

# DIOPHANTINE EQUATIONS WITH BERNOULLI POLYNOMIALS

Manisha Kulkarni & B. Sury

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  $r$ -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 odd Bernoulli number  $B_r = 0$  for  $r$  odd  $> 1$  and the first few are :

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

The Bernoulli polynomials  $B_n$  are related to the sums of  $n$ -th powers of the first few natural numbers as follows. For any  $n \geq 1$ , the sum  $1^n + 2^n + \dots + k^n$  is a polynomial function  $S_n(k)$  of  $k$  and  $S_n(x) = \frac{B_{n+1}(x) - B_{n+1}}{n+1}$ . In this paper, for nonzero rational numbers  $a, b$  and rational polynomials  $C(y)$ , we study the Diophantine equation<sup>1</sup>

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

with  $m \geq n > \deg C + 2$  for solutions in integers  $x, y$ . More generally, we look for rational solutions with bounded denominators. One says that an equation  $f(x) = g(y)$  has infinitely many rational solutions with bounded denominator if there exist a positive integer  $\lambda$  such that  $f(x) = g(y)$  has infinitely many rational solutions  $x, y$  satisfying  $x, y \in \frac{1}{\lambda}\mathbb{Z}$ . The 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 were studied earlier in [2]. We have proved there that in this case there are effective finiteness results for  $x \in \mathbb{Z}$  and  $y \in \mathbb{Q}$ . Note that, our results in this paper do not give effective results as in [2]. In [4], we have some results for general  $g$ . We prove :

---

<sup>1</sup>Mathematics Reviews Subject Classification : 11 D 45

**Main theorem**

For any polynomial  $C(y) \in \mathbb{Q}[y]$  and and  $m \geq n > \deg C + 2$ , the equation

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

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

$$aB_m(x) = bB_n(y) + c$$

has only finitely many solutions for all  $m, n > 2$ .

**Remarks**

(a) The condition  $n > \deg(C) + 2$  in the theorem is optimal as can be seen from the fact that the equation

$$B_3(2x - \frac{1}{2}) = 8B_3(y) + \frac{3}{2}y - \frac{3}{4}$$

has infinitely many rational solutions corresponding to  $x = 2y - \frac{1}{2}$ .

(b) The particular case of the theorem when  $a = n, b = m, n \neq m$  and the polynomial  $C(y)$  is the constant  $nB_m - mB_n$ , has been discussed in [1].

We shall make extensive use of the following theorem of Bilu & Tichy:

**Theorem.**

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). A standard pair  $(f, g)$  is one of the following.

## Standard Pairs

A standard pair of the first kind is

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

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

A standard pair of the second kind is

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

A standard pair of the third kind is

$$(D_k(x, a^t), D_t(x, a^k))$$

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

A standard pair of the fourth kind is

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

where  $(k, t) = 2$ .

A standard pair of the fifth kind is

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

*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 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 and,
- (ii) if  $m = 2k$ , then any nontrivial decomposition of  $B_m(x)$  is equivalent to  $B_m(x) = h((x - \frac{1}{2})^2)$ .

**Proof of 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)** Suppose  $m = n$  and  $m$  is an odd integer.

In this case, the equation looks like  $B_m(x) = bB_m(y) + C(y) \dots \dots \dots (1)$   
 Assume that equation (1) has infinitely many rational solutions with bounded denominator. Then by [3],  $B_m(x) = \phi(f_1(\lambda(x)))$  and  $bB_m(y) + C(y) = \phi(g_1(\mu(y)))$  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  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator. Now as  $m$  is an odd integer, by [1]  $B_m(x)$  is indecomposable.

Therefore, either  $\deg \phi(x) = m$  and  $\deg f_1(x) = 1$  or  $\deg \phi(x) = 1$  and  $\deg f_1(x) = m$ .

(i) Let  $\deg \phi(x) = m$ . Then  $B_m(x) = \phi(Ax + B)$  for some  $A, B \in \mathbb{Q}$ . Therefore for some  $u, v \in \mathbb{Q}$ ,  $B_m(ux+v) = \phi(x)$ . This gives  $bB_m(x)+C(x) = B_m(rx+s)$ . Hence  $C(x) = B_m(rx+s) - bB_m(x)$ . Now 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 coefficient 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  $s = \frac{1-r}{2}$ .

Finally, the coefficient of  $x^{m-2}$  gives

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

Putting 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  $\deg \phi(x) = 1$  and  $\deg f_1(x) = m$ .

