

isib/ms/2005/7

February 18th, 2005

<http://www.isibang.ac.in/~statmath/eprints>

The general Diophantine equation of the  
form  $B_m(x) = g(y)$

MANISHA KULKARNI AND B.SURY

Indian Statistical Institute, Bangalore Centre  
8th Mile Mysore Road-560 059, India



# The general Diophantine equation of the form $B_m(x) = g(y)$

**Manisha Kulkarni**

Poornaprajna Institute of Scientific Research

Davanhalli, Bangalore

India.

email : manisha@isibang.ac.in

**B.Sury**<sup>1</sup>

Statistics & Mathematics Unit

Indian Statistical Institute

8th Mile Mysore Road

Bangalore - 560 059

India.

email : sury@isibang.ac.in

## Abstract

In this paper we consider the general Diophantine equation of the form

$$B_m(x) = g(y)$$

where  $g$  is any nonzero polynomial in one variable over  $\mathbb{Q}$ , of degree  $n \geq 3$  and  $B_m$  is the Bernoulli polynomial of degree  $m \geq 3$ . We prove a finiteness theorem for rational solutions with a bounded denominator.<sup>2</sup>

For integral polynomials  $f, g$ , the study of Diophantine equations of the form  $f(x) = g(y)$  has had a long history. Ideas of Baker, Beukers, Fried, Schinzel, Shorey, Siegel, Tijdeman and others culminated in 2000, in a general finiteness theorem due to Y.Bilu and R.Tichy [3], for Diophantine equations of the form  $f(x) = g(y)$  where  $f, g$  are polynomials in one variable with rational coefficients. To apply Siegel's theorem on finiteness of integral points on the curve given by the equation  $f(x) = g(y)$ , one needs to compute the genus of this curve and, when the genus is zero, to determine the number of points at infinity. The Bilu-Tichy theorem produces a set  $\mathcal{F}$  of five families of pairs of polynomials (called standard pairs) over  $\mathbb{Q}$ , such that any pair  $(f, g)$  of polynomials over  $\mathbb{Q}$  for which the curve  $f(x) = g(y)$  has genus zero and at most two points at infinity, is a pair in  $\mathcal{F}$  upto a linear change of variables. Moreover, they show that each pair  $(f, g)$  for

---

<sup>1</sup>Corresponding author

<sup>2</sup>Mathematics Subject Classification 11D45, 11B68, 14H25

which  $f(x) = g(y)$  has infinitely many solutions can be determined from standard pairs - the precise statement is given in Theorem D below. This theorem has been used to solve various classes of equations of the form  $f(x) = g(y)$ . In [1], [2], [7], [8], [9], equations involving the Bernoulli polynomials and polynomials of the form  $x(x+1) \cdots (x+m-1) + r$  with  $r$  rational, were studied. We recall that the Bernoulli polynomials  $B_m(x)$  are defined by the generating series

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

Then,  $B_m(x) = \sum_{i=0}^m \binom{m}{i} B_{m-i} x^i$  where  $B_r = B_r(0)$  is the  $r$ -th Bernoulli number. In [8], [9], equations of the following forms were analyzed and proved to have only finitely many integral solutions in  $x, y$  with some exceptions (all of which are completely determined) :

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

$$aB_m(x) = b(y(y+1) \cdots (y+n-1) + C(y) ,$$

$$a(x(x+1) \cdots (x+m-1) = bB_n(y) + C(y).$$

where  $a, b \in \mathbb{Q}^*$ , and  $m \geq n > \deg(C) + 2$ .

In this paper we consider the general Diophantine equation of the form

$$B_m(x) = g(y)$$

where  $m \geq 3$  and  $g$  is any nonzero polynomial over  $\mathbb{Q}$ , of degree  $n \geq 3$ . We prove a finiteness theorem for rational solutions with a bounded denominator. Here, for rational polynomials  $F, G$ , one says that *the equation  $F(x) = G(y)$  has infinitely many rational solutions with a bounded denominator if there exist a positive integer  $\lambda$  such that  $F(x) = G(y)$  has infinitely many rational solutions  $x, y$  satisfying  $x, y \in \frac{1}{\lambda}\mathbb{Z}$ .*

We prove :

**Main Theorem.**

*Suppose  $B_m(x) = g(y)$  has infinitely many rational solutions  $x, y$  with bounded denominator. Then, we are in one of the following cases.*

(i)  $g(y) = B_m(h(y))$  for some  $h$  is a polynomial over  $\mathbb{Q}$ .

