Divisibility Properties of Integers x and k Satisfying $1^k + 2^k + \cdots + (x-1)^k = x^k$

P. Moree
Mathematical Institute, University of Leiden
P.O. Box 9512, 2300 RA Leiden, The Netherlands

H.J.J. te Riele
CWI, P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

J. Urbanowicz*
Institute of Mathematics, Polish Academy of Sciences
ul. Śniadeckich 8, 00-950 Warszawa, Poland

Abstract

Based on congruences mod p and on properties of Bernoulli polynomials and numbers, several conditions are derived for $x, k \geq 2$ if they satisfy the diophantine equation $1^k + 2^k + \cdots + (x-1)^k = x^k$. By using the results of experiments with these conditions on an SGI workstation it is proved that x can not be divisible by any irregular prime < 10000 and that k is divisible by the least common multiple of all the integers ≤ 200. Moreover, it is proved that x can not be divisible by any regular prime.

1991 Mathematics Subject Classification: 11D41, 11B68, 11Y50.
Keywords & Phrases: Sums of powers, regular and irregular primes,
Bernoulli numbers, congruences, diophantine equations.

* *Note 1:* This research was done while the third author was visiting the University of Leiden, supported by the Netherlands Organization for Scientific Research (NWO), under grant 611-307-019/018.
Note 2: This report has been submitted for publication elsewhere.

Report NM-R9215, August 1992
ISSN 0169-0388
CWI
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

1 Introduction

We are interested in natural numbers x and k satisfying the Erdös-Moser diophantine equation

$$1^k + 2^k + \cdots + (x-1)^k = x^k. \tag{1}$$

Notice that $(x,k) = (3,1)$ is the only solution for $k = 1$. From now on we assume that $k \geq 2$. Erdös and Moser [Mos53] conjectured that in this case (1) has no solutions. However, it has not even been proved that (1) has only finitely many solutions (x,k). Assume that (x,k) is a solution of (1). Moser [Mos53] proved that x exceeds C, where $C = 10^{1000000}$. Best and one of the authors [BtR76] proved that for every k there is at most one x satisfying (1). From their work and also from an analytical expression of Delange [Del91, Théorème 2] for $\sum_{1 \leq m < y}(y-m)^k$ with y real and > 1, it follows that k/x tends to $\log 2$ as x tends to infinity. So we have a lower bound for k which is of the same order of magnitude as Moser's lower bound C for x. Lemma 7 below provides an explicit lower bound.

On the *divisibility properties* of x and k very little is published. Moser [Mos53] proved that k is *even* and x is *odd*. In this paper we will establish further divisibility properties of x and k. In Section 2 we give a number of mathematical preliminaries. Section 3 gives our main mathematical results which are proved in Section 4. Numerical searches based on the results of Section 3 are described in Section 5. Combination of the mathematical and numerical results yields that if (x,k) is a solution of (1) then

- k should be divisible by the number $M = 2^8 \cdot 3^5 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdots 199$ $(\log_{10}(M) = 94.359\cdots)$, and
- x is neither divisible by a regular prime, nor by any irregular prime < 10000.

The paper concludes with some heuristics to support the truth of the Erdös-Moser conjecture. For other references on the Erdös-Moser conjecture, see, e.g., [Guy81, p. 85], or the introduction of [Urb88]. The present paper is an extension, both mathematically and numerically, of [LU].

A possible generalization of (1) is the equation

$$a_1^k + a_2^k \cdots + a_{x-1}^k = a_x^k,$$

where $a_1, a_2, \cdots$ is any arithmetic progression. We expect that the methods we use for (1) will yield similar results for this equation.

For the more general equation

$$y_1^k + y_2^k + \cdots + y_{n-1}^k = y_n^k$$

it is proved in [DL63] that this equation has infinitely many integer solutions $y_1, y_2, \cdots, y_n$ with $y_i \neq 0$ whenever $k \geq 18$ and $n \geq 1 + k^2$.

Acknowledgements. We wish to thank R. Tijdeman for his contribution in the realization of our cooperation. Furthermore we like to thank R. Guy, C. Pomerance, and P. Stevenhagen for their stimulating remarks, and J. Buhler and S. Wagstaff, Jr. for informing us about the latest results concerning irregular primes.

2 Mathematical preliminaries

Let k and x be integers ≥ 2. Put $S_k(x) = \sum_{1 \leq m \leq x-1} m^k$ and, for any prime p,

$$f_k(x;p) = \sum_{\substack{1 \leq m \leq x-1 \\ p \not| m}} m^k - x^k$$

and $f_k(1;p) = -1$. Recall that Euler's totient, $\varphi(n)$, is the number of integers in $[1,n]$ coprime with n and that $\varphi(p^\lambda) = p^{\lambda-1}(p-1)$ for any prime p and positive integer λ. A rational number u/v with coprime integers u and v is said to be p-integral if $p \not| v$, and to be divisible by p^μ if $p^\mu | u$. If $\alpha = p^\mu u/v$ with $p \not| u,v$, and μ integral, then $\mathrm{ord}_p \alpha := \mu$. Let B_n, respectively $B_n(x)$ denote the nth Bernoulli number, respectively polynomial. The following results are well-known and can be found in [IR90, Chapter 15] or [Was82]:

P1. $B_n \in \mathbb{Q}$, $B_n(0) = B_n$, $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$ and $B_n = 0$ if $n \geq 3$ and odd. If n is even then $\mathrm{sgn}(B_n) = (-1)^{n/2+1}$.

P2. (The von Staudt-Clausen theorem) If $|B_n| = S_n/T_n$, $2|n$ and $(S_n, T_n) = 1$, then $p|T_n$ if and only if $p-1|n$, and $p-1|n$ implies $pB_n \equiv -1 \pmod{p}$. From the latter congruence it follows that T_n is squarefree.

P3. (The Kummer congruence) If $n \geq 2$, $n \equiv r \pmod{p-1}$, $n \not\equiv 0 \pmod{p-1}$, then B_n/n is p-integral and $B_n/n \equiv B_r/r \pmod{p}$. More generally, if $n \equiv r \pmod{\varphi(p^\lambda)}$, $n \not\equiv 0 \pmod{p-1}$ and $\lambda \geq 1$, then we have

$$(1-p^{n-1})\frac{B_n}{n} \equiv (1-p^{r-1})\frac{B_r}{r} \pmod{p^\lambda}.$$

P4. For $x_1, x_2 \in \mathbb{C}$

$$B_n(x_1+x_2) = \sum_{i=0}^{n} \binom{n}{i} B_i(x_1) x_2^{n-i}.$$

In the special case $x_1 = 0$, $x_2 = x$ we have

$$B_n(x) = \sum_{i=0}^{n} \binom{n}{i} B_i x^{n-i}.$$

P5. (The power summation formula) For natural numbers $n \geq 1$ and $a \geq 2$ we have

$$B_n(a) = nS_{n-1}(a) + B_n.$$

P6. For even n we have

$$2A_n < |B_n/n| \leq \pi^2 A_n/3,$$

where $A_n := (n-1)!/(2\pi)^n$.

An odd prime p is said to be *regular* if $p \nmid B_r$ for every even integer r in the interval $[0, p-3]$. If this condition is not satisfied p is called *irregular* and the pairs (r, p) with $p \mid B_r$ are called *irregular pairs*. Their number, the *index of irregularity*, is denoted by $i(p)$. For a fixed irregular pair (r, p), let $a_0 \in [0, p)$ be the unique integer such that $a_0 \equiv B_r/rp \pmod{p}$, $a_1 \in [0, p)$ be the unique integer such that $a_1 \equiv B_{r+p-1}/p(r+p-1) \pmod{p}$ (see P3) and $T_{r,p}$ the set of integers t in $[0, p)$ satisfying $-a_1 \equiv t(a_1 - a_0) \pmod{p}$. The only integers n with $n \equiv r \pmod{p-1}$ such that $p^2 | (B_n/n)$ are the n such that $n \equiv r + t(p-1) \pmod{\varphi(p^2)}$ and $t \in T_{r,p}$ (see [Joh74]). An algorithm to compute the sets $T_{r,p}$ can be found in [Joh74]. Wagstaff [Wag78] found that for every irregular pair (r, p) with $p < 125000$ the set $T_{r,p}$ has only one element. Buhler et al. [BCS] have calculated all irregular primes up to one million, but they have not calculated the sets $T_{r,p}$.

3 Statement of the mathematical results

The main result of this paper is Theorem 1. The computational results of this paper are derived from Theorem 1' and Lemma 10 below. Theorem 1' is used to show that k can not belong to certain congruence classes, and in combination with Lemma 10 it is used to investigate the divisibility of x.

Theorem 1
Let p^λ be a prime power > 1 and let r, $p-1\nmid r$, be any even integer in the interval $[2,\varphi(p^\lambda))$. Put $\varepsilon = \min(3,\lambda)$. For $i = 1,\cdots,\varepsilon$ let ϱ_i be the remainder of r on division by $\varphi(p^i)$. If $f_r(a;p) \not\equiv 0 \pmod{p^\lambda}$ for all $a \in [2, p^\lambda - 1]$ coprime with p and if there exists $1 \le i \le \varepsilon$ such that $p^i \nmid (B_{\varrho_i}/\varrho_i)$ (and $p^j | (B_{\varrho_j}/\varrho_j)$ for $j < i$), then the equation (1) has no solutions (x,k) with $k \ge \lambda$ and $k \equiv r \pmod{\varphi(p^\lambda)}$, and with the additional condition $k \equiv 1 \pmod{p}$ in the case $i = 3$, $\varrho_1 \not\equiv 2 \pmod{p-1}$ and $p \nmid B_{\varrho_1 - 2}$.

