Indag. Mathem., N.S., 16 (1), 51–65 March 21, 2005

A class of Diophantine equations involving Bernoulli polynomials

by Manisha Kulkarni and B. Sury

Stat.-Math. Unit, Indian Statistical Institute, 8th Mile, Mysore Road, Bangalore 560 059, India

Communicated by Prof. R. Tijdeman at the meeting of September 27, 2004

Let a, b be nonzero rational numbers and $C(y)$ a polynomial with rational coefficients. We study the Diophantine equations

$$aB_m(x) = bf_n(y) + C(y)$$

and

$$af_m(x) = bB_n(y) + C(y)$$

with $m \geqslant n > \deg C + 2$ for solutions in integers x, y. Here $f_n(x) = x(x+1)\cdots(x+n-1)$ and the Bernoulli polynomials $B_n(x)$ are defined by the generating series

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!}.$$

Then, $B_n(x) = \sum_{i=0}^{n} \binom{n}{i} B_{n-i}x^i$ where $B_r = B_r(0)$ is the rth Bernoulli number. In fact, B_r are rational numbers defined recursively by $B_0 = 1$ and $\sum_{i=0}^{n-1} \binom{n}{i} B_i = 0$ for all $n \geqslant 2$. The odd Bernoulli number $B_r = 0$ for r odd > 1 and the first few are:

$$B_0 = 1, \quad B_1 = -1/2, \quad B_2 = 1/6, \quad B_4 = -1/30.$$

MSC: 11D45

E-mails: manisha@isibang.ac.in (M. Kulkarni), sury@isibang.ac.in (B. Sury).

The Bernoulli polynomials B_n are related to the sums of nth powers of the first few natural numbers as follows. For any $n \geqslant 1$, the sum $1^n + 2^n + \cdots + k^n$ is a polynomial function $S_n(k)$ of k and $S_n(x) = (B_{n+1}(x+1) - B_{n+1})/(n+1)$.

One says that an equation $f(x) = g(y)$ has infinitely many rational solutions with bounded denominator if there exist a positive integer λ such that $f(x) = g(y)$ has infinitely many rational solutions x, y satisfying $x, y \in \frac{1}{\lambda}\mathbb{Z}$ and, more generally, we look for rational solutions with bounded denominators.

Earlier, we have studied the equations of the type $f(x) = g(y)$ for:

(i) $f(x) = x(x+1)\cdots(x+m-1)$ and a general $g(y)$ [2,4] and
(ii) $f(x) = aB_m(x)$, $g(y) = bB_n(y) + C(y)$ where $m \geqslant n > \deg(C) + 2$ [5].

Here, we prove the following two theorems:

Theorem 1. *For $m \geqslant n > \deg(C) + 2$, the equation*

$$aB_m(x) = bf_n(y) + C(y)$$

has only finitely many rational solutions with bounded denominator except in the following situations:

(i) *$m = n$, $m+1$ is a perfect square, $a = b(\sqrt{m+1})^m$,*
(ii) *$m = 2n$, $(n+1)/3$ is a perfect square, $a = b(\frac{n}{2}\sqrt{\frac{n+1}{3}})^n$.*

In each case, there is a uniquely determined polynomial C for which the equation has infinitely many rational solutions with a bounded denominator. Further, C is identically zero when $m = n = 3$ and has degree $n - 4$ when $n > 3$.

Theorem 2. *For $m \geqslant n > \deg(C) + 2$, the equation*

$$af_m(x) = bB_n(y) + C(y)$$

has only finitely many rational solutions with bounded denominator excepting the following situations when it has infinitely many:

$$m = n, \quad m+1 \text{ is a perfect square}, \quad b = a\left(\sqrt{m+1}\right)^m.$$

In these situations, the polynomial C is also uniquely determined to be

$$C(x) = af_m\left(\left(\pm\sqrt{m+1}\right)x + \frac{1 - m \mp \sqrt{m+1}}{2}\right) - bB_m(x)$$

and has degree $m - 4$.

Remarks. (a) The condition $n > \deg(C) + 2$ in the two theorems is sharp as can be seen from the fact that the equation

$$B_4(y+2) = f_4(y) + 2y^2 + 6y + \frac{119}{30}$$

holds for all y.

(b) A (common) particular case of the theorems was proved in [1].

(c) In the exceptional cases (i) and (ii) in the first theorem, the unique polynomial C for which the equation has infinitely many solutions, is given as follows: In case (i),

$$C(x) = aB_m\left(\frac{x + (m \pm \sqrt{m+1} - 1)/2}{\pm\sqrt{m+1}}\right) - bf_m(x).$$

In case (ii), writing $n + 1 = 3u^2$ and writing $\phi(x)$ for the unique polynomial of degree n for which $\phi(x^2) = B_{2n}(x + 1/2)$,

$$C(x) = a\phi\left(\frac{2x + 6u^3 + 24u^2 + 6u - 16}{u(3u^2 - 1)}\right) - bf_{3u^2-1}(x).$$

(d) It should be noted that when $a = b$, the computations are much easier and yield in all cases that there are only finitely many solutions.

