isibc/ms/2005/27
March 22nd, 2005
http://www.isibang.ac.in/~statmath/eprints

The Diophantine equation $1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} = g(y)$ and more

Manisha Kulkarni and B.Sury

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

Revised Version of: isibc/ms/2005/07

The Diophantine equation $1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} = g(y)$ and more

Manisha Kulkarni
Poornaprajna Institute of Scientific Research
Davanhalli, Bangalore
India.
email : manisha@isibang.ac.in

B.Sury[1]
Statistics & Mathematics Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore - 560 059
India.
email : sury@isibang.ac.in

Introduction

A remarkable finiteness theorem for Diophantine equations[2] of the form $f(x) = g(y)$ where f, g are polynomials in one variable with rational coefficients, was proved by Y.Bilu and R.Tichy [5]. This 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. In principle, whenever one has enough information about the possible decompositions $f(x) = f_1(f_2(x))$, one can use the Bilu-Tichy theorem to prove finiteness results for solutions of equations of the form $f(x) = g(y)$. See [2], [3], [8], [9], [10], [11] for some of these results.

In this paper, we prove finiteness theorems for integral solutions (with necessary exceptions) for certain equations of the form $f(x) = g(y)$ which includes the polynomials

$$f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + ... + \frac{x^n}{n!}$$

for any $n \geq 3$, and the Bernoulli polynomials $B_n(x)$, where g is an arbitrary polynomial of degree $m \geq 3$ in $\mathbb{Q}[y]$. In fact, the theorems show finiteness of the number of rational solutions with any bounded denominator. Before stating the main results, we recall two definitions.
For a polynomial $P(x) \in \mathbb{C}[x]$, a complex number c is said to be an *extremum*, if $P(x) - c$ has multiple roots. The *type of* c (with respect to P) is defined to be the tuple $(\mu_1, \cdots, \mu_s)$ of the

[1]Corresponding author
[2]Mathematics Subject Classification 11D45,11B68,14H25

multiplicities of the distinct roots of $P(x) - c$.
The Dickson polynomial $D_m(t, c)$ of degree m is defined by

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

The main results are :

Theorem A
Let f, g be polynomials of degrees n, m respectively, with rational coefficients. Suppose each extremum (with respect to f) has type $(1, 1, \cdots, 1, 2)$. Then, for $n, m \geq 3$, the equation $f(x) = g(y)$ has only finitely many rational solutions (x, y) with a bounded denominator except in the following two cases :
(i) $g(y) = f(h(y))$ for some nonzero polynomial $h(y) \in \mathbb{Q}(y)$,
(ii) $n = 3, (m, 3) = 1$ and $f(x) = c_0 + c_1 D_3(\lambda(x), c^m)$, $g(y) = c_0 + c_1 D_m(\mu(y), c^3)$ for linear polynomials λ and μ over $\mathbb{Q}$ and $c_i \in \mathbb{Q}$ with $c_1, c \neq 0$.
In each exceptional case, there are infinitely many solutions.

Corollary
Let $E_n(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$ with $n \geq 3$ and let $g \in \mathbb{Q}[y]$ be of degree $m \geq 3$. Then, the equation $E_n(x) = g(y)$ has only finitely many rational solutions with a bounded denominator except in the following two cases :
(i) $g(y) = E_n(h(y))$ for some nonzero polynomial $h(y) \in \mathbb{Q}(y)$,
(ii) $n = 3, m$ is odd, and $g(x) = \frac{1}{3} + \frac{1}{6\lambda^3} D_m(\mu(x), a^3)$, where $-a \in (\mathbb{Q}^*)^2, \lambda^2 = -a^m$, and μ is a linear polynomial over $\mathbb{Q}$.
In each exceptional case, there are infinitely many solutions.

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.

