ACTA ARITHMETICA
151.2 (2012)

On some generalizations of the diophantine equation $s(1^k + 2^k + \cdots + x^k) + r = dy^n$

by

Csaba Rakaczki (Debrecen and Miskolc)

Dedicated to Professor Kálmán Győry on his 70th birthday

1. Introduction. In this paper we study the diophantine equation

$$F(S_k(x)) = dy^n \quad \text{in integer unknowns } x, y, n \geq 2, \tag{1}$$

where $F(x) \in \mathbb{Q}[x]$ and $0 \neq d \in \mathbb{Z}$. Here $S_k(x) = 1^k + 2^k + \cdots + x^k$ is the sum of the first x kth powers for a positive integer k. As is known, $S_k(x)$ is strongly related to the Bernoulli polynomials, namely

$$S_k(x) = \frac{B_{k+1}(x+1) - B_{k+1}(0)}{k+1}. \tag{2}$$

For $k = 0, 1, 2, \ldots$, the Bernoulli polynomials $B_k(x)$ are defined by

$$\frac{te^{tx}}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k(x)t^k}{k!}, \quad |t| < 2\pi. \tag{3}$$

In 1956, Schäffer [15] investigated the equation

$$S_k(x) = y^n. \tag{4}$$

He proved the following.

Theorem A. *For fixed $k \geq 1$ and $n \geq 2$,* (4) *has at most finitely many solutions in positive integers x and y, unless*

$$(k, n) \in \{(1, 2), (3, 2), (3, 4), (5, 2)\}, \tag{5}$$

where, in each case, there are infinitely many such solutions.

Schäffer's proof used an ineffective method due to Thue and Siegel so his result is also ineffective. This means that the proof does not provide any algorithm to find all solutions. Applying Baker's method, Győry, Tijdeman

2010 *Mathematics Subject Classification*: Primary 11D41; Secondary 11B68.
Key words and phrases: Bernoulli polynomials, higher degree equations.

DOI: 10.4064/aa151-2-4

and Voorhoeve [10] proved a more general and effective result in which the exponent n is also unknown.

Theorem B (Győry, Tijdeman and Voorhoeve [10]). *Let $k \geq 2$ and r be fixed integers with $k \notin \{3,5\}$ if $r = 0$, and let s be a square-free odd integer. Then*

$$sS_k(x) + r = y^n \tag{6}$$

in positive integers x, $y \geq 2$, $n \geq 2$ has only finitely many solutions, and they can all be effectively determined.

Later, various generalizations and analogues of Theorem B have been established by several authors [4]–[7], [11], [12], [17], [18]. For a survey of these results we refer to [9] and the references given there. Here we present only the result of Brindza [4].

Theorem C (Brindza [4]). *Set $A = \mathbb{Z}[x]$, $\kappa = (k+1)\prod_{p-1|(k+1)!} p$ (p prime), and*

$$F(y) = Q_n y^n + \cdots + Q_1 y + Q_0 \in A[y].$$

If $Q_i(x) \equiv 0 \pmod{\kappa^i}$ for $i = 2, \ldots, m$, $Q_1(x) \equiv \pm 1 \pmod 4$, and $k \notin \{1,2,3,5\}$ then all solutions of the equation

$$F(S_k(x)) = y^n \tag{7}$$

in integers x, $y \geq 2$, $n \geq 2$ satisfy $\max(x,y,n) < c_1$, where c_1 is an effectively computable constant depending only on F and k.

The purpose of the present paper is to give a generalization of Theorem B and an extension of Theorem C to the case when the polynomials $Q_i(x)$ are arbitrary constant polynomials. Our new results are in Section 2. The proofs are given in Sections 3–5. In Section 6 we list the results and lemmas which we need for the proofs of our Theorems 2.1 and 2.3.

2. New results

Theorem 2.1. *Let $F(x)$ be a polynomial with rational coefficients and $d \neq 0$ be an integer. Suppose that $F(x)$ is not an nth power. Then the equation*

$$F(S_k(x)) = dy^n \tag{8}$$

has only finitely many integer solutions $x, y \geq 2$, $n \geq 2$, which can be effectively determined provided that $k \geq 6$.

We remark that we do not impose any conditions on the coefficients of the polynomial $F(x)$. In the special case when $F(x) = sx + r$ is a linear polynomial we can prove the following extension of the result of Győry, Tijdeman and Voorhoeve [10].

Theorem 2.2. *Let $k>1$, $r,s\neq 0$ be fixed integers. Then apart from the cases when* (i) $k=3$ *and either* $r=0$ *or* $s+64r=0$, *and* (ii) $k=5$ *and either* $r=0$ *or* $s-324r=0$, *the equation*

$$s(1^k+2^k+\cdots+x^k)+r=y^n \tag{9}$$

in integers $x>0$, y with $|y|\geq 2$, and $n\geq 2$ has only finitely many solutions which can be effectively determined.

In the proof of this theorem we will exhibit, in each exceptional case, an equation which has infinitely many integer solutions x, y and $n\geq 2$.

We note that in the case $k=1$ the equation

$$8t^{2n}(1+2+\cdots+x)+t^{2n}=y^n, \qquad t\in\mathbb{N}, \tag{10}$$

has infinitely many integer solutions $x=(z^n-1)/2$, $y=(zt)^2$, n, where $z\geq 1$ is an arbitrary integer.

The proofs of the above theorems are based upon Lemma 6.6 and the next result.

Theorem 2.3. *For every $b\in\mathbb{C}$ the polynomial $B_{2m}(x)+b$ has at least three simple zeros if $m\geq 4$.*

We remark that $B_6(x)-B_6(0)=(2x^2-2x-1)(x(x-1))^2/2$ and $B_4(x)-B_4(1/2)=(4x^2-4x-1)(2x-1)^2/16$.

3. Proof of Theorem 2.3. From Lemmas 6.6, 6.4 and 6.1(iii) we know that there is at most one complex number b for which the polynomial $B_{2m}(x)+b$ does not have three simple zeros. Now assume that $m\geq 4$ and the polynomial $B_{2m}(x)+b$ does not have three simple zeros for some complex number b. Then either

$$\text{(a) } B_{2m}(x)+b=F(x)^2 \quad \text{or} \quad \text{(b) } B_{2m}(x)+b=G(x)F(x)^2,$$

where $F(x),G(x)\in\mathbb{C}[x]$ and $G(x)$ is a quadratic polynomial with non-zero discriminant.

