Compositio Mathematica **131:** 173–188, 2002.

Diophantine Equations and Bernoulli Polynomials

YU. F. BILU[1], B. BRINDZA[2], P. KIRSCHENHOFER[3], Á. PINTÉR[2] and R. F. TICHY[4]

[1]*A2X, Université Bordeaux 1, 351 cours de la Libération, 33405 Talence cedex, France. e-mail: yuri@math.u-bordeaux.fr*

[2]*Department of Mathematics, PO Box 12, H-4010, Debrecen, University of Debrecen, Hungary. e-mail: apinter@math.klte.hu*

[3]*Montanuniversität Leoben, Franz Josef-Str. 18, 8700 Leoben, Austria. e-mail: kirsch@unileoben.ac.at*

[4]*Institut für Mathematik (A), Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria. e-mail: tichy@weyl.math.tu-graz.ac.at*

with an appendix by

A. SCHINZEL

Mathematical Institute PAN, PO Box 137, 00-950 Warszawa, Poland. e-mail: schinzel@plearn.edu.pl

(Received: 1 March 2000; accepted in final form: 17 April 2001)

Abstract. Given $m, n \geqslant 2$, we prove that, for sufficiently large y, the sum $1^n + \cdots + y^n$ is not a product of m consecutive integers. We also prove that for $m \neq n$ we have $1^m + \cdots + x^m \neq 1^n + \cdots + y^n$, provided x, y are sufficiently large. Among other auxiliary facts, we show that Bernoulli polynomials of odd index are indecomposable, and those of even index are 'almost' indecomposable, a result of independent interest.

Mathematics Subject Classifications (2000). Primary: 11D41; Secondary: 11B68, 11B65, 11J86.

Key words. Diophantine equations, Bernoulli polynomials, power sums, products of consecutive integers, indecomposable polynomials.

1. Introduction

In this paper, we study the Diophantine equations $R_m(x) = S_n(y)$ and $S_m(x) = S_n(y)$, where

$$R_m(x) = x(x+1)\cdots(x+m-1), \qquad S_m(x) = 1^m + 2^m + \cdots + (x-1)^m.$$

Various Diophantine equations involving the polynomials $R_m(x)$ and $S_m(x)$ have been extensively investigated. Mention should be made, for instance, of the celebrated theorem of Erdős and Selfridge [13]: for $m, n \geqslant 2$, the equation $y^n = R_m(x)$ has no solutions in positive integers x, y (that is, a product of several

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

consecutive integers is never a perfect power). An incomplete list of the most recent related works is [3, 8–10, 19, 21, 24], where further references will be found.

In this paper we prove the following two theorems.

THEOREM 1.1. *For* $m \geqslant 2$, $n \geqslant 1$ *and* $(m, n) \neq (2, 1)$, *the equation* $R_m(x) = S_n(y)$ *has, at most, finitely many solutions in rational integers* x, y.

THEOREM 1.2. *For* $n > m \geqslant 1$, *the equation* $S_m(x) = S_n(y)$ *has, at most, finitely many solutions in rational integers* x, y.

Some particular cases of Theorem 1.2 are established in [9]. We recall also that Beukers *et al.* [3] completely solved the finiteness problem for the equation $R_m(x) = R_n(y)$, even in a more general setting.

We deduce Theorems 1.1 and 1.2 from the general finiteness criterion for the Diophantine equation $f(x) = g(y)$, recently established in [5] (see Theorem 5.1 below). Since the proof of Theorem 5.1 is based on the noneffective theorem of Siegel, Theorems 1.1 and 1.2 are noneffective. In Section 3 we show, using Baker's method, that Theorem 1.1 can be made effective when $n \in \{1, 3\}$ or $m \in \{2, 4\}$. In [16], the equation $R_m(x) = S_n(y)$ was completely solved in the special cases $(m, n) = (2, 2), (2, 5), (4, 2), (4, 5)$.

One of the purposes of this paper is to illustrate how the general criterion from [5] applies to a concrete equation (see [4, 12] for different examples of this kind).

It is interesting to compare our method with those of [8–10, 13, 19, 21]. Our method is much less sensitive to the specific form of the equation. For instance, it extends, with some modifications, to the equations*

$$AR_m(x) + BS_n(y) = C \quad \text{and} \quad AS_m(x) + BS_n(y) = C,$$

where A, B and C are arbitrary integers with $AB \neq 0$. Moreover, a similar argument must work for any equation of the form $F_m(x) = G_n(y)$, where $\{F_m\}$ and $\{G_n\}$ are infinite families of polynomials depending on the parameters m and n in some 'good' way. See [4, 12] for examples.

On the other hand, our method yields only noneffective results and requires m and n to be fixed, while the results obtained by the more elementary methods are usually effective and sometimes allow variable m and/or n.

Besides the criterion from [5], the proofs of Theorems 1.1 and 1.2 require some other auxiliary facts. In particular, we completely characterize in Theorem 4.1 the decompositions of Bernoulli polynomials $B_n(x)$ (that is, all representations of $B_n(x)$ as $G_1(G_2(x))$, where G_1 and G_2 are polynomials). This result seems to be of independent interest.

*At least for $m \geqslant 3$; for $m = 2$ one would have to overcome some difficulties in generalizing Lemma 2.2.

PLAN OF THE PAPER

In Section 2 we collect facts about Bernoulli polynomials to be used in the text. In Section 3 we show that some special cases of Theorems 1.1 and 1.2 allow effective treatment. In Section 4 we investigate the decomposition of Bernoulli polynomials. In Section 5 we recall the finiteness criterion from [5] and prove Theorems 1.1 and 1.2. The final Section 6, written by A. Schinzel, describes an alternative approach to the decomposition of Bernoulli-type polynomials.

2. Bernoulli Polynomials

In this section we summarize some properties of the polynomials $S_n(x)$ and the closely related Bernoulli polynomials. We denote by $B_n(x)$ the nth Bernoulli polynomial, defined by the generating series $te^{tx}/(e^t - 1) = \sum_{n=0}^{\infty} B_n(x)t^n/n!$, and by $B_n = B_n(0)$ the nth Bernoulli number.

The following properties of Bernoulli numbers and polynomials will be often used in the text, sometimes without special reference.

$$B_n(x) = \sum_{i=0}^{n} \binom{n}{i} B_i x^{n-i} = x^n - \frac{n}{2}x^{n-1} + \frac{n(n-1)}{12}x^{n-2} + \cdots; \tag{1}$$

$$B'_{n+1}(x) = (n+1)B_n(x); \tag{2}$$

$$S_n(x) = (B_{n+1}(x) - B_{n+1})/(n+1); \tag{3}$$

$$B_n(x) = (-1)^n B_n(1-x); \tag{4}$$

$$f(x+1) - f(x) = nx^{n-1} \Longleftrightarrow f(x) = B_n(x) + \text{const}; \tag{5}$$

$$B_3 = B_5 = B_7 = \ldots = 0. \tag{6}$$

Recall also the von Staudt theorem

$$\Lambda_{2n} = \prod_{(p-1)|2n, p \text{ prime}} p, \tag{7}$$

where Λ_n is the denominator of B_n. In particular, Λ_n is a square-free integer, divisible by 6.