Remark 1. By Lemmas 2 and 3 below the condition $f_r(a;p) \not\equiv 0 \pmod{p^\lambda}$ for all $a \in [2, p^\lambda - 1]$ coprime with p, is equivalent with the condition $f_r(a;p) \not\equiv 0, -3a^r \pmod{p^\lambda}$ for all $a \in [2, (p^\lambda - 1)/2]$ coprime with p. This reduces the amount of numerical work needed to check this condition by a factor of about 2.
Remark 2. The condition $f_r(a;p) \not\equiv 0, -3a^r \pmod{p^\lambda}$ for all $a \in [2, (p^\lambda - 1)/2]$ coprime with p, can be weakened to $f_r(a;p) \not\equiv 0, -3a^r \pmod{p^\lambda}$ for all $a \in [2, (p^\lambda - 1)/2]$ coprime with p and such that $\mu a \not\equiv \pm 1 \pmod{p}$, where $\mu = 1$ or 2, for if $\mu a \equiv \pm 1 \pmod{p}$, it would follow that $p | \mu x \pm 1$ and hence, by Lemma 4 below, that $p - 1 | k$, which yields a contradiction with the assumption $p - 1 \nmid r$.
Remark 3. By Moser's result that k is even if (x,k) is a solution of (1), and the fact that $\varphi(p^\lambda)$ is even, we can restrict ourselves to the case where r is even.

Since in practice the condition $p^i \nmid (B_{\varrho_i}/\varrho_i)$ for $i \ge 2$ is only rarely not satisfied, and it requires arithmetic modulo p^i $(i \ge 2)$ to check whether or not $p^i | (B_{\varrho_i}/\varrho_i)$ (for $i = 2$ see [Joh74]), for numerical work (cf. Section 5) we will use Theorem 1 only for $i = 1$. In order to check whether $p \nmid (B_{\varrho_1}/\varrho_1)$ we use congruences due to Vandiver ([Van37] or [Wag78, (4)]) and Voronoi ([Wag78, (1)]). So we arrive at the following numerical variant of Theorem 1.

Theorem 1'
Let p^λ be a prime power with $\lambda \le C$ and let r, $p - 1 \nmid r$, be any even integer in the interval $[2,\varphi(p^\lambda))$. Let $\varrho = \varrho_1$ be the remainder of r on division by $p - 1$. If

$$f_r(a;p) \not\equiv 0, -3a^r \pmod{p^\lambda}$$

for all $a \in [2, (p^\lambda - 1)/2]$ coprime with p and (only in the case $p \ge 37$) if at least one of the three integers

$$S_1 := (2^{\varrho-1} + 1) \sum_{p/6 < s < p/5} s^{\varrho-1} - 2^{\varrho-1} \sum_{3p/10 < s < p/3} s^{\varrho-1},$$

$$S_2 := \sum_{p/6<s<p/4} s^{\varrho-1} \quad \text{or} \quad S_3 := \sum_{p/4<s<p/3} s^{\varrho-1}$$

is not divisible by p, then the equation (1) *has no solutions* (x,k) *with* $k \equiv r \pmod{\varphi(p^\lambda)}$.

Remark. Note that S_1 has about $p/15$ terms while S_2 and S_3 have about $p/12$ terms each, hence in order to check non-divisibility by p one should first test S_1 and next S_2 and S_3. The two sums which occur in S_1 are parts of the sums in S_2 and S_3, respectively.

If (r,p^λ) is a pair with r even, $p-1 \nmid r$, $r \in [2,\varphi(p^\lambda))$ such that $f_r(a;p) \not\equiv 0 \pmod{p^\lambda}$ for all $a \in [2,p^\lambda-1]$ coprime with p, we call (r,p^λ) a *potentially good pair*. If, furthermore, $\lambda \leq C$ and at least one of the integers S_1, S_2 and S_3 is not divisible by p, then (r,p^λ) is called a *good pair*. If (at least) one of the above conditions is not satisfied, then (r,p^λ) is said to be not a good pair. In this terminology Theorem 1' can be reformulated as follows:

'*If* (r,p^λ) *is a good pair, then the equation* (1) *has no solutions* (x,k) *with* $k \equiv r \pmod{\varphi(p^\lambda)}$'.

Note that if (r,p^λ) is not a good pair, this need not imply that there is a solution with $k \equiv r \pmod{\varphi(p^\lambda)}$. Using Remark 1 after Theorem 1, and Lemma 2 below it follows that if (r,p^λ) is a good pair, then for every integer k with $\lambda < k \leq C$ and every integer $i \geq 0$ such that $r + i\varphi(p^\lambda) < \varphi(p^k)$, the pair $(r+i\varphi(p^\lambda), p^k)$ is also good (cf. Table 1).

To prove that k must be divisible by many different prime factors (which will be done in Section 5), we use the following result repeatedly.

Theorem 2
Let p be a prime and let $\{q_1, q_2, \cdots, q_{p-1}\}$ be a set of (not necessarily distinct) odd prime powers such that $p|\varphi(q_i)$ for $i = 1, \cdots, p-1$. Let M by any positive integer such that $\mathrm{lcm}(\varphi(q_1), \cdots, \varphi(q_{p-1})) \mid pM$, and let $\{r_1, r_2, \cdots, r_{p-1}\}$ denote the set of numbers such that for $i = 1, \cdots, p-1$, $r_i \equiv iM \pmod{\varphi(q_i)}$ and $0 \leq r_i < \varphi(q_i)$. Then, if (r_i, q_i) is a good pair for $i = 1, \cdots, p-1$, all solutions k of (1) *which are multiples of M are also multiples of pM.*

Remark 1. In fact, this theorem also holds if p is a *composite* number, but in our computations we only have used it for p a prime.
Remark 2. If p is a prime dividing M put $\mu = \mathrm{ord}_p(M)$. If $p^{\mu+1} \nmid \varphi(q_i)$ it follows that $r_i \equiv 0 \pmod{\varphi(q_i)}$ for $i = 1, \cdots, p-1$, so that none of the (r_i, q_i) is a good pair. Notice that we should require that $p^{\mu+1} | \varphi(q_i)$ in order that $r_i \not\equiv 0 \pmod{\varphi(q_i)}$ for $i = 1, \cdots, p-1$.
Corollary (Theorem 2 for $q_i = q$, $1 \leq i \leq p-1$ with q a prime)
Let p and q be primes with q regular and $q \equiv 1 \pmod{p}$, and

$$\sum_{j=1}^{a-1} j^{i\frac{q-1}{p}} \not\equiv a^{i\frac{q-1}{p}}, -2a^{i\frac{q-1}{p}} \pmod{q}$$

for $a = 2, \cdots, (q-1)/2$ and $i = 1, \cdots, p-1$. Then all solutions k of (1) which are multiples of $(q-1)/p$ are multiples of $q-1$.

Since $a^{(q-1)/2} \equiv (\frac{a}{q}) \pmod q$ (as is well-known), where $(\frac{a}{q})$ denotes the Legendre symbol, the condition of the corollary becomes for $p = 2$ that

$$\sum_{j=1}^{a-1}(\frac{j}{q}) \not\equiv (\frac{a}{q}), -2(\frac{a}{q}) \pmod q$$

for $a = 2, \cdots, (q-1)/2$. Assume that $q \geq 23$. Taking $a = 2$, 4, 6, 8 it follows that $-1 = (\frac{2}{q}) = (\frac{3}{q}) = (\frac{5}{q}) = -(\frac{7}{q})$. Taking $a = 10$ it follows that for no $q \geq 23$ the condition of the corollary can be satisfied. Therefore the corollary does not work for $p = 2$ and $q \geq 23$. This argument can be easily extended to show that for every prime $q \geq 23$ and for every $\lambda \geq 1$, $(q^{\lambda-1}(q-1)/2, q^\lambda)$ is not a good pair. From this it can be deduced that by using Theorem 2 alone, we can not prove that $16 \mid k$.

It appears that $((q-1)/3, q)$ is not a good pair for many primes q with $q \equiv 1 \pmod 3$. This makes it difficult to apply Theorem 2 for $p = 3$ and so the cases $p = 2$ and $p = 3$ have to be dealt with by another method. Theorem 3 provides such a method.

Theorem 3
For $1 \leq i \leq s$, let a, ν_i be integers ≥ 1 and let p, q_i be primes such that $p^{a+\nu_i} \parallel q_i - 1$, and put

$$R(i) = \{1 \leq j \leq p^{\nu_i} \mid p \text{ is coprime with } j \text{ and } \left(j\frac{q_i-1}{p^{\nu_i}}, q_i\right) \text{ is not a good pair}\}.$$

Write

$$\begin{aligned} R \;=\; & \{(j_1, ..., j_s) \in R(1) \times \cdots \times R(s) \mid \\ & \gcd(q_m - 1, q_n - 1) \text{ divides } \left(j_m\frac{q_m-1}{p^{\nu_m}} - j_n\frac{q_n-1}{p^{\nu_n}}\right) \\ & \text{for every } 1 \leq m < n \leq s\}. \end{aligned}$$

Suppose that (x, k) is a solution of (1) with

$$\operatorname{lcm}\left(\frac{q_1-1}{p^{\nu_1}}, \cdots, \frac{q_s-1}{p^{\nu_s}}\right) \mid k.$$

Then we have $p^{a+1} \mid k$ provided that the set R is empty.