Then, as  $m$  is an odd integer,  $(f_1(x), g_1(x))$  can be either first or third kind of standard pair. Since here  $(\deg f_1, \deg g_1) = m \neq 1$ ,  $(f_1(x), g_1(x))$  can only be 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

$B_m(rx+s) = \phi_0 + \phi_1 x^m$  or  $bB_m(rx+s) + C(rx+s) = \phi_0 + \phi_1 x^m$  for some  $r, s \in \mathbb{Q}$  with  $r \neq 0$ .

Now as  $\deg C(x) < m-2$ , 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  $6s^2 - 6s + 1 = 0$ ,  $s \in \mathbb{Q}$  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  $2d$ .

In this case, the equation becomes  $B_{2d}(x) = bB_{2d}(y) + C(y) \dots \dots \dots (2)$

Assume that this equation has infinitely many rational solutions with bounded denominator. Then, as in the previous case, we have by [3],

$B_{2d}(x) = \phi(f_1(\lambda(x)))$  and  $bB_{2d}(y) + C(y) = \phi(g_1(\mu(y)))$  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  $Q$  such that  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator. Now as  $m$  is even, by [1] either the above is not a nontrivial decomposition (that is,  $\deg \phi = 2d$  or  $\deg \phi = 1$ ) or,  $B_{2d}(x)$  is equivalent to  $\phi((x - \frac{1}{2}))^2$  where  $\deg \phi(x) = d$ .

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

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

for some  $r, s \in \mathbb{Q}$  with  $r \neq 0$ .

Comparing the coefficients of  $x^{2d}, x^{2d-1}, x^{2d-2}$  we have

$$r^{2d} = b, \quad r = 1 - 2s, \quad s(s-1) = 0.$$

This gives  $rx+s = x$  or  $1-x$  and so,  $b = 1$  and  $C(x) \equiv 0$  since  $B_{2d}(x) = B_{2d}(1-x)$ .

If  $\deg \phi = 1$ , then since both  $f_1, g_1$  have degree  $2d > 2$ , the standard pair  $(f_1, g_1)$  must be of the first kind.

Thus, we have  $r, s \in \mathbb{Q}$  with  $r \neq 0$  so that either

$$B_{2d}(rx+s) = \phi_0 + \phi_1 x^{2d}$$

or

$$bB_{2d}(rx + s) + C(rx + s) = \phi_0 + \phi_1 x^{2d}.$$

Clearly, either of these implies that  $s^2 - s + \frac{1}{6} = 0$  exactly as in case (1).

Now, we consider the case when  $\deg \phi = d$ ; then for some  $r, s \in \mathbb{Q}$ ,  $B_{2d}(rx + s) = \phi((x - \frac{1}{2}))^2$  and

$bB_{2d}(x) + C(x) = \phi(kx^2 + lx + m)$ , for some  $k, l, m \in \mathbb{Q}$  with  $k \neq 0$ .

Let  $\phi(x) = \phi_0 + \phi_1 x + \dots + \phi_d x^d$ .

We digress to make a simple observation:

**Lemma**

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

**Proof**

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

Returning to our case, by the lemma, we have  $B_{2d}(x) = \phi((x - \frac{1}{2}))^2$ .

Therefore we have  $b\phi((x - \frac{1}{2}))^2 = \phi(kx^2 + lx + m) - C(x)$ .

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

$$x^{2d} - dx^{2d-1} + \frac{d(2d-1)}{6}x^{2d-2} + \dots = \phi_0 + \phi_1(x - \frac{1}{2})^2 + \dots + \phi_d(x - \frac{1}{2})^{2d}.$$

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

Now consider the equation,  $b\phi((x - \frac{1}{2}))^2 = \phi(kx^2 + lx + m) - C(x)$ .

$b(\phi_0 + \phi_1(x - \frac{1}{2})^2 + \dots + \phi_d(x - \frac{1}{2})^{2d}) = \phi_0 + \phi_1(kx^2 + lx + m) + \dots + \phi_d(kx^2 + lx + m)^d - C(x)$ .

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

By comparing the coefficients of  $x^{2d}$  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 whether  $d$  is odd or even.

By comparing the coefficients of  $x^{2d-1}$  on both sides we get  $b\phi_d \binom{2d}{2d-1} (\frac{-1}{2}) = \phi_d \binom{d}{d-1} k^{d-1} l$ . This gives  $k = -l$ .

By comparing the coefficients of  $x^{2d-2}$  we get,

$\phi_{d-1}(1 - \frac{1}{k}) = d(\frac{m}{k} - \frac{1}{4})$ . Putting the value of  $\phi_{d-1}$ , we get  $m = \frac{2d-1+(4-2d)k}{12}$ .

Therefore, in this case

$$kx^2 + lx + m = kx^2 - kx + \frac{2d - 1 + (4 - 2d)k}{12}.$$

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

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

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

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

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  $C(x) = \phi(kx^2 + lx + m) - \phi((x - \frac{1}{2})^2)$  is identically zero.