For the proofs of (1)–(7) see, for instance, [18, Chapters 1 and 2]. We conclude this section by two lemmas to be used in the sequel.

LEMMA 2.1. *Let m, r be integers with $m > 1$. Then the (complex) roots of the polynomial $P(x) := B_{2m}(x) - B_{2m} + r/2$ are of multiplicity at most 2. Also, $P(x)$ has at least 4 simple roots, unless $r = 0$ and $m \in \{2, 3\}$.*

Proof. Brillhart [6, Corollary of Theorem 16] proved that the polynomial $B_{2m-1}(x)$ has only simple roots. (See [15, Section 3] for a more general result.) Since $P'(x) = 2mB_{2m-1}(x)$, the polynomial $P(x)$ may have roots of multiplicity at most 2. This proves the first assertion.

Now we shall prove that $P(x)$ has at least 4 simple roots. When r is even this is a particular case of Theorem 2 of Győry, Tijdeman and Voorhoeve [15]. Hence we may assume that r is odd. We follow the argument of [15] with some changes.

Let δ be the denominator of $P(x)$, that is, the smallest positive integer such that $\delta P(x) \in \mathbb{Z}[x]$. Since r is odd, δ must be even; write $\delta = 2d$. The von Staudt theorem (7) implies that d is an odd square-free integer.

By the Gauss lemma, $2dP(x) = Q(x)T(x)^2$, where $Q(x), T(x) \in \mathbb{Z}[x]$ are primitive polynomials* and the roots of $Q(x)$ are exactly the simple roots of $P(x)$. Since the leading coefficient of $2dP(x)$ is $2d$, which is a square-free integer, the leading coefficient of $T(x)$ must be ± 1, and the leading coefficient of $Q(x)$ is $2d$.

We have to show that $\deg Q(x) \geqslant 4$. Thus, assume that $\deg Q(x) < 4$. If $\deg Q(x) = 0$ then $Q(x) = 2d$, which is impossible because $Q(x)$ is primitive. The only remaining possibility is $\deg Q(x) = 2$. Since $P(x) = P(1-x)$, we have $Q(x) = Q(1-x)$ as well, which implies that $Q(x) = 2dx^2 - 2dx + c$, where $c \in \mathbb{Z}$. We have $(c, 2d) = 1$ because $Q(x)$ is primitive. We also have $T(x) = T(1-x)$, which implies that $m - 1 = \deg T(x)$ is even. Hence, m is odd.

Since the polynomial $T(x)^2$ is monic, we have

$$2dP(x) = (2dx^2 - 2dx + c)(x^{2m-2} + \ldots) \equiv cx^{2m-2} + \cdots \pmod{2d},$$

where '...' denotes terms of lower degree. Since the coefficient of x^{2m-2} in $2dP(x)$ is $dm(2m-1)/3$, we have $c \equiv dm(2m-1)/3 \pmod{2d}$. Since $(c, 2d) = 1$, this is possible only when either $d = 3$ and $m(2m-1)$ is not divisible by 3, or $d = 1$ and $m(2m-1)$ is divisible by 3.

Assume that $d = 3$ and $m(2m-1)$ is not divisible by 3. We have $6P(0) = 3r$. Also, using (5), we obtain

$$6P(-1) = 6P(0) + 12m = 3r + 12m.$$

On the other hand,

$$6P(0) = cT(0)^2 \quad \text{and} \quad 6P(-1) = (12 + c)T(-1)^2.$$

Since $(c, 2d) = (c, 6) = 1$, the number c is not divisible by 3. It follows that both the integers $3r$ and $3r + 12m$ must be divisible by 9. Hence, m is divisible by 3, a contradiction.

*A polynomial with integer coefficients is *primitive* if the greatest common divisor of its coefficients is 1.

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

Thus, $d = 1$ and $m(2m-1)/3 \in \mathbb{Z}$. By (6), we have

$$2P(x) = 2x^{2m} - 2mx^{2m-1} + \frac{m(2m-1)}{3}x^{2m-2} + \sum_{k=0}^{m-2} a_k x^{2k} \tag{8}$$

with $a_1, \ldots, a_{m-2} \in \mathbb{Z}$. Assume that $|c| > 1$. Since $(c, 2d) = (c, 2) = 1$, the number c has an odd prime divisor p. Denote by $a \mapsto \bar{a}$ the reduction $\bmod\, p$. Then

$$\overline{2P}(x) = \overline{Q}(x)\overline{T}(x)^2 = \bar{2}x(x - \bar{1})\overline{T}(x)^2.$$

It follows that $\bar{0}$ is a root of $\overline{2P}(x)$ of odd multiplicity. However, (8) implies that this multiplicity cannot be any of $1, 3, \ldots, 2m-3$. We conclude that $\bar{0}$ is a root of $\overline{2P}(x)$ of multiplicity $2m-1$, which means that $\overline{T}(x)^2 = x^{2m-2}$ and $\overline{2P}(x) = \bar{2}x^{2m} - \bar{2}x^{2m-1}$. Comparing this with (8), we conclude that $2m \equiv 2 (\bmod\, p)$ and $m(2m-1)/3 \equiv 0 (\bmod\, p)$, which is impossible. This shows that $c = \pm 1$.

Assume that $c = 1$. Then $Q(x) = 2x^2 - 2x + 1$, which means that $P(x)$ vanishes at $\alpha = (1+i)/2$. Notice that α^{2k} is real (respectively, pure imaginary) when k is even (respectively, odd). Since m is odd,

$$\begin{aligned} 0 &= 3 \cdot 2^{m-1} \mathrm{Re} P(\alpha) \\ &= -3m(-1)^{(m-1)/2} + m(2m-1)(-1)^{(m-1)/2} + \\ &\quad + 12 \sum_{k=0}^{(m-3)/2} a_{2k} 2^{m-3-2k}(-1)^k \\ &\equiv 2m^2 \equiv 2 \pmod 4, \end{aligned}$$

a contradiction.

We are left with $c = -1$, in which case $Q(x) = 2x^2 - 2x - 1$ and $P(x)$ vanishes at $\beta = (1+\sqrt{3})/2$. If $m = 3$ then $r/2 = B_6 - B_6(\beta) = 0$, which is impossible, because r is odd. Finally, for $m \geqslant 5$ the polynomial $P(x) = B_{2m}(x) - B_{2m}(\beta)$ has at least 4 roots of odd multiplicity [15, p. 238]. Since the multiplicities do not exceed 2, these roots are simple. Lemma 2.1 is proved.

