# Diophantine equations with Bernoulli polynomials 

by<br>Manisha Kulkarni and B. Sury (Bangalore)

The Bernoulli polynomials $B_{n}(x)$ are defined by the generating series

$$
\frac{t e^{t x}}{e^{t}-1}=\sum_{n=0}^{\infty} B_{n}(x) \frac{t^{n}}{n!}
$$

Then $B_{n}(x)=\sum_{i=0}^{n}\binom{n}{i} B_{n-i} x^{i}$ where $B_{r}=B_{r}(0)$ is the $r$ th 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 $n \geq 2$. The first few are:

$$
B_{0}=1, \quad B_{1}=-1 / 2, \quad B_{2}=1 / 6, \quad B_{4}=-1 / 30
$$

and $B_{r}=0$ for $r$ odd $>1$.
The Bernoulli polynomials $B_{n}(x)$ are related to the sums of $n$th powers of natural numbers as follows. For any $n \geq 1$, the sum $1^{n}+2^{n}+\cdots+k^{n}$ is a polynomial function $S_{n}(k)$ of $k$ and

$$
S_{n}(x)=\frac{B_{n+1}(x+1)-B_{n+1}}{n+1}
$$

In this paper, for nonzero rational numbers $a, b$ and rational polynomials $C(y)$, we study the Diophantine equation

$$
a B_{m}(x)=b B_{n}(y)+C(y)
$$

with $m \geq n>\operatorname{deg} C+2$. More generally, we look for rational solutions $x, y$ with bounded denominators. One says that an equation $f(x)=g(y)$ has infinitely many rational solutions with bounded denominators if there exists a positive integer $\lambda$ such that $f(x)=g(y)$ has infinitely many rational solutions $x, y$ satisfying $x, y \in \frac{1}{\lambda} \mathbb{Z}$. Equations of the type $f(x)=g(y)$ for $f(x)=x(x+1) \cdots(x+m-1)$ and various polynomials $g(y)$ have been studied extensively during the last decade. Also the special case when $g(y)=y^{n}-r$, where $r$ is any rational number, was studied earlier in [2]. We have proved there that in this case there are effective finiteness results for $x \in \mathbb{Z}$ and

[^0]$y \in \mathbb{Q}$. Note that our results in this paper do not give effective results as in [2]. In [4], we have some results for general $g$.

In this paper, we prove:
Main Theorem. For any polynomial $C(y) \in \mathbb{Q}[y]$ and $m \geq n>$ $\operatorname{deg} C+2$, the equation

$$
a B_{m}(x)=b B_{n}(y)+C(y)
$$

has only finitely many rational solutions with bounded denominators except when $m=n, a= \pm b$ and $C(y) \equiv 0$; in these exceptional cases, there are infinitely many rational solutions with bounded denominators if, and only if, $a=b$ or $a=-b$ and $m=n$ is odd.

In particular, if $c$ is a nonzero constant, then the equation

$$
a B_{m}(x)=b B_{n}(y)+c
$$

has only finitely many solutions for all $m, n>2$.
Remarks. (a) The condition $n>\operatorname{deg} C+2$ in the theorem is optimal as can be seen from the fact that the equation

$$
B_{3}\left(2 x-\frac{1}{2}\right)=8 B_{3}(y)+\frac{3}{2} y-\frac{3}{4}
$$

has infinitely many rational solutions corresponding to $x=2 y-1 / 2$.
(b) The particular case of the theorem when $a=n, b=m, n \neq m$ and the polynomial $C(y)$ is the constant $n B_{m}-m B_{n}$, has been discussed in [1].

We shall make extensive use of the following theorem of Bilu \& Tichy:
Theorem. For nonconstant polynomials $f(x), g(x) \in \mathbb{Q}[x]$, the following are equivalent:
(a) The equation $f(x)=g(y)$ has infinitely many rational solutions with bounded denominators.
(b) We have $f=\phi\left(f_{1}(\lambda)\right)$ and $g=\phi\left(g_{1}(\mu)\right)$, where $\lambda(x), \mu(x) \in \mathbb{Q}[X]$ are linear polynomials, $\phi(x) \in \mathbb{Q}[X]$, and $\left(f_{1}(x), g_{1}(x)\right)$ is a standard pair over $\mathbb{Q}$ such that the equation $f_{1}(x)=g_{1}(y)$ has infinitely many rational solutions with bounded denominators.

