Diophantine Equations
Editor: N. Saradha

Publisher: Narosa Publishing House, New Delhi, India

On the Diophantine Equation $1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} = g(y)$

Manisha Kulkarni and B. Sury*

To Professor T.N.Shorey on the occasion of his sixtieth birthday

1 Introduction

Questions on counting often involve finding integer solutions† of equations of the form $f(x) = g(y)$ for integral polynomials f, g. For instance, for fixed but distinct natural numbers m, n, a natural question is how often $\binom{x}{m} = \binom{y}{n}$ or, more generally, whether the Diophantine equation $a\binom{x}{m} + b\binom{y}{n} = c$ for some integers a, b, c with $ab \neq 0$, has only finitely many integer solutions. Stoll & Tichy proved more generally that if $a, b, c \in \mathbb{Q}$ and $ab \neq 0$, then for $m > n \geq 3$, the above equation has only finitely many integral solutions x, y. Independently, Rakaczki established a more precise finiteness result on this binomial equation and extended this result to more general equations (see Acta Arith. 110(2003), 339-360 and Periodica Math. Hungar. 49(2004), 119-132). Another natural example comes from counting lattice points in generalized octahedra. The number of integral points on the n-dimensional octahedron $|x_1| + |x_2| + \cdots + |x_n| \leq r$ is given by the expression $p_n(r) = \sum_{i=0}^{n} 2^i \binom{n}{i}\binom{r}{i}$ and the question of whether two octahedra of different dimensions m, n can contain the same number of integral points becomes equivalent to the solvability of $p_m(x) = p_n(y)$ in integers x, y. This question was treated by Bilu, Stoll & Tichy who showed that when $m > n \geq 2$, the above equation has only finitely many integral solutions. One more result of this kind proved by Stoll & Tichy is that for the sequences of classical orthogonal polynomials $p_m(x)$ like the Laguerre, Legendre and Hermite polynomials, an equation of the form $ap_m(x) + bp_n(y) = c$ with $a, b, c \in \mathbb{Q}$ and $ab \neq 0$ and $m > n \geq 4$ has only finitely many solutions in integers x, y. The above results and many others appearing in the last 5 or 6 years have been made possible by a beautiful

*Corresponding author
†Mathematics Subject Classification 11D45,11B68,14H25

theorem of Bilu & Tichy recalled below. To motivate it, let us start more generally, for a polynomial $F(x,y) \in \mathbb{Z}[x,y]$, with the basic question of deciding if $F(x,y) = 0$ has only finitely many solutions with x, y in $\mathbb{Z}$. When $F(x,y)$ is absolutely irreducible, then a celebrated 1929 theorem due to Siegel shows the finiteness of the number of integer solutions except when the (projective completion of the) curve defined by $F(x,y) = 0$ has genus 0 and at most 2 points at infinity. This theorem generalizes also to S-integers in algebraic number fields but is, unfortunately, ineffective. To determine finiteness or otherwise of the integral solutions of any given $F(x,y) = 0$ using Siegel's theorem, one splits $F(x,y)$ into irreducible factors in $\mathbb{Q}[x,y]$, and for each factor which is irreducible over $\bar{\mathbb{Q}}$ one finds the genus and the number of points at infinity. Then, for each of those factors which have genus 0 and ≤ 2 points at infinity, one can try to determine whether the number of integral solutions is finite or not. The other most successful way of tackling the problem of finiteness is the usage of Baker's 1960's method of linear forms in logarithms. In several of the classical problems, $F(x,y)$ has the special form $f(x) - g(y)$. In this case, there are nice results answering the sub-problems which rise while attempting to apply Siegel's theorem. For instance, Ehrenfeucht (1958) proved:

If $(\deg f,\ \deg g) = 1$*, then* $f(X) - g(Y)$ *is irreducible.*

There are some cases when one can observe that $f(X) - g(Y)$ is reducible. For instance, note that if f, g, F are arbitrary polynomials with $\deg F > 0$, then $f_1(X) - g_1(Y)$ is a factor of $f(X) - g(Y)$ where $f(X) = F(f_1(X))$ and $g(Y) = F(g_1(Y))$. Over $\mathbb{C}$, $T_n(X) + T_n(Y)$ is a product of quadratic factors (and a linear factor if n is odd) where $T_n(X)$ is the Chebychev polynomial. In general, Fried & MacRae (1969) proved:

$f(X) - g(Y)$ has a factor of the form $f_1(X) - g_1(Y)$ if, and only if, there is $F(T) \in \mathbb{C}[T]$ such that

$$f(T) = F(f_1(T))\ ,\ g(T) = F(g_1(T)).$$

Fried had made a deep study of the factors of $f(X) - g(Y)$. He proved in 1973 that given f, g there are f_1, f_2, g_1, g_2 in $\mathbb{Z}[X]$ such that:

(i) $f(X) = f_1(f_2(X)), g(X) = g_1(g_2(X))$,
(ii) Splitting fields of $f_1(X) - t$ and of $g_1(X) - t$ over $\mathbb{Q}(t)$ (where t is a new indeterminate) are the same, and
(iii) the irreducible factors of $f(X) - g(Y)$ are in bijection with those of $f_1(X) - g_1(Y)$.