LEMMA 2.2. *For $n \geqslant 2$, the polynomial $S_n(x) + 1/4$ has at least 3 simple roots.*

Proof. For even n this is proved by Kano [17, Section 4]. Now let n be odd and write $n + 1 = 2m$. Then the polynomial $S_{n+1}(x) + 1/4 = (B_{2m}(x) - B_{2m} + m/2)/(n+1)$ has at least 4 simple roots by Lemma 2.1.

3. Effective Results for Small *m* or *n*

In this section we show that, when either $n \in \{1, 3\}$ or $m \in \{2, 4\}$, Theorem 1.1 can be proved effectively; that is, one can write down an explicit upper bound for the solutions (though we do not display an actual expression for such a bound). As one may expect, we use Baker's method.

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

THEOREM 3.1. *When* $m \geqslant 2$, *all solutions of the equation* $R_m(x) = S_3(y)$ *in* $x, y \in \mathbb{Z}$ *satisfy* $\max\{|x|, |y|\} \leqslant c_1$, *where* c_1 *is an effectively computable constant depending only on m. When* $m \geqslant 3$, *the same is true for the integer solutions of the equation* $R_m(x) = S_1(y)$.

THEOREM 3.2. *For* $m \in \{2, 4\}$ *and* $n \geqslant 2$, *all solutions of the equation* $R_m(x) = S_n(y)$ *in* $x, y \in \mathbb{Z}$ *satisfy* $\max\{|x|, |y|\} < c_2$, *where* c_2 *is an effectively computable constant depending only on n.*

The proofs of these theorems rely on the classical result of A. Baker [1].

LEMMA 3.3 ([1]). *Let* $g(x) \in \mathbb{Q}[x]$ *be a polynomial having at least three simple roots. Then all solutions of the equation* $g(x) = y^2$ *in* $x, y \in \mathbb{Z}$ *satisfy* $\max\{|x|, |y|\} \leqslant c$, *where c is an effectively computable constant depending only on the coefficients of g.* □

Proof of Theorem 3.1. We start with the equation $R_m(x) = S_3(y)$. Since $S_3(y) = (y(y-1)/2)^2$, it is sufficient to show that the solutions $x, z \in \mathbb{Z}$ of the equation $z^2 = R_m(x)$ are effectively bounded in terms of m. If $m \geqslant 3$ then the polynomial $R_m(x)$ has at least three simple roots, and the required assertion follows from Lemma 3.3. In the case $m = 2$ we obtain the equation $z^2 = x(x+1)$, which has only two integer solutions $(0, 0)$ and $(-1, 0)$. This can be easily seen, e.g., by rewriting it as $(2x + 2z + 1)(2x - 2z + 1) = 1$.

The equation $R_m(x) = S_1(y)$ is a particular case of the equation effectively studied by Yuan [24]. On can also argue directly as follows. Rewrite the equation as $(2y-1)^2 = 8R_m(x) + 1$. By Lemma 4 from [9], the polynomial $8R_m(x) + 1$ has only simple roots. Since $m \geqslant 3$, we may apply Lemma 3.3.

Proof of Theorem 3.2. Rewriting the equation $R_2(x) = S_n(y)$ as $(2x-1)^2 = 4S_n(y) + 1$, we see that its solutions are effectively bounded by Lemmas 2.2 and 2.3. An effective finiteness theorem for the equation $S_n(y) = R_4(x) = (x^2 + 3x + 1)^2 - 1$ was obtained by Brindza [7]. See [15, 23] for more general results.

We also recall the known effective results for the equations $S_1(x) = S_n(y)$ and $S_3(x) = S_n(y)$.

THEOREM 3.4. *For* $m \in \{1, 3\}$ *and* $n \neq m$, *the solutions* $x, y \in \mathbb{Z}$ *of the equation* $S_m(x) = S_n(y)$ *satisfy* $\max\{|x|, |y|\} < c_3$, *where* c_3 *is an effectively computable constant depending only on n.*

For $m = 1$ this is Theorem 1 of [9]. For $m = 3$ and $n \neq 1, 3, 5$ this is a consequence of the much more general effective theorem of Győry *et al.* [15, Theorem 1]. We are left with the equation $S_3(x) = S_5(y)$, that is $3(x^2 - x)^2 = (2y^2 - 2y - 1)(y^2 - y)^2$. Putting $y^2 - y = z$, we obtain the equation $3(x^2 - x)^2 = 2z^3 - z^2$, which defines a curve of genus 1. Hence, its solutions are effectively bounded by the famous result of Baker and Coates [2].

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

4. Decomposition of Bernoulli Polynomials

A *decomposition* of a polynomial $F(x) \in \mathbb{C}[x]$ is an equality of the form $F(x) = G_1(G_2(x))$, where $G_1(x), G_2(x) \in \mathbb{C}[x]$; the decomposition is *nontrivial* if $\deg G_1, \deg G_2 > 1$. Two decompositions $F(x) = G_1(G_2(x))$ and $F(x) = H_1(H_2(x))$ are called *equivalent* if there exists a linear polynomial $\ell(x) \in \mathbb{C}[x]$ such that $G_1(x) = H_1(\ell(x))$ and $H_2(x) = \ell(G_2(x))$. The polynomial $F(x)$ is called *decomposable* if it has at least one nontrivial decomposition, and *indecomposable* otherwise

Let $n = 2m$ be an even positive integer. Since $B_n(x) = B_n(1-x)$ by (4), we have

$$B_n(x) = \widetilde{B}_m\big((x-1/2)^2\big), \tag{9}$$

where $\widetilde{B}_m(x) \in \mathbb{Q}[x]$ is a polynomial of degree m.

The main result of this section is that, besides (9), Bernoulli polynomials admit no nontrivial decompositions.

THEOREM 4.1. *The polynomial $B_n(x)$ is indecomposable for odd n. If $n = 2m$ is even, then any nontrivial decomposition of $B_n(x)$ is equivalent to (9). In particular, the polynomial $\widetilde{B}_m(x)$ is indecomposable for any m.*

We need a very simple lemma. Let $\triangle$ be the difference operator on the ring of polynomials $\mathbb{C}[x]$, defined by $\triangle f(x) = f(x+1) - f(x)$.

LEMMA 4.2. *For any $f(x), p(x) \in \mathbb{C}[x]$, we have $\triangle f \mid \triangle(p(f))$.*

Proof. It is sufficient to show that $\triangle f \mid \triangle\big(f^k\big)$ for $k = 0, 1, 2, \ldots$ This is, however, obvious, since for any two polynomials g and h, the difference $g - h$ divides $g^k - h^k$.

