ACTA ARITHMETICA
161.3 (2013)

Diophantine equations with Euler polynomials

by

Dijana Kreso (Graz) and Csaba Rakaczki (Miskolc)

1. Introduction. If $\mathbb{K}$ is a field and $g, h \in \mathbb{K}[x]$, then $f = g \circ h$ is their functional composition and (g, h) is a (functional) *decomposition* of f over $\mathbb{K}$. The decomposition is *nontrivial* if g and h are of degree at least 2. A polynomial is said to be *indecomposable* if it is of degree at least 2 and does not have a nontrivial decomposition. Given $f \in \mathbb{K}[x]$ with $\deg f > 1$, a *complete decomposition* of f over $\mathbb{K}$ is a decomposition $f = f_1 \circ \cdots \circ f_m$, where the polynomials $f_i \in \mathbb{K}[x]$ are indecomposable over $\mathbb{K}$ for all $i = 1, \ldots, m$. Two decompositions $f = g_1 \circ h_1 = g_2 \circ h_2$ are said to be *equivalent* over $\mathbb{K}$, written $g_1 \circ h_1 \sim_{\mathbb{K}} g_2 \circ h_2$, if there exists a linear polynomial $l \in \mathbb{K}[x]$ such that

$$g_2 = g_1 \circ l \quad \text{and} \quad h_2 = l^{-1} \circ h_1.$$

Clearly a complete decomposition of a polynomial of degree greater than 1 always exists. However it is not unique and not even up to equivalence. Nonuniqueness of prime factorization in $(\mathbb{C}[x], \circ)$ was of central interest to J. F. Ritt, who proved remarkable results on this topic in his fundamental 1922 paper [16]. In particular, he showed the "essential uniqueness" of factorization in $(\mathbb{C}[x], \circ)$, by showing that the sequence of the degrees of the indecomposable polynomials in a complete decomposition over $\mathbb{C}$ of a polynomial $f \in \mathbb{C}[x]$ is uniquely determined by f up to permutation. Ritt's results have been extended to any field of characteristic zero by Engstrom [11] and Levi [13] in the 1940s, and to any field $\mathbb{K}$ of positive characteristic, provided that the degree of the polynomial under consideration is not divisible by the characteristic of $\mathbb{K}$, by Dorey and Whaples [10] in 1974. For an exhaustive explanatory work on this topic, we refer the reader to [18].

Ritt's polynomial decomposition results have been applied to a great variety of topics. Fried [12] was the first to notice a connection with rational

2010 *Mathematics Subject Classification*: Primary 11D41; Secondary 11B68.
Key words and phrases: Euler polynomials, higher degree equations.

DOI: 10.4064/aa161-3-5

points on curves. In 2000, Bilu and Tichy [7] succeeded in fully combining polynomial decomposition with the classical theorem of Siegel on finiteness of integral points on curves of genus greater than 0, to give a complete ineffective criterion for the finiteness of the number of integer solutions x, y of diophantine equations of the form $f(x) = g(y)$, where $f(x)$ and $g(x)$ are polynomials with rational coefficients. Their result led to a great number of papers over the past decade, in which the question of finiteness of the number of integer solutions has been solved for many concrete diophantine equations in two separated variables. In particular, we mention the work of Bilu, Brindza, Kirschenhofer, Pintér and Tichy [6] with an appendix by Schinzel on equations with power sums of consecutive integers $S_k(x) = 1^k + \cdots + x^k$, the related paper [14], where the finiteness of the number of integer solutions of the equation $1^k + \cdots + x^k = g(y)$, with arbitrary $g(x) \in \mathbb{Q}[x]$, has been investigated, as well as the most recent work of Bazsó, Kreso, Luca and Pintér [3] on a direct generalization of the problem treated in [6] to the case of the power sum of elements of an arithmetic progression. We mention that the study of diophantine equations involving power sums of consecutive integers has a long history, dating back to the 1956 work of Schäffer [17].

