ON THE DIOPHANTINE EQUATION $1^k+2^k+\ldots+x^k+R(x)=y^z$

BY

M. VOORHOEVE, K. GYÖRY and R. TIJDEMAN

Mathematisch Centrum Amsterdam, Netherlands

University of Debrecen Debrecen, Hungary

Rijksuniversiteit Leiden, Netherlands

1. Introduction

In J. J. Schäffer [4] the equation

$$1^k+2^k+\ldots+x^k=y^m \tag{1}$$

is studied. Schäffer proves that for fixed $k>0$ and $m>1$ the equation (1) has an infinite number of solutions in positive integers x and y only in the cases

$$\text{(I) } k=1,\ m=2;\quad \text{(II) } k=3,\ m\in\{2,4\};\quad \text{(III) } k=5,\ m=2.$$

He conjectures that all other solutions of (1) have $x=y=1$, apart from $k=m=2$, $x=24$, $y=70$. In [1], the present authors have extended Schäffer's result by proving that for fixed $r, b\in\mathbf{Z}$, $b\neq 0$ and fixed $k\geqslant 2$, $k\notin\{3,5\}$ the equation

$$1^k+2^k+\ldots+x^k+r=by^z \tag{2}$$

has only finitely many solutions in integers $x, y\geqslant 1$ and $z>1$ and all solutions can be effectively determined. In this paper we prove a further generalization.

THEOREM. *Let $R(x)$ be a fixed polynomial with rational integer coefficients. Let $b\neq 0$ and $k\geqslant 2$ be fixed rational integers such that $k\notin\{3,5\}$. Then the equation*

$$1^k+2^k+\ldots+x^k+R(x)=by^z \tag{3}$$

in integers $x, y\geqslant 1$ and $z>1$ has only finitely many solutions.

The proof of our theorem differs from our proof in [1] in quite a few respects. We combine a recent result of Schinzel and Tijdeman [5] with an older, ineffective theorem by W. J. Le Veque [2]. Thus, we can determine an effective upper bound for z, but not for x and y. However, we think that it is possible to prove an effective version of Le Veque's theorem. By such a theorem one could determine effective upper bounds for x. and y, like in [1] for the equation (2).

In section 2 we quote the general results mentioned above; in section 3 we formulate a special lemma and prove that this lemma implies our theorem. In section 4 we shall prove our lemma, thus completing the proof of the theorem. In section 5 we show that our theorem is not valid for $k \in \{1, 3, 5\}$ and discuss the number of solutions in integers $x, y \geqslant 1$ of (3) for fixed $z > 1$ and fixed $k \in \{1, 3, 5\}$.

2. Auxiliary results

LEMMA 1. $1^k + 2^k + \ldots + x^k = (B_{k+1}(x+1) - B_{k+1}(0))/(k+1)$, *where*

$$B_q(x) = x^q - \tfrac{1}{2} q x^{q-1} + \frac{1}{6}\binom{q}{2} x^{q-2} - \ldots = \sum_{l=0}^{q} \binom{q}{l} B_l x^{q-l} \tag{4}$$

is the q-th Bernoulli polynomial.

Proof. Well-known (see e.g. Rademacher [3], pp. 1–7). □

LEMMA 2. (Le Veque.) *Let $P(x) \in \mathbf{Q}[x]$,*

$$P(x) = a_0 x^N + a_1 x^{N-1} + \ldots + a_N = a_0 \prod_{i=1}^{n} (x - \alpha_i)^{r_i},$$

with $a_0 \neq 0$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. Let $0 \neq b \in \mathbf{Z}$, $m \in \mathbf{N}$ and define $s_i := m/(m, r_i)$. Then the equation

$$P(x) = by^m$$

has only finitely many solutions $x, y \in \mathbf{Z}$ unless $\{s_1, \ldots, s_n\}$ is a permutation of one of the n-tuples

(i) $\{s, 1, \ldots, 1\}$, $s \geqslant 1$; (ii) $\{2, 2, 1, \ldots, 1\}$.