Corollary. Let a, ν be integers ≥ 1 and let q be a prime such that $p^{a+\nu} \parallel q - 1$ and $(j(q-1)/p^\nu, q)$ is a good pair for every $1 \leq j \leq p^\nu$ with p coprime with j. Then if (x, k) is a solution of (1) with $(q-1)/p^\nu \mid k$, it follows that $(q-1)/p^{\nu-1} \mid k$.

Let M, a and b be arbitrary integers with $0 < a < b$. Assume that (x, k) is a solution of (1) and that M is a divisor of k. For Theorem 5 below it is convenient if one can

exclude that $k \equiv a \pmod{b}$. We now present a result which can be used to achieve this in some cases.

Put $g = \gcd(b, M)$ and $G = b/g$. For q a prime let e_q denote the exponent of q in M, and a_q the exponent of q in G. Put $H = \prod_q q^{e_q}$, where the product runs over those primes q for which $a_q \geq 1$. If $g \nmid a$ then, by using Lemma 9 below, we can exclude that $k \equiv a \pmod{b}$, so now we assume that $g \mid a$. Put $a' = a/H$ (notice that a' is an integer).

Theorem 4
Let M, a and b be arbitrary integers with $0 < a < b$ and let g, G, H, a' be defined as above. Suppose $g \mid a$ and there exists a prime p' of the form $p' = 1 + g_1 GH$, $\gcd(g_1, G) = 1$ and $g_1 \mid M$ such that (Htg_1, p') is a good pair, where t, $0 \leq t < G$, satisfies $t \equiv a'/g_1 \pmod{G}$, then there are no solutions (x, k) of (1) with $M \mid k$ and $k \equiv a \pmod{b}$.

Remark. We have $Htg_1 \not\equiv 0 \pmod{p' - 1}$.
Proof. It suffices to show that $t \not\equiv 0 \pmod{G}$. So suppose $t \equiv 0 \pmod{G}$. Then $a' \equiv 0 \pmod{G}$ and so $G \mid a$. Since $g \mid a$ (by assumption) and $\mathrm{lcm}(g, G) = b$, it follows that $b \mid a$. Contradiction. □

Suppose that (x, k) is a solution of (1). Our strategy in proving that x has no small prime factors is to prove first, by using Theorem 2, that $M|k$ for a (preferably large) integer M and then to use the following result.

Theorem 5
Suppose that (x, k) is a solution of (1) and $M|k$ for some integer M. Let p be a prime and put $g = \gcd(p - 1, M)$. If p or (in case p is irregular) the irregular pair(s) (r, p) corresponding to p satisfy one of the following conditions:

a) *p is regular*

b) *p is irregular and $p - 1 \mid M$*

c) *p is irregular and $g \nmid r$*

d) *p is irregular, $g \mid r$ and by* Theorem 4 *it can be deduced that $k \not\equiv r \pmod{p - 1}$,*

then p can not divide x.

Theorem 6
If the number C_1 is such that for all irregular pairs (r, p) with $p \leq C_1$, $p^2 \nmid (B_r/r)$, then there is no solution (x, k) of (1) with x a prime $\leq C_1$.

Remark 1. By Theorems 5a and 5b it follows that furthermore x should be irregular and $x - 1 \nmid k$.
Remark 2. By the work of Wagstaff [Wag78] it follows that we can take $C_1 = 125000$. It has been conjectured that the largest possible C_1 is finite (see [Rib79, p.22]).

4 Proof of the Theorems

4.1 Lemmas

We state and prove some lemmas which will be used in the proofs of the theorems.

Lemma 1
Let m be a positive integer. Then for every integer s we have

$$\mathrm{ord}_p\left(\frac{x^{m-s}}{m!}\right) > (m-s)\mathrm{ord}_p x - \frac{m}{p-1}.$$

Proof. The proof follows at once by using the well-known fact that for $m \geq 1$ we have

$$\mathrm{ord}_p(m!) = \frac{m - A(m,p)}{p-1},$$

where $A(m,p) \geq 1$ denotes the sum of the digits of m written in the base p. □

The next lemma is well-known (in the case $\lambda = 1$ see, e.g., [IR90, p. 235]).

Lemma 2
If p is odd and $p-1 \nmid k$, then $S_k(p^\lambda) \equiv 0 \pmod{p^\lambda}$ for every $\lambda \geq 1$.

Proof. Notice that modulo p^λ, $S_k(p^\lambda)$ is unchanged by multiplication with g^k, where g is any primitive root modulo p (which exists for every odd prime). Since $p-1 \nmid k$ by assumption, $g^k \not\equiv 1 \pmod{p}$. Together with $p^\lambda \mid (g^k-1)S_k(p^\lambda)$ it follows from this that $S_k(p^\lambda) \equiv 0 \pmod{p^\lambda}$. □

Lemma 3
For even k, and for a prime p and integers a, λ satisfying $1 \leq \lambda \leq k$, $1 \leq a \leq p^\lambda - 1$, $p \nmid a$ we have

$$f_k(p^\lambda - a; p) \equiv S_k(p^\lambda) - f_k(a;p) - 3a^k \pmod{p^\lambda}.$$

Proof. For $a = 1$ and $a = p^\lambda - 1$ the result holds true because of the definition of $f_k(1;p)$ and since $f_k(p^\lambda - 1; p) \equiv S_k(p^\lambda) - 2 \pmod{p^\lambda}$. We have, using that k is even (in the sums below the numbers m only run through values with $p \nmid m$),

$$\begin{aligned} f_k(p^\lambda - a; p) &\equiv \sum_{1 \leq m \leq p^\lambda - a - 1} m^k - (p^\lambda - a)^k \\ &\equiv \sum_{a+1 \leq m \leq p^\lambda - 1} (p^\lambda - m)^k - (p^\lambda - a)^k \end{aligned}$$

$$\equiv \sum_{1\le m\le p^\lambda-1} m^k - \sum_{1\le m\le a-1} m^k - 2a^k$$
$$\equiv S_k(p^\lambda) - f_k(a;p) - 3a^k \pmod{p^\lambda}.$$

Hence, the lemma follows immediately. □

Lemma 4 [Mos53]
Suppose (x,k) *is a solution of* (1). *Then* $p|x-1$, $p|x+1$, $p|2x-1$ *or* $p|2x+1$ *implies* $p-1|k$. □

For $k\ge 1$ put $\alpha(k) = \sqrt[k]{2}/(\sqrt[k]{2}-1)$.

Lemma 5
Suppose (x,k) *is a solution of* (1). *Then* $x > k$.

Proof. In [Lun75] it is proved that $x > \alpha(k)$, if (x,k) is a solution of (1). Using the inequality $2 < (1+\frac{1}{m-1})^m$ for every $m \ge 2$ (which is easy to show), it follows that $k < \alpha(k) < x$. □

Lemma 6
Suppose (x,k) *is a solution of* (1) *with even* k. *Then* $x \le 3k/2+1$.

Proof. We show that $x < 3(k+1)/2$. Put $t_i = \binom{k+1}{2i} B_{2i} x^{k-2i}/(k+1)$ for $i = 1,\cdots,k/2$. Using (1), P5, P4 and P1 we see that it suffices to prove that $\sum_{i=1}^{k/2} t_i > 0$. By P1 the signs of the t_i alternate and $t_1 > 0$. So the lemma follows if we show that $|t_{i+1}/t_i| < 1$ for $i = 1,\cdots,k/2-1$. Indeed, by P6 and Lemma 5 it follows that for $i = 1,\cdots,k/2-1$

$$\left|\frac{t_{i+1}}{t_i}\right| = \frac{A_{2i+2}\pi^2(k-2i+1)(k-2i)}{6A_{2i}x^2(2i+1)(2i+2)} < \frac{k^2}{24x^2}.$$

□

Lemma 7
Suppose (x,k) *is a solution of* (1). *Then* $k > C$.

Proof. The proof follows by Lemma 6 on using the lower bound C^2 for x, which is proved in [ZK83]. □

Put $P_{k+1}(x) = B_{k+1}(x) - B_{k+1} - (k+1)x^k$. By P5 we can rewrite the equation (1) in the form $P_{k+1}(x) = 0$.