(ii)  $m$  is even and  $g(y) = \phi(h(y))$ , where  $h$  is a polynomial over  $\mathbb{Q}$ , whose square-free part has at most two zeroes, such that  $h$  takes infinitely many square values in  $\mathbb{Z}$  and,  $\phi$  is the unique polynomial such that  $B_m(x) = \phi((x - \frac{1}{2})^2)$ .

(iii)  $m = 3, (6, n) = 1$  and  $g(x) = r^3 D_n(\delta(x), \alpha^3)$  where  $r, \alpha \in \mathbb{Q}$  satisfy  $r^2 \alpha^n = \frac{1}{12}$ ,  $\delta$  is a linear polynomial over  $\mathbb{Q}$  and  $D_n(x, c)$  is the Dickson polynomial

$$D_n(x, c) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-c)^i x^{n-2i}.$$

Furthermore, in each of these cases, there are infinitely many solutions with a bounded denominator.

In [8] and [9], the following results were proved :

**Theorem A** ([8]).

For any polynomial  $C$  over  $\mathbb{Q}$  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  $m, n > 2$ .

**Theorem B** ([9]).

Let  $C$  be any polynomial over  $\mathbb{Q}$  and  $m \geq n > \deg(C) + 2$ . Then, the equation

$$aB_m(x) = b(y(y+1) \cdots (y+n-1) + C(y))$$

has only finitely many rational solutions  $x, y$  with a bounded denominator, except in the following situations :

- (i)  $m = n, m+1$  is a perfect square,  $a = b(\sqrt{m+1})^m$ ,
- (ii)  $m = 2n, \frac{n+1}{3}$  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 C** ([9]).

Let  $C$  be any polynomial over  $\mathbb{Q}$  and  $m \geq n > \deg(C) + 2$ . Then, the equation

$$a(x(x+1) \cdots (x+m-1) = bB_n(y) + C(y)$$

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

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

In these situations, the polynomial  $C$  is also uniquely determined, and has degree  $m - 4$ .

### Remarks.

1. The Theorems A and B fall into the case (i) above.
2. In each of the three cases of the main theorem, there are infinitely many solutions. This is obvious in cases (i) and (ii). In case (iii), for each  $n$  as above, there exist infinitely many  $r, \alpha$  such that  $r^2 \alpha^n = \frac{1}{12}$ . For instance, writing  $n = 2N + 1$ , for any  $k$ , take  $r = \frac{3^{Nk+N+k}}{2}$ ,  $\alpha = 3^{2k+1}$ .

Let us state precisely the result from [3] which will be our main tool here.

### Theorem D ([3]).

For non-constant polynomials  $f, g$  over  $\mathbb{Q}$ , the following are equivalent:

- (a) The equation  $f(x) = g(y)$  has infinitely many rational solutions in  $x, y$  with a bounded denominator.
- (b) We have  $f = \phi(f_1(\lambda))$  and  $g = \phi(g_1(\mu))$  where  $\lambda, \mu$  are linear polynomials over  $\mathbb{Q}$ ,  $\phi$  is some polynomial over  $\mathbb{Q}$ , 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  $x, y$  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

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

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

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

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

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  $p \in k[x]$ .

The theorem of Bilu and Tichy above involves decompositions of polynomials which we recall :

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.

These definitions carry over to any field in place of  $\mathbf{C}$ .

Therefore, it becomes important to find all possible decompositions for all the polynomials under consideration. For the Bernoulli polynomials such a decomposition theorem is not very difficult to prove :

**Theorem E** ([1]).

Let  $m \geq 2$ . Then,

- (i)  $B_m$  is indecomposable if  $m$  is odd and,
- (ii) if  $m = 2k$ , then any nontrivial decomposition of  $B_m$  is equivalent to  $B_m(x) = \phi((x - \frac{1}{2})^2)$  for a unique polynomial  $\phi$  over  $\mathbf{Q}$ .

**Proof of the main theorem:**

Before proceeding, we note that  $B_m(x) = \sum_{i=0}^m \binom{m}{i} B_{m-i} x^i$  and that  $B'_m(x) = m B_{m-1}(x)$ . Further, it is known due to results of Brillhart [4] and Inkeri [?] that the Bernoulli polynomial  $B_m$  has only simple roots if  $m > 3$  is odd, and has no rational roots if  $m > 2$  is even.