Davenport, Fried, Lewis, Runge, Schinzel and Siegel are some people who have made fundamental contributions to the question of irreducibility of $f(X) - g(Y)$. In 2000, Y.Bilu & R.Tichy [5] obtained for the equation

$f(x) = g(y)$ with $f \in \mathbb{Q}[x], g \in \mathbb{Q}[y]$, a remarkable theorem which makes Siegel's theorem much more explicit (although still ineffective). 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 which $f(x) = g(y)$ has infinitely many solutions can be determined from standard pairs. The theorem (recalled as Theorem 3.1 below) has already been used in the last 5 or 6 years by several authors to study the finiteness question for equations of the form $f(x) = g(y)$ where f and/or g are from an infinite sequence of polynomials. 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], [6], [9], [10], [11], [12], [13] for some of these results. In all the examples referred to, we have an equation of the form $f(x) = g(y)$ where f, g are from an explicit infinite sequence of polynomials. In fact, if $\{f_m\}$ and $\{g_n\}$ are infinite sequences of polynomials with integer or rational coefficients, one considers for each fixed m and n, the equation $f_m(x) = g_n(y)$ for solutions in integers. Typically, the results proved are of the form that the number of solutions is finite unless there is some restriction on m and n. We note that due to the ineffective nature of the proofs here, if we do not fix m, n and ask for a finiteness result, nothing is known. We mention for instance the famous (and unproved as yet) conjecture Erdős made in 1975:

For every $\lambda \in \mathbb{Q}$, *the number of integral solutions* (x, y, m, n) *of*

$$x(x+1)\cdots(x+m-1) = \lambda y(y+1)\cdots(y+n-1)$$

with $y \geq x + m$, $min(m, n) \geq 3, m > 1, n > 1$ *is finite.*

In this paper, we prove finiteness of the number of rational solutions with bounded denominators (and point out all the exceptions) for certain equations of the form $f(x) = g(y)$ which includes the polynomials

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

for any $n \geq 3$, and the Bernoulli polynomials $B_n(x)$, where g is an arbitrary polynomial of degree $m \geq 3$ in $\mathbb{Q}[y]$. The result for the Bernoulli polynomials was obtained by us in August 2004 and subsequently we learnt that C.Rakaczki [12] has obtained it independently. Before stating the main results, we recall three 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 multiplicities of the distinct roots of $P(x) - c$. A polynomial over $\mathbb{C}$ is said to be *indecomposable* if it is not of the form $f_1 \circ f_2$ for complex polynomials f_1, f_2 of degrees ≥ 2.

We also need the definition of Dickson polynomial $D_m(t, c)$ of degree m given by

$$D_m(t,c) = \sum_{i=0}^{[\frac{m}{2}]} \frac{m}{m-i} \left(\begin{array}{c} m-i \\ i \end{array} \right) (-c)^i t^{m-2i}.$$

The main results are:

Theorem 1.1 *Let* $E_n(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$ *with* $n \geq 3$. *Then, we have:*

(a) E_n *is indecomposable for each* n,

(b) *for* $g \in \mathbb{Q}[y]$ *of degree* $m \geq 3$, *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* $g(x) = \frac{1}{3} + \frac{1}{6} D_m(\mu(x), -1)$, *where* μ *is a linear polynomial over* $\mathbb{Q}$.

In each exceptional case, there are infinitely many solutions.

As a matter of fact, the proof works more generally and we have:

Theorem 1.2 *Let* f, g *be polynomials of degrees* n, m *respectively, with rational coefficients. Suppose each extremum (with respect to* f*) has type* $(1, 1, \ldots, 1, 2)$. *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) $g(x) = f(h(x))$ *for some nonzero polynomial* $h(x) \in \mathbb{Q}(x)$,

(ii) $n = 3, m \geq 3$ *and*

$$f(x) = c_0 + c_1 D_3(\lambda(x), c^m), \quad g(x) = c_0 + c_1 D_m(\mu(x), c^3)$$

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.