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):

- A standard pair of the first kind is

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

where $0 \leq r<t,(r, t)=1$ and $r+\operatorname{deg} p(x)>0$.

- A standard pair of the second kind is

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

- A standard pair of the third kind is

$$
\left(D_{k}\left(x, a^{t}\right), D_{t}\left(x, a^{k}\right)\right),
$$

where $(k, t)=1$. Here $D_{t}$ is the $t$ th Dickson polynomial.

- 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

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

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 $F(x) \in \mathbb{C}[x]$ is an equality of the form $F(x)=G_{1}\left(G_{2}(x)\right)$, where $G_{1}(x), G_{2}(x) \in \mathbb{C}[x]$. The decomposition is called nontrivial if $\operatorname{deg} G_{1}>1, \operatorname{deg} G_{2}>1$.

Two decompositions $F(x)=G_{1}\left(G_{2}(x)\right)$ and $F(x)=H_{1}\left(H_{2}(x)\right)$ are called equivalent if there exists a linear polynomial $l(x) \in \mathbb{C}[x]$ such that $G_{1}(x)=H_{1}(l(x))$ and $H_{2}(x)=l\left(G_{2}(x)\right)$. A polynomial is 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. Let $m \geq 2$. Then
(i) $B_{m}(x)$ is indecomposable if $m$ is odd,
(ii) if $m=2 k$, then any nontrivial decomposition of $B_{m}(x)$ is equivalent to $B_{m}(x)=h\left((x-1 / 2)^{2}\right)$.
Proof of the Main Theorem. We note once for all that we may assume $a=1$ as we may replace $b$ by $b / a$ and the polynomial $C(y)$ by $C(y) / a$, and the assertions remain the same.

First, we deal with the case $m=n$.
CASE 1: $m=n$ and $m$ is an odd integer. In this case, the equation looks like

$$
\begin{equation*}
B_{m}(x)=b B_{m}(y)+C(y) \tag{1}
\end{equation*}
$$

Assume that (1) has infinitely many rational solutions with bounded denominators. Then by [3],

$$
B_{m}(x)=\phi\left(f_{1}(\lambda(x))\right), \quad b B_{m}(y)+C(y)=\phi\left(g_{1}(\mu(y))\right)
$$

where $\lambda(x), \mu(x) \in \mathbb{Q}[X]$ are linear polynomials, $\phi(x) \in \mathbb{Q}[X]$, and the pair $\left(f_{1}(x), g_{1}(x)\right)$ is a standard pair over $\mathbb{Q}$ such that $f_{1}(x)=g_{1}(y)$ has infinitely many rational solutions with bounded denominators. Now as $m$ is an odd integer, $B_{m}(x)$ is indecomposable by [1]. Therefore, either $\operatorname{deg} \phi(x)=m$ and $\operatorname{deg} f_{1}(x)=1$, or $\operatorname{deg} \phi(x)=1$ and $\operatorname{deg} f_{1}(x)=m$.
(i) Let $\operatorname{deg} \phi(x)=m$. Then $B_{m}(x)=\phi(A x+B)$ for some $A, B \in \mathbb{Q}$. Therefore for some $u, v \in \mathbb{Q}, B_{m}(u x+v)=\phi(x)$. This gives $b B_{m}(x)+C(x)=$ $B_{m}(r x+s)$. Hence

$$
C(x)=B_{m}(r x+s)-b B_{m}(x)
$$

As deg $C(x)<m-2$, the coefficients of $x^{m}, x^{m-1}$ and $x^{m-2}$ are zero on the left hand side of the above equation.