In case (a) we have $B_{2m}(x)=F(x)^2-b=T(F(x))$, where $T(x)=x^2-b$. Lemma 6.3 implies that every non-trivial decomposition of $B_{2m}(x)$ is equivalent to $\widetilde{B}_m((x-1/2)^2)$, where $\widetilde{B}_m(x)\in\mathbb{Q}[x]$ is an indecomposable polynomial of degree m. This gives $m=2$, which contradicts our assumption that $m\geq 4$.

In case (b) we only give the strategy of the proof, which uses lemmas of Section 6:

Step 1. We deduce that b is rational and so $G(x)$, $F(x)\in\mathbb{Q}[x]$. See Lemma 6.9.

Step 2. We show that $G(x)$ is of the form x^2-x+u/v, where $v>0$, $u\in\mathbb{Z}$ with $(u,v)=1$, and $F(1-x)=\pm F(x)$. See Lemmas 6.10–6.12.

Step 3. Every polynomial with rational coefficients can be written uniquely as a product of a rational number and a primitive polynomial. Hence we can assume that

$$vb_{2m-2}(B_{2m}(x)+b) = (vx^2-vx+u)f(x)^2 = (vx^2-vx+u)\sum_{i=0}^{2m-2} b_i x^i, \tag{11}$$

where $f(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a primitive polynomial.

Step 4. We prove that v is even if $a_0 \neq 0$. See Lemmas 6.13 and 6.14. If $a_0 = 0$ then $b = -B_{2m}(0) = -B_{2m}$ and Lemma 6.5 yields $m \leq 3$.

Step 5. We infer that $2 \parallel v$ or $2^2 \parallel v$. See Lemmas 6.15–6.17.

Step 6. If $2 \parallel v$ then we get a contradiction provided that m is odd. See Lemmas 6.18–6.21.

Step 7. We show that if $2^2 \parallel v$ then m is even. See Lemma 6.22.

Step 8. We get a contradiction if m is even. See Lemmas 6.23 and 6.24.

4. Proof of Theorem 2.1. First we give an effective upper bound for the exponent n in (8). Write $F(x) = A(x-\beta_1)^{r_1}\cdots(x-\beta_t)^{r_t}$. Then

$$\begin{aligned} F(S_k(x-1)) &= A_1(B_{k+1}(x)-\gamma_1)^{r_1}\cdots(B_{k+1}(x)-\gamma_t)^{r_t} \\ &= A\prod_{i=1}^{s}(x-\delta_i)^{l_s}. \end{aligned} \tag{12}$$

We know from Theorem 2.3 and Lemma 6.6 that any shifted Bernoulli polynomial has at least three simple zeros. Thus, $F(S_k(x))$ has at least two distinct zeros by (12). Now we can apply Lemma 6.7 to derive an effective upper bound for n. We therefore may assume that n is fixed. Since $F(x)$ is not an nth power we can assume that $n/(n,r_1) \neq 1$. Using again the fact that any shifted Bernoulli polynomial has at least three simple zeros we can deduce that $l_1 = l_2 = l_3 = r_1$ in (12). On applying Lemma 6.8 we find that there are only finitely many solutions x, y of equation (8).

5. Proof of Theorem 2.2. In the case $k \geq 6$, Theorem 2.2 is a simple consequence of Theorem 2.1. Suppose that $1 < k < 6$ and write equation (9) in the form

$$\frac{s}{k+1}(B_{k+1}(x+1)+b) = y^n, \quad \text{where} \quad b = \frac{r(k+1)}{s} - B_{k+1}(0). \tag{13}$$

Let $\Delta(k,b)$ denote the discriminant of the polynomial $B_{k+1}(x+1)+b$. It is easy to see that $\Delta(k,b)$ is a polynomial in b. In the following table we give the zeros of $\Delta(k,b)$ for $k = 2,3,4,5$.

k	Solutions of $\varDelta(k,b)=0$
2	$\frac{\sqrt{3}}{36},\ -\frac{\sqrt{3}}{36}$
3	$\frac{1}{30},\ -\frac{7}{240}$
4	$\pm\frac{\sqrt{375+20\sqrt{30}}}{900},\ \pm\frac{\sqrt{375-20\sqrt{30}}}{900}$
5	$-\frac{1}{42},\ \frac{31}{1344},\ -\frac{1}{189}$

Using the fact that b is rational we find that the polynomials $B_3(x+1)+b$ and $B_5(x+1)+b$ have only simple zeros. By Lemmas 6.7 and 6.8, we obtain the assertion of Theorem 2.2 for $k=2$ and 4.

Now let $k=3$. We know that equation (13) may have infinitely many integer solutions x, y, $n\geq 2$ only if $B_4(x+1)+b$ has multiple zeros, that is, if $b=1/30$ or $-7/240$. In the first case we deduce that $r=0$ from (13) and $B_4(0)=-1/30$. But then, if s is a fourth power, equation (9) has infinitely many integer solutions x, y and n by Theorem A. If $b=-7/240$ then $s+64r=0$ and so our equation is

$$-r(4x^2+4x-1)(2x+1)^2=y^n. \tag{14}$$

Since the polynomial on the left side of (14) has two simple zeros, we infer from Lemmas 6.7 and 6.8 that (14) has only finitely many integer solutions x, y and $n\geq 3$. If $n=2$, $s=448$ and $r=-7$ then the equation

$$448S_3(x)-7=y^2 \tag{15}$$

has the integer solutions

$$x=\frac{b_n-1}{2},\qquad y=a_nb_n,\quad n=0,1,\ldots,$$

where $(a_0,b_0)=(7,3)$, $(a_{n+1},b_{n+1})=(8a_n+21b_n,3a_n+8b_n)$.

