MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 208
OCTOBER 1994, PAGES 799–815

DIVISIBILITY PROPERTIES OF INTEGERS x, k SATISFYING $1^k + \cdots + (x-1)^k = x^k$

P. MOREE, H.J.J. TE RIELE, AND J. URBANOWICZ

ABSTRACT. Based on congruences mod p and on properties of Bernoulli polynomials and Bernoulli numbers, several conditions are derived for $x, k \geq 2$ to satisfy the Diophantine equation $1^k + 2^k + \cdots + (x-1)^k = x^k$. It is proved that $\mathrm{ord}_2(x-3) = \mathrm{ord}_2 k + 3$ and that x cannot be divisible by any regular prime. Furthermore, by using the results of experiments with the above conditions on an SGI workstation it is proved that x cannot be divisible by any irregular prime < 10000 and that k is divisible by the least common multiple of all the integers ≤ 200.

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 [12] 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 [12] proved that x exceeds C, where $C = 10^{1000000}$. Best and one of the authors [1] proved that for every k there is at most one x satisfying (1). From their work and also from an analytical expression of Delange [4, 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 has been published. Moser [12] proved that k is *even* and that $x \equiv 0$ or $3 \pmod 8$. In this paper we will establish further divisibility properties of x and k. In §2 we give a number of mathematical preliminaries. Section 3 gives our main mathematical results which are proved in §4. Numerical searches based on the results of §3

Received by the editor September 9, 1992 and, in revised form, August 19, 1993.
1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11B68, 11Y50.
Key words and phrases. Sums of powers, regular and irregular primes, Bernoulli numbers, congruences, Diophantine equations.
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.

are described in §5. Combination of the mathematical and numerical results yields that if (x, k) is a solution of (1) then

(i) $x \equiv 3 \pmod{2^{\mathrm{ord}_2 k+3}}$, x is not divisible by any regular prime, and if x is divisible by some irregular prime p, then $p > 10000$.

(ii) k should be divisible by the number $M = 2^8 \cdot 3^5 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdots 199$ ($\log_{10}(M) = 94.359\ldots$).

For other references on the Erdös-Moser conjecture, see, e.g., [5, pp. 85–86], or the introduction of [16]. The present paper is an extension, both mathematically and numerically, of [9]. Further numerical material can be found in [11],[1] where we also present a heuristic argument to support the truth of the conjecture of Erdös and Moser.

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 [3] that this equation has infinitely many integer solutions $y_1, y_2, \ldots, y_n$ with $y_i \neq 0$ whenever $k \geq 18$ and $n \geq 1 + k^2$.

Remark. In Lemma 11 of this paper we prove that $x \equiv 3 \pmod 8$, following Moser [12], but we would like to mention that already in 1987, A. Schinzel communicated a proof to one of us (JU) that $x \equiv 3 \pmod{2^{\mathrm{ord}_2 k+1}}$. In Lemma 12 we sharpen this result to $x \equiv 3 \pmod{2^{\mathrm{ord}_2 k+3}}$ and show that this is best possible. This implies, with $2^8 \mid k$ (cf. (ii) above), that $x \equiv 3 \pmod{2^{11}}$.

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,

$$f_k(x; p) = \sum_{\substack{1 \leq m \leq x-1 \\ p \nmid m}} m^k - x^k,$$

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 $p \nmid v$, and to be divisible by p^μ if $p^\mu \mid u$. If $\alpha = p^\mu u/v$ with $p \nmid u, v$, 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 [6, Chapter 15] or [19]:

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 $n \geq 2$ 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.

[1]This is available upon request from the second author, or through anonymous ftp from ftp.cwi.nl.

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

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

This formula enables us to express the left-hand side of (1) in terms of Bernoulli polynomials. Putting $P_{k+1}(x) = B_{k+1}(x) - B_{k+1} - (k+1)x^k$, it follows that (1) is equivalent to $P_{k+1}(x) = 0$.

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 [8]). An algorithm to compute the sets $T_{r,p}$ can be found in [8]. Wagstaff [18] found that for every irregular pair (r, p) with $p < 125000$ the set $T_{r,p}$ has only one element. Buhler et al. [2] have calculated all irregular primes up to one million,[2] 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 cannot belong to certain congruence classes, and in combination with Lemma 10 it is used to investigate the divisibility of x.

[2]This was extended recently to four million.