Equating the coefficients of $x^{m}$ on both sides, we get $r^{m}=b$. We have a contradiction already when $b$ is not an $m$ th power in $\mathbb{Q}$. If it is an $m$ th power, then there is a unique rational solution $r$ of $r^{m}=b$ as $m$ is odd. Similarly, equating the coefficients of $x^{m-1}$ on both sides, we get $s=(1-r) / 2$. Finally, the coefficient of $x^{m-2}$ gives

$$
0=\frac{m(m-1) r^{m-2}}{2}\left(s^{2}-s+\frac{1-r^{2}}{6}\right)
$$

Inserting the value of $s$, we get $r^{2}=1$, i.e., $r= \pm 1$. Clearly, the two values of $s$ corresponding to $r=1$ and $r=-1$ are, respectively, $s=0$ and $s=1$. But both of these imply that $C$ is identically zero because $B_{m}(1-x)=-B_{m}(x)$ for odd $m$.
(ii) Suppose $\operatorname{deg} \phi(x)=1$ and $\operatorname{deg} f_{1}(x)=m$. Then, as $m$ is an odd integer, $\left(f_{1}(x), g_{1}(x)\right)$ can be a standard pair of either the first or third kind. Since here $\left(\operatorname{deg} f_{1}, \operatorname{deg} g_{1}\right)=m \neq 1,\left(f_{1}(x), g_{1}(x)\right)$ can only be of the first kind. So either $f_{1}(x)=x^{m}$ or $g_{1}(x)=x^{m}$. Now let $\phi(x)=\phi_{0}+\phi_{1}(x)$ for some $\phi_{0}, \phi_{1} \in \mathbb{Q}$. Therefore, either

$$
B_{m}(r x+s)=\phi_{0}+\phi_{1} x^{m} \quad \text { or } \quad b B_{m}(r x+s)+C(r x+s)=\phi_{0}+\phi_{1} x^{m}
$$

for some $r, s \in \mathbb{Q}$ with $r \neq 0$. As $\operatorname{deg} C(x)<m-2$, the coefficients of $x^{m-1}$ and $x^{m-2}$ on the left hand side of the above equations come only from the $B_{m}$ part. Equating the coefficients of $x^{m-2}$, we get $6 s^{2}-6 s+1=0, s \in \mathbb{Q}$, which is not possible.

Therefore when $m=n$ and $m$ is an odd integer equation (1) has only finitely many solutions unless $b= \pm 1$ and $C \equiv 0$.

CASE 2: $m=n$ is an even integer $2 d$. In this case, the equation becomes

$$
\begin{equation*}
B_{2 d}(x)=b B_{2 d}(y)+C(y) \tag{2}
\end{equation*}
$$

Assume that it has infinitely many rational solutions with bounded denom-
inators. Then, as in the previous case, by [3] we have

$$
B_{2 d}(x)=\phi\left(f_{1}(\lambda(x))\right), \quad b B_{2 d}(y)+C(y)=\phi\left(g_{1}(\mu(y))\right)
$$

where $\lambda(x), \mu(x), \phi(x)$ and $\left(f_{1}(x), g_{1}(x)\right)$ are as before. As $m$ is even, by [1], either the above is not a nontrivial decomposition (that is, $\operatorname{deg} \phi=2 d$ or $\operatorname{deg} \phi=1$ ), or $B_{2 d}(x)$ is equivalent to $\phi\left((x-1 / 2)^{2}\right)$, where $\operatorname{deg} \phi(x)=d$.

In the former case, if $\operatorname{deg} \phi=2 d$, then we have

$$
B_{2 d}(r x+s)=b B_{2 d}(x)+C(x)
$$

for some $r, s \in \mathbb{Q}$ with $r \neq 0$. Comparing the coefficients of $x^{2 d}, x^{2 d-1}, x^{2 d-2}$ we have $r^{2 d}=b, r=1-2 s$, and $s(s-1)=0$. This gives $r x+s=x$ or $1-x$, and so $b=1$ and $C(x) \equiv 0$ since $B_{2 d}(x)=B_{2 d}(1-x)$.

If $\operatorname{deg} \phi=1$, then since both $f_{1}, g_{1}$ have degree $2 d>2$, the standard pair $\left(f_{1}, g_{1}\right)$ must be of the first kind. Thus, we have $r, s \in \mathbb{Q}$ with $r \neq 0$ so that either

$$
B_{2 d}(r x+s)=\phi_{0}+\phi_{1} x^{2 d}
$$

or

$$
b B_{2 d}(r x+s)+C(r x+s)=\phi_{0}+\phi_{1} x^{2 d}
$$

Clearly, either of these implies that $s^{2}-s+1 / 6=0$ exactly as in Case 1.
Now, we consider the case when $\operatorname{deg} \phi=d$; then

$$
\begin{gathered}
B_{2 d}(r x+s)=\phi\left((x-1 / 2)^{2}\right) \quad \text { for some } r, s \in \mathbb{Q} \\
b B_{2 d}(x)+C(x)=\phi\left(k x^{2}+l x+m\right) \quad \text { for some } k, l, m \in \mathbb{Q} \text { with } k \neq 0
\end{gathered}
$$