(e) Evidently, one may assume $a = 1$ by replacing b by b/a and $C(y)$ by $C(y)/a$.

We shall make extensive use of the following theorem of Bilu and Tichy [3]:

Theorem A. *For non-constant polynomials $f(x)$ and $g(x) \in \mathbb{Q}[x]$, the following are equivalent*:

(a) *The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.*
(b) *We have $f = \phi(f_1(\lambda))$ and $g = \phi(g_1(\mu))$ where $\lambda(x), \mu(x) \in \mathbb{Q}[X]$ are linear polynomials, $\phi(x) \in \mathbb{Q}[X]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.*

Standard pairs are defined as follows. In what follows, a and b are nonzero elements of some field, m and n are positive integers, and $p(x)$ is a nonzero polynomial (which may be constant).

STANDARD PAIRS

A standard pair of the first kind is

$$\left(x^t, ax^r p(x)^t\right) \quad \text{or} \quad \left(ax^r p(x)^t, x^t\right)$$

where $0 \leqslant r < t$, $(r, t) = 1$ and $r + \deg p(x) > 0$.

A standard pair of the second kind is

$$\left(x^2, (ax^2+b)p(x)^2\right) \quad \text{or} \quad \left((ax^2+b)p(x)^2, x^2\right).$$

A standard pair of the third kind is

$$\left(D_k(x, a^t), D_t(x, a^k)\right)$$

where $(k, t) = 1$. Here D_t is the tth Dickson polynomial

$$D_t(x, c) = \sum_{i=0}^{[t/2]} \frac{t}{t-i}\binom{t-i}{i}(-c)^i x^{t-2i}.$$

A standard pair of the fourth kind is

$$\left(a^{-t/2}D_t(x, a), b^{-k/2}D_k(x, a)\right)$$

where $(k, t) = 2$.

A standard pair of the fifth kind is

$$\left((ax^2-1)^3, 3x^4-4x^3\right) \quad \text{or} \quad \left(3x^4-4x^3, (ax^2-1)^3\right).$$

By a standard pair over a field k, we mean that $a, b \in k$, and $p(x) \in k[x]$.

The theorem of Bilu and Tichy above shows the relevance of the following definition:

A *decomposition* of a polynomial $F(x) \in \mathbf{C}[x]$ is an equality of the form $F(x) = G_1(G_2(x))$, where $G_1(x), G_2(x) \in \mathbf{C}[x]$. The decomposition is called *nontrivial* if $\deg G_1 > 1$, $\deg G_2 > 1$.

Two decompositions $F(x) = G_1(G_2(x))$ and $F(x) = H_1(H_2(x))$ are called *equivalent* if there exist a linear polynomial $l(x) \in \mathbf{C}[x]$ such that $G_1(x) = H_1(l(x))$ and $H_2(x) = l(G_2(x))$. The polynomial called *decomposable* if it has at least one nontrivial decomposition, and *indecomposable* otherwise.

We shall also use the following result due to Bilu et al. [1]:

Theorem B. *Let $m \geqslant 2$. Then,*

(i) *$B_m(x)$ is indecomposable if m is odd and,*
(ii) *if $m = 2k$, then any nontrivial decomposition of $B_m(x)$ is equivalent to $B_m(x) = h((x-1/2)^2)$.*

The equation $S_m(x) = S_n(y)$ has been studied in [1]. This is a particular case of our result.

We first consider the first theorem. Evidently, we may assume $a = 1$ and we look at the equation $B_m(x) = bf_n(y) + C(y)$ where $f_n(x) = x(x+1)\cdots(x+n-1)$ and $m \geqslant n > \deg(C) + 2$.

Proof of Theorem 1. As remarked in the beginning (remark (e)), we may assume that $a = 1$.

Case I: Let us first consider the case when $m = n = 2d$.