In the present paper, we study a related problem, with the power sum of consecutive integers being replaced by the alternating power sum, $T_k(n) = -1^k + 2^k - \cdots + (-1)^n n^k$. The quantity $T_k(n)$ is related to the kth Euler polynomial via the identity

$$T_k(n) = \frac{E_k(0) + (-1)^n E_k(n+1)}{2}.$$

The Euler polynomials are defined by the following generating function:

$$\sum_{k=0}^{\infty} E_k(x)\frac{t^k}{k!} = \frac{2e^{tx}}{e^t + 1}.$$

Our main result is a full classification of complete decompositions of Euler polynomials over the set of complex numbers. Since the Euler polynomials appear in many classical results and play an important role in various approximation and expansion formulas in discrete mathematics and in number theory (see for instance [1], [8]), our result might be of broader interest. We emphasize that there is a novelty in our approach to this decomposition task. In Section 2, we recall and develop lemmas which are interesting in the context of polynomial decomposition. We then combine these results with the properties of Euler polynomials to prove the following theorem.

THEOREM 1.1. *The Euler polynomials $E_k(x)$ are indecomposable over $\mathbb{C}$ for all odd k. If $k = 2m$ is even, then every nontrivial decomposition of*

$E_k(x)$ over $\mathbb{C}$ is equivalent to

$$E_k(x) = \widetilde{E}_m\left(\left(x-\frac{1}{2}\right)^2\right), \quad \text{where} \quad \widetilde{E}_m(x) = \sum_{j=0}^{m} \binom{2m}{2j} \frac{E_{2j}}{2^{2j}} x^{m-j}, \tag{1.1}$$

and E_j is the jth Euler number defined by $E_j = 2^j E_j(1/2)$. In particular, the polynomial $\widetilde{E}_m(x)$ is indecomposable over $\mathbb{C}$ for any $m \in \mathbb{N}$.

Theorem 1.1 combined with the aforementioned criterion of Bilu and Tichy enables us to characterize those polynomials $g(x) \in \mathbb{Q}[x]$ for which the diophantine equation

$$-1^k + 2^k - \cdots + (-1)^x x^k = g(y) \tag{1.2}$$

may have infinitely many integer solutions, provided $k \geq 7$. Apart from five exceptional cases we list, the equation (1.2) has only finitely many integer solutions. More precisely, the following theorem holds.

THEOREM 1.2. *Let $k \geq 7$ be an integer and $g(x) \in \mathbb{Q}[x]$ with $\deg g \geq 2$. Then the diophantine equation* (1.2) *has only finitely many solutions $x \in \mathbb{N}$, $y \in \mathbb{Z}$ unless one of the following holds:*

(i) $g(x) = f(E_k(p(x)))$,
(ii) $g(x) = f(\widetilde{E}_s(p(x)^2))$,
(iii) $g(x) = f(\widetilde{E}_s(\delta(x)p(x)^2))$,
(iv) $g(x) = f(\widetilde{E}_s(\gamma\delta(x)^t))$,
(v) $g(x) = f\big(\widetilde{E}_s((a\delta(x)^2 + b)p(x)^2)\big)$,

where $t \geq 3$ is odd, $a, b, \gamma \in \mathbb{Q} \setminus \{0\}$, $p(x) \in \mathbb{Q}[x]$,

$$f(x) = \pm x/2 + E_k(0)/2 \quad \text{and} \quad \widetilde{E}_s(x) = \sum_{j=0}^{s} \binom{2s}{2j} \frac{E_{2j}}{2^{2j}} x^{s-j}.$$

In the proof of Theorem 1.2, in each of these exceptional cases, we find a choice of parameters leading to an infinite family of integer solutions to (1.2).

In relation to our problem, we mention a paper by Dilcher [9] where an effective finiteness theorem has been established for the diophantine equation

$$-1^k + 3^k - \cdots - (4x-3)^k + (4x-1)^k = y^n, \tag{1.3}$$

viewed as a "character-twisted" analogue of Schäffer's equation, and a recent paper by Bennett [4], where the same equation has been completely solved for $3 \leq k \leq 6$ using methods from diophantine approximations as well as techniques based upon the modularity of Galois representations. We point out that by using our techniques, an ineffective finiteness theorem on the

number of integer solutions can be obtained for the diophantine equation

$$-1^k + 3^k - \cdots - (4x-3)^k + (4x-1)^k = g(y) \tag{1.4}$$

with $k \in \mathbb{N}$ and an arbitrary $g(x) \in \mathbb{Q}[x]$.