Let $\phi(x)=\phi_{0}+\phi_{1} x+\cdots+\phi_{d} x^{d}$.
We digress to make a simple observation:
Lemma. If $B_{2 d}(r x+s)=\phi\left((x-1 / 2)^{2}\right)$ for some $r, s \in \mathbb{Q}$ with $r \neq 0$, then $(r, s)=(1,0)$ or $(-1,1)$. In particular, $B_{2 d}(x)=\phi\left((x-1 / 2)^{2}\right)$.

Proof. By comparing the coefficients of $x^{2 d}$ and $x^{2 d-1}$ on both sides, it easily follows that $(r, s)=(1,0)$ or $(-1,1)$. As $B_{2 d}(x)=B_{2 d}(1-x)$, we have $B_{2 d}(x)=\phi\left((x-1 / 2)^{2}\right)$.

Returning to our case, by the Lemma, we have $B_{2 d}(x)=\phi\left((x-1 / 2)^{2}\right)$. Therefore

$$
b \phi\left((x-1 / 2)^{2}\right)=\phi\left(k x^{2}+l x+m\right)-C(x)
$$

Also, the equality $B_{2 d}(x)=\phi\left((x-1 / 2)^{2}\right)$ gives

$$
\begin{aligned}
x^{2 d}-d x^{2 d-1}+\frac{d(2 d-1)}{6} & x^{2 d-2}+\cdots \\
& =\phi_{0}+\phi_{1}\left(x-\frac{1}{2}\right)^{2}+\cdots+\phi_{d}\left(x-\frac{1}{2}\right)^{2 d}
\end{aligned}
$$

By comparing the coefficients of $x^{2 d}$ in this equation, we get $\phi_{d}=1$. Further, the coefficients of $x^{2 d-1}$ give $\phi_{d-1}=-d(2 d-1) / 12$.

Now consider the equation, $b \phi\left((x-1 / 2)^{2}\right)=\phi\left(k x^{2}+l x+m\right)-C(x)$. We have

$$
\begin{aligned}
& b\left(\phi_{0}+\phi_{1}\left(x-\frac{1}{2}\right)^{2}+\cdots+\phi_{d}\left(x-\frac{1}{2}\right)^{2 d}\right) \\
& \quad=\phi_{0}+\phi_{1}\left(k x^{2}+l x+m\right)+\cdots+\phi_{d}\left(k x^{2}+l x+m\right)^{d}-C(x)
\end{aligned}
$$

As $\operatorname{deg} C(x)<2 d-2$, the coefficients of $x^{2 d}, x^{2 d-1}, x^{2 d-2}$ do not have any contribution from $C(x)$.

By comparing the coefficients of $x^{2 d}$ on both sides, we get $b \phi_{d}=\phi_{d} k^{d}$. This implies $k^{d}=b$, which either has no solutions in rational $k$ or one or two solutions according as $d$ is odd or even.

By comparing the coefficients of $x^{2 d-1}$ on both sides we get

$$
b \phi_{d}\binom{2 d}{2 d-1}\left(\frac{-1}{2}\right)=\phi_{d}\binom{d}{d-1} k^{d-1} l
$$