Theorem B
Let $g(y) \in \mathbb{Q}[y]$ have degree $n \geq 3$ and let $m \geq 3$. The equation $B_m(x) = g(y)$ has only finitely many rational solutions $x,\ y$ with any bounded denominator apart from the following exceptions :

(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, ϕ 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* $r^2\alpha^n = \frac{1}{12}$, δ *is a linear polynomial over* $\mathbb{Q}$ *and* $D_n(x,c)$ *is the Dickson polynomial*

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

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

In the above statements, for polynomials with rational coefficients F, G, one has said that *the equation* $F(x) = G(y)$ *has infinitely many rational solutions with a bounded denominator to mean that there exist a positive integer* λ *such that* $F(x) = G(y)$ *has infinitely many rational solutions* $x,\ y$ *satisfying* $x, y \in \frac{1}{\lambda}\mathbb{Z}$.

In the process of the proof, we also prove that the polynomial $E_n(x)$ is indecomposable; that is, E_n is not of the form $f_1 \circ f_2$ for complex polynomials f_1, f_2 of degrees ≥ 2. In fact, E_n belongs to a class of polynomials $f(x)$ for which one has a common proof of indecomposability and of finiteness of solutions of $f(x) = g(y)$ (see the lemma below). For the Bernoulli polynomials, the possible decompositions have been discussed in [2].

An indecomposability criterion

In this section, we start with a sufficient criterion for indecomposability of a complex polynomial and prove that the polynomials

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$$

are indecomposable for each n.

Lemma
Let f *be any complex polynomial and suppose* $f = g \circ h$ *for complex polynomials* g, h *of degrees* ≥ 2*. Then, if* $\alpha \in \mathbb{C}$ *is so that* $g'(\alpha) = 0$*, then the polynomial* $h(x) - \alpha$ *divides both* $f(x) - g(\alpha)$ *and* $f'(x)$*.*
In particular, if $f(x) \in \mathbb{C}[x]$ satisfies the condition that any extremum $\lambda \in \mathbb{C}$ has the type $(1, 1, \cdots, 1, 2)$, then f is indecomposable over $\mathbb{C}$; that is, if $f(x) = f_1(f_2(x))$ for polynomials $f_1, f_2 \in \mathbb{C}[x]$, then either f_1 or f_2 must be linear.
Proof.
The former statement implies the latter one. For, it implies that If $f(x) = G_1(G_2(x))$ is a decomposition of $f(x)$ with deg $G_1, G_2 > 1$, then there exists $\lambda \in \mathbb{C}$ such that deg gcd $(f(x) - \lambda, f'(x)) \geq$ deg G_2. But, then the type of λ (with respect to f) cannot be $(1, 1, \cdots, 1, 2)$.

So, we prove the former statement. Evidently, for any $\alpha \in \mathbb{C}$, the polynomial $h(x) - \alpha$ divides $f(x) - g(\alpha)$. Moreover, if α is such that $g'(\alpha) = 0$, then consider any root θ of $h(x) - \alpha$. Suppose its multiplicity is a. Then, since the multiplicity of θ in $h'(x)$ is $a - 1$ and since $g'(h(\theta)) = g'(\alpha) = 0$, it follows that $(x - \theta)^a$ divides $f'(x) = g'(h(x))h'(x)$. This proves the proposition.

Remarks.
The proof shows the following refined version for polynomials over $\mathbb{Q}$. If $f(x) \in \mathbb{Q}[x]$ is so that each extremum $\lambda \in \bar{\mathbb{Q}}$ of degree $\leq \frac{\deg f}{2} - 1$ has type $(1, 1, \cdots, 1, 2)$, then f is indecomposable over $\mathbb{Q}$.

Proposition.
Each extremum of the polynomial

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$$

has the type $(1, 1, \cdots, 1, 2)$. *In particular,* $E_n(x)$ *is indecomposable for all* n. *Moreover,* E_n *has only simple roots for any* n.