Proof of Theorem 4.1. Let $B_n(x) = G_1(G_2(X))$ be a nontrivial decomposition of $B_n(x)$. By Lemma 4.2 and (5) we have $\triangle G_2(x) \mid \triangle B_n(x) = nx^{n-1}$. This means that $\triangle G_2(x) = \kappa x^t$ with $t \leqslant n-1$ and $\kappa \in \mathbb{C}^*$. Again using (5), we obtain $G_2(x) = \lambda B_k(x) + \mu$, where $\lambda \in \mathbb{C}^*$, $\mu \in \mathbb{C}$ and $k = t+1$. Thus, the decomposition $B_n(x) = G_1(G_2(X))$ is equivalent to $B_n(x) = P(B_k(x))$, where $P(x) = G_1(\lambda x + \mu)$. Since the decomposition is nontrivial, we have $2 \leqslant k < n$.

If $k = 2$, then our decomposition is equivalent to (9). Now assume that $k \geqslant 3$. Since both polynomials $B_n(x)$ and $B_k(x)$ are monic, so is $P(x)$. Also, $p := \deg P(x) \geqslant 2$ because the decomposition is nontrivial. Comparing the coefficients of x^{n-2} in $B_n(x)$ and $P(B_k(x))$, we obtain $n(n-1)/12 = pk(pk-k)/8 + pk(k-1)/12$. Since $pk = n$, we may rewrite this as $2(n-1) = 3(n-k) + 2(k-1)$, which implies $k = n$, a contradiction. The theorem is proved.

A totally different approach to the decomposition of Bernoulli and related polynomials is suggested in the appendix by A. Schinzel.

It is not difficult to classify the decompositions of the polynomial $R_m(x)$ as well.

THEOREM 4.3. *The polynomial $R_m(x)$ is indecomposable if m is odd. If $m = 2k$ is even then any nontrivial decomposition of $R_m(x)$ is equivalent to $R_m(x) =$*

$\widetilde{R}_k\big((x-(m-1)/2)^2\big)$, *where*

$$\widetilde{R}_k(x) = (x-1/4)(x-9/4)\cdots\big(x-(2k-1)^2/4\big). \tag{10}$$

In particular, the polynomial $\widetilde{R}_k(x)$ *is indecomposable for any* k.

Proof. If $F(x) = G_1(G_2(x))$ is a decomposition of a polynomial $F(x) \in \mathbb{C}[x]$ with $\deg G_1 > 1$, then there exists $\lambda \in \mathbb{C}$ such that $\deg\gcd(F(x)-\lambda, F'(x)) \geqslant \deg G_2$. Indeed, if α is a root of $G_1'(x)$ and $\lambda = G_1(\alpha)$ then $G_2(x) - \alpha$ divides both the polynomials $F(x) - \lambda$ and $F'(x)$.

On the other hand, Beukers, Shorey and Tijdeman [3, Proposition 3.4] proved that $\deg\gcd\big(R_m(x)-\lambda, R_m'(x)\big) \leqslant 2$ for any $\lambda \in \mathbb{C}$. Hence for any nontrivial decomposition $R_m(x) = G_1(G_2(x))$ we have $\deg G_2 = 2$. Write $G_2(x) = \alpha(x-\beta)^2 + \gamma$. Then our decomposition is equivalent to $R_m(x) = P\big((x-\beta)^2\big)$ with some polynomial $P(x) \in \mathbb{C}[x]$. Since the roots of $R_m(x)$ are symmetric with respect to β, we have $\beta = (m-1)/2$, which completes the proof.

Next, we show that for $m, n \geqslant 2$, the polynomial $S_n(x)$ cannot be presented as $R_m(P(x))$, where $P(x)$ is another polynomial. Actually, we obtain a slightly more general result with $P(x) = p(x)\sqrt{\alpha x^2 + \beta x + \gamma} + \delta$.

THEOREM 4.4. *There exist no polynomial* $p(x) \in \mathbb{C}[x]$ *and no* $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ *such that*

$$S_n(x) = R_m\Big(p(x)\sqrt{\alpha x^2 + \beta x + \gamma} + \delta\Big). \tag{11}$$

for some $m, n \geqslant 2$.

For the proof, we need a simple lemma. To formulate it, consider the following question. Let $f(x), g(x)$ be two polynomials with rational coefficients. Assume that $f(x) = g(\lambda x + \mu)$ for some $\lambda \in \mathbb{C}^*$ and $\mu \in \mathbb{C}$. Is it true that $\lambda, \mu \in \mathbb{Q}$?

Simple examples like $\big(\sqrt{2}x\big)^2 = 2x^2$ show that in general this is false. Lemma 4.5 gives a sufficient condition for rationality of λ and μ, which is rather restrictive, but suitable for our purposes.

LEMMA 4.5. *In the set-up from above, assume that all roots of* $g(x)$ *are rational, and that* $f(x)$ *vanishes at* $\beta \in \mathbb{Q}$, *but is not of the form* $h\big((x-\beta)^d\big)$, *where* $h(x) \in \mathbb{Q}[x]$ *and* $d > 1$. *Then* $\lambda, \mu \in \mathbb{Q}$.

Proof. Without loss of generality $\beta = 0$, so that $0 = f(0) = g(\mu)$. Hence $\mu \in \mathbb{Q}$. It follows that $f(\lambda x) = g(x-\mu) \in \mathbb{Q}[x]$. Write $f(x) = a_n x^n + \cdots + a_0$. Since both the polynomials $f(x)$ and $f(\lambda x)$ have rational coefficients, we have $\{\lambda^k : a_k \neq 0\} \subset \mathbb{Q}$. Also, $\gcd\{k : a_k \neq 0\} = 1$, because $f(x)$ is not of the form $h\big(x^d\big)$ with $d > 1$. This implies that λ belongs to the multiplicative group generated by the set $\{\lambda^k : a_k \neq 0\}$. Hence $\lambda \in \mathbb{Q}$, as wanted.

Proof of Theorem 4.4. We start with the following particular case of Theorem 4.4: for $m, n \geqslant 2$ there exists no polynomial $p(x) \in \mathbb{C}[x]$ such that

$$S_n(x) = R_m(p(x)). \tag{12}$$

Assuming the contrary, let $p(x)$ be such a polynomial. Theorem 4.1 implies that $\deg p(x) \leqslant 2$. Assume first that $\deg p(x) = 1$, in which case $m = n + 1$, and write $p(x) = \lambda x + \mu$. Since all the roots of $R_m(x)$ are rational, and $S_n(x)$ vanishes at 0, but is not of the form $h(x^d)$ with $d > 1$, Lemma 4.5 implies that $\lambda, \mu \in \mathbb{Q}$. Comparing the leading terms of $S_n(x)$ and $R_m(p(x))$, we obtain $1/m = \lambda^m$. Thus, $\sqrt[m]{m} \in \mathbb{Q}$, which is impossible.