This gives $k=-l$.
By comparing the coefficients of $x^{2 d-2}$ we get

$$
\phi_{d-1}\left(1-\frac{1}{k}\right)=d\left(\frac{m}{k}-\frac{1}{4}\right)
$$

Inserting the value of $\phi_{d-1}$, we get $m=(2 d-1+(4-2 d) k) / 12$.
Therefore, in this case

$$
k x^{2}+l x+m=k x^{2}-k x+\frac{2 d-1+(4-2 d) k}{12}
$$

By Bilu-Tichy's theorem, if equation (2) has infinitely many rational solutions with bounded denominators, then

$$
\left(x-\frac{1}{2}\right)^{2}=k y^{2}-k y+\frac{2 d-1+(4-2 d) k}{12}
$$

has infinitely many rational solutions with bounded denominators. This is seen to be equivalent to considering the equation

$$
X^{2}-k Y^{2}=\frac{(2 d-1)(1-k)}{12}
$$

Unless the right hand side is zero, such an equation has only finitely many rational solutions with bounded denominators, by Dirichlet's unit theorem. Now, the right hand side is zero if, and only if, $k=1$ and then we have $b=1, l=-1, m=1 / 4$, and $C(x)=\phi\left(k x^{2}+l x+m\right)-\phi\left((x-1 / 2)^{2}\right)$ is identically zero.

Therefore when $m=n=2 d$, equation (2) has only finitely many rational solutions with bounded denominators unless $b=1$ and $C \equiv 0$.

CASE 3: $m>n>\operatorname{deg} C(y)+2$ and $m$ is odd. The equation is

$$
\begin{equation*}
B_{m}(x)=b B_{n}(y)+C(y) \tag{3}
\end{equation*}
$$

Suppose that (3) has infinitely many rational solutions with bounded denominators. Then again by [3] we have

$$
B_{m}(x)=\phi\left(f_{1}(\lambda(x))\right), \quad b B_{n}(y)+C(y)=\phi\left(g_{1}(\mu(y))\right)
$$

where $\lambda(x), \mu(x), \phi(x)$ and $\left(f_{1}(x), g_{1}(x)\right)$ are as before.
As $m$ is an odd integer, $B_{m}(x)$ is indecomposable by [1]. Therefore, either $\operatorname{deg} \phi(x)=m$ and $\operatorname{deg} f_{1}(x)=1$, or $\operatorname{deg} \phi(x)=1$ and $\operatorname{deg} f_{1}(x)=m$.

If $\operatorname{deg} \phi(x)=m$, then $n=m \operatorname{deg} g_{1}(\mu(x))$. Since $\operatorname{deg} g_{1}(\mu(x)) \geq 1$, we get $n \geq m$, which is a contradiction.

Hence $\operatorname{deg} \phi(x)=1$. This implies $\operatorname{deg} f_{1}(x)=m$ and $g_{1}(y)=n$. Let $\phi(x)=\phi_{0}+\phi_{1} x$ for some rational numbers $\phi_{0}, \phi_{1}$. As $m$ is odd, the standard pair $\left(f_{1}, g_{1}\right)$ can only be of the first or third kind.
(i) Suppose $\left(f_{1}, g_{1}\right)$ is a standard pair of the first kind. Then either $f_{1}(x)=x^{m}$ or $g_{1}(x)=x^{n}$. Therefore, either

$$
B_{m}(r x+s)=\phi\left(x^{m}\right)=\phi_{0}+\phi_{1} x^{m}
$$

or

$$
b B_{n}(r x+s)+C(r x+s)=\phi\left(x^{n}\right)=\phi_{0}+\phi_{1} x^{n}
$$

As $\operatorname{deg} C(x)<n-2$, the coefficients of $x^{n}, x^{n-1}, x^{n-2}$ in the last equation are the same as those of $b B_{n}(r x+s)$. Therefore, either the coefficient of $x^{m-2}$ in $B_{m}(r x+s)$ is zero or the coefficient of $x^{n-2}$ in $b B_{n}(r x+s)+C(r x+s)$ is zero. As in the previous case, this gives $6 s^{2}-6 s+1=0, s \in \mathbb{Q}$, which is not possible. Therefore $\left(f_{1}, g_{1}\right)$ cannot be a standard pair of the first kind.
(ii) Suppose $\left(f_{1}, g_{1}\right)$ is a standard pair of the third kind. That is, $\left(f_{1}, g_{1}\right)$ $=\left(D_{m}\left(x, \alpha^{n}\right), D_{n}\left(x, \alpha^{m}\right)\right)$ and $(m, n)=1$. Therefore, $B_{m}(r x+s)=\phi_{0}+$ $\phi_{1} D_{m}\left(x, \alpha^{n}\right)$. This means

$$
\sum_{i=0}^{n}\binom{n}{i} B_{n-i}(r x+s)^{i}=\phi_{0}+\phi_{1} \sum_{i=0}^{[m / 2]} d_{m, i}\left(x^{m-2 i}\right)
$$