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 $i = 1, \ldots, \varepsilon$ 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 $1 \leq i \leq \varepsilon$ 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 $k \geq \lambda$ 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 to 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, there is no loss that Theorem 1 is restricted to the case that r is even.

Since in practice the condition $p^i \nmid (B_{\varrho_i}/\varrho_i)$ for $i \geq 2$ is only rarely not satisfied, and it requires arithmetic modulo p^i $(i \geq 2)$ to check whether or not $p^i | (B_{\varrho_i}/\varrho_i)$ (for $i = 2$ see [8]), for numerical work (cf. §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 [17], [18, (4)] and Voronoi [18, (1)]. So we arrive at the following numerical variant of Theorem 1.

Theorem 1′. *Let p^λ be a prime power with $\lambda \leq C$ $(= 10^{10^6})$ 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 $p \geq 37$) 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 nondivisibility 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 $k \equiv r \pmod{\varphi(p^\lambda)}$. By 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, $p^\lambda = 5, 5^2$).

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

Theorem 2. *Let* p *be a prime and let* $\{q_1, q_2, \ldots, q_{p-1}\}$ *be a set of (not necessarily distinct) odd prime powers such that* $p \mid \varphi(q_i)$ *for* $i = 1, \ldots, p-1$. *Let* M *be any positive integer such that* $\operatorname{lcm}(\varphi(q_1), \ldots, \varphi(q_{p-1})) \mid pM$, *and let* $\{r_1, r_2, \ldots, r_{p-1}\}$ *denote the set of numbers such that for* $i = 1, \ldots, p-1$, $r_i \equiv iM \pmod{\varphi(q_i)}$ *and* $0 \leq r_i < \varphi(q_i)$. *Then, if* (r_i, q_i) *is a good pair for* $i = 1, \ldots, p-1$, *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 $\varphi(q_i) \mid M$ for some i with $1 \leq i \leq p-1$, then $r_i = 0$ and (r_i, q_i) is not a good pair. We should therefore require that no number $\varphi(q_i)$ divides M; that is, that $\operatorname{ord}_p(\varphi(q_i)) \geq 1 + \operatorname{ord}_p(M)$ for $i = 1, \ldots, p-1$.

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 $a = 2, \ldots, (q-1)/2$ *and* $i = 1, \ldots, p-1$. *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

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

for $a = 2, \ldots, (q-1)/2$. Assume that $q \geq 23$ and that the condition of the corollary holds. Taking $a = 2, 4, 6, 8$, we conclude that $-1 = (\frac{2}{q}) = (\frac{3}{q}) = (\frac{5}{q}) = -(\frac{7}{q})$. Taking $a = 10$, we conclude that for no $q \geq 23$ can the condition of the corollary 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 cannot 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*

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

Write

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

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

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

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 $e_q = \operatorname{ord}_q M$, $a_q = \operatorname{ord}_q G$. 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 $GH \mid a$. Since $g \mid a$ (by assumption) and $b \mid \operatorname{lcm}(g, GH)$, 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 $M \mid k$ 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 $M \mid k$ for some integer M. Let p be an odd 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 does not divide x.

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

Remark 1. By Theorems 5(a) and 5(b) it follows that x should furthermore be irregular and $x - 1 \nmid k$.

Remark 2. By the work of Wagstaff [18] it follows that we can take $C_1 = 125000$. It has been conjectured that the largest possible C_1 is finite (see [13, p.22]).

4. Proofs 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 and let p be a prime number. Then for every integer s we have*

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

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

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

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., [6, 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 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 $p \nmid m$),

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

Hence, the lemma follows immediately. □

Lemma 4 [12]. *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 [10] 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), we conclude 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 $i = 1, \ldots, k/2$. 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 $i = 1, \ldots, k/2 - 1$. Indeed, by P6 and Lemma 5 it follows that for $i = 1, \ldots, k/2 - 1$

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

Lemma 7. *Suppose* (x, k) *is a solution of* (1). *Then* $k > C = 10^{1000000}$.