Proof.
Note that $E'_{n+1} = E_n$ for any $n \geq 0$. Therefore, it is clear that, for each $n \geq 0$, the roots of E_n are simple, for $E_{n+1}(\alpha) = 0$ implies $E'_{n+1}(\alpha) = E_n(\alpha) = E_{n+1}(\alpha) - \alpha^{n+1}/(n+1)! = -\alpha^{n+1}/(n+1)! \neq 0$.
Now, let λ be a complex number such that $E_{n+1}(x) - \lambda$ has a multiple root α. Then $E_n(\alpha) = 0$ and $\lambda = E_{n+1}(\alpha) = \alpha^{n+1}/(n+1)!$.
If β is another multiple root of $E_{n+1}(x) - \lambda$, then $\alpha^{n+1} = \beta^{n+1}$. This implies that there exists $\theta \neq 1$ with $\theta^{n+1} = 1$ such that E_n has two roots $\alpha, \alpha\theta$. We show that this is impossible. Note that n must be > 1.
Let ζ be a primitive $(n+1)$-th root of unity. Then $\theta = \zeta^i$ for some $0 < i \leq n$. It is a well-known result of Schur that E_n is irreducible over $\mathbf{Q}$ and that the Galois group of its splitting field K is A_n or S_n according as whether 4 divides n or not.
Now, write $K = \mathbf{Q}(\alpha, \alpha\theta, \alpha_3, \cdots, \alpha_n)$ for the splitting field of E_n.
Firstly, let $n \not\equiv 0 \bmod 4$. We shall use the fact that the Galois group contains the n-cycle $\sigma = (\alpha, \alpha\zeta^i, \alpha_3, \cdots, \alpha_n)$.
Since $\sigma(\zeta^i)$ must be a power of ζ, it follows that each α_j with $3 \leq j \leq n$ must be $\alpha\zeta^k$ for some k. Thus, the set $\{\alpha, \alpha\zeta^i, \alpha_3, \cdots, \alpha_n\}$ of all the roots of E_n is the set of all $\alpha\zeta^r$ $(0 \leq r \leq n)$ with one $\alpha\zeta^m$ missing for some $1 \leq m \leq n$.
Now, the sum of the roots of E_n gives

$$-n = \sum_{r \neq m} \alpha\zeta^r = -\alpha\zeta^m.$$

Therefore, $\alpha = n\zeta^{-m}$.

The product of all roots of E_n gives

$$(-1)^n n! = \alpha^n \zeta^{n(n+1)/2-m} = n^n \zeta^{n(n+1)/2-m-mn} = n^n \zeta^{n(n+1)/2}.$$

Hence $1 = |\zeta^{n(n+1)/2}| = n!/n^n$, which is impossible for $n > 1$.
Now, let $4|n$. Then, the Galois group, which is A_n, contains each $(n-1)$-cycle of the form $(\alpha, \alpha\zeta^i, \alpha_{i_1}, \cdots, \alpha_{i_{n-3}})$ where $\alpha_{i_1}, \cdots, \alpha_{i_{n-3}}$ are any $n-3$ among $\alpha_3, \cdots, \alpha_n$. Therefore, each α_j with $3 \leq j \leq n$ is of the form $\alpha\zeta^k$ for some k and, the argument above goes through as it is. This proves the proposition.

The Bilu-Tichy theorem

For the proofs of theorems A and B, the main tool used is the following remarkable result due to Y.Bilu and R.Tichy :

Theorem 1 ([5]).
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 λ, μ are linear polynomials over $\mathbb{Q}$, ϕ is some polynomial over $\mathbb{Q}$, and $(f_1(x), g_1(x))$ is a standard pairover $\mathbb{Q}$ 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

$$(x^t, ax^r p(x)^t) \quad or \quad (ax^r p(x)^t, x^t)$$

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

A standard pair of the second kind is

$$(x^2, (ax^2+b)p(x)^2) \quad or \quad ((ax^2+b)p(x)^2, x^2).$$

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

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

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

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

In the course of our proof, we need some basic facts about Dickson polynomials. These are summarised in the following result due to Bilu :