If the equation has infinitely many solutions, the Bilu–Tichy theorem gives $B_{2d} = \phi \circ f_1 \circ \lambda$ and $bf_{2d} + C = \phi \circ g_1 \circ \mu$ where λ, μ are linear polynomials over $\mathbb{Q}$ and (f_1, g_1) is a standard pair over $\mathbb{Q}$. Since we know from [1] that the only nontrivial decomposition of B_{2d} up to equivalence where has $f_1(x) = (x - 1/2)^2$, it follows that either:

(a) $\deg \phi = 1$, or
(b) $\deg \phi = d$ and $B_{2d}(x) = \phi((l_0 + l_1 x - 1/2)^2)$ and $bf_{2d}(x) + C(x) = \phi(kx^2 + lx + t)$ and the equation $(x - 1/2)^2 = ky^2 + ly + t$ has infinitely many solutions, or
(c) $\deg \phi = 2d$ in which case

$$B_{2d}(rx + s) = bf_{2d}(x) + C(x).$$

First, suppose (a) holds, i.e., $\deg \phi = 1$. This means that (f_1, g_1) is a standard pair with $\deg f_1 = \deg g_1 = 2d > 2$. This is impossible as seen by looking at the conditions on the degrees of standard pairs.

Next, we consider (b), i.e., the possibility where ϕ has degree d.

We use the following observation, see [5]:

Lemma. *If* $B_{2d}(rx + s) = \phi((x - 1/2))^2$ *for some* $r, s \in \mathbb{Q}$ *with* $r \neq 0$, *then* $(r, s) = (1, 0)$ *or* $(-1, 1)$. *In particular,* $B_{2d}(x) = \phi((x - 1/2)^2)$.

Therefore, $B_{2d}(x) = \phi((x - 1/2)^2)$ and $bf_{2d}(x) + C(x) = \phi(kx^2 + lx + t)$.

Considering the coefficients of $x^{2d}, x^{2d-1}, x^{2d-2}$ and x^{2d-3} of the second equation, we get the following expressions.

Coefficient of x^{2d} is $b = \phi_d k^d = k^d$ (the fact that $\phi_d = 1$ we know from the first equation).

Coefficient of x^{2d-1} gives $l = k(2d - 1)$.

Coefficient of x^{2d-2} gives $t = k(d - 1)(2d - 1)/3 + (2d - 1)/12$.

Coefficient of x^{2d-3} gives

$$\begin{aligned} c_{2d-3} + b\frac{d^2(d-1)(2d-1)^2(2d-3)}{6} \\ = d(d-1)k^{d-2}lt + \binom{d}{3}k^{d-3}l^3 + \phi_{d-1}(d-1)k^{d-2}l \end{aligned}$$

where c_{2d-3} is the coefficient of x^{2d-3} in $C(x)$.

From the equation $B_{2d}(x) = \phi((x - 1/2)^2)$, we obtain $\phi_d = 1$ and $\phi_{d-1} = -d(2d - 1)/12$. Using this and the values of b, k, l, t, we obtain $c_{2d-3} = 0$. Thus, $\deg C < 2d - 3$.

We now proceed to show that d must be of a special form and in that case C must be determined uniquely to be of degree $2d - 4$.

The infinitude of the number of solutions of

$$\begin{aligned}(x-1/2)^2 &= ky^2+ly+t\\ &= ky^2+k(2d-1)y+\frac{k(d-1)(2d-1)}{3}+\frac{2d-1}{12}\\ &= k(y+d-1/2)^2-\frac{k(2d+1)(2d-1)}{12}+\frac{2d-1}{12}\end{aligned}$$

forces that $k(2d+1)=1$ and that k is a square in $\mathbb{Q}$. Therefore, we get $d=2r(r+1)$ for some natural number r.

Then C is uniquely determined to be

$$C(x)=B_{4r(r+1)}\left(\frac{x+2r^2+3r}{2r+1}\right)-\frac{1}{(2r+1)^{4r(r+1)}}f_{4r(r+1)}(x).$$

The claim that $\deg(C)=2d-4$ when $d=2r(r+1)$, etc., is seen as follows.

We use the property $B_{2d}(x+1)-B_{2d}(x)=2dx^{2d-1}$ of the Bernoulli polynomials. We have

$$(*)\qquad 4r(r+1)\left(\frac{x+2r^2+3r}{2r+1}\right)^{4r^2+4r-1}=C(x+2r+1)-C(x)$$
$$+\frac{1}{(2r+1)^{4r(r+1)}}\big(f_{4r(r+1)}(x+2r+1)-f_{4r(r+1)}(x)\big)\cdots.$$

Already, from this one can see that C cannot be a constant; otherwise a comparison with $x=0$ gives

$$(2r+2)(2r+3)\cdots\big(4r^2+6r\big)=4r(r+1)\big(2r^2+3r\big)^{4r^2+4r-1}.$$

The last identity is impossible since a prime p exists with $2r^2+3r<p\leqslant 4r^2+6r$ and this divides the left side and not the right.