Proof. The proof follows by Lemma 6 on using the lower bound C^2 for x, which is proved in [20]. □

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

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

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

$$\text{(3)} \quad \begin{aligned} &\frac{P_{k+1}(x)}{(k+1)kx} - \frac{B_k}{k} - x^2 \frac{k-1}{6} B_{k-2} \\ &\quad = x^2 \left[\frac{x^{k-2}}{(k+1)k} - \frac{3x^{k-3}}{2k} + \sum_{i=1}^{k/2-2} \binom{k+1}{2i} B_{2i} \frac{x^{k-2i-2}}{(k+1)k} \right]. \end{aligned}$$

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

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

Furthermore, the assumption $p|x$ implies $\operatorname{ord}_p(x^{m-3}/m!) \geq 2$ 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

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

Using this and P2, we conclude 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

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

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

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

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

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

On using (3) the proof becomes complete. □

Lemma 9 [15, Theorem 5.4.2]. *Let $s, a_1, \ldots, a_s, k_1, \ldots, k_s$ be natural numbers with $s \geq 2$. The system of simultaneous congruences $x \equiv a_i \pmod{k_i}$, $i = 1, \ldots, s$, 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 an odd prime dividing x. Then*

(a) $k \not\equiv 0, 2 \pmod{p-1}$,
(b) *p is an irregular prime,*
(c) $\operatorname{ord}_p(\frac{B_k}{k}) \geq 2\operatorname{ord}_p x$,
(d) $k \equiv r_i \pmod{p-1}$, *for some $i \in \{1, \ldots, i(p)\}$, where (r_i, p) denotes the ith irregular pair and $i(p)$ the index of irregularity,*
(e) $k \equiv r_i + t(p-1) \pmod{p(p-1)}$, *for some $i \in \{1, \ldots, i(p)\}$ and $t \in T_{r,p}$, where the set $T_{r,p}$ is defined in §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 Lemma 8 we get

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

Therefore, by P2 and $\operatorname{ord}_p(x^2\frac{k-1}{6}B_{k-2}) \geq 0$, $p - 1|k$ implies $\operatorname{ord}_p x < 0$. 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 $\operatorname{ord}_p(B_k/k) = 0$. Therefore, by (4) and $\operatorname{ord}_p(x^2\frac{k-1}{6}B_{k-2}) \geq 1$, we get $\operatorname{ord}_p x \leq 0$. 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 [8]. □

In the next lemma we deal with the case $p = 2$, which is not covered by Lemma 10.

Lemma 11. *If* (x, k) *is a solution of* (1), *then* $x \equiv 3 \pmod 8$.

Proof. If $k = 1$, then $x = 3$, so we may assume that $k \geq 2$. We start from equality (3). Since (x, k) is a solution of (1), by Moser's result k must be even and $x \equiv 0$ or $3 \pmod 8$. Moreover, by assumption we have $P_{k+1}(x) = 0$ and we drop this term ($\frac{k}{2} + 2$ terms are left). Multiply each term between brackets by x^2. Now suppose that x is even. Then using the fact that $\operatorname{ord}_2(B_{2i}) = -1$ for every $i \geq 1$ (which follows by P2), we readily deduce that each of the 2-orders of the terms in (3) different from B_k/k exceeds $\operatorname{ord}_2(B_k/k)$. This impossibility proves that $x \equiv 3 \pmod 8$. □

Lemma 12. *If* $k \geq 8$ *and* (x, k) *is a solution of* (1), *then*

$$\operatorname{ord}_2(x-3) = 3 + \operatorname{ord}_2 k.$$

Proof. By Moser's result and by Lemma 11, k must be even and $x \equiv 3 \pmod 8$. First, let us notice that for any natural $k \geq 3$ and r, the congruence $a \equiv r \pmod 8$ implies

$$\begin{aligned} a^k &= \sum_{i=0}^{k} \binom{k}{i} (a-r)^i r^{k-i} \\ &\equiv r^k + k(a-r)r^{k-1} + \binom{k}{2}(a-r)^2 r^{k-2} \pmod{2^{\operatorname{ord}_2 k+6}}, \end{aligned}$$

because for $i \geq 3$

$$\operatorname{ord}_2 \frac{(a-r)^i}{i!} \geq \operatorname{ord}_2 \left(\frac{2^{3i}}{i!} \right) > 2i \geq 6.$$