Proof. This follows from Le Veque [2], Theorem 1, giving the stated result in the case $b = 1$, $P \in \mathbf{Z}[x]$. Let d be an integer such that $dP(x) \in \mathbf{Z}[x]$. Then $b^{m-1} d^m P(x)$ is a polynomial with integer coefficients, satisfying

$$b^{m-1} d^m P(x) = (bdy)^m.$$

According to Le Veque's theorem there are only finitely many solutions x and bdy. □

LEMMA 3. (Schinzel, Tijdeman.) *Let $0 \neq b \in \mathbf{Z}$ and let $P(x) \in \mathbf{Q}[x]$ be a polynomial with at least two distinct zeros. Then the equation*

$$P(x) = by^z$$

in integers x, $y>1$, z implies that $z<C$, where C is an effectively computable constant depending only on P and b.

Proof. See Schinzel & Tijdeman [5]. For a generalization compare Shorey, van der Poorten, Tijdeman, Schinzel [6], Theorem 2. □

3. A lemma; proof of the theorem

From section 2 it is clear that we have to prove that the polynomial

$$P(x) = B_q(x) - B_q + qR(x-1)$$

satisfies the conditions in Lemmas 2 and 3 with respect to the multiplicity of its zeros, unless $q \in \{2, 4, 6\}$. We shall formulate such a result, postponing its proof for the time being, and show that this result implies our theorem.

LEMMA 4. *For $q \geq 2$ let $B_q(x)$ be the q-th Bernoulli polynomial. Let $R^*(x) \in \mathbf{Z}[x]$ and set*

$$P(x) = B_q(x) - B_q + qR^*(x). \tag{5}$$

Then

(i) *$P(x)$ has at least three zeros of odd multiplicity, unless $q \in \{2, 4, 6\}$.*

(ii) *For any odd prime p, at least two zeros of $P(x)$ have multiplicities relatively prime to p.*

Proof of the Theorem. Let $R(x-1)=R^*(x)$. We know from Lemma 4 that the polynomial

$$1^k+2^k+\ldots+x^k+R(x) = \frac{1}{k+1}\left(B_{k+1}(x+1) - B_{k+1} + (k+1)R^*(x+1)\right)$$

has at least two distinct zeros. Hence it follows from the equation (3) by applying Lemma 3 that z is bounded. We may therefore assume that z is fixed. So we have obtained the following equation in integers x and y

$$P(x) = by^m, \tag{6}$$

where P is given by (5) with $q=k+1$. Write $P(x)=a_0\prod_{i=1}^n(x-\alpha_i)^{r_i}$, where $a_0 \neq 0$, $\alpha_i \neq \alpha_j$ if $i \neq j$. If $p \mid m$ for an odd prime p, then by Lemma 4 at least two zeros of P have multiplicities prime to p, so we may assume that $(r_1, p) = (r_2, p) = 1$. Setting $s_i = m/(m, r_i)$, we find that $p \mid s_1$ and $p \mid s_2$. If m is even, then by Lemma 4 at least three zeros have odd multiplicity, say r_1, r_2 and r_3 are odd. Hence s_1, s_2 and s_3 are even. Consequently, the exceptional cases in Lemma 2 cannot occur and thus (6) has only finitely many solutions for any $m > 1$. This proves the theorem. □

4. Proof of Lemma 4

By the Staudt-Clausen theorem (see Rademacher [3], p. 10), the denominators of the Bernoulli numbers B_1, B_{2k} $(k = 1, 2, \ldots)$ are even but not divisible by 4. Choose the minimal $d \in \mathbf{N}$ such that $dP(x) \in \mathbf{Z}[x]$, so

$$dP(x) = d \sum_{l=0}^{q-1} \binom{q}{l} B_l x^{q-l} + dqR^*(x) \in \mathbf{Z}[x];$$

hence $d \binom{q}{1} B_1 \in \mathbf{Z}$ and

$$\binom{q}{2k} dB_{2k} \in \mathbf{Z}, \quad \text{for } k = 1.\ 2, \ldots, [\tfrac{1}{2}(q-1)].$$