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

$$
\binom{m}{1} r^{m-1} s+\binom{m}{m-1} B_{1} r^{m-1}=0
$$

This gives $s=1 / 2$. The coefficients of $x^{m-2}$ give

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

which on simplification yields $r^{2} \alpha^{n}=(m-1) / 24$. By considering the coefficients of $x^{m-4}$ and using the values of $\phi_{1}, r^{2} \alpha^{n}$, we get $m=9 / 2$, which is a contradiction. Hence $\left(f_{1}, g_{1}\right)$ cannot be a standard pair of the third kind either.

This implies that when $m>n>\operatorname{deg} C(y)+2$ and $m$ is odd, equation (3) can have only finitely many rational solutions with bounded denominators.

CASE 4: $m>n>\operatorname{deg} C(y)+2$ and $m$ is an even integer $2 d$. Assume that the equation

$$
\begin{equation*}
B_{m}(x)=b B_{n}(y)+C(y) \tag{4}
\end{equation*}
$$

has infinitely many rational solutions with bounded denominators. Then again, by $[3], B_{2 d}(x)=\phi\left(f_{1}(\lambda(x))\right)$ and $b B_{n}(y)+C(y)=\phi\left(g_{1}(\mu(y))\right)$, where $\lambda(x), \mu(x), \phi(x)$ and $\left(f_{1}(x), g_{1}(x)\right)$ are as before. As $m$ is even, by [1], either the above decomposition is trivial or $B_{2 d}(x)$ is equivalent to $\phi\left((x-1 / 2)^{2}\right)$, where $\operatorname{deg} \phi(x)=d$ and $b B_{n}(y)+C(y)=\phi\left(g_{1}(\mu(y))\right)$.

We first consider the case of a trivial decomposition for $B_{2 d}$; that is, either $\operatorname{deg} \phi=1$ or $\operatorname{deg} \phi=2 d$. The latter cannot happen because $\operatorname{deg} \phi$ divides $n$ which is $<2 d$. Suppose $\operatorname{deg} \phi=1$. Then $\operatorname{deg} f_{1}=2 d$ and $\operatorname{deg} g_{1}=n$. Now, since $2 d>n>2$, the standard pair is not of the second kind. If it is of the first kind, we have $r, s \in \mathbb{Q}$ with $r \neq 0$ and either

$$
B_{2 d}(r x+s)=\phi_{0}+\phi_{1} x^{2 d}
$$

or

$$
b B_{n}(r x+s)+C(r x+s)=\phi_{0}+\phi_{1} x^{n} .
$$

In both cases, we have a contradiction as before.
If $\left(f_{1}, g_{1}\right)$ is of the third or fourth kind, the very same computation done in Case 3 gives a contradiction as it shows that $2 d=9 / 2$.

If $\left(f_{1}, g_{1}\right)$ is of the fifth kind, then $2 d=6, n=4$ and

$$
B_{6}(x)=\phi_{0}+\phi_{1}\left(a(r x+s)^{2}-1\right)^{3} .
$$

This means that the derivative $B_{6}^{\prime}(x)$ has a multiple root; however, $B_{6}^{\prime}(x)=$ $6 B_{5}(x)$ and one knows that $B_{\text {odd }}(x)$ has only simple roots by a result of Brillhart.

Alternatively, even by direct computation, comparison of the coefficients of $x^{6}, x^{5}$ and $x^{4}$ gives $r^{2}=12 / 5 a, s=-r / 2, \phi_{1}=(5 / 12)^{3}$ and then the coefficients of $x^{2}$ do not match.