To use the above identity $(*)$ to find the coefficient of $x^{2d-4}=x^{4r^2+4r-4}$ of $C(x)$, we find the coefficient of x^{4r^2+4r-5} on both sides. Clearly, on the left side, it is $(4r^2+4r-4)(2r+1)C_{4r^2+4r-4}$. Thus, we need to check that the coefficient of x^{4r^2+4r-5} is nonzero. This is computed to be

$$\frac{4r(r+1)}{(2r+1)^{4r^2+4r-1}}\binom{4r^2+4r-1}{4}\big(2r^2+3r\big)^4-\frac{u(r)}{(2r+1)^{4r(r+1)}}$$

where $u(r)$ is the coefficient of x^{4r^2+4r-5} in $f_{4r(r+1)}(x+2r+1)-f_{4r(r+1)}(x)$, i.e., $u(r)$ is the coefficient of x^{4r^2+4r-5} in $(x+2r+1)(x+2r+2)\cdots(x+4r^2+6r)-x(x+1)\cdots(x+4r^2+4r-1)$.

Let $v(r)=(2r+1)(4r^2+4r)(2r^2+3r)^4\binom{4r^2+4r-1}{4}$.

Using MAPLE, we can explicitly compute $u(r)$ and $v(r)$ as polynomials in r.

$$\begin{aligned}u(r) &= \frac{4096}{3}r^{19}+\frac{47104}{3}r^{18}+\frac{231424}{3}r^{17}+206848r^{16}+\frac{14069248}{45}r^{15}\\&+\frac{655616}{3}r^{14}-\frac{2556544}{45}r^{13}-\frac{10018816}{45}r^{12}-\frac{6033008}{45}r^{11}\\&+\frac{6376}{5}r^{10}+\frac{146144}{9}r^{9}-\frac{433384}{45}r^{8}-\frac{126929}{45}r^{7}+\frac{643973}{90}r^{6}\\&+\frac{157321}{36}r^{5}+\frac{7211}{8}r^{4}+\frac{30647}{360}r^{3}+\frac{1091}{360}r^{2}+\frac{1}{5}r,\end{aligned}$$

$$\begin{aligned}v(r) &= \frac{4096}{3}r^{19}+\frac{47104}{3}r^{18}+\frac{231424}{3}r^{17}+206848r^{16}+\frac{937984}{3}r^{15}\\&+\frac{656384}{3}r^{14}-54912r^{13}-\frac{645056}{3}r^{12}-114864r^{11}+\frac{97544}{3}r^{10}\\&+47120r^{9}+4524r^{8}-6336r^{7}-864r^{6}+324r^{5}.\end{aligned}$$

Thus, in fact, the first four coefficients of $u(r)$ and $v(r)$ match!

However, MAPLE shows that they are never equal because

$$\begin{aligned}v(r)-u(r) &= \frac{r(2r+1)(r^2+r-1)}{360}\big(2048r^{11}+43008r^{10}+278528r^{9}\\&+976640r^{8}+2152320r^{7}+3022208r^{6}+2589888r^{5}\\&+1250288r^{4}+297852r^{3}+29844r^{2}+1019r+72\big)\end{aligned}$$

which is obviously positive for all positive r.

Thus, $C_{4r^2+4r-4}\neq 0$, i.e., $\deg C = 2d-4$.

Finally, we consider the possibility (c), i.e.,

$$B_{2d}(rx+s)=bf_{2d}(x)+C(x).$$

Comparing the coefficients of x^{2d}, x^{2d-1} and x^{2d-2} we get

$$r^{2d}=b,\quad 2s-1=r(2d-1),\quad s^2-s+\frac{1}{6}=\frac{r^2(d-1)(6d-1)}{6}.$$

This gives

$$(4d+2)s^2-(4d+2)s-2d^2+3d=0.$$

This is possible for a rational number s if, and only if, $2d+1$ is a perfect square, say $(2u+1)^2$. We obtain

$$r=\pm\frac{1}{2u+1},\quad s=\frac{1}{2}\pm\frac{4u^2+4u-1}{2(2u+1)},\quad b=\frac{1}{(2u+1)^{4u^2+4u}}.$$

With these values of r, s, we find that C is the same as it was for case (b). Therefore, the same computation shows that C has degree $2d-4$.

This completes the case I when $m=n$ is even.

Case II: Let $m = n$ be odd and $> \deg C + 2$.

As before, infinitude of solutions implies the existence of a decomposition

$$B_m(x) = \phi \circ f_1 \circ \lambda(x), \qquad bf_m(x) + C(x) = \phi \circ g_1 \circ \mu(x)$$

with λ, μ linear. Now, as m is odd, B_m is indecomposable. Hence either $\deg \phi = m$, $\deg f_1 = 1$ or $\deg \phi = 1$, $\deg f_1 = m$.