If the equation  $B_m(x) = g(y)$  has infinitely many solutions, the Bilu-Tichy theorem gives  $B_m(x) = \phi \circ f_1 \circ \lambda(x)$  and  $g(x) = \phi \circ g_1 \circ \mu(x)$  where  $\lambda, \mu$  are linear polynomials over  $\mathbb{Q}$  and  $(f_1, g_1)$  is a standard pair over  $\mathbb{Q}$  such that  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator. From Theorem E, we know that the only nontrivial decomposition of  $B_m$  up to equivalence has  $f_1(x) = (x - \frac{1}{2})^2$ ; therefore there is a trichotomy :

- (a)  $\deg \phi = m$ , or
- (b)  $m = 2d$ ,  $\deg \phi = d$  and  $B_m(x) = \phi(\lambda(x - \frac{1}{2})^2)$ , or
- (c)  $\deg \phi = 1$ .

**Case (a)**  $\deg \phi = m$  and suppose  $B_m(x) = g(y)$  has infinitely many solutions. Then as above, there are linear polynomials  $\lambda, \mu \in \mathbb{Q}[x]$ , and a standard pair  $(f_1(x), g_1(x))$  such that  $B_m(x) = \phi \circ f_1 \circ \lambda(x)$  and  $g(x) = \phi \circ g_1 \circ \mu(x)$ .

Since  $\deg \phi = m = \deg B_m$ , we get that  $\phi(x) = B_m(\delta(x))$  for some linear polynomial  $\delta(x) = u + vx \in \mathbb{Q}[x]$ . Then,  $g(x) = B_m(h(x))$  where  $h = \delta \circ g_1 \circ \mu$ . This is as asserted in case (i) of the theorem.

**Case (b)**  $\deg \phi = \frac{m}{2}$ . If the equation  $B_m(x) = g(y)$  has infinitely many solutions then, as before, there are linear polynomials  $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ , and a standard pair  $(f_1, g_1)$  such that  $B_m(x) = \phi \circ f_1 \circ \lambda(x)$  and  $g(y) = \phi \circ g_1 \circ \mu(y)$  and  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator. Therefore,  $B_m(x) = \phi(\delta(f_1 \circ \lambda(x)))$  and  $g(y) = \phi(\delta(g_1 \circ \mu(y)))$  where  $\delta(x)$  is a linear polynomial,  $\deg f_1 = 2$  and  $\phi(x)$  is such that  $B_m(x) = \phi((x - \frac{1}{2})^2)$ . Write  $h_1(x) = \delta(f_1(\lambda(x)))$ ,  $h_2(x) = \delta(g_1(\mu(x)))$ . Then  $(B_m(x), g(y))$  can be written as  $(\phi(h_1(x)), \phi(h_2(y)))$ .

We show that the square-free part of  $h_2(y)$  has at most two zeroes. In our case, since  $h_1(x)$  is the square of a linear polynomial and  $h_1(x) = h_2(y)$  has infinitely many rational solutions with bounded denominator, it follows immediately from Siegel's theorem that  $h_2$  has at most two zeroes of odd multiplicity. This completes the discussion of case(b) and leads to case (ii) of the Theorem.

**Case (c)**  $\deg \phi = 1$ .

If the equation  $B_m(x) = g(y)$  has infinitely many solutions, then, as before, there are



linear polynomials  $\lambda(x), \mu(x) \in Q[x]$ , and a standard pair  $(f_1, g_1)$  such that  $B_m(x) = \phi \circ f_1 \circ \lambda(x)$  and  $g(y) = \phi \circ g_1 \circ \mu(y)$  and  $f_1(x) = g_1(y)$  has infinitely many rational solutions with bounded denominator. In this case, we have  $\deg f_1 = m$  and  $\deg g_1 = \deg g = n$ .

Let  $\phi(x) = \phi_0 + \phi_1 x$  for some rational numbers  $\phi_0, \phi_1$ .

Suppose the standard pair  $(f_1, g_1)$  is of the *second* kind. Then  $(f_1, g_1) = (x^2, (ax^2 + b)p(x)^2)$  or switched. But this will imply that either  $m = 2$  or  $n = 2$  which is a contradiction to our assumption that  $m, n \geq 3$ . Therefore  $(f_1, g_1)$  can not be of the second kind.

Suppose the standard pair  $(f_1, g_1)$  is of the *third* kind. Then,

$$(f_1(x), g_1(y)) = (D_m(x, \alpha^n), D_n(x, \alpha^m))$$

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

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

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  $x^{m-2}$  gives

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

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

First, assume  $m \geq 4$ . 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, when  $m \geq 4$ ,  $(f_1, g_1)$  can not be a standard pair of the third kind.