When $k=5$ and $b=31/1344$ the polynomial $B_6(x+1)+b$ has four simple zeros. Thus, there are only finitely many integer solutions x, y, and $n\geq 2$. If $b=-1/42$ we have again $r=0$, and equation (9) has infinitely many integer solutions x, y for $n=2$ by Theorem A. Finally, if $b=-1/189$ we can infer that $s=2^23^4r$, and so we get the equation

$$r(6x^2+6x+1)(3x^2+3x-1)^2=y^n. \tag{16}$$

It is obvious that the polynomial on the left side has two simple zeros. Using again Lemmas 6.7 and 6.8, we deduce that equation (16) has only finitely many integer solutions x, y and $n\geq 3$. If $n=2$, $s=324$ and $r=1$ then the equation

$$324S_5(x)+1=y^2 \tag{17}$$

has the integer solutions

$$x = \frac{a_n - 3}{6}, \qquad y = b_n(3x^2 + 3x - 1), \quad n = 1, 2, \ldots,$$

where $(a_0, b_0) = (3, 1)$, $(a_{n+1}, b_{n+1}) = (5a_n + 12b_n, 2a_n + 5b_n)$.

6. Auxiliary results. For the well-known properties of Bernoulli polynomials and numbers we refer to Rademacher [14, pp. 1–17]. In the next two lemmas we list some properties of Bernoulli polynomials that will be often used, sometimes without special reference.

Lemma 6.1. *For a positive integer n, let $B_n(x)$ denote the nth Bernoulli polynomial and set $B_n = B_n(0)$. Then:*

(i) $B_n(x) = (-1)^n B_n(1 - x)$.
(ii) $B_n(x + 1) - B_n(x) = nx^{n-1}$.
(iii) $B'_n(x) = nB_{n-1}(x)$.
(iv) $(-1)^{n-1}B_{2n} > 0$ *for* $n \geq 1$.
(v) $|B_{2n}| > 2(2n)!/(2\pi)^{2n}$.
(vi) $B_n(1/2) = (2^{1-n} - 1)B_n$.
(vii) $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$.

Lemma 6.2 (The von Staudt–Clausen Theorem). *The denominator of the Bernoulli number B_{2n} is the product of those different primes p for which $p - 1$ divides $2n$.*

A *decomposition* of a polynomial $H(x) \in \mathbb{C}[x]$ is an equality of the form $H(x) = H_1(H_2(x))$, where $H_1(x), H_2(x) \in \mathbb{C}[x]$; the decomposition is *non-trivial* if $\deg H_1(x), \deg H_2(x) > 1$. Two decompositions $H(x) = H_1(H_2(x))$ and $H(x) = G_1(G_2(x))$ are *equivalent* if there exists a linear polynomial $t(x) \in \mathbb{C}[x]$ such that $H_1(x) = G_1(t(x))$ and $G_2(x) = t(H_2(x))$. The polynomial $F(x)$ is called *decomposable* if it has at least one non-trivial decomposition, and *indecomposable* otherwise.

The following lemma was proved by Bilu et al. [1].

Lemma 6.3. *The polynomial $B_n(x)$ is indecomposable for odd n. If $n = 2m$ is even, then any non-trivial decomposition of $B_n(x)$ is equivalent to $B_n(x) = \widetilde{B}_m((x - 1/2)^2)$, where $\widetilde{B}_m(x) \in \mathbb{Q}[x]$ is an indecomposable polynomial of degree m.*

Lemma 6.4. *Bernoulli polynomials have no multiple zeros.*

Proof. See [2] and [8]. ■

The next lemma is due to Győry, Tijdeman and Voorhoeve [10].

Lemma 6.5. *For every $r \in \mathbb{Z}$ the polynomial $B_k(x) - B_k + r$ has at least three simple zeros if $k = 3$ and at least four simple zeros if $k \geq 4$, unless $r = 0$ and $k \in \{4, 6\}$.*

Lemma 6.6 (Pintér and Rakaczki [13]). *If $k \geq 5$ is odd then the polynomial $B_k(x)+b$ has at least three zeros of odd multiplicities for every complex number b. If $k \geq 8$ is even then there is at most one complex number b for which the polynomial $B_k(x)+b$ does not have three zeros of odd multiplicities.*

The following well known effective result on superelliptic equations was proved by Schinzel and Tijdeman [16].

Lemma 6.7. *Let $0 \neq d \in \mathbb{Z}$, and let $P(x) \in \mathbb{Z}[x]$ be a polynomial with at least two distinct zeros. Then the equation*

$$P(x) = dy^z \tag{18}$$

in integers x, $y > 1$, z implies that $z < C$, where $C = C(P, d)$ is an effectively computable constant.

Lemma 6.8 (Brindza [3]). *Let K be an algebraic number field with the ring of integers O_K, and let*

$$f(x) = a_0x^N + \cdots + a_N = a_0\prod_{i=1}^{n}(x - \alpha_i)^{r_i}$$

be a polynomial in $O_K[x]$ with $a_0 \neq 0$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. Further, let $d \in O_K$, $m > 1$ and $q_i = m/(m, r_i)$, $i = 1, \dots, n$. Suppose that $(q_1, \dots, q_n)$ is not a permutation of $(q, 1, \dots, 1)$ or $(2, 2, 1, \dots, 1)$, where $q \geq 1$. Then the equation

$$f(x) = dy^m \qquad \text{in } x, y \in O_K$$

has only finitely many solutions, and they can all be effectively determined.