Theorem 2 ([1])
(a) *The Dickson polynomial* $D_l(x,0)$ *has exactly one extremum* 0*; it is of type* (l).
(b) *If* $a \neq 0$ *and* $l \geq 3$ *then* $D_l(x,a)$ *has exactly the two extrema* $\pm 2a^{\frac{l}{2}}$.
If l *is odd, then both are of type* $(1,2,2\cdots,2)$.
If l *is even, then* $2a^{\frac{l}{2}}$ *is of type* $(1,1,2,\cdots,2)$ *and* $-2a^{\frac{l}{2}}$ *is of type* $(2,2,\cdots,2)$.

Finiteness for $E_n(x)=g(y)$

In this section, we prove that for any polynomial $f \in \mathbb{Q}[x]$ of degree ≥ 3 which satisfies the hypothesis of the lemma above, there is a finiteness theorem for the number of solutions of $f(x)=g(y)$ for any $g(y)\in\mathbb{Q}[y]$ of degree ≥ 3 apart from necessary exceptions.

Theorem A.
Let f,g *be polynomials of degrees* n,m *respectively, with rational coefficients. Suppose each extremum (with respect to* f*) has type* $(1,1,\cdots,1,2)$*. Then, for* $n,m\geq 3$*, the equation* $f(x)=g(y)$ *has only finitely many rational solutions* (x,y) *with a bounded denominator except in the following two cases :*
(i) $g(y)=f(h(y))$ *for some nonzero polynomial* $h(y)\in\mathbb{Q}(y)$*,*
(ii) $n=3,(m,3)=1$ *and* $f(x)=c_0+c_1D_3(\lambda(x),c^m)$*,* $g(y)=c_0+c_1D_m(\mu(y),c^3)$ *for linear polynomials* λ *and* μ *over* $\mathbb{Q}$ *and* $c_i\in\mathbb{Q}$ *with* $c_1,c\neq 0$.
In each exceptional case, there are infinitely many solutions.

Corollary.
Let $E_n(x)=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots+\frac{x^n}{n!}$ *with* $n\geq 3$ *and* $g\in\mathbb{Q}[x]$ *be of degree* $m\geq 3$*. Then, the equation* $E_n(x)=g(y)$ *has only finitely many rational solutions with a bounded denominator*

except in the following two cases :
(i) $g(y) = E_n(h(y))$ for some nonzero polynomial $h(y) \in \mathbb{Q}(y)$,
(ii) $n = 3, m$ is odd, and $g(x) = \frac{1}{3} + \frac{1}{6\lambda^3} D_m(\mu(x), a^3)$, where $-a \in (\mathbb{Q}^*)^2, \lambda^2 = -a^m$, and μ is a linear polynomial over $\mathbb{Q}$.
In these exceptional cases, there are infinitely many solutions.

Proof.
By the above proposition, E_n satisfies the hypothesis of theorem A. It is easy to check that the case (ii) of theorem A can occur only if

$$E_3(x) = \frac{1}{3} + \frac{1}{6\lambda_0^3} D_3(\lambda_0(1+x), a^m),$$

when $-a^m = \lambda_0^2$. This forces m to be odd and $-a$ to be a square in $\mathbb{Q}^*$.

Proof of Theorem A.
Assume that the equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator. Then by the Bilu-Tichy theorem (theorem 2), $f(x) = \phi(f_1(\lambda(x)))$ and $g(y) = \phi(g_1(\mu(y)))$ 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. As $f(x)$ is indecomposable, either deg $\phi(x) = n$ and deg $f_1(x) = 1$, or deg $\phi(x) = 1$ and deg $f_1(x) = n$.

First, let us suppose that deg $\phi = n$.
Clearly, then $\phi(x) = f(\delta(x))$ for some linear polynomial $\delta(x) = u + vx \in \mathbb{Q}[x]$. Then, $g(x) = f(h(x))$ where $h = \delta \circ g_1 \circ \mu$. This is the exceptional case (i) of the theorem.