Now assume that $\deg p(x) = 2$, in which case $n + 1 = 2m$. By Theorem 4.1, the decomposition $B_{2m}(x) = 2mR_m(p(x)) + B_{2m}$ is equivalent to $B_{2m}(x) = \widetilde{B}_m((x - 1/2)^2)$, which means that there exist $\lambda \in \mathbb{C}^*$ and $\mu \in \mathbb{C}$ such that $p(x) = \lambda(x - 1/2)^2 + \mu$ and $\widetilde{B}_m(x) = 2mR_m(\lambda x + \mu) + B_{2m}$.

If $m = 2$ then $\widetilde{B}_2(x) - B_4 = (x - 1/4)^2 = 4R_2(\lambda x + \mu)$, which is impossible because the latter polynomial has only simple roots. Thus, $m \geqslant 3$. The polynomial $\widetilde{B}_m(x) - B_{2m}$ vanishes at $1/4$, but is not of the form* $h((x - 1/4)^d)$ with $d > 1$. Hence $\lambda, \mu \in \mathbb{Q}$ by Lemma 4.5. Comparing the leading coefficients, we obtain $\lambda^m = 1/(2m)$. However, $\sqrt[m]{2m} \notin \mathbb{Q}$ for $m \geqslant 3$. This shows that (12) is impossible for $p(x) \in \mathbb{C}[x]$.

Now we can prove Theorem 4.4 in its full generality. Thus, suppose that (11) holds. We may assume that $r(x) := \alpha x^2 + \beta x + \gamma$ is not a complete square, since otherwise $p(x)\sqrt{r(x)} + \delta$ is a polynomial, which has already been treated in the first part of the proof. Since

$$R_m\left(p(x)\sqrt{r(x)} + \delta\right) \\ = r(x)^{m/2}p(x)^m + r(x)^{(m-1)/2}p(x)^{m-1}(m\delta + m(m-1)/2) + \cdots$$

is a polynomial, the number m must be even. Furthermore,

$$m\delta + m(m-1)/2 = 0,$$

which implies that $\delta = -(m-1)/2$. Consequently

$$R_m\left(p(x)\sqrt{r(x)} + \delta\right) = R_m\left(p(x)\sqrt{r(x)} - \frac{m-1}{2}\right) = \widetilde{R}_k\left(r(x)p(x)^2\right),$$

where $k = m/2$ and $\widetilde{R}_k(x)$ is defined in (10). Thus, $S_n(x) = \widetilde{R}_k(\widetilde{p}(x))$, where $\widetilde{p}(x) = r(x)p(x)^2$.

If $k = 1$ then $\widetilde{R}_k(x) = x - 1/4$ and $S_n(x) + 1/4 = r(x)p(x)^2$, which contradicts Lemma 2.2. If $k \geqslant 2$ then, arguing as in the first part of the proof, one shows that $S_n(x) = \widetilde{R}_k(\widetilde{p}(x))$ is impossible for any polynomial $\widetilde{p}(x)$. The theorem is proved.

---

*Indeed, assume that $\widetilde{B}_m(x) - B_{2m} = h((x - 1/4)^d)$ with $d > 1$. Since $\widetilde{B}_m(x)$ is indecomposable, the only possibility is $\widetilde{B}_m(x) - B_{2m} = (x - 1/4)^m$, in which case $B_{2m}(x) - B_{2m} = (x^2 - x)^m$. But $B_{2m}(x) - B_{2m}$ cannot have roots of multiplicity $m \geqslant 3$ by Lemma 2.1.

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

5. Proof of Theorems 1.1 and 1.2

5.1. STANDARD PAIRS AND THE CRITERION

In this subsection we recall the finiteness criterion from [5]. To do this, we need to define five kinds of 'standard pairs' of polynomials. In what follows α and β are nonzero rational numbers, μ, ν and q are positive integers, ρ is a nonnegative integer and $v(x) \in \mathbb{Q}[x]$ is a nonzero polynomial (which may be constant).

A *standard pair of the first kind* is $(x^q,\ \alpha x^\rho v(x)^q)$ or switched, $(\alpha x^\rho v(x)^q,\ x^q)$, where $0 \leqslant \rho < q$, $(\rho, q) = 1$ and $\rho + \deg v(x) > 0$.

A *standard pair of the second kind* is $\left(x^2,\ (\alpha x^2 + \beta)v(x)^2\right)$ (or switched).

Denote by $D_\mu(x, \delta)$ the μth Dickson polynomial, defined by the functional equation $D_\mu(z + \delta/z, \delta) = z^\mu + (\delta/z)^\mu$ or by the explicit formula

$$D_\mu(x, \delta) = \sum_{i=0}^{\lfloor \mu/2 \rfloor} d_{\mu,i} x^{\mu-2i} \qquad \text{with} \quad d_{\mu,i} = \frac{\mu}{\mu - i}\binom{\mu - i}{i}(-\delta)^i. \tag{13}$$

A *standard pair of the third kind* is $\left(D_\mu(x, \alpha^\nu),\ D_\nu(x, \alpha^\mu)\right)$, where $\gcd(\mu, \nu) = 1$.

A *standard pair of the fourth kind* is

$$\left(\alpha^{-\mu/2} D_\mu(x, \alpha),\ -\beta^{-\nu/2} D_\nu(x, \beta)\right),$$

where $\gcd(\mu, \nu) = 2$.

A *standard pair of the fifth kind* is $\left((\alpha x^2 - 1)^3,\ 3x^4 - 4x^3\right)$ (or switched).

The following theorem is the main result of [5]. It extends and completes the previous work of Davenport, Lewis, Schinzel and Fried [11, 14, 20].

THEOREM 5.1. *Let $R(x), S(x) \in \mathbb{Q}[x]$ be nonconstant polynomials such that the equation $R(x) = S(y)$ has infinitely many solutions in rational integers x, y. Then $R = \varphi \circ f \circ \kappa$ and $S = \varphi \circ g \circ \lambda$, where $\kappa(x), \lambda(x), \in \mathbb{Q}[x]$ are linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $(f(x), g(x))$ is a standard pair.*

The proof relies, besides other tools, on Siegel classical theorem about integral points [22]. Since Siegel's theorem is ineffective, so is Theorems 5.1.

5.2. TWO LEMMAS

We will also need two simple, though somewhat technical lemmas. In the sequel $a_1, b_1, e_1 \in \mathbb{Q}^*$ and $a_0, b_0, e_0 \in \mathbb{Q}$.