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

**Case (3)**  $m > n > \deg C(y) + 2$  and  $m$  is odd.

The equation is

$$B_m(x) = bB_n(y) + C(y) \dots \dots \dots (3)$$

Suppose that the equation (3) has infinitely many rational solutions with a bounded denominator. Then as before, by [3] we have,  $B_m(x) = \phi(f_1(\lambda(x)))$  and  $bB_n(y) + C(y) = \phi(g_1(\mu(y)))$  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  $Q$  such that  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator.

Now as  $m$  is an odd integer, by [1]  $B_m(x)$  is indecomposable. Therefore, either  $\deg \phi(x) = m$  and  $\deg f_1(x) = 1$  or  $\deg \phi(x) = 1$  and  $\deg f_1(x) = m$ . If  $\deg \phi(x) = m$ , then  $n = m(\deg g_1(\mu(x)))$ . Since  $\deg g_1(\mu(x)) \geq 1$ , we get  $n \geq m$  which is contradiction.

Hence  $\deg \phi(x) = 1$ . This implies  $\deg f_1(x) = m$  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  $(f_1, g_1)$  can only be of the 1st or of the 3rd kind.

(i) Suppose  $(f_1, g_1)$  is a standard pair of the first kind. Then, either  $f_1(x) = x^m$  or  $g_1(x) = x^n$ . Therefore,

either  $B_m(rx+s) = \phi(x^m) = \phi_0 + \phi_1 x^m$  or  $bB_n(rx+s) + C(rx+s) = \phi(x^n) = \phi_0 + \phi_1 x^n$ .

Now as  $\deg C(x) < n - 2$ , coefficients of  $x^n$ ,  $x^{n-1}$ ,  $x^{n-2}$  in the equation  $bB_n(rx+s) + C(rx+s) = \phi_0 + \phi_1 x^n$  are same as that of  $bB_n(rx+s)$ . Therefore, either the coefficient of  $x^{m-2}$  in  $B_m(rx+s)$  is zero or the coefficient of  $x^{n-2}$  in  $bB_n(rx+s) + C(rx+s)$  is zero. This gives as in the previous case  $6s^2 - 6s + 1 = 0$ ,  $s \in \mathbb{Q}$  which is not possible. Therefore  $(f_1, g_1)$  can not be a standard pair of the first kind.

(ii) Suppose  $(f_1, g_1)$  is a standard pair of the third kind.

That is,  $(f_1, g_1) = (D_m(x, \alpha^n), D_n(x, \alpha^m))$  and  $(m, n) = 1$ .

Therefore,  $B_m(rx+s) = \phi_0 + \phi_1(D_m(x, \alpha^n))$ .

This means  $\sum_{i=0}^n \binom{n}{i} B_{n-i}(rx+s)^i = \phi_0 + \phi_1 \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} d_{m,i}(x^{m-2i})$ ,

where  $d_{m,i} = \frac{m}{m-i} \binom{m-i}{i} (-\alpha^n)^i$ . 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  $s = \frac{1}{2}$ .

The coefficients of  $x^{m-2}$  give  $\frac{m(m-1)}{12} r^{m-2} (6s^2 - 6s + 1) = \frac{m}{m-1} \binom{m-1}{1} (-\alpha^n) \phi_1$

which on simplification yields  $r^2 \alpha^n = \frac{m-1}{24}$ .

By considering the coefficients of  $x^{m-4}$  and on using the values of  $\phi_1$ ,  $r^2 \alpha^n$ , we get  $m = \frac{9}{2}$  which is a contradiction. Hence  $(f_1, g_1)$  can not be a standard pair of the third kind also.

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

**Case (4)**  $m > n > \deg C(y) + 2$  and  $m$  is an even integer  $2d$ .

Assume that equation  $B_m(x) = bB_n(y) + C(y) \dots \dots \dots (4)$

has infinitely many rational solutions with bounded denominator. Then as before, by [3],

$B_{2d}(x) = \phi(f_1(\lambda(x)))$  and  $bB_n(y) + C(y) = \phi(g_1(\mu(y)))$  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  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator.



Now as  $m$  is even, by [1], either the above decomposition is trivial or  $B_{2d}(x)$  is equivalent to  $\phi((x - \frac{1}{2}))^2$  where  $\deg \phi(x) = d$  and  $bB_n(y) + C(y) = \phi(g_1(\mu(y)))$ .

We first consider the case of a trivial decomposition for  $B_{2d}$ ; that is, either  $\deg \phi = 1$  or  $\deg \phi = 2d$ . The latter cannot happen because  $\deg \phi$  divides  $n$  which is  $< 2d$ .