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

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. Earlier, we had studied in [10], [11] some equations involving Bernoulli polynomials before obtaining the general result for $B_m(x) = g(y)$ in 2004 (stated here as the next theorem). As mentioned above, Rakaczki has obtained it independently. *Rakaczki [12] misses the case $m = 3$ in the statement below as he uses an earlier result of ours [9] where this lapse first occurs. We regret this error. Indeed, the equation $x(x + 1)(x + 2) = g(y)$ does have infinitely many rational solutions with a bounded denominator for g of any degree $n \geq 3$ when $g(x) = \frac{1}{3^{3(n+1)/2}} D_n(\mu(x), 3^3)$ and $\mu(x)$ is a linear polynomial over $\mathbb{Q}$. This follows from the fact that*

$$(x - 1)x(x + 1) = D_3(x, 1/3) = \frac{1}{b^3} D_3(bx, (3d^2)^m)$$

where $b = 3^{(m+1)/2}d^m$.

Since Rakaczki's proof is already published, we confine ourselves with stating the result in our form (which is somewhat different from his), outlining one part of the proof and pointing out the exceptional cases explicitly.

Theorem 1.3 *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) *$g(y) = B_m(h(y))$ where 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) *$m = 3, n \geq 3$ odd and $g(x) = \frac{1}{8(3^{3(n+1)/2})} D_n(\delta(x), 3^3)$.*

(iv) *$m = 4, n \geq 3$ odd and $g(x) = \frac{1}{2^{2(n+3)}} D_n(\delta(x), 2^4) - \frac{1}{480}$.*

(v) *$m = 4, n \equiv 2$ mod 4 and $g(x) = \frac{-\beta^{-n/2}}{64} D_n(\delta(x), \beta) - \frac{1}{480}$.*

Here δ is a linear polynomial over $\mathbb{Q}$ and $\beta \in \mathbb{Q}^*$. Furthermore, in each of the exceptional cases, there are infinitely many solutions with a bounded denominator.

2 Indecomposability of E_n

We start with a simple observation which gives a sufficient condition for indecomposability of a complex polynomial. This has already been observed by others in some form or the other (for example, see Stoll [13, Lemma 3.3], or [6, Lemma 3]).

Observation 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 $\mathbb{C}$.

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 $(1, 1, \ldots, 1, 2)$.

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 concludes the proof.

□

Remark 2.1 The proof shows the following refined version holds 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 $(1, 1, \ldots, 1, 2)$, then f is indecomposable over $\mathbb{Q}$.

In order to prove indecomposability of E_n's using the above lemma, the key result needed is the following:

Proposition 2.2 *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 $(1, 1, \ldots, 1, 2)$. 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 $\mathbb{Q}$ and that the Galois group of its splitting field K is A_n or S_n according as to whether 4 divides n or not. Now, write $K = \mathbb{Q}(\alpha, \alpha\theta, \alpha_3, \ldots, \alpha_n)$ 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 $\sigma = (\alpha, \alpha\zeta^i, \alpha_3, \ldots, \alpha_n)$. 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 $\{\alpha, \alpha\zeta^i, \alpha_3, \ldots, \alpha_n\}$ 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 $(\alpha, \alpha\zeta^i, \alpha_{i_1}, \ldots, \alpha_{i_{n-3}})$ where $\alpha_{i_1}, \ldots, \alpha_{i_{n-3}}$ are any $n-3$ among $\alpha_3, \ldots, \alpha_n$. 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.

□

3 The Bilu-Tichy Theorem

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

Theorem 3.1 ([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* $f = \phi \circ f_1 \circ \lambda$ *and* $g = \phi \circ g_1 \circ \mu$ *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 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.

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 $(k, t) = 1$.
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

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

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 3.2 ([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* $(1, 2, 2 \ldots, 2)$*.*

If l *is even, then* $2a^{\frac{l}{2}}$ *is of type* $(1, 1, 2, \ldots, 2)$ *and* $-2a^{\frac{l}{2}}$ *is of type* $(2, 2, \ldots, 2)$*.*

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

Deduction of Theorem 1.1 from Theorem 1.2

By Proposition 2.2, E_n satisfies the hypothesis of Theorem 1.2. As

$$E_3(x) = \frac{1}{3} + \frac{1}{6}D_3(x+1, -1),$$

it is easy to check that the case (ii) of Theorem 1.2 gives the exceptional case (ii) of Theorem 1.1.

Proof of Theorem 1.2 Assume that the equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator. Then by the Bilu-Tichy Theorem 3.1, $f(x) = \phi(f_1(\lambda(x)))$ 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 a bounded denominator. As $f(x)$ is indecomposable, either $\deg \phi(x) = n$ and $\deg f_1(x) = 1$, or $\deg \phi(x) = 1$ and $\deg f_1(x) = n$.

Firstly, 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. Then, 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) cannot be of the second kind.