If  $m = 3$ , we get  $r^2 \alpha^n = \frac{1}{12}$ . Thus,  $n$  is odd, as the power of 3 dividing the right side is odd. Also  $(3, n) = 1$ . Since we have an equality of polynomials

$$B_3(rx + \frac{1}{2}) = r^3 D_3(x, \frac{1}{12r^2})$$

and since  $D_3(x, \alpha^n) = D_n(x, \alpha^3)$  has infinitely many rational solutions with a bounded denominator when  $(3, n) = 1$ , this case occurs and we are in case (iii) of the theorem.

The same argument goes through if the pair is of the *fourth* kind as the number  $\phi_1$  above is simply replaced by  $\alpha^{-m/2} \phi_1$ . Note that  $m = 3$  cannot occur here as  $m$  is even.

If  $(f_1, g_1)$  is of the *fifth* kind, then  $(m, n) = (6, 4)$  or  $(4, 6)$  and  $(f_1(x), g_1(y)) = ((\alpha x^2 - 1)^3, 3x^4 - 4x^3)$  or switched. We will give the proof when  $(m, n) = (6, 4)$  and a similar argument works when  $(m, n) = (4, 6)$ .

Let  $(m, n) = (6, 4)$ . Then,

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

This means that the derivative  $B'_6(x) = 6B_5(x)$  has a multiple root with multiplicity 2. However, one knows that  $B_5(x)$  has only simple roots by the result of Brillhart [4] quoted in the beginning of the proof of the theorem. Hence  $(f_1, g_1)$  can not be a standard pair of *fifth* kind.

Finally, suppose the standard pair  $(f_1, g_1)$  is of the *first* kind. Then, we have either

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

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

$$B_m(ux + v) = \phi_0 + \phi_1 a x^r p(x)^t$$

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

Suppose

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

Then coefficient of  $x^{m-2}$  is zero on the right hand side. On the left hand side, the coefficient of  $x^{m-2}$  is  $\frac{m(m-1)}{12} r^{m-2} (6s^2 - 6s + 1)$ . Equating this to zero, we get  $6s^2 - 6s + 1 = 0$  for a rational number  $s$ , which is impossible. Hence  $f_1(x)$  can not be  $x^m$ .

Now suppose  $f_1(x) = a x^r p(x)^t$  and  $g_1(x) = x^t$ . Note that  $t = \deg g \geq 3$ .

**Suppose  $m$  is even.**

Then

$$B_m(ux + v) = \phi_0 + \phi_1 a x^r p(x)^t.$$

$\deg p > 0$  as we have already seen that  $B_m(x) = \phi_0 + \phi_2 x^m$  is impossible for any rational number  $\phi_2$ .

Now the derivative of  $B'_m(x) = mB_{m-1}(x)$  and from the above equality, every root of  $p(x)$  is a multiple root of  $B_{m-1}(x)$  with multiplicity at least  $(t-1)$ . But as  $m-1$  is odd, we know that  $B_{m-1}(x)$  has only simple roots by the result of Brillhart quoted earlier [4]. Therefore  $t = 2$ ; but then  $\deg g = 2$ , which is a contradiction.

Therefore when  $m$  is even  $f_1(x)$  can not be of the type  $a x^r p(x)^t$ .

**Suppose  $m$  is odd.**

Now  $f_1(x) = ax^r p(x)^t$  where  $r, t$  as above and  $g_1(x) = x^t$ . Then

$$g(x) = \phi_0 + \phi_1 \mu(x)^t$$

and

$$B_m(x) = \phi_0 + \phi_1 a \lambda(x)^r p(\lambda(x))^t.$$

Thus, for some rational numbers  $u, v$  we get,  $B_m(ux+v) = \phi_0 + \phi_1 ax^r p(x)^t$  and  $m = td+r$  where  $d$  is the degree of the polynomial  $p$ . Since the degree of  $g$  is at least three, we get  $t \geq 3$ . Now by looking at the derivative of  $B_m(ux+v)$ , we have

$$umB_{m-1}(ux+v) = \phi_1 a [rx^{r-1}p(x)^t + tp(x)^{t-1}x^r p'(x)]$$

So every root of  $p$  is a multiple root of  $B_{m-1}$  of multiplicity  $(t-1)$ . Therefore, taking derivative again, it follows that every root of  $p$  is a root of  $B_{m-2}$  of multiplicity at least  $t-2$ . As  $m-2$  is odd,  $B_{m-2}$  has only simple roots; therefore,  $t \leq 3$ . Hence  $t = 3$ . Note also that  $p$  must have only simple roots and all its roots are irrational since it is true of  $B_{m-1}$  by the result of Inkeri [?] quoted in the beginning of the proof.