If d is odd, then necessarily $\binom{q}{1}$ and $\binom{q}{2k}$ must be even for $k = 1, 2, \ldots, [\frac{1}{2}(q-1)]$. Write $q = 2^\lambda r$, where $\lambda \geq 1$ and r is odd. Then $\binom{q}{2^\lambda}$ is odd, giving a contradiction unless $r = 1$. So

$$d \text{ is odd} \Leftrightarrow q = 2^\lambda \quad \text{for some } \lambda \geq 1. \tag{7}$$

If $q \neq 2^\lambda$ for any $\lambda \geq 1$ then

$$d \equiv 2 \pmod 4. \tag{8}$$

We distinguish three cases

A. Let $q \geq 3$ be odd. Then $d \equiv 2 \pmod 4$ and for $l = 1, 2, 4, \ldots, q-1$

$$d \binom{q}{l} B_l \equiv \binom{q}{l} \pmod 2.$$

Now

$$dP(x) \equiv x^{q-1} + \sum_{\lambda=1}^{\frac{1}{2}(q-1)} \binom{q}{2\lambda} x^{q-2\lambda} \pmod 2.$$

Hence,

$$d(P(x) + xP'(x)) \equiv x^{q-1} \pmod 2.$$

Any common factor of $dP(x)$ and $dP'(x)$ must therefore be congruent to a power of x (mod 2). Since $dP'(0)\equiv qdB_{q-1}\equiv 1$ (mod 2), we find that $dP(x)$ and $dP'(x)$ are relatively prime (mod 2). So any common divisor of $dP(x)$ and $dP'(x)$ in $\mathbf{Z}[x]$ is of the shape $2S(x)+1$. Write $dP(x)=T(x)Q(x)$, where $T(x)=\prod_i T_i(x)^{k_i}\in\mathbf{Z}[x]$ contains the multiple factors of dP and $Q\in\mathbf{Z}[x]$ contains its simple factors. Then $T(x)$ is of the shape $2S(x)+1$ with $S\in\mathbf{Z}[x]$, so

$$Q(x)\equiv dP(x)\equiv x^{q-1}+\ldots \quad (\text{mod } 2).$$

Thus the degree of $Q(x)$ is at least $q-1$, proving case A if $q>3$. If $q=3$, then

$$2P(x)\equiv 2x^3+x\equiv 2x(x+1)(x-1) \quad (\text{mod } 3),$$

showing that P has three simple roots, which proves Lemma 4 if q is odd.

B. Suppose $q=2^\lambda$ for some $\lambda\geqslant 1$, so d is odd. We first prove (i) so we may assume that $\lambda\geqslant 3$. Now $\binom{q}{2k}$ is divisible by 4 unless $2k=\frac{1}{2}q=2^{\lambda-1}$. Similarly, $\binom{q}{2k}$ is divisible by 8 unless $2k$ is divisible by $2^{\lambda-2}$. We have therefore for some odd d', writing $\nu=\frac{1}{4}q$

$$dP(x)\equiv dx^{4\nu}+2x^{3\nu}+d'x^{2\nu}+2x^{\nu} \quad (\text{mod } 4). \tag{9}$$

Write $dP(x)=T^2(x)Q(x)$, where $T(x)$, $Q(x)\in\mathbf{Z}[x]$ and Q contains each factor of odd multiplicity of P in $\mathbf{Z}[x]$ exactly once. Assume that $\deg Q(x)\leqslant 2$. Since

$$T^2(x)Q(x)\equiv x^{4\nu}+x^{2\nu}=x^{2\nu}(x^{2\nu}+1) \quad (\text{mod } 2),$$