Lemma 8
Let p *be an odd prime number and let* k *be an even integer* ≥ 6. *If* $p|x$ *then we have*

$$(2)\qquad \operatorname{ord}_p\left(\frac{P_{k+1}(x)}{(k+1)kx} - \frac{B_k}{k} - x^2\frac{k-1}{6}B_{k-2}\right) \ge \begin{cases} 2\operatorname{ord}_p x + 1, & \text{if } p \ne 5,\\ 2\operatorname{ord}_p x, & \text{if } p = 5.\end{cases}$$

Proof. In virtue of P4 and P1 for any (x,k) we get

$$\frac{P_{k+1}(x)}{(k+1)kx} - \frac{B_k}{k} - x^2\frac{k-1}{6}B_{k-2} = \tag{3}$$

$$= x^2\left[\frac{x^{k-2}}{(k+1)k} - \frac{3x^{k-3}}{2k} + \sum_{i=1}^{k/2-2}\binom{k+1}{2i}B_{2i}\frac{x^{k-2i-2}}{(k+1)k}\right].$$

Assume that $p|x$. Then it is easy to see that for $k \geq 6$ we have

$$\mathrm{ord}_p\left(\frac{x^{k-2}}{(k+1)k} - \frac{3x^{k-3}}{2k}\right) \geq 1.$$

Furthermore, the assumption $p|x$ implies $\mathrm{ord}_p(x^{m-3}/m!) \geq 2$ in the cases $p \geq 5$ and $m \geq 6$ or $p = 3$ and $m \geq 8$, since by Lemma 1 with $s = 3$ we have

$$\mathrm{ord}_p(\frac{x^{m-3}}{m!}) > (m-3)\mathrm{ord}_p x - \frac{m}{p-1} \geq m - 3 - \frac{m}{p-1} \geq 1.$$

Using this and P2 it follows that for $1 \leq i \leq k/2-3$ if $p \geq 5$ and for $1 \leq i \leq k/2-4$ if $p = 3$, we have

$$\mathrm{ord}_p\left(\binom{k+1}{2i}B_{2i}\frac{x^{k-2i-2}}{(k+1)k}\right) = \mathrm{ord}_p\left(\frac{(k-1)!}{(2i)!}B_{2i}\frac{x^{k-2i-2}}{(k+1-2i)!}\right) \geq 1.$$

For $k \geq 6$, $p \geq 3$ and $p \neq 5$ we have

$$\mathrm{ord}_p\left(\binom{k+1}{k-4}B_{k-4}\frac{x^2}{(k+1)k}\right) \geq 1.$$

For $p = 5$ this order is not negative and for $p = 3$ we have

$$\mathrm{ord}_3\left(\binom{k+1}{k-6}B_{k-6}\frac{x^4}{(k+1)k}\right) \geq 1.$$

On using (3) the proof becomes complete. □

Lemma 9 [Sha83, Theorem 5.4.2]
Let $s, a_1, \cdots, a_s, k_1, \cdots, k_s$ be natural numbers with $s \geq 2$. The system of simultaneous congruences $x \equiv a_i \pmod{k_i}$, $i = 1, \cdots, s$, has a solution if and only if $\gcd(k_i, k_j) \mid a_i - a_j$ for every $1 \leq i < j \leq s$. □

Lemma 10
Suppose that (x,k) is a solution of (1) with k even and that p is a prime dividing x. Then

a) $k \not\equiv 0, 2 \pmod{p-1}$.

b) *p is an irregular prime.*

c) $\mathrm{ord}_p(\frac{B_k}{k}) \geq 2\,\mathrm{ord}_p x$.

d) $k \equiv r_i \pmod{p-1}$, *for some* $i \in \{1, \cdots, i(p)\}$, *where* (r_i, p) *denotes the* i*th irregular pair and* $i(p)$ *the index of irregularity.*

e) $k \equiv r_i + t(p-1) \pmod{p(p-1)}$, *for some* $i \in \{1, \cdots, i(p)\}$ *and* $t \in T_{r,p}$, *where the set* $T_{r,p}$ *is defined in Section 2.*

Proof. Assume that (x, k) is a solution of (1) with $p|x$ and k is even. Then by Lemma 7 we have $k \geq 6$. By Moser's results [Mos53] we have $x \equiv 3 \pmod 4$ and hence p is odd. So, by Lemma 8 we get

$$\mathrm{ord}_p\left(\frac{B_k}{k} + x^2\frac{k-1}{6}B_{k-2}\right) \geq 2\,\mathrm{ord}_p x. \tag{4}$$

Therefore, by P2 and $\mathrm{ord}_p(x^2\frac{k-1}{6}B_{k-2}) \geq 0$, $p-1|k$ implies $\mathrm{ord}_p x < 0$. Contradiction. If $k \equiv 2 \pmod{p-1}$, then by P2, P3 and P1 we have $B_k/k \equiv B_2/2 \equiv 1/12 \not\equiv 0 \pmod p$ and we obtain $\mathrm{ord}_p(B_k/k) = 0$. Therefore, by (4) and $\mathrm{ord}_p(x^2\frac{k-1}{6}B_{k-2}) \geq 1$, we get $\mathrm{ord}_p x \leq 0$. Contradiction. Part b) immediately follows from (4), P2 and P3. Part c) is a consequence of (4), Part a) and P2. Parts d) and e) are consequences of Part c) and the work of Johnson [Joh74]. □

4.2 Proofs of the Theorems

Proof of Theorem 1. Let p^λ be a prime power and r, ϱ_i $(i = 1, \cdots, \varepsilon)$ be integers satisfying the assumptions of the theorem. Suppose (x, k) is a solution of (1) with $k \geq \lambda$, $k \equiv r \pmod{\varphi(p^\lambda)}$. The proof falls naturally in the case where $p|x$ and the case where $p\nmid x$.
First assume that $p|x$. If $\lambda \geq 1$ and $p\nmid(B_{\varrho_1}/\varrho_1)$, then $p\nmid(B_k/k)$ by P3. This yields a contradiction with Lemma 10c). If $\lambda \geq 2$ and $p^2\nmid(B_{\varrho_2}/\varrho_2)$ then $p^2\nmid(B_k/k)$ by P3 again. This contradicts Lemma 10c). By Lemma 7 it follows that $k \geq 6$. If $\lambda \geq 3$, $p^3\nmid(B_{\varrho_3}/\varrho_3)$ and $p|B_{\varrho_1-2}$, then we have a contradiction with (2) by P3. If $\lambda \geq 3$, $p^3\nmid(B_{\varrho_3}/\varrho_3)$, $p\nmid B_{\varrho_1-2}$ and $p \equiv 1 \pmod k$, we also have a contradiction with (2) by P3 again. So $p\nmid x$ and x can be written in the form $b + \tau p^\lambda$ with $1 \leq b \leq p^\lambda$ and b coprime with p. By Lemma 4 we can assume that $b \geq 2$. Since $n \equiv m \pmod{p^\lambda}$ implies $n^k \equiv m^k \pmod{p^\lambda}$ and $k \geq \lambda$ (by assumption), we find that $f_k(x; p) \equiv \tau S_k(p^\lambda) + f_k(b; p) \pmod{p^\lambda}$. Hence, by Lemma 2, $f_k(x; p) \equiv f_k(b; p) \pmod{p^\lambda}$. Since for $p\nmid n$ we have $n^k \equiv n^r \pmod{p^\lambda}$ by Euler's extension of Fermat's little theorem, it follows that $f_k(x; p) \equiv f_r(b; p) \pmod{p^\lambda}$. Put $a = b$ if $b \leq (p^\lambda - 1)/2$ and $a = p^\lambda - b$ otherwise. Since $f_k(x; p) \equiv 0 \pmod{p^\lambda}$ it follows from $f_k(x; p) \equiv f_r(b; p) \pmod{p^\lambda}$ and Lemma 3 that either $f_r(a; p) \equiv 0$ or $-3a^r \pmod{p^\lambda}$ with $a \leq (p^\lambda - 1)/2$. We get a contradiction with the assumptions and this shows that there are no solutions of (1) with $k \equiv r \pmod{\varphi(p^\lambda)}$ and $k \geq \lambda$. □

Proof of Theorem 1'. Put $c(x,y,z,m) = x^{p-2m} + y^{p-2m} - z^{p-2m} - 1$. The result follows from Theorem 1, Lemma 7, P3, the Vandiver congruence

$$c(2,5,6,m)\frac{B_{2m}}{4m} \equiv (2^{2m-1}+1) \sum_{p/6<s<p/5} s^{2m-1} - 2^{2m-1} \sum_{3p/10<s<p/3} s^{2m-1} \pmod{p}$$

([Van37, p. 574]) which holds for $p \geq 11$, the congruences

$$c(3,4,6,m)\frac{B_{2m}}{4m} \equiv \sum_{p/6<s<p/4} s^{2m-1} \pmod{p},$$

$$c(2,3,4,m)\frac{B_{2m}}{4m} \equiv \sum_{p/4<s<p/3} s^{2m-1} \pmod{p},$$

which are well-known consequences of Voronoi's congruence [Wag78] and hold for $p \geq 11$ too, and Fermat's little theorem. □

Proof of Theorem 2. Suppose the hypothesis of the theorem is satisfied. Suppose furthermore that (x,k) is a solution of (1) with $M|k$. We have to show that $pM|k$. To this end it suffices to show that $k \not\equiv iM \pmod{pM}$ for $i = 1, \cdots, p-1$. By the definition of r_i $(i = 1, \cdots, p-1)$ and M it suffices to show that $k \not\equiv r_i \pmod{\varphi(q_i)}$ for $i = 1, \cdots, p-1$. But since (r_i, q_i) is a good pair for $i = 1, \cdots, p-1$ (by assumption), this follows on applying Theorem 1'. □