Therefore,  $B_m(rx+s) = \phi_0 + \phi_1 ax^r p(x)^3$  and  $m = 3d+r$ . Now as  $r < t = 3$ , we get  $r = 1$  or  $2$ .

If  $r = 2$ , then  $B_m(ux+v) = \phi_0 + \phi_1 ax^2 p(x)^3$ . By taking the derivative, it follows that  $mB_{m-1}$  has at least one rational root. But we know that, if  $B_k$  has a rational root then  $k$  must be odd by Inkeri's result [?] quoted above. In our case, this gives a contradiction since  $m-1$  is even.

Let  $r = 1$ . Then  $B_m(x) - \phi_0 = \lambda(x)p(x)^3$  for a linear polynomial  $\lambda(x)$  and a polynomial  $p(x)$  of degree  $(m-1)/3$  over  $\mathbb{Q}$ . As every root of  $p(x)$  is a multiple root of  $B_m(x) - \phi_0$  with multiplicity  $\geq 3$ , such a root is also a root of  $B_{m-1}(x)$  and of  $B_{m-2}(x)$ .

From this discussion, it follows that  $p$  has no rational roots, since this is true for  $B_{m-1}$  and all its roots are simple (since this is true for  $B_{m-2}$ ).

We show now that it is impossible for the equality of polynomials

$$B_m(x) - \phi_0 = \lambda(x)p(x)^3$$

to hold where  $\lambda$  is linear and  $B_m(\alpha) = \phi_0$  and  $B_{m-1}(\alpha) = 0$ . To show this, we note that since  $x = 0, \frac{1}{2}, 1$  are zeroes of  $B_m(x)$ . Hence, writing  $\lambda(x) = c_0 + c_1x$ , we have

$$-\phi_0 = c_0 p(0)^3 = (c_0 + c_1/2)p(1/2)^3 = (c_0 + c_1)p(1)^3.$$

Note that  $B_{m-1}(\alpha) = \phi_0 \neq 0$  as  $B_m$  has only simple roots.

As  $p$  is not zero at rational numbers, we have

$$\frac{c_0 + \frac{c_1}{2}}{c_0} = s^3, \quad \frac{c_0 + c_1}{c_0} = t^3$$

for nonzero rational numbers  $s, t$ . Hence we have

$$s^3 - 1 = 2(t^3 - 1)$$

where evidently  $s \neq 1 \neq t$ . The above equation is equivalent to

$$x^3 + y^3 = 2z^3$$

in nonzero integers  $x, y, z$  which are not all equal (as  $t \neq 1 \neq s$ ). But, it is well-known and easy to prove ([5], P.37), that the above equation has no solutions other than  $xyz = 0$  or  $x = y = z$ . This completes the proof of the main theorem.

## Acknowledgments

The first author would like to thank the Indian Statistical Institute, Bangalore for all facilities and help they provided during this research. Both authors are indebted to Yuri Bilu for having introduced them to this subject.

## References

- [1] Y. Bilu, B. Brindza, P. Kirschenhofer, A. Pintér and R.F. Tichy. Diophantine Equations and Bernoulli Polynomials. With an appendix by A. Schinzel. *Compositio Math.* 131 (2002), 173 - 180.
- [2] Y. Bilu, M. Kulkarni and B. Sury. On the Diophantine equation  $x(x+1)\cdots(x+m-1)+r=y^n$ . *Acta Arithmetica* CXIII (2004), 303 - 308.
- [3] Y. Bilu and R.F. Tichy. The Diophantine Equation  $f(x) = g(y)$ . *Acta Arithmetica* XCV (2000), 261 - 288.
- [4] J. Brillhart. On the Euler and Bernoulli polynomials. *J. Reine. Angew. Math.* 234 (1969). 45 - 64.
- [5] Y. Hellegouarch. Invitation to mathematics of Fermat-Wiles. Translated from the 2nd (2001) edition by Leila Schneps. Academic Press, Inc., San Diego, CA 2002.
- [6] K. Inkeri Real roots of Bernoulli Polynomials. *Am. Univ. Turku. Ser A I*, 37 (1959) 20pp

- [7] M. Kulkarni and B. Sury. On the Diophantine equation  $x(x+1) \cdots (x+m-1) = g(y)$ . *Indagationes Math.* 14 (2003), 35-44.
- [8] M. Kulkarni and B. Sury. Diophantine equations with Bernoulli polynomials. *Acta Arithmetica*, in press.
- [9] M. Kulkarni and B. Sury. A class of Diophantine equations involving Bernoulli polynomials. *Indagationes Mathematicae*, in press.