$T^2(x)$ must be divisible by $x^{2\nu-2}$ (mod 2). So

$$T(x)=x^{\nu-1}T_1(x)+2T_2(x),$$
$$T^2(x)=x^{2\nu-2}T_1^2(x)+4T_3(x),$$

for certain T_1, T_2, $T_3\in\mathbf{Z}[x]$. If $q>8$, then $\nu>2$ so the last identity is incompatible with (9) because of the term $2x^\nu$. Hence $\deg Q\geqslant 3$, which proves (i). If $q=8$, then $d=3$ and

$$dP(x)\equiv 3x^8+2x^6+x^4+2x^2\equiv -x^2(x+1)(x-1)(x^2+1)(x^2+2) \quad (\text{mod } 4).$$

All these factors—except x^2—are simple, so $\deg Q\geqslant 6>3$ if $q=8$, proving (i) in case B.

To prove (ii), let p be an odd prime and write $dP(x)=(T(x))^pQ(x)$, where Q, $T\in\mathbf{Z}[x]$ and all the roots of multiplicity divisibly by p are incorporated in $(T(x))^p$. We have, writing $\mu=\frac{1}{2}q$,

$$dP(x)=(T(x))^pQ(x)\equiv x^\mu(x^\mu+1)\equiv x^\mu(x+1)^\mu \quad (\text{mod } 2).$$

Since μ is prime to p, Q has at least two different zeros, proving (ii) in case B.

C. Suppose q is even and $q \neq 2^\lambda$ for any λ. Then $d \equiv 2 \pmod 4$ and hence

$$dP(x) \equiv \sum_{k=1}^{\frac{1}{2}(q-2)} \binom{q}{2k} x^{2k} \equiv \sum_{l=1}^{q-1} \binom{q}{l} x^l \equiv (x+1)^q - x^q - 1 \pmod 2.$$

Write $q = 2^\lambda r$, where $r > 1$ is odd. Then

$$dP(x) \equiv (x+1)^q - x^q - 1 \equiv ((x+1)^r - x^r - 1)^{2^\lambda} \pmod 2.$$

Since $r > 1$ is odd, $(x+1)^r - x^r - 1$ has x and $x+1$ as simple factors (mod 2). Thus

$$dP(x) \equiv x^{2^\lambda}(x+1)^{2^\lambda} H(x) \pmod 2,$$

where $H(x)$ is neither divisible by x nor by $x+1$ (mod 2). As in the preceding case, $P(x)$ must have two roots of multiplicity prime to p. This proves part (ii) of the lemma.

In order to prove part (i) we may assume that $q \geqslant 10$, because $q = 2, 4, 6$ are the exceptional cases and $q = 8$ is treated in section B. Now d and q are even, so dq is divisible by 4 and, in view of (8)

$$dP(x) \equiv 2x^q - qx^{q-1} + \tfrac{1}{6}d\binom{q}{2}x^{q-2} + \dots + dB_{q-2}\binom{q}{2}x^2 \pmod 4. \tag{10}$$

Write $dP(x) = T^2(x)Q(x)$, where $T, Q \in \mathbf{Z}[x]$ and $Q(x)$ contains each factor of odd multiplicity of P exactly once. Let

$$T(x) \equiv x^{\lambda_1} + x^{\lambda_2} + \dots + x^{\lambda_m} \pmod 2,$$

where $\lambda_1 > \lambda_2 > \dots > \lambda_m \geqslant 0$. Then

$$T^2(x) \equiv x^{2\lambda_1} + x^{2\lambda_2} + \dots + x^{2\lambda_m} + 2\sum_l p_l x^l \pmod 4,$$

where p_l is the number of solutions of $\lambda_i + \lambda_j = l$, $\lambda_i < \lambda_j$, $i, j \in \{1, \dots, m\}$.