LEMMA 5.2. *None of the polynomials $R_m(a_1x + a_0)$ and $S_n(b_1x + b_0)$ is of the form $e_1x^q + e_0$ with $q \geqslant 3$.*

LEMMA 5.3. *The polynomial $S_n(b_1x + b_0)$ is not of the form $e_1 D_\nu(x, \delta) + e_0$, where $D_\nu(x, \delta)$ is the Dickson polynomial (13) with $\nu > 4$ and $\delta \in \mathbb{Q}^*$.*

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

To prove these lemmas we use explicit expressions for the coefficients of the polynomials

$$R_m(a_1x + a_0) = r_m x^m + r^{m-1} x_{m-1} + \cdots + r_0$$

and

$$S_n(b_1x + b_0) = s_{n+1}x^{n+1} + s_n x^n + \cdots + s_0.$$

We have

$$r_m = a_1^m, \qquad r_{m-1} = \frac{a_1^{m-1}}{2} m(2a_0 + m - 1), \tag{14}$$

$$r_{m-2} = \frac{a_1^{m-2}}{24} m(m-1)(3m^2 + (12a_0 - 7)m + 12a_0^2 - 12a_0 + 2), \tag{15}$$

$$s_{n+1} = \frac{b_1^{n+1}}{n+1}, \qquad s_n = \frac{b_1^n}{2}(2b_0 - 1), \tag{16}$$

$$s_{n-1} = \frac{b_1^{n-1}}{12} n(6b_0^2 - 6b_0 + 1), \tag{17}$$

$$s_{n-3} = \frac{b_1^{n-3}}{720} n(n-1)(n-2)(30b_0^4 - 60b_0^3 + 30b_0^2 - 1) \tag{18}$$

Proof of Lemma 5.2. If $R_m(a_1x + a_0) = e_1x^q + e_0$ with $q = m \geqslant 3$, then $r_{m-1} = r_{m-2} = 0$. Equality $r_{m-1} = 0$ implies that $a_0 = (1-m)/2$. Substituting this into the equality $r_{m-2} = 0$ we obtain $m \in \{0, \pm 1\}$, a contradiction.

(One may also argue as follows. Since $R_m(a_1x + a_0)$ has m distinct real roots, its derivative should have $m - 1$ distinct real roots, which is not the case for $(e_1x^q + e_0)'$.)

If $S_n(b_1x + b_0) = e_1x^q + e_0$ with $q = n + 1 \geqslant 3$ then $s_{n-1} = 0$, which implies $6b_0^2 - 6b_0 + 1 = 0$. Hence $b_0 \notin \mathbb{Q}$, a contradiction.

Proof of Lemma 5.3. If $S_n(b_1x + b_0) = e_1 D_v(x, \delta) + e_0$ with $v = n + 1 > 4$ then

$$s_{n+1} = e_k, \tag{19}$$

$$s_n = 0, \tag{20}$$

$$s_{n-1} = -e_1 v\delta, \tag{21}$$

$$s_{n-3} = e_1(v-3)v\delta^2/2. \tag{22}$$

Relations (19) and (20) imply that $b_0 = 1/2$ and $e_k = b_1^v/v$. Substituting this, together

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

with $n = v - 1$, into (21) and (22), we obtain, respectively,

$$-b_1^{v-2}(v-1)/24 = -b_1^v\delta, \tag{23}$$

$$7b_1^{v-4}(v-1)(v-2)(v-3)/5760 = b_1^v\delta^2(v-3)/2. \tag{24}$$

After extracting b_1 from (23) and substituting it into (24), we obtain $7(v-2)(v-3) = 5(v-1)(v-3)$, which implies $v \in \{3, 9/2\}$, a contradiction.

5.3. PROOF OF THEOREM 1.1

If $R_m(x) = S_n(y)$ has infinitely many solutions, then, by Theorem 5.1, $R_m(a_1x + a_0) = \varphi(f(x))$ and $S_n(b_1x + b_0) = \varphi(g(x))$, where (f, g) is a standard pair, a_0, a_1, b_0, b_1 are rational numbers with $a_1b_1 \neq 0$ and $\varphi(x)$ is a polynomial with rational coefficients.

Assume first of all that $\deg\varphi > 1$. Then $\deg f, \deg g \leqslant 2$ by Theorems 4.1 and 4.3. We have $S_n(x) = \varphi(g_1(x))$, where $g_1(x) = g\big(b_1^{-1}(x - b_0)\big)$.

If $\deg f = 1$ then, after modifying a_1 and a_1, we may assume that $R_m(a_1x + a_0) = \varphi(x)$. We obtain $S_n(x) = R_m(a_1g_1(x) + a_0)$, which contradicts Theorem 4.4.

If $\deg f = 2$ then, after modifying a_1 and a_1, we may assume that $R_m(a_1x + a_0) = \varphi(x^2 + \alpha)$ with $\alpha \in \mathbb{C}$. We obtain

$$S_n(x) = R_m(a_1\sqrt{g_1(x) - \alpha} + a_0).$$

This again contradicts Theorem 4.4 because $\deg g_1(x) \leqslant 2$.

Thus, $\deg\varphi(x) = 1$, and we have

$$R_m(a_1x + a_0) = e_1f(x) + e_0, \qquad S_n(b_1x + b_0) = e_1g(x) + e_0,$$

where $e_1 \in \mathbb{Q}^*$ and $e_0 \in \mathbb{Q}$. In particular, $\deg f = m \geqslant 2$ and $\deg g = n + 1 \geqslant 2$. In view of Theorems 3.1 and 3.2, we may assume that

none of the polynomials f, g is of degree 2 or 4. (25)

In particular, the standard pair (f, g) cannot be of the second or fifth kind.

If it is of the first kind then one of the polynomials $R_m(a_1x + a_0)$ or $S_n(b_1x + b_0)$ is of the form $e_1x^q + e_0$, where $q \geqslant 3$ by (25). This is, however, impossible by Lemma 5.2.

If (f, g) is a standard pair of the fourth kind, then $S_n(b_1x + b_0) = e_1D_v(x, \delta) + e_0$, where $v = n + 1$ and $\delta \in Q^*$. Since v is even we have $v > 4$ by (25), which contradicts Lemma 5.3.