Proof of Theorem 3. Suppose the hypothesis is satisfied. Then $p^a \mid k$. Assume that $p^{a+1} \nmid k$. Together with the assumption

$$\operatorname{lcm}\left(\frac{q_1-1}{p^{\nu_1}}, \cdots, \frac{q_m-1}{p^{\nu_m}}\right) \mid k$$

it follows that $k \equiv j_i(q_i-1)/p^{\nu_i} \pmod{q_i-1}$ for some j_i in $[1, p^{\nu_i}]$ coprime to p for $1 \leq i \leq s$. Since whenever $(j_i(q_i-1)/p^{\nu_i}, q_i)$ is a good pair $k \not\equiv j_i(q_i-1)/p^{\nu_i} \pmod{q_i-1}$ by Theorem 1', it follows that $j_i \in R(i)$. Consequently we must have that $k \equiv j_i(q_i-1)/p^{\nu_i} \pmod{q_i-1}$ for some tuple $(j_1, \cdots, j_s) \in R(1) \times \cdots \times R(s)$. By Lemma 9 $(j_1, \cdots, j_s)$ must be in R. Since R is empty (by assumption), the assumption $p^{a+1} \nmid k$ leads to a contradiction. Therefore $p^{a+1} \mid k$. □

Proof of Theorem 4. Suppose (x,k) is a solution of (1) with $M \mid k$ and $k \equiv a \pmod{b}$. Note that $GH \mid b$. So in particular $k \equiv a \pmod{GH}$. Since $\gcd(g_1, G) = 1$ implies $\gcd(g_1, H) = 1$, it follows from $H \mid M$ and $g_1 \mid M$ that $Hg_1 \mid M$ and so $k \equiv 0 \pmod{Hg_1}$. Note that there exist integers u and v such that $a + uGH = vHg_1$. Since $H \mid a$ this is equivalent with $a' + uG = vg_1$ and so $v \equiv a'/g_1 \pmod{G}$. It follows that $k \equiv Htg_1 \pmod{p'-1}$. Since (Htg_1, p') is a good pair (by assumption), Theorem 1' yields $k \not\equiv Htg_1$

(mod $p'-1$). So the conclusion of the theorem follows. □

Proof of Theorem 5. Parts a) and b) are consequences of respectively Lemma 10b) and Lemma 10a). To prove Part c) assume $p|x$. By Lemma 10d) it follows that $k \equiv r \pmod{p-1}$, where (r,p) is some irregular pair. Since $g \mid k$ and $g \mid p-1$ we must have $g \mid r$. This contradiction with the assumption $g \nmid r$ shows that $p \nmid x$. On using Part c) the proof of Part d) is obvious. □

Proof of Theorem 6. Suppose that (x,k) is a solution of (1) with x a prime $\leq C_1$, where C_1 satisfies the hypothesis of the theorem. Then by Lemma 10d) we have $k \equiv r \pmod{x-1}$, with (r,x) an irregular pair. Notice that $r \geq 2$. By Lemma 5 it then follows that $k = r$. Then $p^2|(B_r/r)$ by Lemma 10c). Contradiction. □

5 Numerical results

We have carried out several numerical experiments with the theorems of Section 3:

5.1. Computation of all the good pairs (r, p^λ) (defined after Theorem 1'), for the even numbers $r \in [2, p^{\lambda-1}(p-1))$, for all the prime powers $p^\lambda \in [5, 997]$, by using Theorem 1'.

5.2. Suppose we know a positive integer M such that if (x, k) is a solution of (1) then $M|k$. We find a prime $p \geq 5$ such that $pM|k$, by finding sets $\{q_1, q_2, \cdots, q_{p-1}\}$ and $\{r_1, r_2, \cdots, r_{q-1}\}$ as described in Theorem 2. This is repeated with M replaced by pM in order to find as many as possible different prime power divisors of k. Next, the same is done for the primes 2 and 3, by means of Theorem 3.

5.3. Finding primes p which can *not* divide x if (x, k) is a solution of (1), by means of Theorem 5 (and Theorem 4).

All computations have been carried out on an SGI workstation. The programs were written in Fortran 77.

5.1 Computation of good pairs

Application of Theorem 2 requires the determination of good pairs, i.e., pairs (r, p^λ) which satisfy the conditions of Theorem 1'. As a first step to the computations described in Section 5.2, we have computed *all* the good pairs (r, p^λ) for the prime powers p^λ which satisfy $5 \leq p^\lambda < 1000$. In Table 1 we list a selection of the results, namely the good pairs (r, p^λ) with $5 \leq p^\lambda \leq 125$. The complete table is available from the second author upon request. Computing time was about 220 CPU seconds. Only in 30 cases a *potentially* good pair (r, p) was found, which was not good. These 30 pairs appeared to be irregular. They are listed in Table 2. The total number of irregular pairs (r, p) with $3 \leq p < 1000$ is 81 [Joh73]. The good pairs (r, p^λ) we actually use in the sequel, are always of the form (r, p), that is we only use congruences modulo primes.

Assuming that the values of $f_r(a; p)$ are randomly distributed modulo p, the probability that (r, p) is potentially good is about $(1 - 2p^{-\lambda})^{(p^\lambda - 1)/2} \approx e^{-1} = 0.3679$ (rounded to four decimals). This means that for each $\lambda \geq 1$ we can expect the quantity

$$G_\lambda(x) := \frac{\sum_{5 \leq p \leq x} \text{card}\{r | (r, p^\lambda) \text{ is a good pair }\}}{\sum_{5 \leq p \leq x} p^{\lambda-1}(p-3)/2}$$

to approximate e^{-1} as $x \to \infty$ (where we neglect the small probability that a potentially good pair is not good). We found $G_1(100) = 0.4016$, $G_1(500) = 0.3648$ and $G_1(1000) = 0.3646$.

5.2 Computations with Theorems 2 and 3 in order to find prime power divisors of k

Let (x, k) be a solution of (1) and suppose we know that $M|k$ for some $M > 1$.

If we can find a prime p such that (1) has *no* solution satisfying one of the $p-1$ congruences

$$k \equiv iM \pmod{pM}, \quad i = 1, \cdots, p-1, \tag{5}$$

then it follows that $pM|k$. Repeating this procedure with M replaced by pM would enable us to find more and more primes, and prime powers, which divide k.

Such a prime p can be found as follows. Let $p^\mu \parallel M$ for some nonnegative integer μ and let q be a prime such that $p^{\mu+1}|q-1$ *and* $q-1|pM$. Take $i \in \{1, \cdots, p-1\}$ and let r_i be the remainder of iM on division by $q-1$. It is easily seen that $r_i \neq 0$. If the pair (r_i, q) is a good pair then we can conclude from Theorem 1' that (1) has no solution with $k \equiv r_i \equiv iM \pmod{q-1}$. This implies that (1) has no solution for $k \equiv iM \pmod{pM}$ since $q-1|pM$. In view of the experiments mentioned in Section 5.1 we may expect to eliminate about $1/e$ of the $p-1$ residue classes (5) with q. By using more of such q-primes we can hope to eliminate *all* the residue classes of (5). If we succeed in doing so, we have found sets $\{q_1, \cdots, q_{p-1}\}$ and $\{r_1, \cdots, r_{p-1}\}$ which satisfy the conditions of Theorem 2 and we can conclude that $pM \mid k$. One possible reason of failure is that the number of available q-primes is *finite* because of the condition $q-1|pM$.

From Moser [Mos53] we know that we may start with $M = 2$. It is not difficult to extend this M to 24 by using results from Table 1 as follows. Since $(2, 5)$ is a good pair it follows that $k \not\equiv 2 \bmod 4$, so that $k \equiv 0 \bmod 4$. Since $(2, 7)$ and $(4, 7)$ are good pairs, it follows that $k \equiv 0 \bmod 6$. From $4 \mid k$ and the fact that $(4, 17)$ and $(12, 17)$ are good pairs, it follows that $k \equiv 0 \bmod 8$.

We have written a computer program which starts from $M = 2^3 \cdot 3$ as a known divisor of k and tries to prove that $pM \mid k$ for a given prime p which does *not* divide M, by finding sets $\{q_1, \cdots, q_{p-1}\}$ and $\{r_1, \cdots, r_{p-1}\}$ (called q-sets and r-sets below) which satisfy the conditions of Theorem 2. It turned out to be relatively simple to extend in this way the value of $M = 24$ with the prime factors 5, 7, 11, ..., 199, in this order. In Table 3 we give the q- and r-sets for $p = 5, 7, 11, 13, 17, 19$. For the addition of the prime p to M we used the value $M = M_p := 2^3 \prod_{3 \le q < p,\ q \text{ prime}} q$. It should be noticed that in one case ($p = 7$) we needed the *largest* available q-prime 421 to complete the proof.

For the primes $23, \cdots, 199$, Table 4 only presents the *different* values of q which occur in the q-sets (in order to save some space), and not the q- and r- sets themselves.