Hence, we are left with the case of a nontrivial decomposition; that is $\operatorname{deg} \phi=d$. Hence $n=d \operatorname{deg} g_{1}(\mu(y))$. As $2 d=m>n$, this implies $\operatorname{deg} g_{1}(\mu(y))=1$. Therefore $d=n=m / 2$. Hence we have

$$
b B_{n}(u x+v)+C(u x+v)=\phi(x), \quad B_{2 n}(x)=\phi(r x+s)^{2}
$$

for some rational numbers $u, v, r, s, u \neq 0, r \neq 0$. By eliminating $\phi(x)$, we get

$$
B_{2 n}(x)=b B_{n}\left(k x^{2}+l x+m\right)+C\left(k x^{2}+l x+m\right)
$$

We now use the property $B_{2 n}(x+1)-B_{2 n}(x)=2 n x^{2 n-1}$ of Bernoulli polynomials; we have

$$
\begin{aligned}
& b B_{n}\left(k(x+1)^{2}+l(x+1)+m\right)-b B_{n}\left(k x^{2}+l x+m\right) \\
& \quad+C\left(k(x+1)^{2}+l(x+1)+m\right)-C\left(k x^{2}+l x+m\right)=2 n x^{2 n-1}
\end{aligned}
$$

Since $\operatorname{deg} C<n-2$, we get $2 \operatorname{deg} C-1<2 n-5$. Hence in the above equation, there is no contribution from $C(x)$ in the coefficients of $x^{2 n-i}$, $i=0, \ldots, 5$. Consider the coefficients of $x^{2 n-i}, i=0, \ldots, 5$, in the equation

$$
b B_{n}\left(k(x+1)^{2}+l(x+1)+m\right)-b B_{n}\left(k x^{2}+l x+m\right)=2 n x^{2 n-1}
$$

The coefficient of $x^{2 n-1}$ is

$$
2 n=b\binom{n}{n-1} k^{n-1}(2 k+l)-b\binom{n}{n-1} k^{n-1} l .
$$

This implies $k^{n} b=1$.
Assume that $b$ is an $n$th power in $\mathbb{Q}$; otherwise we are already through. The coefficient of $x^{2 n-2}$ being 0 implies

$$
\begin{aligned}
0=\binom{n}{n-1} k^{n-1}(k+l+ & m)-\binom{n}{n-1} k^{n-1} m \\
& +\binom{n}{n-2} k^{n-2}(2 k+l)^{2}-\binom{n}{n-2} k^{n-2} l^{2}
\end{aligned}
$$

This gives $k=-l$.
The vanishing of the coefficient of $x^{2 n-3}$ gives

$$
\begin{aligned}
0= & \binom{n}{2} k^{n-2}(2 k+l) m-\binom{n}{2} k^{n-2} 2 l m+\binom{n}{3} k^{n-3}(2 k+l)^{3}-\binom{n}{3} k^{n-3} l^{3} \\
& +\binom{n}{n-1}\binom{n-1}{n-2} B_{1} k^{n-2}(2 k+l)-\binom{n}{n-1}\binom{n-1}{n-2} B_{1} k^{n-2} l .
\end{aligned}
$$

Simplifying this we get $m=1 / 2-k(n-2) / 6$. Finally, using the vanishing of the coefficient of $x^{2 n-5}$ gives us

$$
(2 n-1)(n-4) k^{2}+15=0
$$

This immediately shows $n<4$. The only possibility is $n=3$, but this gives $k^{2}=3$ and is impossible for a rational $k$.

Therefore when $m>n>\operatorname{deg} C+2$ and $m$ is even then equation (4) has only finitely many rational solutions with bounded denominators.

This proves the theorem in all cases.

Acknowledgements. We acknowledge with great pleasure the continued interest shown by Yuri Bilu in this work.

## References

[1] Yu. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér and R. F. Tichy, Diophantine equations and Bernoulli polynomials, Compositio Math. 131 (2002), 173-188.
[2] Yu. Bilu, M. Kulkarni and B. Sury, On the Diophantine equation $x(x+1) \cdots(x+m-1)$ $+r=y^{n}$, Acta Arith. 113 (2004), 303-308.
[3] Yu. Bilu and R. F. Tichy, The Diophantine equation $f(x)=g(y)$, ibid. 95 (2000), 261-288.
[4] M. Kulkarni and B. Sury, On the Diophantine equation $x(x+1) \cdots(x+m-1)=g(y)$, Indag. Math. 14 (2003), 35-44.

Stat-Math Unit
Indian Statistical Institute
8th Mile, Mysore Road
Bangalore 560 059, India
E-mail: manisha@isibang.ac.in sury@isibang.ac.in


[^0]:    2000 Mathematics Subject Classification: Primary 11D41.