Now, suppose deg $\phi = 1$.
In this case, we have deg $f_1 = n$ and deg $g_1 =$ deg $g = m$.
Let $\phi(x) = \phi_0 + \phi_1 x$ for some rational numbers μ and λ.

Case (i) Suppose the standard pair (f_1, g_1) is of the *first* kind.
Therefore, we have either $f_1(x) = x^t$ and $g_1(x) = ax^r p(x)^t$, or $f_1(x) = ax^r p(x)^t$ and $g_1(x) = x^t$. So $t \geq 3$ in either situation since $t = m$ or $t = n$. In the first situation, we have $f(x) - \phi_0 = \phi_1 \lambda(x)^t$ which contradicts the hypothesis on f. We consider the second situation now. Then,

$$f(x) - \phi_0 = \phi_1 a \lambda(x)^r p(\lambda(x))^t.$$

Once again, this implies $r \leq 2$. Further, since $t \geq 3$, degree of p must be zero. In other words, $n = r \leq 2$, a contradiction of our assumption that $n \geq 3$. Hence (f_1, g_1) can not be a standard pair of the *first* kind.

Case(ii) 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 with the pair switched. But this will imply that either $m = 2$ or $n = 2$ which contradicts our assumption that $m,\ n \geq 3$. Therefore (f_1, g_1) can not be of the second kind.

Case(iii) 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 with the pair switched.
We give the proof when $(m, n) = (4, 6)$ and a similar argument works when $(m, n) = (6, 4)$.
Let $(m, n) = (4, 6)$. Then,

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

This again contradicts the assumption on f. Hence (f_1, g_1) can not be a standard pair of the *fifth* kind.

Case (iv) Suppose the standard pair (f_1, g_1) is of the *third* kind.
Then $f_1(x) = (D_n(x, a^m)$ and $f(x) - \phi_0 = \phi_1 D_n(\delta(x), a^m)$ where $\delta(x)$ is a linear polynomial in $\mathbb{Q}[x]$. By assumption, we know that for any complex number λ, the polynomial $f(x) - \lambda$ can have at most one multiple root.
If $a = 0$, then $f(x) - \phi_0 = \phi_1 \delta(x)^n$, which is not possible as $n \geq 3$. Therefore, $a \neq 0$ and $f_1(x) = D_n(x, a^m)$. By Theorem 2, $D_n(x, a^m)$ has two extrema and, therefore, $f(x)$ also has two extrema.
If n is an odd integer then, by theorem 2, both extrema are of the type $(1, 2, 2, \cdots, 2)$, but every extremum of f has type $(1, 1, \cdots, 1, 2)$. Thus, we must have $n = 3$. When $n = 3$, we get the exceptional case (ii) of the theorem. Since the equation

$$D_3(x, a^m) = D_m(y, a^3)$$

has infinitely many rational solutions x, y with a bounded denominator for any $a \in \mathbb{Q}^*$, it follows that $f(x) = g(y)$ also does.
If n is even, then by theorem 2, there is an extremum of the type $(2, 2, 2, \cdots 2)$. But, since any extremum of f must have the type $(1, 1, \cdots, 1, 2)$, this case cannot occur. Therefore (f_1, g_1) can not be of the third kind.

Case (v) Suppose the standard pair (f_1, g_1) is of the *fourth* kind.
In this case $(f_1, g_1) = (a^{-n/2} D_n(x, a), b^{-m/2} D_m(x, a))$ where gcd $(m, n) = 2$.
As $a \neq 0$, and as n is even and > 3, $D_n(x, a)$ has an extremum of the type $(2, 2, \cdots, 2)$ which cannot happen for f. This means (f_1, g_1) cannot be of the fourth kind also. This completes the proof of theorem 1.