Example. Consider the case $p = 23$. Theorem 2 is applied with $M = M_{23} = 2^3 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. The program generates primes of the form $q = 46t + 1$ for which $\frac{q-1}{23} \mid M$. The first is $q = 47$. We have $M \bmod 46 = 14$ and the program checks which of the pairs $(14i \bmod 46, 47)$, $i = 1, \cdots, 22$, are good. This is found to be the case for $i = 1, 2, 10, 11, 12, 13, 14, 15, 17, 18, 19, 22$ (cf. Table 1). It follows that $q_i = 47$ for these 12 values of i and that $r_i = 14, 28, 2, 16, 30, 44, 12, 26, 8, 22, 36, 32$, respectively, for these 12 values of i. The next q-prime is 139. We have $M \bmod 138 = 60$ and, by checking the

remaining values of i, it is found that $(60i \bmod 138, 139)$ is a good pair for $i = 8, 9, 16$. It follows that $q_8 = q_9 = q_{16} = 139$ and that $r_8 = 66$, $r_9 = 126$, and $r_{16} = 132$. Continuing in this way, the remaining residue classes are eliminated with $q = 277$ $(i = 4, 20)$, $q = 461$ $(i = 5, 6, 7, 21)$, and $q = 691$ $(i = 3)$. □

With the knowledge that $2^3 \cdot 3 \cdot 5 \cdots 199 \mid k$ we next increased the powers of the primes ≥ 5 and ≤ 19 in k with Theorem 2. Table 5 is similar to Table 3, but now the primes p to be added to M are already in M at least to the first power. Moreover, Table 5 gives the values of M used for each addition of p. For $p = 13, 17, 19$ we only give the different primes in the q-sets. It follows that $5^4 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \mid k$. Computing time was about 1000 CPU seconds. We expect it to be easy to extend the set of prime power divisors of k, if more computing time would be spent.

In order to increase the exponents of 2 and 3 in k, we used Theorem 3 (and, in one case, Theorem 4) to prove that $2^8 \mid k$ and $3^5 \mid k$. For the proofs that $2^7 \mid k$ and $2^8 \mid k$ we could use the corollary to Theorem 3 with $p = 2$, $\nu = 3$ and $a = 6$ respectively $a = 7$. The details of our use of Theorem 3 are given in Table 6. M' in Table 6 denotes the number $\mathrm{lcm}((q_1 - 1)/p^{\nu_1}, \cdots, (q_s - 1)/p^{\nu_s})$. In one case, namely in the proof that $2^6 \mid k$, we eliminated $k \equiv 2080 \bmod 3328$, where $2080 = 5(q_1 - 1)/8$, by using Theorem 4 with $M = 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdots 199$, $a = 2080 = 5 \cdot 2^5 \cdot 13$ and $b = q_1 - 1 = 3328 = 2^8 \cdot 13$. The good pair (Htg_1, p') we found is $(16416, 43777)$, with $H = 2^5$, $t = 3$, $g_1 = 3^2 \cdot 19$, $p' = 1 + g_1 GH$, and $G = 2^3$.

Summarizing this section, we have shown that if (x, k) is a solution of (1), then

$$2^8 3^5 5^4 7^3 11^2 13^2 17^2 19^2 23 \cdots 199 \mid k$$

where the three dots represent the product of the primes between 23 and 199. In particular, $\mathrm{lcm}(1, \cdots, 200) \mid k$.

5.3 Computations with Theorem 5 (and Theorem 4) in order to find primes which cannot divide x

We have written a program which for a given irregular pair (r, p) checks the conditions b), c), and d) of Theorem 5 with $M = 2^8 3^5 5^4 7^3 11^2 13^2 17^2 19^2 23 \cdots 199$, as computed in the previous section. Conditions b) and c) are easy to check. Condition d) was checked by means of Theorem 4 with $a = r$ and $b = p - 1$. We ran our program for the first 500 irregular primes (the 500-th being 10061), 382 of them having index 1, 102 having index 2, and 16 having index 3, so that these correspond to 634 irregular *pairs*. We found 424 pairs satisfying condition b), 125 satisfying condition c), and 85 satisfying condition d). In Tables 7-9 we list the latter 85 pairs and the corresponding good sieving pairs (Htg_1, p') for which Theorem 4 holds (in all 85 cases, $H = 1$). In order to find these 85 good pairs, our program had to generate a total of 260 primes p' in Theorem 4, an average of about 3 per good pair. The largest sieving prime used was $p' = 293177$, for the irregular pair $(2672, 5639)$. Computer time used was about 340 CPU seconds.

In conclusion, we have shown that if (x, k) is a solution of (1), then x is not divisible by any irregular prime < 10000.

p^λ	r
5	2
7	2 4
11	2 6
13	2 4 8 10
17	2 4 6 12
19	4 10 16
23	4 8 14 16
29	2 10 16 26
31	2 4 6 8 14 16 18 22 24 28
37	6 10 22 26 28 30
41	12 14 18 26 34 36
43	2 4 8 18 24 26 40
47	2 8 12 14 16 22 26 28 30 32 36 44
53	2 6 8 14 22 28 30 34 36 40 44 46
59	2 4 6 8 10 12 16 18 20 30 32 34 36 46 54 56
61	6 8 22 26 28 34 38 46 48 52 58
67	6 8 10 12 14 16 18 24 50 52 54
71	4 6 8 10 18 22 24 30 38 48 52 54 56
73	8 10 26 30 32 34 38 46 52 62 64 66 70
79	8 12 24 28 30 32 36 46 58 62 66 70
83	2 8 10 18 22 26 30 34 36 50 52 66 68 70 74 80
89	18 24 38 40 42 48 56 58 68 72 74 76 84 86
97	8 14 16 20 26 28 36 38 46 54 68 76 78 80 88
101	2 12 16 20 26 28 30 32 38 40 44 60 70 72 76 88 98
103	2 6 8 12 14 30 40 46 48 52 60 72 78 86 96 98
107	2 4 8 12 14 18 38 54 56 62 66 68 74 80 86 88 94 96 100
109	6 12 14 16 20 30 38 44 52 58 60 62 64 66 70 80 84 86 88 96 98 104 106
113	2 16 18 20 24 32 38 40 46 48 50 52 60 62 66 72 76 80 82 86 88 90 96 102 106 108 110
5^2	2 6 10 14 18
7^2	2 4 8 10 14 16 20 22 26 28 32 34 38 40
11^2	2 6 12 16 22 26 32 36 42 44 46 52 56 62 66 72 76 82 86 88 92 96 102 106
5^3	2 6 10 14 18 22 26 30 34 38 42 46 50 54 58 62 66 70 74 78 82 86 90 94 98

Table 1: Good pairs (r, p^λ) for the prime powers p^λ with $5 \leq p^\lambda \leq 125$

p	r
103	24
131	22
257	164
347	280
353	186, 300
401	382
409	126
463	130
467	94, 194
491	292, 336, 338
547	270
557	222
587	90
617	20, 174
619	428
653	48
659	224
673	502
691	12
751	290
797	220
809	628
821	744
827	102
953	156

Table 2: Potentially good pairs (r, p) with $p < 1000$ that are not good

p	$\{q_1, \cdots, q_{p-1}\}$ $\{r_1, \cdots, r_{p-1}\}$
5	$\{31, 31, 11, 11\}$ $\{24, 18, 2, 6\}$
7	$\{281, 29, 43, 43, 211, 421\}$ $\{120, 16, 24, 18, 180, 300\}$
11	$\{23, 23, 67, 23, 617, 67, 67, 67, 23, 67\}$ $\{4, 8, 12, 16, 504, 24, 6, 54, 14, 18\}$
13	$\{53, 859, 79, 53, 79, 53, 53, 53, 79, 313, 157, 313\}$ $\{36, 462, 30, 40, 24, 8, 44, 28, 12, 48, 84, 120\}$
17	$\{137, 103, 103, 103, 137, 137, 409, 409,$ $443, 103, 103, 103, 2381, 103, 103, 239\}$ $\{32, 30, 96, 60, 24, 56, 360, 120, 390, 48, 12, 78, 280, 6, 72, 70\}$
19	$\{419, 191, 419, 229, 229, 419, 419, 419, 457,$ $419, 229, 191, 647, 419, 229, 229, 419, 761\}$ $\{110, 30, 330, 60, 132, 242, 352, 44, 192,$ $264, 108, 180, 442, 286, 168, 12, 198, 80\}$