2. Decomposition of Euler polynomials. In this section, we recall and establish some results on polynomial decomposition, and then use them to classify decomposition properties of Euler polynomials over the complex numbers.

The following lemma describes the structure of the set of all decompositions of a fixed monic polynomial into two factors when the corresponding field is either of characteristic 0 or of positive characteristic but the degree of the polynomial is not divisible by the characteristic, the case known as "tame" in the literature. In the "wild" case, when the degree is divisible by the characteristic, Ritt's first theorem does not hold in general, as is shown by an example due to Dorey and Whaples [10]. Similarly, the following lemma fails in the wild case.

LEMMA 2.1. *Let $F(x) \in \mathbb{K}[x]$ be a monic polynomial such that* $\deg F$ *is not divisible by the characteristic of the field $\mathbb{K}$. Then for every nontrivial decomposition $F = F_1 \circ F_2$ over any field extension $\mathbb{L}$ of $\mathbb{K}$, there exists a decomposition $F = \tilde{F}_1 \circ \tilde{F}_2$ such that:*

- $F_1 \circ F_2 \sim_{\mathbb{L}} \tilde{F}_1 \circ \tilde{F}_2$,
- $\tilde{F}_1(x)$ *and* $\tilde{F}_2(x)$ *are monic with coefficients in* $\mathbb{K}$,
- $\operatorname{coeff}(x^{\deg \tilde{F}_1 - 1}, \tilde{F}_1(x)) = 0$.

Moreover, the decomposition $\tilde{F}_1 \circ \tilde{F}_2$ is unique.

Proof. Let $\mathbb{L}$ be an arbitrary extension field of $\mathbb{K}$ and let $F(x) = F_1(F_2(x))$ be a nontrivial decomposition over $\mathbb{L}$. There exists an equivalent decomposition $\bar{F}_1 \circ \bar{F}_2$ such that $\bar{F}_1(x)$ and $\bar{F}_2(x)$ are monic polynomials in $\mathbb{L}[x]$. Indeed, let k be the degree of $F_2(x)$ and $b_k \in \mathbb{L}$ be the leading coefficient of $F_2(x)$. Then

$$F_1 \circ F_2 \sim_{\mathbb{L}} \bar{F}_1 \circ \bar{F}_2,$$

where $\bar{F}_1(x)$, $\bar{F}_2(x) \in \mathbb{L}[x]$ are given by

$$\bar{F}_1(x) = F_1(b_k x), \quad \bar{F}_2(x) = b_k^{-1} F_2(x),$$

and are clearly monic.

Hence, we may assume that $F_1(x)$ and $F_2(x)$ are monic polynomials. Furthermore, let t be the degree of F_1 and a_{t-1} be the coefficient of x^{t-1} in $F_1(x)$. Then

$$F_1 \circ F_2 \sim_{\mathbb{L}} \tilde{F}_1 \circ \tilde{F}_2,$$

where $\tilde{F}_1(x), \tilde{F}_2(x) \in \mathbb{L}[x]$ are given by

$$\tilde{F}_1(x) = F_1(x - t^{-1}a_{t-1}), \quad \tilde{F}_2(x) = F_2(x) + t^{-1}a_{t-1}.$$

It is easy to verify that the coefficient of x^{t-1} in $\tilde{F}_1(x)$ is 0 and since F_1 and F_2 are monic, so are $\tilde{F}_1$ and $\tilde{F}_2$. Let $\tilde{F}_1(x) = x^t + a_{t-1}x^{t-1} + \cdots + a_0 \in \mathbb{L}[x]$ and $\tilde{F}_2(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0 \in \mathbb{L}[x]$, where $a_{t-1} = 0$. Further, let $F(x) = c_n x^n + \cdots + c_1 x + c_0$. Clearly, $n = kt$ and $t, k \geq 2$ by assumption.