Thus, (f, g) is a standard pair of the third kind We must have $n = 2$, because the cases $n \in \{1, 3\}$ and $n > 3$ are impossible by (25) and Lemma 5.3, respectively. Thus, for some $\alpha \in \mathbb{Q}^*$ we have

$$R_m(a_1x + a_0) = e_1D_m(x, \alpha^3) + e_0,$$
$$S_2(b_1x + b_0) = e_1D_3(x, \alpha^m) + e_0.$$

In the sequel, we use the notation of Subsection 5.2 and relations (14–18). Since $r_{m-1} = s_2 = 0$, we have $a_0 = (1-m)/2$ and $b_0 = 1/2$. Further,

$$s_3 = b_1^3/3 = e_1, \tag{26}$$

$$s_1 = -b_1/24 = -3e_1\alpha^m, \tag{27}$$

$$r_m = a_1^m = e_1, \tag{28}$$

$$r_{m-2} = -a_1^{m-2}m(m-1)(m+1)/24 = -e_1 m\alpha^3. \tag{29}$$

Now (26) and (27) imply that $\alpha^m = b_1^{-2}/24$, while (28) and (29) imply that $\alpha^3 = a_1^{-2}(m^2-1)/24$. Also, $a_1^m = e_1 = b_1^3/3$. Hence

$$b_1^{-6}/24^3 = \alpha^{3m} = a_1^{-2m}((m^2-1)/24)^m = 9b_1^{-6}((m^2-1)/24)^m.$$

Thus, $(3^5 \cdot 2^9)^{1/m} \in \mathbb{Q}$, which is impossible. The theorem is proved. □

5.4. PROOF OF THEOREM 1.2

We again wish to come to a contradiction, assuming that $S_m(a_1x + a_0) = \varphi(f(x))$ and $S_n(b_1x + b_0) = \varphi(g(x))$, where (f, g) is a standard pair, a_0, a_1, b_0, b_1 are rational numbers with $a_1b_1 \neq 0$ and $\varphi(x)$ is a polynomial with rational coefficients.

If $k := \deg\varphi > 1$, then $\deg f, \deg g \leqslant 2$ by Theorem 4.1. Since $m < n$, we have $\deg f = 1$ and $\deg g = 2$. In particular, $m + 1 = k$ and $n + 1 = 2k$.

Let α, β and e_k be the leading coefficients of f, g and φ, respectively. Comparing the leading coefficients of $S_m(a_1x + a_0)$ and $\varphi(f(x))$, we obtain $a_1^k/k = e_k\alpha^k$. Similarly, $b_1^{2k}/(2k) = e_k\beta^{2k}$. It follows that $\left(\alpha a_1^{-1}b_1^2\beta^{-2}\right)^k = 2$, which is impossible because $2^{1/k} \notin \mathbb{Q}$.

Thus, $\deg\varphi(x) = 1$, and we have

$$S_m(a_1x + a_0) = e_1 f(x) + e_0, \qquad S_n(b_1x + b_0) = e_1 g(x) + e_0,$$

where $e_1 \in \mathbb{Q}^*$ and $e_0 \in \mathbb{Q}$. In particular, $\deg f = m + 1$ and $\deg g = n + 1$. In view of the theorems, we may assume that none of m and n is equal to 1 or 3. This implies that $n \geqslant 4$ and that the standard pair (f, g) cannot be of the second or fifth kind.

If it is of the first kind then one of the polynomials $S_m(a_1x + a_0)$ or $S_n(b_1x + b_0)$ is of the form $e_1x^q + e_0$, where $q \geqslant 3$. This is impossible by Lemma 5.2.

If (f, g) is a standard pair of the third or fourth kind, then $S_n(b_1x + b_0) = e_1D_\nu(x, \delta) + e_0$, where $\nu = n + 1 > 4$ and $\delta \in \mathbb{Q}^*$. This contradicts Lemma 5.3. The theorem is proved. □

6. Arithmetical Approach to Decomposition of Bernoulli Polynomials (by A. Schinzel)

In this appendix we use an arithmetical method to prove the following theorem.

https://doi.org/10.1023/A:1014972217217 Published online by Cambridge University Press

THEOREM 6.1. *The Bernoulli polynomial $B_n(x)$ cannot be presented as $rP(Q(x))$, where r is a rational number, $P(x) \in \mathbb{Z}[x]$ ia a monic polynomial of degree greater than 1, and $Q(x) \in \mathbb{Q}[x]$. When $n \neq 2, 4$, the same holds for the polynomial $\Phi_n(x) := B_n(x) - B_n$.*

Notice that $\Phi_2(x) = P(Q(x))$ where $P(x) = x^2 - x$ and $Q(x) = x$ and $\Phi_4(x) = P(Q(x))$ where $P(x) = x^2$ and $Q(x) = x^2 - x$.

COROLLARY 6.2. *The polynomial $B_n(x)$ cannot be presented as $R_m(Q(x))$, where $m \geqslant 2$ and $Q(x) \in \mathbb{Q}[x]$. The same is true for $\Phi_n(x)$ when $n \neq 2$, and for $S_n(x)$ when $n \neq 1$.*

Proof. In view of Theorem 6.1, it remains to show that neither $\Phi_4(x) = (x^2 - x)^2$ nor $S_3(x) = ((x^2 - x)/2)^2$ can be of the form $R_2(Q(x))$ or $R_4(Q(x))$. Since $R_2(x) = (x - 1/2)^2 - 1/4$ and $R_4(x) = (x^2 + 3x + 1)^2 - 1$, the contrary would, in any case, imply an equality of the form $(T(x) - U(x))(T(x) + U(x)) = 1$ for certain nonconstant polynomials $T(x)$ and $U(x)$, which is impossible.

For the proof of Theorem 6.1 we need an auxiliary result.

LEMMA 6.3. *If $\Phi_n(x) \in \mathbb{Z}[x]$, then $n \in \{1, 2, 4\}$.*

Proof. Assume that

$$\Phi_n(x) \in \mathbb{Z}[x] \quad \text{and} \quad n > 1. \tag{30}$$

Since $B_1 = -1/2$, we have

$$n \equiv 0 \bmod 2. \tag{31}$$

By the von Staudt theorem (7) we have $6|\Lambda_k$ for any even k. Hence (30) implies that

$$6 \mid \binom{n}{k} \tag{32}$$

for all positive even $k < n$. However, if $n = \sum_{i=1}^{r} 2^{\alpha_i}$, where $\alpha_1 > \alpha_2 > \cdots > \alpha_r > 0$ and $r > 1$, then $k = \sum_{i=1}^{r-1} 2^{\alpha_i}$ is even, $0 < k < n$ and by virtue of Lucas' theorem, $\binom{n}{k}$ is odd. Hence, conditions (31) and (32) imply $n = 2^{\alpha}$. Similarly, assume that $n = \sum_{i=1}^{s} \varepsilon_i 3^{\beta_i}$, where $s > 1$, $\beta_1 > \beta_2 > \cdots > \beta_s \geqslant 0$ and $\varepsilon_i \in \{1, 2\}$ If for at least one j we have $\varepsilon_j = 2$, then $k = \sum_{i \neq j} \varepsilon_i 3^{\beta_i}$ is even and, again by Lucas' theorem, $\binom{n}{k} \not\equiv 0 \bmod 3$. Also, if $s > 2$ and for at least two subscripts j_1, j_2 we have $\varepsilon_{j_1} = \varepsilon_{j_2}$, then $k = \sum_{i \neq j_1, j_2} \varepsilon_i 3^{\beta_i}$ is even, $0 < k < n$ and $\binom{n}{k} \not\equiv 0 \bmod 3$. Hence (31) and (32) imply $n = 2^{\alpha} = 3^{\beta_1} + 3^{\beta_2}$ with $\beta_1 \geqslant \beta_2$. It follows that $\beta_2 = 0$ and either $\alpha = 1$, $\beta_1 = 0$ or $\alpha = 2$, $\beta_1 = 1$, which gives $n = 2$ or $n = 4$.

