}{m+1} + \frac{2a}{2m-1} + \frac{2(a+1)}{2m+1} \geq 4 - \frac{1}{2} - \frac{1}{3} = 3\frac{1}{6}.$$

Using that $a(k+1) < m < (a+1)(k+1)$ (Proposition 2), we see that in the latter equation the four terms involving a are bounded above by $6/(k+1)$. Since $k \geq 10^{22}$ (Lemma 2), we can proceed as in the proof of Theorem 2 and find the same bound for m, namely $m > 1.485 \cdot 10^{9321155}$.

Earlier it was shown that if $k > 1$, then $k \geq 10^{22}$. To this end Proposition 6 with $C = 3.16$, $s = 664579 = \pi(10^7)$ and n the 200-th highly composite number was applied. Instead we apply it with $C = 3\frac{1}{6} - 10^{-10}$, $s = 4990906$ and n the 259-th composite number c_{250} (this has the property that the number of divisors of $c_{259} < s$, whereas the number of divisors of c_{260} exceeds s). Since $n = c_{259} > 5.5834 \cdot 10^{27}$ it follows that $k \geq 2n > 10^{28}$. Since $m > a(k+1)$, the proof is completed. □

`Challenge`: Reach the benchmark 10^{10^7} in Theorem 7.

`Acknowledgement`. The proof of the odd exponent case of the Carlitz-von Staudt theorem is due to B. Sury. Part of this article was written whilst I had 4 interns (Valentin Buciumas, Raluca Havarneanu, Necla Kayaalp and Muriel Lang), studying variants of the Erdős-Moser equation. Raluca and Valentin found a (reparable) mistake in Moser's paper and Muriel showed that 2027 is the smallest prime in $P(N_2)$, but does not satisfy condition 2 of Theorem 6. I thank them all for their questions, comments and cheerful presence. Their further work will be reported on in a future publication.

Paul Tegelaar pointed out a computational mistake with serious consequences in an earlier version.

References

[1] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, viii+102 pp.

[2] M.R. Best and H.J.J. te Riele, On a conjecture of Erdős concerning sums of powers of integers, Report NW 23/76, Mathematisch Centrum Amsterdam, 1976.

[3] L. Brenton and A. Vasiliu, Znam's problem, *Math. Mag.* **75** (2002), 3–11.

[4] 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.

[5] L. Carlitz, The Staudt-Clausen theorem, *Math. Mag.* **34** (1960/1961), 131–146.

[6] L. Dicuangco, P. Moree and P. Solé, The lengths of Hermitian self-dual extended duadic codes, *J. Pure Appl. Algebra* **209** (2007), 223–237.

[7] B. Fein, B. Gordon and J.H. Smith, On the representation of -1 as a sum of two squares in an algebraic number field, *J. Number Theory* 3 (1971), 310–315.

[8] 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, submitted for publication.

[9] R.K. Guy, *Unsolved problems in number theory*, Third edition, Problem Books in Mathematics, Springer-Verlag, New York, 2004.

[10] B.C. Kellner, Über irreguläre Paare höhere Ordnungen, Diplomarbeit, Mathematisches Institut der Georg–August–Universität zu Göttingen, Germany, 2002. (Also available at `http://www.bernoulli.org/~bk/irrpairord.pdf`)

[11] B.C. Kellner, The equivalence of Giuga's and Agoh's conjectures, Preprint: arXiv:math.NT/0409259.

[12] P. Moree, On a theorem of Carlitz-von Staudt, *C. R. Math. Rep. Acad. Sci. Canada* **16** (1994), 166–170.

[13] P. Moree, Diophantine equations of Erdős-Moser type, *Bull. Austral. Math. Soc.* **53** (1996), 281–292.

[14] P. Moree, On the divisors of $a^k + b^k$, *Acta Arith.* **80** (1997), 197–212.

[15] P. Moree, On primes in arithmetic progression having a prescribed primitive root. II, *Funct. Approx. Comment. Math.* **39** (2008), 133–144.

[16] P. Moree, Artin's primitive root conjecture -a survey, http://front.math.ucdavis.edu/0412.5262

[17] P. Moree, A tophat for Moser's four mathemagical rabbits, submitted for publication.

[18] P. Moree, H. te Riele and J. Urbanowicz, Divisibility properties of integers x, k satisfying $1^k + \cdots + (x-1)^k = x^k$, *Math. Comp.* **63** (1994), 799–815.

[19] L. Moser, On the diophantine equation $1^n + 2^n + 3^n + \cdots + (m-1)^n = m^n$. *Scripta Math.* **19** (1953). 84–88.

[20] Leo Moser, http://www-history.mcs.st-andrews.ac.uk/Biographies/Moser__Leo.html

[21] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[22] J.B. Rosser and L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, *Math. Comp.* **29** (1975), 243–269.

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany
E-mail address: `moree@mpim-bonn.mpg.de`