Now we will show that $\tilde{F}_1$ and $\tilde{F}_2$ have coefficients in $\mathbb{K}$. From

$$F(x) = \tilde{F}_1(\tilde{F}_2(x)) = \tilde{F}_2(x)^t + a_{t-2}\tilde{F}_2(x)^{t-2} + \cdots + a_1\tilde{F}_2(x) + a_0, \tag{2.1}$$

by expanding $\tilde{F}_2(x)^t$ we get the following system of equations which completely determine the coefficients of $\tilde{F}_2(x)$:

$$\begin{cases} c_{n-1} = tb_{k-1}, \\ c_{n-2} = tb_{k-2} + \binom{t}{2} b_{k-1}^2, \\ \vdots \\ c_{n-k} = tb_0 + \displaystyle\sum_{i_1+2i_2+\cdots+(k-1)i_{k-1}=k} d_{i_1,i_2,\ldots,i_{k-1}}\, b_{k-1}^{i_1} b_{k-2}^{i_2} \ldots b_1^{i_{k-1}}, \end{cases} \tag{2.2}$$

where

$$d_{i_1,i_2,\ldots,i_{k-1}} = \binom{t}{i_1, i_2, \ldots, i_{k-1}}.$$

Since $c_i \in \mathbb{K}$, it follows that $b_i \in \mathbb{K}$ for all $i = 0, 1, \ldots, k-1$ and hence $\tilde{F}_2(x) \in \mathbb{K}[x]$. Furthermore, from (2.1), it is clear that the coefficients of $\tilde{F}_1$ are uniquely determined by F and $\tilde{F}_2$. Recursively, $a_i \in \mathbb{K}$ for all $i = t-2, \ldots, 1, 0$. Together with $a_t = 1$ and $a_{t-1} = 0$, it follows that $\tilde{F}_1(x) \in \mathbb{K}[x]$ as well. ∎

Remark 2.2. The proof fails in the wild case, when the degree is divisible by the characteristic, since in this case there does not exist a multiplicative inverse of the degree in the relevant field. Note that in the proof we assume that $t^{-1} \in \mathbb{K}$.

Remark 2.3. We also remark that our restriction to monic polynomials is not a restriction at all. For a nonmonic polynomial F, we may apply Lemma 2.1 to the polynomial obtained by multiplying the coefficients of $F \in \mathbb{K}[x]$ with the multiplicative inverse in $\mathbb{K}$ of the leading coefficient of F. Also, Lemma 2.1 implies that indecomposability over any field extension implies indecomposability over the original field, provided that we are in the tame case. This result is attributed to Schinzel. In fact, our proof of Lemma 2.1 is based on the proof of this fact from [18, Theorem 6, Chapter 1.3].

Further, we will need the following lemma.

Lemma 2.4. *Let $F \in \mathbb{K}[x]$ be such that $\deg F$ is not divisible by the characteristic of the field $\mathbb{K}$. If $g_1 \circ g_2$ and $h_1 \circ h_2$ are two decompositions of*

F over $\mathbb{K}$ satisfying

$$\deg g_1 = \deg h_1 \quad \textit{and hence} \quad \deg g_2 = \deg h_2,$$

then these decompositions are equivalent over $\mathbb{K}$.

Proof. Already in Ritt's fundamental paper [16], this fact is shown for $K = \mathbb{C}$ via Riemann surface techniques, and was later proved by Levi [13] in an elementary way. See also [19] for a recently found elementary proof. ∎

The following observation will be of great help in the proof of Theorem 1.1.

LEMMA 2.5. *Let n be an even positive integer. If*

$$(x+1)^n - x^n = G(x)H(x)$$

with $G(x), H(x) \in \mathbb{R}[x]$, then the coefficients of $G(x)$ and $H(x)$ are either all positive or all negative.