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

The main result of this section is :

Theorem B.
Let $g(y) \in \mathbb{Q}[y]$ have degree $n \geq 3$ and let $m \geq 3$. The equation $B_m(x) = g(y)$ has only finitely many rational solutions (x, y) with any bounded denominator apart from the following exceptions :

(i) $g(y) = B_m(h(y))$ *for some polynomial* h *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,* ϕ *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* $r^2\alpha^n = \frac{1}{12}$, δ *is a linear polynomial over* $\mathbb{Q}$ *and* $D_n(x, c)$ *is the Dickson polynomial*

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

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

The decomposition of Bernoulli polynomials has been investigated in [2] where they prove :

Theorem 3 ([2]).
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* ϕ *over* $\mathbb{Q}$.

Proof of theorem B:
Let us assume that $B_m(x) = g(y)$ has infinitely many rational solutions with a bounded denominator. Before proceeding further, we recall that

$$B_m(x) = \sum_{i=0}^{m} \binom{m}{i} B_{m-i} x^i$$

and that $B'_m(x) = mB_{m-1}(x)$. Further, it is known due to results of Brillhart [4] and Inkeri [7] 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 λ, μ 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 3, 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 $\phi = m$.
Suppose $B_m(x) = g(y)$ has infinitely many solutions. Then as above, there are linear polynomials $\lambda, \mu \in Q[x]$, 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 $\delta(x) = u + vx \in Q[x]$. 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 claim 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 classical 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 $\phi_0,\ \phi_1$.

That the standard pair (f_1, g_1) cannot be of the *second* kind follows exactly as it did for the corresponding case in theorem A.

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 $\sum_{i=0}^{m} \binom{m}{i} B_{m-i}(rx + s)^i = \phi_0 + \phi_1 \sum_{i=0}^{[\frac{m}{2}]} d_{m,i} x^{m-2i}$,
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 ϕ_1 above is simply replaced by $\alpha^{-m/2}\phi_1$. Note that $m = 3$ cannot occur here as m is even.

Suppose (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. Exactly as in the corresponding case in theorem A, on using the result of Brillhart [4] that $B_{odd}(x)$ has only simple roots, it follows that (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 $f_1(x) = ax^r p(x)^t$ and $g_1(x) = x^t$. Note that $t = \deg g \geq 3$.

Suppose m is even.
Then

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

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

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 followsthat 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 ≥ 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 λ 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 $\lambda(x) = c_0 + c_1 x$, 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

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

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 ([6], 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.

References

[1] Y. Bilu Quadratic Factors of $f(x) - g(y)$ Acta Arithmetica, 90 (1999), 341- 355.

[2] 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.

[3] 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.

[4] J. Brillhart. On the Euler and Bernoulli polynomials. J. Reine. Angew. Math. 234 (1969). 45 - 64.

[5] Y. Bilu and R.F. Tichy. The Diophantine Equation $f(x) = g(y)$. Acta Arithmetica XCV (2000), 261 - 288.

[6] Y.Hellegouarch. Invitation to mathematics of Fermat-Wiles. Translated from the 2nd (2001) edition by Leila Schneps. Academic Press, Inc., San Diego, CA 2002.

[7] K. Inkeri Real roots of Bernoulli Polynomials. Am. Univ. Turku. Ser A I, 37 (1959) 20pp

[8] M. Kulkarni and B. Sury. On the Diophantine equation $x(x+1)\cdots(x+m-1) = g(y)$. Indagationes Math. 14 (2003), 35-44.

[9] M. Kulkarni and B. Sury. Diophantine equations with Bernoulli polynomials. Acta Arithmetica, Vol. 116 (2005) 25-34.

[10] M. Kulkarni and B. Sury. A class of Diophantine equations involving Bernoulli polynomials. Indagationes Mathematicae, in press.

[11] Th.Stoll. Diophantine equations involving polynomial families. Ph.D.Thesis, TU Graz 2003.