First, let us suppose that $\deg \phi = 1$. Then $\deg f_1 = m = \deg g_1$. The standard pair (f_1, g_1) must, therefore, be of the first kind. So, for some $r, s \in \mathbb{Q}$ with $r \neq 0$, we have either

$$B_m(rx + s) = \phi_0 + \phi_1 x^m$$

or

$$bf_m(rx + s) + C(rx + s) = \phi_0 + \phi_1 x^m.$$

If the first possibility occurs, we equate the coefficients of x^{m-2}, and get $6s^2 - 6s + 1 = 0$, $s \in \mathbb{Q}$, which is not possible.

Suppose the second possibility occurs. Let us compare the coefficients of x^m, x^{m-1} and x^{m-2}. We have

$$br^m = \phi_1, \qquad v = \frac{1-m}{2}, \qquad v^2 + (m-1) + \frac{(m-1)(2m-1)}{6} = 0,$$

respectively. Substituting the value of v into the last equation, one gets $m^2 = 1$ which is impossible.

Thus, we suppose that $\deg \phi = m$. Then, we have $u, v \in \mathbb{Q}$ with $u \neq 0$ such that

$$C(x) = B_m(ux + v) - bf_m(x).$$

Comparing the coefficients of x^m, x^{m-1}, x^{m-2} on both sides and noting that the left side does not contribute anything, we have:

$$u^m = b, \qquad v = \frac{m-1}{2}u + \frac{1}{2}, \qquad u^2 = \frac{1}{m+1}.$$

Thus, first of all, this forces m to be such that $m + 1$ is a perfect square, say, $4r^2$. This also determines u, v in terms of r as $u = \pm 1/(2r)$ and $v = (2r^2 - 1)u + 1/2$.

Hence C is uniquely determined to be the polynomial

$$C(x) = B_{4r^2-1}\left(\pm\frac{x + 2r^2 + r - 1}{2r}\right) - \frac{1}{(2r)^{4r^2-1}} f_{4r^2-1}(x).$$

Notice that the expression for C we obtained in case I and the expression here have the common form

$$C(x) = aB_m\left(\frac{x + (m \pm \sqrt{m+1} - 1)/2}{\sqrt{m+1}}\right) - bf_m(x).$$

A calculation exactly as in the case of even m shows that the coefficient of x^{m-3} on the right side is zero. Therefore, C must either be zero or have degree smaller than $m-3$.

If $m=3$, we must have $C \equiv 0$ and

$$f_3(x) = -8B_3\left(\frac{-x}{2}\right).$$

Let $m > 3$.

Of course, one can easily check as in the even case that C cannot be a constant. Indeed, if it were, we would have

$$(2r-1)\left(2r^2+r-1\right)^{4r^2-2} = (2r+2)(2r+3)\cdots\left(4r^2+2r-2\right).$$

But, if $r > 1$ (which is the case when $m > 3$), there is a prime p with $2r^2+r-1 < p \leqslant 4r^2+2r-2$; this divides the right hand side and not the left hand side. In fact, the polynomial C has degree $m-4$. To see this, we may proceed as in the m even case using the property $B_m(x+1) - B_m(x) = mx^{m-1}$.

Case III: Let m be odd and $> n > \deg C + 2$.

As before writing $B_m = \phi \circ f_1 \circ \lambda$, we have either $\deg \phi = 1$ or $= m$. Since $bf_n + C = \phi \circ g_1 \circ \mu$ has degree $n < m$, the degree of ϕ must be 1. Thus, the standard pair (f_1, g_1) must be of either the first or the third kind.

If it is of the first kind, the above argument for $m = n$ carries over verbatim to give $n^2 = 1$, which is a contradiction.

If it is the third kind, we have $B_m(rx+s) = D_m(x, a^n)$ and we have already derived a contradiction by concluding $m = 9/2$ in this case.

Finally, we are left with:

Case IV: Let m be even and $> n > \deg C + 2$.

Writing $B_m = \phi \circ f_1 \lambda$ and $bf_n = \phi \circ g_1 \circ \mu$, we must have either $\deg \phi = m$ or $\deg \phi = 1$ or $\deg \phi = m/2$ and $f_1 = (x - 1/2)^2$.

Note that in the last case $n = m/2$ since $m > n$ and n is a multiple of $\deg \phi = m/2$. Also, then $\deg g_1 = 1$.

Since $m > n \geqslant \deg \phi$, the possibility $\deg \phi = m$ cannot occur.

Now, if $\deg \phi = 1$, then (f_1, g_1) is a standard pair with $\deg f_1 = m$, $\deg g_1 = n$.

We have already seen in case II that if this pair is of the first kind, we get a contradiction to either of the equations

$$B_m(rx+s) = \phi_0 + \phi_1 x^m$$

or

$$bf_n(rx+s) + C(rx+s) = \phi_0 + \phi_1 x^n.$$

Since $m, n > 2$, this standard pair cannot be of the second kind.