Thus, if $k \geq 4$ is even and r is odd (which implies that $r^{k-2} \equiv 1 \pmod 8$), we have

$$a^k \equiv r^k + k(a-r)r + \frac{k(k-1)}{2}(a-r)^2 \pmod{2^{\operatorname{ord}_2 k+6}},$$

and in consequence we get

$$a^k \equiv r^k + k(a-r)r \pmod{2^{\operatorname{ord}_2 k+5}}.$$

Applying this congruence to the equation (1) gives

$$\begin{aligned} 0 &= \sum_{a=1}^{x-3} a^k + (x-2)^k + (x-1)^k - x^k \\ &\equiv \sum_{r \in \{\pm 1, \pm 3\}} t_r r^k + k \cdot \sum_{r \in \{\pm 1, \pm 3\}} s_r r + (x-2)^k - x^k \pmod{2^{\operatorname{ord}_2 k+5}}, \end{aligned}$$

where

$$t_r := \sum_{\substack{1 \leq a \leq x-4, \\ a \equiv r \pmod 8}} 1 \quad \text{and} \quad s_r := \sum_{\substack{1 \leq a \leq x-4, \\ a \equiv r \pmod 8}} (a-r),$$

because $a^k \equiv 0 \pmod{2^{\operatorname{ord}_2 k+5}}$, if $k \geq 8$ and $2 | a$.

Writing $x = 8u + 3$, we derive without difficulty the following equalities:

$$t_r = u = \frac{x-3}{8}, \qquad \sum_{r\in\{\pm 1,\pm 3\}} t_r r^k = \frac{x-3}{4}(1+3^k),$$

$$s_1 = s_3 = 4u(u-1), \qquad s_{-1} = s_{-3} = 4u(u+1),$$

$$k \cdot \sum_{r\in\{\pm 1,\pm 3\}} s_r r = -k \cdot 32u \equiv 0 \pmod{2^{\mathrm{ord}_2 k+5}}.$$

Moreover, we have

$$(x-2)^k \equiv 1 + k(x-3) \pmod{2^{\mathrm{ord}_2 k+5}}$$

and

$$x^k \equiv 3^k + 3k(x-3) \pmod{2^{\mathrm{ord}_2 k+5}}.$$

Collecting, this yields the congruence

$$\frac{x-3}{4}(1+3^k) + 1 - 2k(x-3) - 3^k \equiv 0 \pmod{2^{\mathrm{ord}_2 k+5}}.$$

Therefore, since

$$3^k - 4k - 1 = \sum_{i=0}^{k} \binom{k}{i} 2^i - 4k - 1$$

$$\equiv -2k + 4\binom{k}{2} + 8\binom{k}{3} + 16\binom{k}{4} \pmod{2^{\mathrm{ord}_2 k+4}}$$

(here we use that for $k \geq 8$, $5 \leq i \leq k$, $\mathrm{ord}_2\left\{\binom{k}{i}2^i\right\} = \mathrm{ord}_2\left\{\frac{k}{i}\binom{k-1}{i-1}2^i\right\} \geq \mathrm{ord}_2 k + i - \mathrm{ord}_2 i \geq \mathrm{ord}_2 k + 4$)

$$\equiv -2k + 2k(k-1) - 4k(k-1)(k-2) + 6k(k-1)(k-2)(k-3)$$

(using $\frac{4}{3} \equiv -4 \pmod{16}$ and $\frac{2}{3} \equiv 6 \pmod{16}$)

$$\equiv 2k(k-2) - 4k^2(k-2) + 4k(k-2) + 6k^3(k-2)$$
$$- 24k^2(k-2) + 18k(k-2)$$
$$\equiv 24k(k-2) - 28k^2(k-2) + 6k^3(k-2)$$
$$\equiv 0 \pmod{2^{\mathrm{ord}_2 k+4}},$$

we obtain the congruence

$$\frac{x-3}{2}(-2k+1) \equiv 4k \pmod{2^{\mathrm{ord}_2 k+4}}.$$

From this the lemma follows immediately. □

4.2. **Proofs of the Theorems.**

Proof of Theorem 1. Let p^λ be a prime power and r, ϱ_i $(i = 1, \ldots, \varepsilon)$ 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 is divided naturally into the cases where $p|x$ and $p \nmid x$.