Case (iii) If (f_1, g_1) is of the *fifth* kind, then $(n, m) = (6, 4)$ 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) cannot 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 3.2, $D_n(x, a^m)$ has two extrema and, therefore, $f(x)$ also has two extrema. If n is an odd integer then, by Theorem 3.2, both extrema are of the type $(1, 2, 2, \ldots, 2)$, but every extremum of f has type $(1, 1, \ldots, 1, 2)$. 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 3.2, there is an extremum of the type $(2, 2, \ldots 2)$. But, since any extremum of f must have the type $(1, 1, \ldots, 1, 2)$, 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. Then $(f_1, g_1) = (a^{-n/2}D_n(x, a), -b^{-m/2}D_m(x, a))$ 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 $(2, 2, \ldots, 2)$ which cannot happen for f. This means (f_1, g_1) cannot be of the fourth kind also. This completes the proof of Theorem 1.2.

□

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

As mentioned in the introduction, Theorem 1.3 has been independently proved by C. Rakaczki [12]. The decomposition of Bernoulli polynomials has been investigated in [2] where they prove:

Theorem 5.1 ([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 $\mathbb{Q}$.*

Outline of Proof of Theorem 1.3

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 [8] 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 3.1 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 5.1, 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) $\deg \phi = 1$.

The cases (a) and (b) easily lead to cases (i) and (ii), respectively of the Theorem. In case (c), using the Bilu-Tichy theorem, the standard pairs of types 2, 3, 4 and 5 are easily dealt with. Among them, the exceptional cases (iii), (iv) and (v) arise, and they correspond to standard pairs of the 3rd, 3rd and 4th kinds, respectively. The final case of standard pairs of the first kind detailed below requires some additional results and our proof is quite different from Rakaczki's.

Suppose there are linear polynomials $\lambda(x),\ \mu(x) \in Q[x]$, and a standard pair (f_1, g_1) of the first kind such that $B_m(x) = \phi \circ f_1 \circ \lambda(x)$, $g(y) = \phi \circ g_1 \circ \mu(y)$ and $\phi(x) = \phi_0 + \phi_1 x$ for some rational numbers $\phi_0,\ \phi_1$ with $\phi_1 \neq 0$. 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 $f_1(x)$ cannot 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

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

$\deg\, p > 0$ as we have already seen that $B_m(x) = \phi_0 + \phi_2 x^m$ is impossible for any rational number ϕ_2. Now the derivative $B'_m(x) = mB_{m-1}(x)$ 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, $B_{m-1}(x)$ has only simple roots by a result of Brillhart [4]. Therefore $t = 2$; but then $\deg\, g = 2$, which is a contradiction. Therefore when m is even $f_1(x)$ cannot 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, $B_m(ux+v) = \phi_0 + \phi_1 a x^r p(x)^t$ 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 [8] quoted in the beginning of the proof. Therefore, $B_m(rx+s) = \phi_0 + \phi_1 a x^r p(x)^3$ and $m = 3d + r$. Now as $r < t = 3$, we get $r = 1$ or 2. If $r = 2$, then $B_m(ux+v) = \phi_0 + \phi_1 a x^2 p(x)^3$. 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 [8] 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 an equality

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

of polynomials 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

$$t^3 + 1 = 2s^3$$

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 ([7], P.37), that the above equation has no solution other than $xyz = 0$ or $x = y = z$. This completes the proof of the theorem.

□

Acknowledgements We thank Professor K.Györy for showing interest in this work and for informing us about Rakaczki's paper. We are also thankful to Professor Rakaczki for some correspondence. The first author is indebted to the Indian Statistical Institute, Bangalore for all facilities and help provided during this research. Thanks are due to the referee for his/her remarks and for pointing out some references which we were unaware of. Finally, both of us would like to express our gratitude to the Tata Institute for having invited us to the conference; we found it a very stimulating experience.

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] A. Dujella and R.F. Tichy, *Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. **52** (2001), 161–169.

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

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

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

[10] M. Kulkarni and B. Sury, *Diophantine equations with Bernoulli polynomials*, Acta Arithmetica **116** (2005), 25–34.

[11] M. Kulkarni and B. Sury, *A class of Diophantine equations involving Bernoulli polynomials*, Indagationes Mathematicae, **16** (2005), 51–65.

[12] C. Rakaczki, *On the Diophantine equation $S_m(x) = g(y)$*, Publ. Math. Debrecen **65** (2004), 439–460.

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

Manisha Kulkarni, Poornaprajna Institute of Scientific Research, Davanhalli, Bangalore, India.

E-mail: manisha@isibang.ac.in

B. Sury, Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore - 560 059, India.

E-mail: sury@isibang.ac.in