Lemma 6.9. *If $B_{2m}(x)+b$ $(m \geq 4)$ does not have three simple zeros then b is rational.*

Proof. Suppose that $B_{2m}(x) + b$ does not have three simple zeros and consider the following euclidean algorithm:

$$\begin{aligned}
&B_{2m}(x) + b = (x - 1/2)B_{2m-1}(x) + r_1(x),\\
&B_{2m-1}(x) = t_1(x)r_1(x) + r_2(x),\\
&r_1(x) = t_2(x)r_2(x) + r_3(x),\\
&\vdots\\
&r_{k-3}(x) = t_{k-2}(x)r_{k-2}(x) + r_{k-1}(x),\\
&r_{k-2}(x) = t_{k-1}(x)r_{k-1}(x) + r_k(x),\\
&r_{k-1}(x) = t_k(x)r_k(x) + r_{k+1}(x).
\end{aligned} \tag{19}$$

Take b as a parameter. We denote by t_i, r_i the degrees of the polynomials $t_i(x)$ and $r_i(x)$, respectively, and $r_k(x)$ the first polynomial whose leading coefficient depends on b. First we prove that the coefficients of the polynomials $t_1(x), \dots, t_{k-1}(x)$ do not depend on b. Indeed, if the coefficients of $t_1(x)$ depend on b then one of the coefficients of $B_{2m-1}(x)$ also depends on b, which is impossible. Assume that we know that the coefficients of $t_1(x), \dots, t_{i-1}(x)$ do not depend on b for some $i \in \{2, \dots, k-1\}$. Notice that x^0 in $r_1(x)$, x^{t_1} in $r_2(x)$, and $x^{t_1+\cdots+t_{i-1}}$ in $r_i(x)$ is the largest power whose coefficient depends on b. If $t_i(x)$ depends on b then we see, using $r_{i+1} < r_i$ and the euclidean algorithm, that the coefficient of x^{r_i+j} depends on b in $r_{i-1}(x)$. Here j is the largest exponent for which the coefficient of x^j depends on b in $t_i(x)$. But $x^{t_1+\cdots+t_{i-2}}$ is the largest power in $r_{i-1}(x)$ whose coefficient depends on b. Thus

$$t_1 + \cdots + t_{i-2} \geq r_i + j \geq r_i \geq r_{k-1}.$$

Since the leading coefficient of $r_{k-1}(x)$ does not depend on b, it is obvious that $r_{k-1} \geq \deg(\gcd(B_{2m}(x) + b, B_{2m-1}(x))) \geq m - 1$.

Comparing the degrees of the polynomials in the algorithm we obtain

$$2m = 1 + \sum_{j=1}^{i-2} t_j + r_{i-2} \geq 1 + r_i + r_{i-2} \geq 3 + 2r_i \geq 3 + 2(m-1) = 2m + 1.$$

This contradiction shows that $t_i(x)$ does not depend on b for $i = 1, \dots, k-1$. Consequently, every coefficient of the polynomials $r_1(x), \dots, r_k(x)$ is of the form $u + vb$, where u, v are rational numbers, and

$$r_k = t_1 + \cdots + t_{k-1}.$$

When $r_k(x) \equiv 0$ all coefficients $u + vb$ of $r_k(x)$ are zero. This means that b must be a rational number.

If $r_k(x) \not\equiv 0$ then

$$2m = 1 + t_1 + \cdots + t_{k-1} + t_k + r_k \geq 2 + 2r_k, \quad \text{that is,} \quad m - 1 \geq r_k. \tag{20}$$

By (20), we deduce that $r_k = m - 1$ and $r_{k+1}(x)$ must be identically zero for some b since otherwise the degree of the greatest common divisor would be less than $m - 1$. Comparing again the degrees of the polynomials in the euclidean algorithm we infer that

$$2m = 1 + t_1 + \cdots + t_{k-1} + r_{k-1} = 1 + r_k + r_{k-1} = 1 + (m-1) + r_{k-1} \tag{21}$$

and

$$r_{k-1}(x) = t_k(x) r_k(x). \tag{22}$$

From (21) and (22) we see that $r_{k-1} = m$, $t_k = 1$ and the coefficient of x^{m-1} in $r_{k-1}(x)$ does not depend on b because otherwise $t_1 + \cdots + t_{k-2} = m - 1 =$

$r_k = t_1 + \cdots + t_{k-1}$. Thus

$$r_{k-1}(x) = u_m x^m + u_{m-1}x^{m-1} + \sum_{i=0}^{m-2} (u_i + v_i b)x^i$$

and

$$r_k(x) = \sum_{j=0}^{m-1} (U_j + V_j b)x^j,$$

where $u_m \neq 0$, u_{m-1}, u_i, v_i, U_j, V_j are rational numbers for $i = 0, \ldots, m-2$, $j = 0, \ldots, m-1$. The remainder when $r_{k-1}(x)$ is divided by $r_k(x)$ is of the form

$$r_{k+1}(x) = \sum_{i=0}^{m-2} \frac{h_i(b)}{(U_{m-1} + V_{m-1}b)^2} x^i,$$

where $h_i(x) \in \mathbb{Q}[x]$ are not all identically zero and of degree at most 3 for $i = 0, \ldots, m-2$. If $r_{k+1}(x)$ is identically zero for some complex number b then b is a root of all polynomials $h_i(x)$, $i = 0, \ldots, m-2$. But if b is not rational then any algebraic conjugate of b is also a root of $h_i(x)$. This means that in this case there are at least two complex numbers, b and its algebraic conjugate, for which the shifted Bernoulli polynomials do not have three simple zeros. However, this is not possible by Lemma 6.6. Thus b must be rational. ■

Denote by S^+ and S^- the sets of those polynomials with real coefficients which are symmetric with respect to the line $x = 1/2$ and the point $P = (1/2, 0)$, respectively:

$$S^+ := \{f(x) \in \mathbb{R}[x] : f(x) = f(1-x)\},$$
$$S^- := \{f(x) \in \mathbb{R}[x] : f(x) = -f(1-x)\}.$$

Lemma 6.10. *Let $f(x) \in S^+$ and $g(x) \in S^-$. Then there are uniquely determined polynomials $q(x) \in S^-$ and $r(x) \in S^+$ with $f(x) = q(x)g(x) + r(x)$ and either $r(x) \equiv 0$ or* $\deg r(x) < \deg g(x)$.