Suppose it is of the third kind. Then,

$$f_1(x) = D_m\left(x, a^n\right), g_1(x) = D_n\left(x, a^m\right)$$

where $(m,n)=1$. Now, $B_m(rx+s)=\phi_0+\phi_1(D_m(x,\alpha^n))$.

This means

$$\sum_{i=0}^{m}\binom{m}{i}B_{m-i}(rx+s)^i=\phi_0+\phi_1\sum_{i=0}^{[m/2]}d_{m,i}\left(x^{m-2i}\right),$$

$$\text{where } d_{m,i}=\frac{m}{m-i}\binom{m-i}{i}\left(-\alpha^n\right)^i.$$

We will compare the coefficients on both sides.

Equating the coefficients of x^m on both sides, we have $r^m=\phi_1$.

The coefficient of x^{m-1} on the right-hand side is zero and, so we get $\binom{m}{1}r^{m-1}s+\binom{m}{m-1}B_1r^{m-1}=0$.

This gives $s=1/2$.

The coefficients of x^{m-2} give

$$\frac{m(m-1)}{12}r^{m-2}\left(6s^2-6s+1\right)=\frac{m}{m-1}\binom{m-1}{1}\left(-\alpha^n\right)\phi_1$$

which on simplification yields $r^2\alpha^n=(m-1)/24$.

By considering the coefficients of x^{m-4} and on using the values of ϕ_1, $r^2\alpha^n$, we get $m=9/2$ which is a contradiction. Hence (f_1,g_1) can not be a standard pair of the third kind also.

The same argument goes through if the pair is of the fourth kind as the number ϕ_1 above is simply replaced by $\alpha^{-m/2}\phi_1$.

Finally, if (f_1,g_1) is of the fifth kind, then $m=6$, $n=4$ and

$$f_1(x)=\left(\alpha x^2-1\right)^3,\qquad g_1(x)=3x^4-4x^3.$$

So

$$B_6(x)=\phi_0+\phi_1\left(\alpha(rx+s)^2-1\right)^3.$$

This means that the derivative $B_6'(x)$ has a multiple root; however, $B_6'(x)=6B_5(x)$ and one knows that $B_{\text{odd}}(x)$ has only simple roots by a result of Brillhart.

Alternatively, even by direct computation, comparison of coefficients of x^6, x^5 and x^4 gives $r^2=12/5\alpha$, $s=-r/2$, $\phi_1=(5/12)^3$ and then the coefficients of x^2 do not match.

Now, we are left with the case $\deg\phi=m/2$ and $f_1=(x-1/2)^2$; so $m=2n$ and g_1 is linear. Clearly, $f_1(x)=g_1(y)$ has infinitely many rational solutions with a bounded denominator.

Now $B_{2n}(ux+v)=\phi((x-1/2)^2)$ and by the lemma observed while discussing case I, we know that we must have $B_{2n}(ux+v)=B_{2n}(x)$.

Hence we have $B_{2n}(x)=\phi((x-1/2)^2)$ and $bf_n(rx+s)+C(rx+s)=\phi(x)$ for some $r,s\in\mathbb{Q}$ with $r\neq 0$. Thus, we have

$$B_{2n}(x)=bf_n\left(r(x-1/2)^2+s\right)+C\left(r(x-1/2)^2+s\right).$$

Using the identity $B_{2n}(x+1) - B_{2n}(x) = 2nx^{2n-1}$, we have, for some $r, t \in \mathbb{Q}$ with $r \neq 0$,

$$2nx^{2n-1} = bf_n(rx^2 + rx + t) - bf_n(rx^2 - rx + t) + C(rx^2 + rx + t) - C(rx^2 - rx + t).$$

In fact, $t = r/4 + s$.

The coefficients of x^{2n-1} and x^{2n-3} give:

$$br^n = 1, \qquad t = \frac{1-n}{2} - \frac{r}{n}.$$

Comparing the coefficients of x^{2n-5} and substituting the above value of t, we have

$$r^2 = \frac{n^2(n+1)}{12}.$$

In other words $(n+1)/3$ must be a square in $\mathbb{Q}$.

Note that since $n > \deg C + 2 \geqslant 2$, this means $n \geqslant 11$. Writing $n + 1 = 3u^2$ with $u \geqslant 2$, we have

$$r = \frac{u(3u^2-1)}{2}, \qquad t = 1 - \frac{u}{2} - \frac{3u^2}{2},$$

$$s = 1 - \frac{3u}{8} - \frac{3u^2}{2} - \frac{3u^3}{8}, \qquad b = \left(\frac{2}{u(3u^2-1)}\right)^{3u^2-1}.$$

Also, the coefficient of x^{n-3} in $C(x) = \phi((x-s)/r) - bf_n(x)$ is seen to be zero by substituting the values of $\phi_n, \phi_{n-1}, \phi_{n-2}, \phi_{n-3}$ obtained from the equation $B_{2n}(x) = \phi((x-1/2)^2)$.