Assume that $\deg Q < 3$. Let

$$Q(x) = ax^2 + bx + c.$$

If a is odd, then $T^2(x)Q(x) \equiv ax^{2\lambda_1+2} + \dots \pmod 4$, which is incompatible with (10). If $4 \mid a$, then $T^2(x)Q(x) \equiv bx^{2\lambda_1+1} + \dots \pmod 4$ so $4 \mid b$. By the definition of d, $dP(x)$ must have some odd coefficients, so c must be odd. Hence $T^2(x)Q(x) \equiv cx^{2\lambda_1} + \dots \pmod 4$, which is again incompatible with (10). Thus $a \equiv 2 \pmod 4$ and $\lambda_1 = \frac{1}{2}(q-2)$. By comparing the coefficient of x^{q-1} in (10) and in $T^2(x)Q(x)$, we find that $b \equiv q \pmod 4$, so b is even and c must be odd. So $Q(x) \equiv 1 \pmod 2$ and

$$dP(x) \equiv T^2(x) \equiv x^{2\lambda_1} + x^{2\lambda_2} + \dots + x^{2\lambda_m} \pmod 2.$$

Let $\Lambda=\{\lambda_1, \lambda_2, \dots, \lambda_m\}$. We have by (10) that

$$\lambda_i \in \Lambda \quad \Leftrightarrow \quad 2 \leqslant 2\lambda_i \leqslant q-2 \text{ and } \binom{q}{2\lambda_i} \equiv 1 \pmod 2. \tag{11}$$

Since $\frac{1}{2}(q-2)\in\Lambda$, we have that $\binom{q}{2}$ is odd, so $q\equiv 2 \pmod 4$, whence $b\equiv 2 \pmod 4$. Thus

$$dP(x) \equiv \sum_{\lambda_i \in \Lambda} (2x^{2\lambda_i+2}+2x^{2\lambda_i+1}+cx^{2\lambda_i}) + 2\sum_l p_l x^l \pmod 4.$$

If $\lambda_i \in \Lambda$ and $\lambda_i < \frac{1}{2}(q-2)$, then by (10) the coefficient of $x^{2\lambda_i+1}$ in $dP(x)$ must vanish, so

$$\left.\begin{array}{l} \lambda_i \in \Lambda \\ \lambda_i < \frac{1}{2}(q-2) \end{array}\right\} \Rightarrow p_{2\lambda_i+1} \text{ is odd.} \tag{12}$$

Observe that by $q \geqslant 10$ we have $\frac{1}{2}(q-2) \geqslant 4$.

Now $\binom{q}{2}$ is odd, so $1\in\Lambda$ by (11). Thus p_3 is odd by (12) and hence, by the definition of the numbers p_l, $2\in\Lambda$. So $\binom{q}{4}$ is odd, thus $q-2\equiv 4 \pmod 8$. Then also $\binom{q}{6}$ is odd, so $3\in\Lambda$ by (11). Since $2\in\Lambda$, p_5 is odd by (12). But if $\{1, 2, 3, 4\}\in\Lambda$, then $p_5=2$. So $4\notin\Lambda$ and $\binom{q}{8}$ is even by (11). Thus $q-6\equiv 0 \pmod{16}$, so $\binom{q}{10}\equiv\binom{q}{12}\equiv\binom{q}{14}\equiv 0 \pmod 2$. Hence $5\notin\Lambda$, $6\notin\Lambda$ and $7\notin\Lambda$. So $p_7=0$. But since $3\in\Lambda$, p_7 is odd by (12). This gives a contradiction, so $\deg Q \geqslant 3$ if $q\geqslant 10$. The proof of Lemma 4 is thus complete. □

5. On the cases $k=1, 3, 5$

Consider the equation (3) for fixed $k\in\{1, 3, 5\}$ and fixed $z=m>1$. Let $R^*(x)=R(x-1)$ and $q=k+1$. Then (3) is equivalent to the equation

$$P(x) = by^m, \tag{13}$$

where $P(x)=B_q(x)-B_q+qR^*(x)$, $q\in\{2, 4, 6\}$ and $b\neq 0$ is a fixed integer divisible by q.