Proof. From the division algorithm for polynomials we know that there exist unique polynomials $q(x), r(x) \in \mathbb{R}[x]$ for which

$$f(x) = q(x)g(x) + r(x), \qquad r(x) \equiv 0 \text{ or } \deg r(x) < \deg g(x). \tag{23}$$

Hence we have to prove only that $q(x) \in S^-$ and $r(x) \in S^+$. Substituting $x = 1 - x$ into (23) and applying $f(x) \in S^+$ and $g(x) \in S^-$ we have

$$f(x) = -q(1-x)g(x) + r(1-x).$$

It follows from the division algorithm that $q(x) = -q(1-x)$ and $r(x) = r(1-x)$. ■

LEMMA 6.11. *Let $f(x) \in S^-$ and $g(x) \in S^+$. Then there are uniquely determined polynomials $q(x) \in S^-$ and $r(x) \in S^-$ with $f(x) = q(x)g(x) + r(x)$ and either $r(x) \equiv 0$ or $\deg r(x) < \deg g(x)$.*

Proof. The proof is similar to that of Lemma 6.10. ∎

LEMMA 6.12. *Assume that $B_{2m}(x) + b = G(x)F(x)^2$, where $b \in \mathbb{Q}$, $G(X), F(x) \in \mathbb{Q}[x]$ are monic polynomials, $\deg G(x) = 2$ and $G(x)$ has non-zero discriminant. Then $G(x) = x^2 - x + u/v$, where $v > 0$, $u \in \mathbb{Z}$, and $F(x) \in S^+ \cup S^-$.*

Proof. One can check that $F(x)$ is the greatest common divisor of the polynomials $B_{2m}(x) + b$ and $B_{2m-1}(x) = B'_{2m}(x)/2m$. From Lemma 6.1(i) we know that $B_{2m}(x) \in S^+$ and $B_{2m-1}(x) \in S^-$. Combining Lemmas 6.10 and 6.11 with the euclidean algorithm (19), we deduce that the greatest common divisor $F(x)$ is in $S^+ \cup S^-$. Now it easily follows that $F(x)^2 \in S^+$ and so $G(x) \in S^+$. Since $\deg G(x) = 2$ and $G(x) \in \mathbb{Q}[x]$ is monic, we infer that $G(x) = x^2 - x + u/v$. ∎

LEMMA 6.13. *$a_{m-1} + \cdots + a_1 = 0$ or $a_{m-1} + \cdots + a_1 + 2a_0 = 0$.*

Proof. Since $f(x) = a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in S^+ \cup S^-$ we see that $f(0) = f(1)$ or $f(0) = -f(1)$. The first equality implies $a_{m-1} + \cdots + a_1 = 0$, and the second yields $a_{m-1} + \cdots + a_1 + 2a_0 = 0$. ∎

Let c_i denote the coefficient of x^i on the left side of (11). Then

$$c_i = \begin{cases} vb_{2m-2} & \text{if } i = 2m, \\ -vb_{2m-2} + vb_{2m-3} & \text{if } i = 2m-1, \\ ub_i - vb_{i-1} + vb_{i-2} & \text{if } 2 \le i \le 2m-2, \\ ub_1 - vb_0 & \text{if } i = 1, \\ ub_0 & \text{if } i = 0. \end{cases} \tag{24}$$

LEMMA 6.14. *v is even provided that $a_0 \neq 0$.*

Proof. Assume that $v \equiv 1 \pmod 2$. We know that

$$c_{2i+1} = vb_{2m-2}\binom{2m}{2m-(2i+1)}B_{2m-(2i+1)} = 0, \qquad i = 0, \ldots, m-2, \tag{25}$$

because $B_3 = B_5 = \cdots = 0$. From (25), (24) and (11) we deduce that $c_1 = ub_1 - vb_0 = 2a_1a_0u - a_0^2v = 0$. This yields $a_0^2v \equiv 0 \pmod 2$, and so $a_0 \equiv 0 \pmod 2$. Assume that we have showed that

$$2 \mid a_0, a_1, \ldots, a_{i-1} \qquad \text{for some } i \in \{1, \ldots, m-2\}. \tag{26}$$

Using the fact that $b_{2j-1} = 2a_{2j-1}a_0 + 2a_{2j-2}a_1 + \cdots + 2a_ja_{j-1} \equiv 0 \pmod 2$ for $j = 1, \ldots, m-1$, we deduce from $c_{2i+1} = ub_{2i+1} - vb_{2i} + vb_{2i-1} = 0$ that $vb_{2i} = v(a_i^2 + 2a_{2i}a_0 + \cdots + 2a_{i+1}a_{i-1}) \equiv 0 \pmod 2$. Thus $a_i \equiv 0 \pmod 2$. It now follows from Lemma 6.13 that $a_{m-1},\ldots,a_0$ are even, which contradicts our assumption that $a_{m-1}x^{m-1}+\cdots+a_1x+a_0$ is a primitive polynomial. ■

Lemma 6.15. *Suppose that the polynomial* $B_{2m}(x)+r/s$ *has a multiple zero, where* $r,s\in\mathbb{Z}$, $s\neq 0$ *and* $(r,s)=1$. *Let* p^β *be a prime power occurring in the prime factorization of* s. *Then* $\beta\le 2m+1$.

Proof. Choose integers A and B such that $AB_{2m}(x)$, $BB_{2m-1}(x)$ are primitive polynomials. Since $B_{2m}(x)+r/s$ has a multiple zero, the polynomials $AB_{2m}(x)+Ar/s$ and $BB_{2m-1}(x)$ have a common zero. It follows that their resultant is zero. If we write $AB_{2m}(x)$ and $BB_{2m-1}(x)$ in the form

$$AB_{2m}(x)=Ax^{2m}+d_{2m-1}x^{2m-1}+\cdots+d_1x+d_0\in\mathbb{Z}[x],$$
$$BB_{2m-1}(x)=Bx^{2m-1}+e_{2m-2}x^{2m-2}+\cdots+e_1x+e_0\in\mathbb{Z}[x]$$

then the above resultant is the following determinant of order $4m-1$:

$\operatorname{Res}(AB_{2m}(x)+Ar/s, BB_{2m-1}(x))=$

$$\begin{vmatrix}
A & d_{2m-1} & d_{2m-2} & \cdots & d_2 & d_1 & d_0+Ar/s & 0 & \cdots & 0\\
0 & A & d_{2m-1} & \cdots & d_3 & d_2 & d_1 & d_0+Ar/s & \cdots & 0\\
\vdots & & & & & & & & & \vdots\\
0 & 0 & 0 & \cdots & A & d_{2m-1} & d_{2m-2} & d_{2m-3} & \cdots & d_0+Ar/s\\
B & e_{2m-2} & e_{2m-3} & \cdots & e_1 & e_0 & 0 & 0 & \cdots & 0\\
0 & B & e_{2m-2} & \cdots & e_2 & e_1 & e_0 & 0 & \cdots & 0\\
0 & 0 & B & \cdots & e_3 & e_2 & e_1 & e_0 & \cdots & 0\\
\vdots & & & & & & & & & \vdots\\
0 & 0 & 0 & \cdots & 0 & B & e_{2m-2} & e_{2m-3} & \cdots & e_0
\end{vmatrix}.$$

Let $s=p_1^{\beta_1}\cdots p_t^{\beta_t}$ be the prime factorization. Since A is the product of distinct primes, the denominator of the rational number $d_0+Ar/s=(d_0s+Ar)/s$ is of the form $p_1^{\alpha_1}\cdots p_t^{\alpha_t}$, where $\alpha_i\in\{0,\beta_i-1,\beta\}$ for $i=1,\ldots,t$. Actually, the above resultant is a polynomial in d_0+Ar/s with integer coefficients of degree $2m-1$ and leading coefficient B^{2m}. Since B is also the product of distinct primes, we infer that $\alpha_i\le 2m$ for $i=1,\ldots,t$. Hence $\beta_i-1\le 2m$, that is, $\beta_i\le 2m+1$. ■

Lemma 6.16. *If* $p^\alpha\mid v$ *then* $\alpha\le 2$.

Proof. Supposing the contrary we have $p^3\mid v$ and $p^2\mid c_1,\ldots,c_{2m}$. This is so because $c_i=vb_{2m-2}\binom{2m}{2m-i}B_{2m-i}$ for $i=1,\ldots,2m$ and the denominator of B_{2m-i} is the product of those different primes p for which $p-1$ divides $2m-i$. It is easy to see that p^2 divides b_{2m-2} since $p^2\mid c_{2m-2}=ub_{2m-2}-vb_{2m-3}+vb_{2m-4}$ and $(u,v)=1$. But then $p^5\mid vb_{2m-2}$ and so

$$p^4\mid c_1,\ldots,c_{2m}. \tag{27}$$

From (24), (27) and $(u,v)=1$ we obtain

$$p^3 \mid b_1,\dots,b_{2m-2}.$$

Assume that

$$p^{2j+1} \mid b_{2j-1}, b_{2j},\dots,b_{2m-2} \quad \text{for some } 1 \le j \le m-2. \tag{28}$$

Then from $p^3 \mid v$ and $p^{2j+1} \mid b_{2m-2}$ we see that $p^{2j+4} \mid vb_{2m-2}$ and thus $p^{2j+3} \mid c_i = ub_i - vb_{i-1} + vb_{i-2}$ for $i = 2j+1,\dots,2m-2$. By combining this with (28) and $p^3 \mid v$ we obtain

$$p^{2j+3} \mid b_{2j+1},\dots,b_{2m-2}. \tag{29}$$

Inserting $j = m-2$ we get $p^{2m-1} \mid b_{2m-2}$ and so $p^{2m+2} \mid vb_{2m-2}$. But then $p^{2m+2} \mid s$ because otherwise $p \mid c_{2m},\dots,c_1,c_0$, which contradicts $c_{2m}x^{2m} + \dots + c_1x + c_0$ being a primitive polynomial. However, $p^{2m+2} \mid s$ contradicts our Lemma 6.15. ■

Lemma 6.17. *$2 \parallel v$ or $2^2 \parallel v$.*

Proof. By Lemma 6.14 we know that v is even. Now the assertion immediately follows from Lemma 6.16 with $p=2$. ■

Lemma 6.18. *If $2 \parallel v$ then $b_{2m-2} \equiv 1 \pmod 2$.*

Proof. If $2 \mid b_{2m-2} = a_{m-1}^2$ then $2^2 \mid b_{2m-2}$ and $2^3 \mid vb_{2m-2}$. It follows that $2^2 \mid c_1,\dots,c_{2m}$. Applying (24) and $(u,v)=1$ one can deduce that $2 \mid b_1,\dots,b_{2m-2}$. Since $b_2 = a_1^2 + 2a_2a_0$, $b_1 = 2a_1a_0$ we find that $2 \mid a_1$ and $4 \mid b_1$. But $c_1 = ub_1 - vb_0 = 0$, $2 \parallel v$, hence $2 \mid b_0$, which contradicts the fact that $b_{2m-2}x^{2m-2} + \dots + b_1x + b_0$ is a primitive polynomial. ■

Lemma 6.19. *If $2 \parallel v$ then $a_0 \equiv 1 \pmod 2$ provided that $m \equiv 1 \pmod 2$ and $a_0 \neq 0$.*

Proof. If $a_0 \equiv 0 \pmod 2$ then $b_0 = a_0^2 \equiv 0 \pmod 4$. We know that

$$\begin{aligned} c_2 &= ub_2 - vb_1 + vb_0 \\ &= vb_{2m-2}\binom{2m}{2m-2}B_{2m-2} = vb_{2m-2}m(2m-1)B_{2m-2}. \end{aligned} \tag{30}$$

By Lemma 6.18 we have $b_2 \equiv 1 \pmod 2$. Further, from Lemma 6.2, $c_2 \in \mathbb{Z}$ and $n \equiv 2n-1 \equiv 1 \pmod 2$ we infer that $c_2 \equiv 1 \pmod 2$. Thus $b_2 \equiv 1 \pmod 2$ by (30). Since $c_1 = ub_1 - vb_0 = 2a_1a_0u - va_0^2 = 0$, it is obvious that $a_1 \equiv 0 \pmod 2$. This means that $b_2 = a_1^2 + 2a_2a_0 \equiv 0 \pmod 2$ which is a contradiction. ■

Lemma 6.20. *If $m \equiv 1 \pmod 2$ then $\binom{2m}{6} + \binom{2m}{4} \equiv 0 \pmod 2$.*

Proof. It is easy to see that

$$\binom{2m}{6}+\binom{2m}{4}\equiv\binom{2m}{6}+\binom{2m}{5}+\binom{2m}{5}+\binom{2m}{4}$$
$$\equiv\binom{2m+1}{6}+\binom{2m+1}{5}\equiv\binom{2m+2}{6}\pmod 2.$$

The assertion follows from

$$\binom{2m+2}{6}=\frac{(2m+2)(2m+1)2m(2m-1)(2m-2)(2m-3)}{6!}$$
$$=\frac{(m+1)(2m+1)m(2m-1)(m-1)(2m-3)}{6\cdot5\cdot3}. \ ■$$

Lemma 6.21. *If* $2\parallel v$ *then* $B_{2m}(x)+b$ *has at least three simple zeros provided that* $m\equiv 1 \pmod 2$.