Suppose  $\deg \phi = 1$ . Then,  $\deg f_1 = 2d$  and  $\deg g_1 = n$ .

Now, since  $2d > n > 2$ , 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

$$B_{2d}(rx + s) = \phi_0 + \phi_1 x^{2d}$$

or

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

In both cases, we have a contradiction as before.

If  $(f_1, g_1)$  is of the third kind, the very same computation done in case (3) gives a contradiction as it shows that  $2d = 9/2$ .

If  $(f_1, g_1)$  is of the fifth kind, then  $2d = 6, n = 4$  and

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

This means that the derivative  $B'_6(x)$  has a multiple root; however,  $B'_6(x) = 6B_5(x)$  and one knows that  $B_{odd}(x)$  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  $r^2 = 12/5a, s = -r/2, \phi_1 = (5/12)^3$  and then the coefficients of  $x^2$  do not match.

Hence, we are left with the case of a nontrivial decomposition; that is,  $\deg \phi = d$ . Hence  $n = d$  ( $\deg g_1(\mu(y))$ ). As  $2d = m > n$ , this implies  $\deg g_1(\mu(y)) = 1$ . Therefore  $d = n = \frac{m}{2}$ . Hence we have,  $bB_n(ux + v) + C(ux + v) = \phi(x)$  and  $B_{2n}(x) = \phi(rx + s)^2$  for some rational numbers  $u, v, r, s, u \neq 0, r \neq 0$ . By eliminating  $\phi(x)$ , we get

$$B_{2n}(x) = bB_n(kx^2 + lx + m) + C(kx^2 + lx + m).$$

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

$$bB_n(k(x + 1)^2 + l(x + 1) + m) - bB_n(kx^2 + lx + m)$$

$$+C(k(x+1)^2 + l(x+1) + m) - C(kx^2 + lx + m) = 2nx^{2n-1}.$$

Since, the degree of  $C$  is  $< n - 2$ ,  $2 \deg C - 1 < 2n - 5$ . Hence in the above equation, there is no contribution from  $C(x)$  in the coefficients of  $x^{2n-i}$ ,  $i = 0, \dots, 5$ . Consider the coefficients of  $x^{2n-i}$ ,  $i = 0, \dots, 5$  in the equation  $bB_n(k(x+1)^2 + l(x+1) + m) - bB_n(kx^2 + lx + m) = 2nx^{2n-1}$ .

The coefficient of  $x^{2n-1} = 2n = b \binom{n}{n-1} k^{n-1} (2k+l) - b \binom{n}{n-1} k^{n-1} l$  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  $x^{2n-2} = 0$  implies

$$0 = \binom{n}{n-1} k^{n-1} (k+l+m) - \binom{n}{n-1} k^{n-1} m + \binom{n}{n-2} k^{n-2} (2k+l)^2 - \binom{n}{n-2} k^{n-2} l^2.$$

This gives  $k = -l$ .

The vanishing of the coefficient of  $x^{2n-3}$  gives

$$0 = \binom{n}{2} k^{n-2} (2k+l)m - \binom{n}{2} k^{n-2} 2lm + \binom{n}{3} k^{n-3} (2k+l)^3 - \binom{n}{3} k^{n-3} l^3 + \binom{n}{n-1} \binom{n-1}{n-2} B_1 k^{n-2} (2k+l) - \binom{n}{n-1} \binom{n-1}{n-2} B_1 k^{n-2} l.$$

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

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

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  $m > n > \deg C + 2$  and  $m$  is even then equation (4) has only finitely many rational solutions with bounded denominator.

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] Y. Bilu, B. Brindza, P. Kirschenhofer, A.Pinter and R.F. Tichy. Diophantine Equations and Bernoulli Polynomials. *Compositio Mathematica* 131 (2002), 173-188.
- [2] Y.Bilu, M. Kulkarni and B.Sury. On the Diophantine equation  $x(x+1)\cdots(x+m-1)+r=y^n$ . To appear in *Acta Arithmetica*, Special volume on R.Tijdeman.
- [3] Y. Bilu and R.F. Tichy. The Diophantine Equation  $f(x) - g(y)$ . *Acta Arithmetica* XCV.3 (2000), 261 - 288.
- [4] M. Kulkarni and B.Sury. On the Diophantine equation  $x(x+1)\cdots(x+m-1) = g(y)$ . *Indagationes Math.*, 14 (2003), 35-44.

### Address :

*Manisha Kulkarni & B.Sury*

Stat- Math Unit

Indian Statistical Institute

8th Mile, Mysore Road

Bangalore - 560 059

India.

email : manisha@isibang.ac.in & sury@isibang.ac.in