If $q=2$, then $P(x)=x^2-x+2R^*(x)$. $P(x)$ has two zeros of multiplicity 1, since $P(x)\equiv x(x-1) \pmod 2$. In view of Lemma 2, (13) has a finite number of integer solutions x, y unless $m=2$. In the case $m=2$ we can choose $R^*(x)=(x^2-x)(2S^2(x)+2S(x))$ for any $S(x)\in\mathbf{Z}[x]$. In that case (13) becomes

$$(x^2-x)(2S(x)+1)^2 = by^2,$$

which amounts to Pell's equation, having an infinite number of solutions in integers $x, y \geq 1$ for infinitely many choices of b.

In the case $q=4$ we have $P(x)=x^4-2x^3+x^2+4R^*(x)$. Since $P(x)\equiv x^2(x-1)^2 \pmod 2$, by Lemma 2 the equation (13) has infinitely many solutions only if $m=2$ or $m=4$. If this is the case, there are infinitely many choices for $R^*(x)$ and b such that (13) has an infinite number of solutions. We may take $R^*(x)=x^2(x-1)^2(4S^4(x)+8S^3(x)+6S^2(x)+2S(x))$ for any $S(x)\in \mathbf{Z}[x]$ and from (13) we get

$$x^2(x-1)^2(2S(x)+1)^4 = by^m, \quad m=2 \text{ or } m=4.$$

Both for $m=2$ and for $m=4$ this equation has an infinite number of solutions in integers $x, y \geq 1$ for infinitely many choices of b.

In the case $q=6$, (13) is equivalent to

$$2P(x) = 2x^6-6x^5+5x^4-x^2+12R^*(x) = x^2(x-1)^2(2x^2-2x-1)+12R^*(x) = by^m, \tag{14}$$

where $12\,|\,b$. Since $2P(x)\equiv 2(x-1)^2x^2(x+1)^2 \pmod 3$, by Lemma 2 the equation (14) has infinitely many solutions in integers $x, y\geq 1$ only if $m=2$. For infinitely many choices of $R^*(x)$ and b there is an infinite number of solutions x, y if $m=2$. We may then choose $R^*(x)=x^2(x-1)^2(2x^2-2x-1)(3S^2(x)+2S(x))$ for any $S(x)\in\mathbf{Z}[x]$ and (14) may be written in the form

$$x^2(x-1)^2(2x^2-2x-1)(6S(x)+1)^2 = by^2.$$

Consequently, (14) has an infinite number of solutions in integers $x, y\geq 1$ for infinitely many choices of b.

References

[1]. GYÖRY, K., TIJDEMAN, R. & VOORHOEVE, M., On the equation $1^k+2^k+\dots+x^k=y^z$. *Acta Arith.*, 37, to appear.
[2]. LE VEQUE, W. J., On the equation $y^m=f(x)$. *Acta Arith.*, 9 (1964), 209–219.
[3]. RADEMACHER, H., *Topics in Analytic Number Theory*. Springer Verlag, Berlin, 1973.
[4]. SCHÄFFER, J. J., The equation $1^p+2^p+3^p+\dots+n^p=m^q$. *Acta Math.*, 95 (1956), 155–159.
[5]. SCHINZEL, A. & TIJDEMAN, R., On the equation $y^m=P(x)$. *Acta Arith.*, 31 (1976), 199–204.
[6]. SHOREY, T. N., VAN DER POORTEN, A. J., TIJDEMAN, R. & SCHINZEL, A., Applications of the Gel'fond-Baker method to Diophantine equations. *Transcendence Theory: Advances and Applications*, pp. 59–78, Academic Press, 1977.

Received August 22, 1978