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 10(c). 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 10(c). 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

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

[17, 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 [18] 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 $i = 1, \ldots, p-1$. By the definition of r_i $(i = 1, \ldots, p-1)$ and M it suffices to show that $k \not\equiv r_i \pmod{\varphi(q_i)}$ for $i = 1, \ldots, p-1$. But since (r_i, q_i) is a good pair for $i = 1, \ldots, p-1$ (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

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

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 $(j_1, \ldots, j_s) \in R(1) \times \cdots \times R(s)$. By Lemma 9, $(j_1, \ldots, j_s)$ 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 to $a' + uG = vg_1$ 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 $k \not\equiv Htg_1 \pmod{p' - 1}$. So the conclusion of the theorem follows. □

Proof of Theorem 5. Parts (a) and (b) are consequences of respectively Lemma 10(b) and Lemma 10(a). To prove part (c), assume $p|x$. By Lemma 10(d) 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 10(d) 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 10(c). Contradiction. □

5. Numerical results

We have carried out several numerical experiments with the theorems of §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 $M \mid k$. We find a prime $p \geq 5$ such that $pM \mid k$, by finding sets $\{q_1, q_2, \ldots, q_{p-1}\}$ and $\{r_1, r_2, \ldots, r_{q-1}\}$ 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 *cannot* 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 §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 (next page) we list the good pairs (r, p^λ) with $5 \leq p^\lambda \leq 25$. In [11, Table 1] the good pairs (r, p^λ) with $5 \leq p^\lambda \leq 125$ are listed. 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. All these 30 pairs appeared to be irregular. They are listed in [11, Table

TABLE 1. Good pairs (r, p^λ) for the prime powers p^λ with $5 \le p^\lambda \le 25$

p^λ	5	7	11	13	17	19	23	5^2
r	2	24	26	24810	24612	41016	48141 6	26101418

2]. The first four are $(24, 103)$, $(22, 131)$, $(164, 257)$, $(280, 347)$. The total number of irregular pairs (r, p) with $3 \le p < 1000$ is 81 [7]. 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^λ, the probability that (r, p^λ) 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 $\lambda \ge 1$ we can expect the quantity

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

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 $M \mid k$ for some $M > 1$. If we can find a prime p such that (1) has *no* solution satisfying one of the $p - 1$ congruences

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

then it follows that $pM \mid k$. 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 $p^{\mu+1} \mid q - 1$ *and* $q - 1 \mid pM$. Take $i \in \{1, \ldots, p-1\}$ and let r_i be the remainder of iM on division by $q-1$. It is easily seen that $r_i \ne 0$. 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 $q - 1 \mid pM$. In view of the experiments mentioned in §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 (1). If we succeed in doing so, we have found sets $\{q_1, \ldots, q_{p-1}\}$ and $\{r_1, \ldots, r_{p-1}\}$ 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 $q - 1 \mid pM$.

From Moser [12] 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 $k \not\equiv 2 \pmod 4$, so that $k \equiv 0 \pmod 4$. Since $(2, 7)$ and $(4, 7)$ are good pairs, it follows that $k \equiv 0 \pmod 6$. From $4 \mid k$ and the fact that $(4, 17)$ and $(12, 17)$ are good pairs, it follows that $k \equiv 0 \pmod 8$.

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 $\{q_1, \ldots, q_{p-1}\}$ and $\{r_1, \ldots, r_{p-1}\}$ (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 [11, Table 3] we give the q- and r-sets for $p = 5, 7, 11, 13, 17, 19$. For the proof that $pM \mid k$, given that $M \mid k$, we used the value $M = M_p := 2^3 \prod_{3 \le q < p,\ q \text{ prime}} q$. For example, for $p = 5$, $M_5 = 24$ and we found the q-set $\{31, 31, 11, 11\}$ and the r-set $\{24, 18, 2, 6\}$. For $p = 7$, $M_7 = 120$ we found the q-set $\{281, 29, 43, 43, 211, 421\}$ and the r-set $\{120, 16, 24, 18, 180, 300\}$. It should be noticed that in this case we needed the *largest* available q-prime 421 to complete the proof.

For the primes 23, ..., 199 Table 4 in [11] only presents the *different* values of q which occur in the q-sets (in order to save space), and not the q- and r-sets themselves.

Example. Consider the case $p = 23$. The values of q which occur in the corresponding q-set are 47, 139, 277, 461, and 691. 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 $M \pmod{46} = 14$ and the program checks which of the pairs $(14i \pmod{46}, 47)$, $i = 1, \ldots, 22$, are good. This is found to be the case for $i = 1, 2, 10, 11, 12, 13, 14, 15, 17, 18, 19, 22$. 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 $M \pmod{138} = 60$ and, by checking the remaining values of i, it is found that $(60i \pmod{138}, 139)$ 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, we eliminated the remaining residue classes 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 the help of Theorem 2. Table 5 of [11] is similar to Table 3 of [11], but now the prime p by which we multiply M is already in M at least to the first power. For example, for $M = 2^3 \prod_{3 \le q \le 97,\ q \text{ prime}} q$ with $M \mid k$ we proved that $5M \mid k$ by finding the q-set $\{1451, 101, 101, 101\}$ and the corresponding r-set $\{580, 60, 40, 20\}$. From the results of Table 5 in [11] 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 [11, Table 6]. In one case, namely in the proof that $2^6 \mid k$, we eliminated $k \equiv 2080 \pmod{3328}$, 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, $\operatorname{lcm}(1, \ldots, 200) \mid k$. From Lemma 12 it follows that $x \equiv 3 \pmod{2^{11}}$.