Proof. Supposing the contrary we have

$$vb_{2m-2}(B_{2m}(x)+b)=(vx^2-vx+u)(b_{2m-2}x^{2m-2}+\cdots+b_1x+b_0) \tag{31}$$

as mentioned before. By Lemmas 6.18 and 6.19, we have $b_{2m-2}\equiv a_0\equiv 1 \pmod 2$. Since $2\parallel v$ and $c_1=ub_1-vb_0=2a_1a_0u-a_0^2v=0$ we get $a_1\equiv 1 \pmod 2$. Now one can check using

$$c_3=ub_3-vb_2+vb_1=u(2a_3a_0+2a_2a_1)-v(a_1^2+2a_2a_0-2a_1a_0)=0$$

that $u(2a_3a_0+2a_2a_1)\equiv 2 \pmod 4$. This yields $a_2\not\equiv a_3 \pmod 2$. At the same time we know from

$$b_6=a_3^2+2a_6a_0+2a_5a_1+2a_4a_2,\qquad b_4=a_2^2+2a_4a_0+2a_3a_1$$

and

$$c_6=ub_6-vb_5+vb_4,\qquad c_4=ub_4-vb_3+vb_2$$

that $b_6\not\equiv b_4$ and $c_6\not\equiv c_4 \pmod 2$, that is, $c_6+c_4\equiv 1 \pmod 2$. From $2\parallel v$, $b_{2m-2}\equiv 1 \pmod 2$ and Lemma 6.2 we can deduce that

$$c_6=vb_{2m-2}\binom{2m}{2m-6}B_{2m-6}=vb_{2m-2}\binom{2m}{6}B_{2m-6}\equiv\binom{2m}{6}\pmod 2$$

and

$$c_4=vb_{2m-2}\binom{2m}{2m-4}B_{2m-4}=vb_{2m-2}\binom{2m}{4}B_{2m-4}\equiv\binom{2m}{4}\pmod 2.$$

But then

$$\binom{2m}{6}+\binom{2m}{4}\equiv 1 \pmod 2,$$

which contradicts Lemma 6.20. ■

Lemma 6.22. *If* $2^2\parallel v$ *then* m *is even.*

Proof. Suppose that 2^2 divides v. Then similarly to the proof of Lemma 6.16, we get $2\,|\,c_1,\dots,c_{2m}$. From $c_{2m-2}=ub_{2m-2}-vb_{2m-3}+vb_{2m-4}$ we obtain $2\,|\,b_{2m-2}=a_{m-1}^2$. Hence $2^2\,|\,b_{2m-2}$, $2^4\,|\,vb_{2m-2}$ and so $2^3\,|\,c_1,\dots,c_{2m}$. Using this fact and (24) one can easily check that

$$2^2\,|\,b_1,\dots,b_{2m-2}\quad\text{and what is more}\quad 2^3\,|\,b_3,\dots,b_{2m-2}. \tag{32}$$

Denote by i the greatest index for which $a_i\equiv 1 \pmod 2$. Such an i exists since $a_{m-1}x^{m-1}+\dots+a_1x+a_0$ is a primitive polynomial. If $i\ge 1$ then we have $b_{2i}=a_i^2+2a_{2i}a_0+\dots+2a_{i+1}a_{i-1}\equiv 1 \pmod 2$, which contradicts (32). This means that

$$a_{m-1}\equiv a_{m-2}\equiv\dots\equiv a_1\equiv 0 \pmod 2\quad\text{and}\quad a_0\equiv 1 \pmod 2.$$

Now denote by j the greatest index for which $a_j\equiv 2 \pmod 4$. Such a j also exists since otherwise $8\,|\,b_1=2a_1a_0$, which, together with $c_1=ub_1-vb_0=0$, implies that $8\,|\,v$.

If $j>1$, then $b_{2j}=a_j^2+2a_{2j}a_0+\dots+2a_{j+1}a_{j-1}\equiv 4 \pmod 8$ since $4\,|\,a_{j+1},\dots,a_{m-1}$ and $a_j\equiv 2 \pmod 4$. This contradicts (32). Now we have

$$a_{m-1}\equiv a_{m-2}\equiv\dots\equiv a_2\equiv 0 \pmod 4\quad\text{and}\quad a_1\equiv 2 \pmod 4. \tag{33}$$

This yields $a_{m-1}+\dots+a_1\equiv 2 \pmod 4$ and hence $f(x)=a_{m-1}x^{m-1}+\dots+a_1x+a_0\in S^-$ by Lemma 6.13. This means that $\deg f(x)=m-1$ is odd and so m is even. ∎

Lemma 6.23. $u=\pm1$.