$\deg C$ is found to be $n-4$.

Therefore, Theorem 1 is proved. □

Proof of Theorem 2. Once again, we may assume $a = 1$ and look at the equation

$$f_m(x) = bB_n(y) + C(y).$$

We shall use our earlier general result on equations of the form $f_m(x) = g(y)$ for an arbitrary polynomial:

Theorem C *(cf. [4]). Suppose $f_m(x) = g(y)$ has infinitely many rational solutions x, y with a bounded denominator. Then we are in one of the following cases:*

(1) *$g(y) = f_m(g_1(y))$ for some $g_1(y) \in \mathbf{Q[Y]}$.*
(2) *m even and $g(y) = \phi(g_1(y))$ where $\phi(X) = (X - (1/2)^2)(X - (3/2)^2)\cdots(X - ((m-1)/2)^2)$ and $g_1(y) \in \mathbf{Q[Y]}$ is a polynomial whose square-free part has at most two zeroes.*
(3) *$m = 4$ and $g(y) = 9/16 + b\delta(y)^2$ where δ is a linear polynomial.*

Here, $g(y) = bB_n(y) + C(y)$ where $m \geqslant n > \deg(C) + 2$.

The last inequality shows that $n > 2$ and so, we are not in case (3) above.

If we are in case (1), then again $m \geqslant n$ shows that $m = n$. Then, we have $r, s \in \mathbb{Q}$ with $r \neq 0$ so that

$$bB_n(x) + C(x) = f_n(rx + s)$$

where $n > \deg(C) + 2$.

Therefore, we have

$$b\sum_{i=0}^{n}\binom{n}{i}B_{n-i}x^i + C(x) = (rx+s)(rx+s+1)\cdots(rx+s+n-1).$$

Comparing the coefficients of x^n, x^{n-1}, x^{n-2}, we get

$$b = r^n, \quad r = -2s - n + 1,$$

respectively, and a straightforward calculation gives

$$r^2 = n + 1.$$

Thus $n + 1$ has to be a perfect square.

Therefore, the equation

$$f_n(x) = bB_n(y) + C(y)$$

has infinitely many solutions if, and only if, $n + 1$ is a square, $r = \sqrt{n+1}$, $b = r^n$ and C is the polynomial

$$C(x) = f_n\left(rx + \frac{1-n-r}{2}\right) - r^n B_n(x).$$

In fact, it turns out that C has degree $n - 4$; a comparison of the coefficients of x^{n-3} yields $c_{n-3} = 0$ and that of x^{n-4} is not zero.

Finally, suppose we are in case (2). Then, either $m = n$ and g_1 has degree 2 or $m = 2n$ and g_1 is linear.

Let us consider the former possibility first. Then, m is even, and $f_m(x) = \phi(f_1(x))$ where

$$f_1(x) = \left(x - \frac{m-1}{2}\right)^2 \quad \text{and}$$

$$\phi(x) = \left(x - \left(\frac{1}{2}\right)^2\right)\left(x - \left(\frac{3}{2}\right)^2\right)\cdots\left(x - \left(\frac{m-1}{2}\right)^2\right).$$

Therefore, writing $g_1(y) = k(y + l)^2 + t$ and assuming that $f_1(x) = g_1(y)$ has infinitely many solutions with a bounded denominator, it follows that $t = 0$ and

k is a square; that is, $g_1(y)$ is the square of a polynomial. Hence, we have $r, s \in \mathbb{Q}$ with $r \neq 0$ and

$$f_n(rx + s) = bB_n(x) + C(x).$$

This is exactly the same expression considered in case (1). Thus, in this case also, we must have that $n + 1$ is a perfect square and C is determined uniquely to be a polynomial of degree $n - 4$.

Let us now consider the latter possibility; that is, suppose $m = 2n$ and $\deg g_1 = 1$. Then,

$$bB_n(x) + C(x) = \left(rx + s - \left(\frac{1}{2}\right)^2\right)\left(rx + s - \left(\frac{3}{2}\right)^2\right)\cdots \left(rx + s - \left(\frac{2n-1}{2}\right)^2\right).$$

Comparing the coefficients of x^n, x^{n-1} and x^{n-2}, we get $b = r^n$,

$$-6r = 12s - (2n + 1)(2n - 1)$$

and

$$\frac{n(n-1)}{2}r^2 = \frac{n(n-1)}{2}s^2 - \frac{(n-1)n(2n+1)(2n-1)}{12}s + \frac{n^2(2n+1)^2(2n-1)^2}{2^5 3^2} - \frac{n(48n^4 - 40n^2 + 7}{480},$$

respectively, and a straightforward calculation gives

$$r^2 = \frac{4(n+1)(2n+1)(2n-1)}{15}.$$

We claim that this gives a contradiction. Indeed, we assert:

Claim. $(n + 1)(2n + 1)(2n - 1)/15$ *is not a square in* $\mathbb{Q}$.