Proof of Theorem 6.1. Let $P(x)$ and $Q(x)$ be as assumed, and let d be the denominator of the polynomial $Q(x)$, that is the smallest positive integer d such that $dQ(x) \in \mathbb{Z}[x]$. By the Gauss Lemma, the denominator of $Q(x)^m$, where $m = \deg P$, is d^m. Since the polynomial $P(x)$ is monic and has integer coefficients, the denominator of $P(Q(x))$ is d^m as well.

Further, comparing the leading coefficient of $B_n(x)$ (or $\Phi_n(x)$) with that of $rP(Q(x))$, we obtain $1 = rq^m$, or $r = q^{-m}$, where q is the leading coefficient of $Q(x)$. This implies that the denominator of $rP(Q(x))$ is a perfect mth power in $\mathbb{Z}$.

On the other hand, by the von Staudt theorem (7) and Lemma 6.3, the denominator of $B_n(x)$ is a square free integer greater that 1, and the same is true for the denominator of $\Phi_n(x)$ when $n \neq 2, 4$. In particular, it cannot be a perfect mth power for $m \geqslant 2$. The theorem is proved.

Acknowledgements

We thank Andrzej Schinzel for his interest in this project, and for his kind permission to include his note as an appendix to our paper. We also thank Thomas Stoll for performing a part of computations in Subsection 5.2. B.B. was supported by the Hungarian National Foundation for Scientific Research, Grant T25371. P.K. and R.F.T. were supported by the Austrian Science Foundation FWF, grants S 8307 and P 14200-MAT, and A.P. was supported by the Hungarian National Foundation for Scientific Research, Grants T25371, T29330, F34891 and FKFP-0066/2001.

References

1. Baker, A.: Bounds for solutions of hyperelliptic equations, *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.
2. Baker, A. and Coates, J.: Integer points on curves of genus 1, *Math. Proc. Cambridge Philos. Soc.* **67** (1970), 592–602.
3. Beukers, F., Shorey, T. N. and Tijdeman, R.: Irreducibility of polynomials and arithmetic progressions with equal product of terms, In: K. Győry, H. Iwaniec, J. Urbanowicz (eds), *Number Theory in Progress: Proc. Int. Conf. in Number Theory in Honor of A. Schinzel, Zakopane, 1997*, W. de Gruyter, 1999, pp. 11–26.
4. Bilu, Yu. F., Stoll, Th. and Tichy, R. F.: Octahedrons with equally many lattice points, *Period. Math. Hungar.* **40** (2000), 229–238.
5. Bilu,Yu. F. and Tichy, R. F.: The Diophantine equation $f(x) = g(y)$, *Acta Arith.* **95** (2000), 261–288.
6. Brillhart, J.: On the Euler and Bernoulli polynomials, *J. Reine Angew. Math.* **234** (1969), 45–64.
7. Brindza, B.: On some generalizations of the diophantine equation $1^k + 2^k + \cdots + x^k = y^z$, *Acta Arith.* **44** (1984), 99–107.
8. Brindza, B.: Power values of sums $1^k + 2^k + \cdots + x^k$, *Number Theory II (Budapest 1987)*, *Colloq. Math. Soc. János Bolyai* **51** (1990), 595–611.
9. Brindza, B. and Pintér, Á.: On equal values of power sums, *Acta Arith.* **77** (1996), 303–307.
10. Brindza, B. and Pintér, Á.: On the irreducibility of some polynomials in two variables, *Acta Arith.* **82** (1997), 303–307.
11. Davenport, H., Lewis, D. J. and Schinzel, A.: Equations of the form $f(x) = g(y)$, *Quart. J. Math. Oxford* **12** (1961), 304–312.
12. Dujella, A. and Tichy, R. F.: Diophantine equations for second order recursive sequences of polynomials, *Quart. J. Math. Oxford* **52** (2001), 161–169.

13. Erdős, P. and Selfridge, J. L.: The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301.
14. Fried, M.: On a theorem of Ritt and related Diophantine problems, *J. Reine Angew. Math.* **264** (1974), 40–55.
15. Győry, K., Tijdeman, R. and Voorhoeve, M.: On the equation $1^k + 2^k + \cdots + x^k = y^z$, *Acta Arith.* **37** (1980), 234–240.
16. Hajdu, L. and Pintér, Á.: Combinatorial diophantine equations, *Publ. Math. Debrecen* **56** (2000), 391–403.
17. Kano, H.: On the Equation $s(1^k + 2^k + \cdots + x^k) + r = by^z$, *Tokyo J. Math.* **13** (1990), 441–448.
18. Rademacher, H.: *Topics in Analytic Number Theory*, Springer-Verlag, Berlin, 1973.
19. Saradha, N., Shorey, T. N. and Tijdeman, R.: On arithmetic progressions of equal length with equal products, *Math. Proc. Cambridge Philos. Soc.* **117** (1995), 193–201.
20. Schinzel, A.: *Selected Topics on Polynomials*, Univ. Michigan Press, Ann Arbor, 1982.
21. Shorey, T. N. and Tijdeman, R.: Some methods of Erdős applied to finite arithmetic progressions, *The Mathematics of Paul Erdős*, *Algorithms Combin.* **13** (1997), 251–267.
22. Siegel, C. L.: Über einige Anwendungen Diophantischer Approximationen, *Abh. Preuss Akad. Wiss. Phys.-Math. Kl.*, 1929, Nr. 1; *Ges. Abh.*, Band 1, 209–266.
23. Voorhoeve, M., Győry, K. and Tijdeman, R.: On the diophantine equation $1^k + 2^k + \cdots + x^k + R(x) = y^z$, *Acta Math.* **143** (1979), 1–8, corrections: *Acta Math.* **159** (1987), 151.
24. Yuan, P. Z.: On the special Diophantine equation $a\binom{x}{n} = by^r + c$, *Publ. Math. Debrecen* **44** (1994), 137–143.