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 500th 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 [11, 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 three 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. The first four lines of Table 7 in [11] are as follows:

TABLE 2. The first 4 irregular pairs (r, p) satisfying condition (d) of Theorem 5, $\gcd(p-1, M)$ with M as computed in §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')
(94,467)	2	(1026,1399)
(194,467)	2	(3456,7457)
(90,587)	2	(90,1759)
(92,587)	2	(2436,3517)

In conclusion, we have shown that if (x, k) is a solution of (1), then x is not divisible by any irregular prime < 10000. By Lemma 10(b) and Lemma 11 it then follows that x is not divisible by any prime < 10000.

ACKNOWLEDGMENTS

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

BIBLIOGRAPHY

1. M. R. Best and H. J. J. te Riele, *On a conjecture of Erdös concerning sums of powers of integers*, Report NW 23/76, Mathematisch Centrum, Amsterdam, May 1976.
2. J. P. Buhler, R. E. Crandall, and R. W. Sompolski, *Irregular primes to one million*, Math. Comp. **59** (1992), 717–722.
3. H. Davenport and D.J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A **274** (1963), 443–460.
4. H. Delange, *Sur les zéros réels des polynômes de Bernoulli*, Ann. Inst. Fourier (Grenoble) **41** (1991), 267–309.
5. R. K. Guy, *Unsolved problems in number theory*, Vol. I, Springer-Verlag, New York, 1981.
6. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1990.
7. W. Johnson, *On the vanishing of the Iwasawa invariant μ_p for $p < 8000$*, Math. Comp. **27** (1973), 387–396.
8. ———, *Irregular prime divisors of the Bernoulli numbers*, Math. Comp. **28** (1974), 653–657.
9. K. Lorentz and J. Urbanowicz, *A note on the equation $1^k + 2^k + \cdots + (x-1)^k = x^k$*, unpublished manuscript, 1989.
10. J. van de Lune, *On a conjecture of Erdös*. I, Report ZW 54/75, Mathematisch Centrum, Amsterdam, September 1975.
11. P. Moree, H. J. J. te Riele, and J. Urbanowicz, *Divisibility properties of integers x and k satisfying $1^k + 2^k + \cdots + (x-1)^k = x^k$*, Report NM-R9215, Centrum voor Wiskunde en Informatica, Amsterdam, August 1992.
12. L. Moser, *On the diophantine equation $1^n + 2^n + \cdots + (m-1)^n = m^n$*, Scripta Math. **19** (1953), 84–88.
13. P. Ribenboim, 13 *lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.
14. A. Schinzel, private communication to J. Urbanowicz.
15. H. N. Shapiro, *Introduction to the theory of numbers*, Wiley-Interscience, New York, 1983.
16. J. Urbanowicz, *Remarks on the equation $1^k + 2^k + \cdots + (x-1)^k = x^k$*, Indag. Math. Ser. A **91** (1988), 343–348.
17. H. S. Vandiver, *On Bernoulli's numbers and Fermat's last theorem*, Duke Math. J. **3** (1937), 569–584.
18. S. S. Wagstaff, Jr., *The irregular primes to* 125000, Math. Comp. **32** (1978), 583–591.
19. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.
20. 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** (1983), 47–48.

MATHEMATICAL INSTITUTE, UNIVERSITY OF LEIDEN, P.O. BOX 9512, 2300 RA LEIDEN, THE NETHERLANDS

E-mail address: moree@rulwinw.LeidenUniv.nl

CENTRE FOR MATHEMATICS AND COMPUTER SCIENCE (CWI), KRUISLAAN 413, 1098 SJ AMSTERDAM, THE NETHERLANDS

E-mail address: herman@cwi.nl

INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES, UL. ŚNIADECKICH 8, 00-950 WARSZAWA, POLAND

E-mail address: urbanowi@impan.impan.gov.pl