Table 3: q- and r- sets used to add p to M ($p \not| M$) with Theorem 2 ($5 \leq p \leq 19$)

p	the different primes occurring in $\{q_1, \cdots, q_{p-1}\}$
23	47 139 277 461 691
29	59 233 349 1103
31	311 373 1303 1427 2357
37	149 223 1259 1481 2221 2591 4441
41	83 821 1231 1559 2297 2543
43	173 431 947 1033 1291 1721 1979 3613
47	283 659 941 1129 1223 1787 4889
53	107 743 1061 2333 2969 3181 3499 3923 5407
59	709 827 2243 3541 3659 4603 4957 6491
61	367 733 1709 1831 2441 3539 4027 4271 4637 5003 8053
67	269 1609 1877 2011 3083 4021 4423 4691 5897 7103
71	569 853 1847 2131 2699 4261 8521
73	293 439 877 1607 1753 3067 3359 3797 6133 8761
79	317 2213 2371 2687 3319 4583 9007
83	167 499 997 1163 4649 5147 5479 6143 9463 12119
89	179 1069 2137 2671 3739 3917 5519 9257 15131
97	389 971 3299 3881 4463 5821 6791 8537 11447 21341 25609
101	607 809 1213 4243 5657 6263 6869 7879 9293 15959
103	619 1031 1237 2267 2473 4327 7211 8447
107	643 857 1499 2141 6421 7919 9203 14767 20117 30389
109	1091 2399 2617 3271 5669 6323 9157 10247 14389 23327
113	227 1583 2713 2939 3391 4973 6329 6781 8363
127	509 3049 3557 5081 5843 7621 9907 11177 11939 13463 19559 27179 28703
131	263 787 1049 2621 3407 3931 5503 8123 14411
137	823 1097 2741 4111 6029 7673 8221 10139 10687 22469
139	557 1669 5839 7229 11399 11677 19183 19739 21407 30859
149	1193 1789 2087 8941 9239 10133 11027 12517 13709 16987 17881
151	907 1511 3323 4229 6343 6947 7853 9967 11779 16007 18121
157	1571 3769 4397 9421 11933 14759 19469 20411 24179 27947 33599
163	653 6521 7499 9781 11411 13693 18583 21191 27059 30319 46619
167	2339 5011 7349 14029 18371 19373 26053 26387 28057 31063 46093
173	347 1039 2423 3461 4153 9689 14879 26297
179	359 1433 3581 4297 6803 7877 13963 18617 20407 21481
181	1087 1811 5431 7603 9413 10499 10861 12671 13757 23893
191	383 2293 3821 4967 16427 17573 19483 21011 22157 29033 40111
193	773 1931 5791 6563 10037 12739 14669 18143 19687 22003
197	4729 7487 8669 11821 13003 13397 16943 22853 26399 38219 40583
199	797 2389 5573 11941 13931 16319 24677 29453 35423 51343

Table 4: The q-primes used to add p to M with Theorem 2 ($23 \leq p \leq 199$)

p	$\{q_1, \cdots, q_{p-1}\}$ $\{r_1, \cdots, r_{p-1}\}$	M
5	$\{1451, 101, 101, 101\}$ $\{580, 60, 40, 20\}$	$2^3 \cdot 3 \cdot 5 \cdots 97 (=: M')$
5	$\{751, 751, 751, 751\}$ $\{150, 300, 450, 600\}$	$5 \cdot M'$
5	$\{97501, 97501, 108751, 73751\}$ $\{19500, 39000, 43500, 44250\}$	$5^2 \cdot M'$
7	$\{1667, 491, 197, 1667, 1471, 197\}$ $\{1428, 210, 168, 714, 1260, 140\}$	M'
7	$\{7547, 7547, 13721, 76147, 17837, 63799\}$ $\{1078, 2156, 3920, 54390, 10192, 45570\}$	$7 \cdot M'$
11	$\{727, 1453, 1453, 727, 727, 7019, 3389, 3631, 3631, 15731\}$ $\{132, 264, 396, 528, 660, 1276, 924, 330, 2640, 8580\}$	M'
13	677 2029 3719 4057 6761 25013	M'
17	3469 8093 16763 39883 44507	M'
19	10831 16607 18773 20939 21661 23827	M'

Table 5: q- and r- sets used to add p to M ($p \mid M$) with Theorem 2 ($5 \leq p \leq 19$) (for $p = 13, 17, 19$ only the different primes in the respective q-sets are given)

p^{a+1}	s	$\nu_1, \cdots, \nu_s$	$q_1, \cdots, q_s$	$R(1), \cdots, R(s)$	M'
2^4	2	3	4673	$\{7\}$	$2^3 \cdot 5 \cdot 17 \cdot 73$
		3	5441	$\{1\}$	
2^5	2	3	641	$\{1\}$	$2^4 \cdot 5 \cdot 11$
		3	1409	$\{1,5\}$	
2^6	1	3	3329	$\{5\}$	$2^5 \cdot 13$
				see text	
2^7	1	3	17921	$\emptyset$	$2^6 \cdot 5 \cdot 7$
2^8	1	3	13313	$\emptyset$	$2^7 \cdot 13$
3^2	2	2	757	$\{4,7\}$	$2^3 \cdot 3 \cdot 7 \cdot 11$
		2	2377	$\{5\}$	
3^3	3	2	2593	$\{2,7,8\}$	$2^5 \cdot 3^2 \cdot 11 \cdot 43$
		2	6967	$\{1,7\}$	
		2	7129	$\{2,4\}$	
3^4	4	2	487	$\{1,2,4,5\}$	$2^4 \cdot 3^3 \cdot 5 \cdot 7$
		2	3889	$\{1,8\}$	
		2	9721	$\{2,4,5\}$	
		2	17011	$\{1,4,5\}$	
3^5	3	2	1459	$\{1,7,8\}$	$2^2 \cdot 3^4 \cdot 5^2$
		2	2917	$\{2,5,7,8\}$	
		2	36451	$\{5,7\}$	

Table 6: Details of Theorem 3 which prove that $2^8 \mid k$ and $3^5 \mid k$

irregular pair (r, p)	$g = \gcd(p-1, M)$	good sieving pair (Htg_1, p')
(94, 467)	2	(1026, 1399)
(194, 467)	2	(3456, 7457)
(90, 587)	2	(90, 1759)
(92, 587)	2	(2436, 3517)
(66, 839)	2	(4256, 15923)
(418, 887)	2	(11050, 11519)
(784, 1229)	4	(3240, 7369)
(510, 1283)	2	(17176, 24359)
(382, 1307)	2	(26502, 27427)
(852, 1307)	2	(2158, 16979)
(304, 1319)	2	(10848, 21089)
(234, 1367)	2	(24822, 28687)
(574, 1439)	2	(33648, 34513)
(1310, 1523)	2	(2832, 9133)
(560, 1619)	2	(19976, 35597)
(270, 1663)	6	(270, 4987)
(1260, 1879)	6	(2512, 5009)
(510, 1987)	6	(10440, 13241)
(772, 1997)	4	(8756, 10979)
(1888, 1997)	4	(5880, 20959)
(1300, 2039)	2	(5376, 32609)
(1230, 2099)	2	(7524, 138469)
(1832, 2153)	8	(756, 11299)
(1660, 2309)	4	(2814, 3463)
(1772, 2309)	4	(13312, 36929)
(1730, 2579)	2	(27510, 38671)
(1600, 2777)	8	(2988, 6247)
(400, 2909)	4	(1854, 4363)
(788, 2957)	4	(3744, 17737)
(776, 2999)	2	(12768, 17989)

Table 7: The first 30 irregular pairs (r, p) satisfying condition d) of Theorem 5, $\gcd(p-1, M)$ with M as computed in Section 5.2, and a corresponding good sieving pair (Htg_1, p') that can be used to apply Theorem 4

irregular pair (r, p)	$g = \gcd(p-1, M)$	good sieving pair (Htg_1, p')
(2020, 3023)	2	(8064, 9067)
(1704, 3119)	2	(1704, 12473)
(2368, 3203)	2	(2368, 12809)
(1836, 3517)	12	(3008, 9377)
(3136, 3533)	4	(10200, 52981)
(360, 3593)	8	(2156, 6287)
(1580, 3671)	10	(11856, 27893)
(2362, 3779)	2	(21252, 22669)
(1840, 3833)	8	(3756, 5749)
(1936, 3989)	4	(9912, 23929)
(3580, 4259)	2	(80224, 195869)
(3726, 4259)	2	(3726, 114967)
(2052, 4349)	4	(15096, 160877)
(3592, 4679)	2	(69084, 88883)
(252, 4783)	6	(16192, 35069)
(594, 5039)	22	(6090, 9619)
(1378, 5099)	2	(72750, 76471)
(4086, 5119)	6	(7498, 39239)
(1482, 5399)	2	(114840, 118757)
(1710, 5443)	6	(50688, 79817)
(2672, 5639)	2	(250744, 293177)
(4284, 5813)	4	(21720, 43591)
(3642, 5927)	2	(21420, 124447)
(342, 5939)	2	(107226, 219707)
(5014, 5939)	2	(10952, 23753)
(5870, 6011)	10	(7072, 31253)
(3396, 6037)	12	(378, 7043)
(5008, 6173)	4	(17352, 18517)
(3474, 6247)	18	(7638, 13187)
(4452, 6287)	14	(4452, 18859)

Table 8: Table 7 continued (30 cases)

irregular pair (r, p)	$g = \gcd(p-1, M)$	good sieving pair (Htg_1, p')
(1776, 6569)	8	(21480, 24631)
(2950, 6659)	2	(36240, 99871)
(4014, 6659)	2	(10672, 26633)
(3994, 6779)	2	(187000, 230453)
(4108, 6827)	2	(58716, 122869)
(3906, 7187)	2	(3906, 21559)
(116, 7559)	2	(75696, 90697)
(3594, 7607)	2	(26412, 235787)
(5026, 7643)	2	(89088, 122273)
(3756, 7727)	2	(34660, 77261)
(950, 7727)	2	(39580, 77261)
(3298, 7823)	2	(89340, 117331)
(3436, 7949)	4	(7410, 11923)
(6636, 8039)	2	(119168, 152723)
(5784, 8293)	12	(4402, 98123)
(6432, 8719)	6	(52928, 92993)
(2688, 8747)	2	(2688, 104953)
(4784, 8753)	16	(3690, 16411)
(2620, 8831)	10	(9684, 10597)
(3830, 8831)	10	(12660, 52981)
(2382, 8923)	6	(70784, 83273)
(572, 8999)	22	(5480, 16361)
(1598, 9467)	2	(67860, 141991)
(152, 9743)	2	(152, 185099)
(4844, 9839)	2	(44196, 59029)

Table 9: Table 7 continued (25 cases)

6 A heuristical approach to the conjecture of Erdös-Moser

In this section we present a heuristical argument that, in combination with the fact that $\mathrm{lcm}(1,\cdots,200) \mid k$ (see Section 5.2), suggests that the Erdös-Moser conjecture might very well hold true. Although the argument is not entirely mathematical, we present it in the form of a 'Theorem'.