Let us write $n+1 = au^2$, $2n+1 = bv^2$, $2n-1 = cw^2$ where a, b, c are square-free. Note that $2n+1$ is coprime to $n+1$ as well as to $2n-1$ and that the two numbers $n+1, 2n-1$ have greatest common divisor 1 or 3. Thus, if $(n + 1)(2n + 1)(2n - 1)/15$ is a square, a, b, c are pairwise coprime and $abc = 15$. A number of cases are possible.

Case I: Suppose $15/b$.

Then, $a = c = 1, b = 15$. This gives

$$n + 1 = u^2, \qquad 2n - 1 = w^2.$$

Hence $2u^2 - 3 = w^2 = 15v^2 - 2$. So w is odd which means

$$-v^2 \equiv 15v^2 = w^2 + 2 \equiv 3 \bmod 8$$

which is impossible.

Case II: Suppose $3 \mid b$ but $5 \nmid b$.

Then, $b = 3$ and either (i) $a = 5$, $c = 1$ or (ii) $a = 1$, $c = 5$.

In case (i), $5u^2 - 1 = 3v^2 = w^2 + 2$, which means that v, w must be odd. Hence u is even, say $u = 2u_1$. This gives

$$20u_1^2 = 3v^2 + 1 \equiv 1 \bmod 3$$

an impossibility.

In case (ii), $3v^2 - 5w^2 = 2$ means v, w are odd. But then

$$2 = 3v^2 - 5w^2 \equiv -2 \bmod 8$$

a contradiction.

Case III: $3 \nmid b$ but $5 \mid b$.

Again, $b = 5$ and either (i) $a = 3$, $c = 1$ or (ii) $a = 1$, $c = 3$.

In case (i), $6u^2 - 1 = 5v^2 = w^2 + 2$. So, v is even, say $v = 2v_1$. Thus,

$$w^2 + 2 = 20v_1^2 \equiv 0 \bmod 4$$

which gives a contradiction.

In case (ii), $2u^2 - 1 = 5v^2 = 3w^2 + 2$. This gives v, w are odd. So,

$$2u^2 = 5v^2 + 1 \equiv 6 \bmod 8$$

an impossibility.

Case IV: $3 \nmid b$, $5 \nmid b$.

Then, $b = 1$ and either (i) $a = 3$, $c = 5$ or (ii) $a = 5$, $c = 3$ or (iii) $a = 15$, $c = 1$ or (iv) $a = 1$, $c = 15$.

In case (i),

$$v^2 = 5w^2 + 2 \equiv 2 \text{ or } 3 \bmod 4$$

an impossibility.

In case (ii),

$$v^2 = 3w^2 + 2 \equiv 2 \text{ or } 5 \bmod 8$$

an impossibility.

In case (iii), $2 = v^2 - w^2$ is impossible mod 4.

Finally, in case (iv), $v^2 - 15w^2 = 2$, which is impossible mod 3.

Therefore, we have shown the claim.

Theorem 2 is proved. □

ACKNOWLEDGEMENTS

It is a pleasure to thank Yuri Bilu for his continued interest in our work. We would also like to thank Abhishek Saha for help with the MAPLE programs. We are grateful to the referee for reading the manuscript carefully and making constructive suggestions.

REFERENCES

[1] Bilu Y., Brindza B., Kirschenhofer P., Pintér A., Tichy R.F. – Diophantine equations and Bernoulli polynomials, With an appendix by A. Schinzel, Compositio Math. **131** (2002) 173–180.

[2] Bilu Y., Kulkarni M., Sury B. – On the Diophantine equation $x(x+1)\cdots(x+m-1)+r=y^n$, Acta Arithmetica **CXIII** (2004) 303–308.

[3] Bilu Y., Tichy R.F. – The Diophantine equation $f(x)=g(y)$, Acta Arithmetica **XCV** (2000) 261–288.

[4] Kulkarni M., Sury B. – On the Diophantine equation $x(x+1)\cdots(x+m-1)=g(y)$, Indag. Math. (N.S.) **14** (2003) 35–44.

[5] Kulkarni M., Sury B. – Diophantine equations with Bernoulli polynomials, Acta Arithmetica, in press.

(Received February 2004)