Proof. Assuming the contrary, there exists a prime p for which $p\,|\,u$. From $c_1=ub_1-vb_0=0$ and $(u,v)=1$ we find that $p\,|\,b_0=a_0^2$ and so $p\,|\,a_0$. Further, from $c_3=ub_3-vb_2+vb_1=0$ we obtain $p\,|\,v(b_2-b_1)=v(a_1^2+2a_2a_0-2a_1a_0)$. This shows that $p\,|\,a_1$. Now assume that

$$p\,|\,a_0,a_1,\dots,a_i\qquad\text{for some } i<m-2. \tag{34}$$

From $c_{2i+3}=ub_{2i+3}-vb_{2i+2}+vb_{2i+1}=0$, we get $p\,|\,b_{2i+2}-b_{2i+1}$. Using

$$b_{2i+2}=a_{i+1}^2+2a_{2i+2}a_0+\dots+2a_{i+2}a_i$$

and

$$b_{2i+1}=2a_{2i+1}a_0+\dots+2a_{i+1}a_i,$$

it follows from (34) that $p\,|\,a_{i+1}$. By inserting $i=m-3$ into (34) we obtain inductively

$$p\,|\,a_0,a_1,\dots,a_{m-2}. \tag{35}$$

Finally, from Lemma 6.13 we infer that $p\,|\,a_{m-1}$, which contradicts our assumption that the polynomial $a_{m-1}x^{m-1}+\dots+a_1x+a_0$ is primitive. ∎

Lemma 6.24. *If m is even then $B_{2m}(x)+b$ has at least three simple zeros.*

Proof. Assuming the contrary, we have (11). Since $f(x) \in S^+ \cup S^-$ and now $\deg f(x) = m - 1$ is odd we get $f(x) \in S^-$. It follows that $f(1/2) = 0$, whence $1/2$ is a root of $B_{2m}(x) + b$, so $b = -B_{2m}(1/2)$. Since we assumed that v and b_{2m-2} are positive, from (11) and Lemma 6.23 we deduce that $B_{2m}(2) - B_{2m}(1/2)$ is also positive. However,

$$(36)\qquad \begin{aligned} B_{2m}(2) - B_{2m}(1/2) &= B_{2m}(2) - B_{2m}(1) + B_{2m}(1) - B_{2m}(1/2) \\ &= 2m + B_{2m} - (2^{1-2m} - 1)B_{2m} = 2m + 2\frac{2^{2m}-1}{2^{2m}}B_{2m}. \end{aligned}$$

From (iv) and (v) of Lemma 6.1 it follows that $B_{2m} < 0$ and $|B_{2m}| > 2(2m)!/(2\pi)^{2m}$. One can deduce from the above that

$$(37)\qquad 2\frac{2^{2m}-1}{2^{2m}}|B_{2m}| > \frac{15}{4}\,\frac{(2m)!}{(2\pi)^{2m}} > 2m \quad \text{if } m \geq 10,$$

and so $B_{2m}(2) - B_{2m}(1/2) < 0$ by (36). Since $u = \pm 1$, by Lemma 6.23, and $v \geq 2$, inserting $x = 2$ into (11) we get a negative integer on the left side and a positive integer on the right side. If we factorize the polynomial $B_{2m}(x) - B_{2m}(1/2)$ for $m = 4, 6, 8$ over $\mathbb{Q}$ we see that it has three simple zeros. Further, $B_4(x) - B_4(1/2) = (4x^2 - 4x - 1)(2x - 1)^2/16$. ∎

Acknowledgements. The author thanks Professor Á. Pintér and the referee for their useful and valuable advice and remarks. This research was carried out as part of the TAMOP-4.2.1.B-10/2/KONV-2010-0001 project with support by the European Union, co-financed by the European Social Fund.

The author was supported, in part, by Grants K75566 and F68872 from HNFSR, and by Hungarian Academy of Sciences.

References

[1] Y. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér and R. F. Tichy, *Diophantine equations and Bernoulli polynomials* (with an appendix by A. Schinzel), Compos. Math. 131 (2002), 173–188.

[2] J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angew. Math. 234 (1969), 45–64.

[3] B. Brindza, *On S-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hungar. 44 (1984), 133–139.

[4] —, *On some generalizations of the diophantine equation* $1^k + 2^k + \cdots + x^k = y^z$, Acta Arith. 44 (1984), 99–107.

[5] B. Brindza and Á. Pintér, *On equal values of power sums*, ibid. 77 (1996), 97–101.

[6] —, —, *On the number of solutions of the equation* $1^k + 2^k + \cdots + (x-1)^k = y^z$, Publ. Math. Debrecen 56 (2000), 271–277.

[7] K. Dilcher, *On a diophantine equation involving quadratic characters*, Compos. Math. 57 (1986), 383–403.

[8] —, *On multiple zeros of Bernoulli polynomials*, Acta Arith. 134 (2008), 149–155.

[9] K. Győry and Á. Pintér, *On the equation* $1^k + 2^k + \cdots + x^k = y^n$, Publ. Math. Debrecen 62 (2003), 403–414.

[10] K. Győry, R. Tijdeman and M. Voorhoeve, *On the equation* $1^k + 2^k + \cdots + x^k = y^z$, Acta Arith. 37 (1980), 233–240.

[11] H. Kano, *On the equation* $s(1^k + 2^k + \cdots + x^k) + r = by^z$, Tokyo J. Math. 13 (1990), 441–448.

[12] Á. Pintér, *A note on the equation* $1^k + 2^k + \cdots + (x-1)^k = y^m$, Indag. Math. 8 (1997), 119–123.

[13] Á. Pintér and Cs. Rakaczki, *On the zeros of shifted Bernoulli polynomials*, Appl. Math. Comput. 187 (2007), 379–383.

[14] H. Rademacher, *Topics in Analytic Number Theory*, Springer, Berlin, 1973.

[15] J. J. Schäffer, *The equation* $1^p + 2^p + \cdots + n^p = m^q$, Acta Math. 95 (1956), 155–189.

[16] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. 31 (1976), 199–204.

[17] J. Urbanowicz, *On the equation* $f(1)1^k + f(2)2^k + \cdots + f(x)x^k + R(x) = by^z$, ibid. 51 (1988), 349–368.

[18] M. Voorhoeve, K. Győry and R. Tijdeman, *On the equation* $1^k + 2^k + \cdots + R(x) = y^z$, Acta Math. 143 (1979), 1–8; Corrigendum, ibid. 159 (1987), 151–152.

Csaba Rakaczki
Number Theory Research Group of the Hungarian Academy of Sciences
Institute of Mathematics
University of Debrecen
H-4010 Debrecen, P.O.B. 12, Hungary
E-mail: rcsaba@math.klte.hu
and
Institute of Mathematics
University of Miskolc
H-3515 Miskolc Campus, Hungary
E-mail: matrcs@uni-miskolc.hu

Received on 16.11.2010
and in revised form on 12.4.2011 (6553)