'Theorem'
Assuming 'random distribution' and 'independence' at the appropriate places, it follows from $\mathrm{lcm}(1,\cdots,v)|k$ *(where* k *belongs to a solution pair* (x,k) *of (1)) that the smallest prime power not dividing* $\mathrm{lcm}(1,\cdots,v)$ *divides* k *with a probability at least*

$$1 - e^{-e^{\log 2 \frac{v}{\log v}(1+\mathcal{O}(\frac{1}{\log v}))}} \tag{6}$$

as v *tends to infinity.*

In order to 'prove' this 'Theorem' we need a property of the divisor function $d(n)$ (which denotes the number of divisors of n).

Lemma 11

$$\log d(\mathrm{lcm}(1,\cdots,v)) = \log 2 \frac{v}{\log v}(1+\mathcal{O}(\frac{1}{\log v})). \tag{7}$$

Proof. Notice that $p^m || \mathrm{lcm}(1,\cdots,v)$ if and only if $p \leq v$ and $m = \lfloor \log v / \log p \rfloor$. Using the multiplicativity of $d(n)$, we see that

$$\log d(\mathrm{lcm}(1,\cdots,v)) = \sum_{p \leq v} \log \left(\left\lfloor \frac{\log v}{\log p} \right\rfloor + 1 \right).$$

The sum can be written as $I_1 + I_2$, where $I_1 = \sum_{p \leq \sqrt{v}} \log(\lfloor \log v / \log p \rfloor + 1)$, $I_2 = (\pi(v) - \pi(\sqrt{v}))\log 2$ and $\pi(v)$ is the prime counting function. Since $I_1 = \mathcal{O}(v^{2/3})$ we arrive, using the Prime Number Theorem, at (7). □

Remark. The function $\psi(x,y)$ is defined as the number of positive integers $\leq x$, having only prime factors $\leq y$; $\Lambda(n)$ denotes the von Mangoldt function, that is $\Lambda(n) = \log p$ if $n = p^\lambda$ (p prime) and 0 otherwise; $\psi(x)$ denotes the von Mangoldt summatory function. Note that

$$\log \mathrm{lcm}(1,\cdots,v) = \psi(v) \text{ and } d(\mathrm{lcm}(1,\cdots,v)) \leq \psi(\mathrm{lcm}(1,\cdots,v),v). \tag{8}$$

Since $\psi(v) \sim v$ (an alternative formulation of the Prime Number Theorem), it might be interesting to compare $\log d(\mathrm{lcm}(1,\cdots,v))$ with $\log \psi(e^v, v)$. It was proved by Erdös [Erd63] that

$$\log \psi(e^v, v) \sim 2 \log 2 \frac{v}{\log v}.$$

This is two times the exact asymptotic value for $\log d(\mathrm{lcm}(1,\cdots,v))$.

'Proof' of the 'Theorem'. Suppose (x,k) is a solution of (1) and suppose that it has been proved that $\mathrm{lcm}(1,\cdots,v)|k$ for some v. Let q^λ be the smallest prime power exceeding v. By Bertrand's Postulate $q^\lambda \leq 2v$. Let $\Delta(v)$ denote the set of divisors of $\mathrm{lcm}(1,\cdots,v)$. Let $Q(v)$ be the set of primes p such that $p-1 \in \Delta(v)$. The largest prime in $Q(v)$ (if $Q(v)$ is non-empty) is $\leq \mathrm{lcm}(1,\cdots,v)+1$, which is at most $e^{1.1v}$ for v sufficiently large, using the Prime Number Theorem in the form $\psi(v) \sim v$ and (8). The probability that an integer t is prime is about $1/\log t$. Hence, using Lemma 11, we conclude that the number of primes in $Q(v)$ to be expected is $\exp((\log 2)v/\log v(1+\mathcal{O}(1/\log v))$. For each prime p in $Q(v)$ we compute the remainder $r_{v,p}$ of $\mathrm{lcm}(1,\cdots,v)$ on division by $p-1$, until we find a good pair $(r_{v,p},p)$. Assuming that the values $f_r(a;p)$ are randomly distributed modulo p, it follows that the probability that $f_r(a;p) \not\equiv 0, -3a^r \pmod p$ for $1 \leq a \leq (p-1)/2$ is about $(1-2/p)^{(p-1)/2}$, which is about $1/e$. (This is supported by our findings in Section 5.) We assume that for large p the probability that $p|B_{r_{v,p}}$ tends to a constant $c \in (0,1)$. (The known facts clearly suggest that even $c=0$.) The probability that none of the pairs $(r_{v,p},p)$ is a good pair is about $(1-(1-c)/e)^{|Q(v)|}$. We repeat this procedure where $r_{v,p}$ is successively congruent to $i \cdot \mathrm{lcm}(1,\cdots,v) \pmod{p-1}$ for $i=2,\cdots,q-1$. The probability that the procedure fails is at most

$$2v\left(1-\frac{1-c}{e}\right)^{|Q(v)|} = e^{-e^{\log 2 \frac{v}{\log v}(1+\mathcal{O}(\frac{1}{\log v}))}}$$

(provided we have 'random distribution' and 'independence', and provided the probability assumption on the Bernoulli numbers holds true). If the procedure does not fail it follows that $q^\lambda|k$ (and $\mathrm{lcm}(1,\cdots,q^\lambda)|k$) on using Theorem 2 with $M = \mathrm{lcm}(1,\cdots,v)$ and $p=q$. □

Remark. We did not use good pairs (r,q) with q a prime power, since there are only $\sum_{p \leq v} \lfloor \log v/\log p \rfloor \sim v/\log v$ prime powers r^λ (r prime, $\lambda \geq 2$) such that $\varphi(r^\lambda)|\mathrm{lcm}(1,\cdots,v)$ and the contribution of the corresponding possible sieve pairs in enlarging the probability (6) is absorbed by the error term in (6).

References

[BCS] J.P. Buhler, R.E. Crandall, and R.W. Sompolski. Irregular primes to one million. To appear in Math. Comp., 1992.

[BtR76] M.R. Best and H.J.J. te Riele. On a conjecture of Erdös concerning sums of powers of integers. Technical Report NW 23/76, Mathematisch Centrum, Amsterdam, May 1976.

[Del91] H. Delange. Sur les zéros réels des polynômes de Bernoulli. *Ann. Inst. Fourier*, 41(2):267–309, 1991.

[DL63] H. Davenport and D.J. Lewis. Homogeneous additive equations. *Proc. Royal Soc. Ser. A*, 274:443–460, 1963.

[Erd63] P. Erdös. Problem 136. *Wiskundige Opgaven*, pages 133–135, 1963.

[Guy81] R.K. Guy. *Unsolved problems in number theory*, volume I. Springer-Verlag, New York, etc., 1981.

[IR90] K. Ireland and M. Rosen. *A classical introduction to modern number theory.* Springer-Verlag, New York, etc., 1990.

[Joh73] W. Johnson. On the vanishing of the Iwasawa invariant μ_p for $p < 8000$. *Math. Comp.*, 27:387–396, 1973.

[Joh74] W. Johnson. Irregular prime divisors of the Bernoulli numbers. *Math. Comp.*, 28:653–657, 1974.

[LU] K. Lorentz and J. Urbanowicz. A note on the equation $1^k+2^k+\cdots+(x-1)^k = x^k$. Unpublished manuscript.

[Lun75] J. van de Lune. On a conjecture of Erdös, I. Technical Report ZW 54/75, Mathematisch Centrum, Amsterdam, September 1975.

[Mos53] L. Moser. On the diophantine equation $1^n + 2^n + \cdots + (m-1)^n = m^n$. *Scripta Math.*, 19:84–88, 1953.

[Rib79] P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, etc., 1979.

[Sha83] H.N. Shapiro. *Introduction to the theory of numbers.* Wiley-Interscience, New York, etc., 1983.

[Urb88] J. Urbanowicz. Remarks on the equation $1^k + 2^k + \cdots + (x-1)^k = x^k$. *Indag. Math., Ser. A*, 91:343–348, 1988.

[Van37] H.S. Vandiver. On Bernoulli's numbers and Fermat's last theorem. *Duke Math. J.*, 3:569–584, 1937.

[Wag78] S.S. Wagstaff, Jr. The irregular primes to 125000. *Math. Comp.*, 32:583–591, 1978.

[Was82] L. C. Washington. *Introduction to cyclotomic fields*. Springer-Verlag, New York, etc., 1982.

[ZK83] G.F. Zhou and C.D. Kang. On the diophantine equation $\sum_{k=1}^{m} k^n = (m+1)^n$. *J. Math. Res. Exposition*, 3(4):47–48, 1983.