Proof. We have $(x+1)^n - x^n = \prod_{i=1}^{n}(x+1-\omega_i x)$, where $\omega_i = e^{2\pi i/n}$, $i = 1, \dots, n$, are the nth roots of unity. Hence, $\omega_n = 1$, $\omega_{n/2} = -1$, and $\omega_{n-j} = \overline{\omega_j}$ for all $j = 1, \dots, n/2-1$. Therefore we have

$$\begin{aligned}(2.3)\qquad (x+1)^n - x^n &= (2x+1)\prod_{j=1}^{n/2-1}(x+1-\omega_j x)(x+1-\overline{\omega_j}x)\\ &= (2x+1)\prod_{j=1}^{n/2-1}((2-(\omega_j+\overline{\omega_j}))x^2 + (2-(\omega_j+\overline{\omega_j}))x + 1).\end{aligned}$$

Clearly $2-(\omega_j+\overline{\omega_j}) > 0$ for all $j \in \{1, \dots, n/2-1\}$. Now the assertion follows from the fact that $\mathbb{R}[x]$ is a unique factorization domain. ∎

Finally, to prove Theorem 1.1 we need some well known properties of Euler polynomials; they will sometimes be used without explicit reference.

LEMMA 2.6 ([8]).

(a) $E_n(x) = (-1)^n E_n(1-x)$.
(b) $E_n(x+1) + E_n(x) = 2x^n$.
(c) $E_n'(x) = nE_{n-1}(x)$.
(d) $E_5(x)$ *is the only Euler polynomial with a multiple root.*
(e) $E_n(x) = \sum_{k=0}^{n}\binom{n}{k}\frac{E_k}{2^k}(x-\frac{1}{2})^{n-k}$, *wherefrom* $E_n(x) = \sum_{k=0}^{n} c_k x^k$ *with*

$$c_k = \sum_{j=0}^{n-k}\binom{n}{j}\frac{E_j}{2^j}\binom{n-j}{k}\left(-\frac{1}{2}\right)^{n-k-j}, \qquad k = 0, 1, \dots, n,$$

where E_j is the jth Euler number. In particular,

$$c_n = 1, \quad c_{n-1} = -\frac{1}{2}n, \quad c_{n-2} = 0, \quad c_{n-3} = \frac{1}{4}\binom{n}{3}, \quad \dots.$$

Proof of Theorem 1.1. Let $n \in \mathbb{N}$ and suppose

$$E_n(x) = G(H(x)) \tag{2.4}$$

is a nontrivial decomposition of the Euler polynomial $E_n(x) \in \mathbb{Q}[x]$ over $\mathbb{C}$. According to Lemma 2.1, we may assume that $G(x)$ and $H(x)$ are monic polynomials with rational coefficients; let $G(x) = x^t + a_{t-1}x^{t-1} + \cdots + a_0 \in \mathbb{Q}[x]$ and $H(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0 \in \mathbb{Q}[x]$. We furthermore assume $a_{t-1} = 0$. Clearly $t, k \geq 2$ by assumption.

Now, since $E_n(1-x) = (-1)^n E_n(x)$, we have

$$G(H(1-x)) = (-1)^n G(H(x)).$$

Case 1: *n is even.* Then $G(H(1-x)) = G(H(x))$ and Lemma 2.4 implies that either $H(1-x) = H(x)$, or $H(1-x) = -H(x)$ and $G(x) = G(-x)$.

In the former case $\deg H = k$ is even and $b_{k-1} = -k/2$. Furthermore, Lemma 2.6 and decomposition (2.4) imply

$$2((x+1)^n - x^n) = E_n(-x-1) - E_n(x) = G(H(-x-1)) - G(H(x)),$$

from which we deduce that $H(-x-1) - H(x)$ divides $(x+1)^n - x^n$ in $\mathbb{Q}[x]$. Since the leading coefficient of $H(-x-1) - H(x)$ is $2k$, Lemma 2.5 shows that all the coefficients of $H(-x-1) - H(x)$ must be positive. Suppose $k \geq 4$. The coefficient of x^{k-4} in $H(-x-1) - H(x)$ is found to be

$$\binom{k}{4} - \binom{k-1}{3} b_{k-1} + \binom{k-2}{2} b_{k-2} - \binom{k-3}{1} b_{k-3} > 0. \tag{2.5}$$

From (2.2) we can determine the coefficients $b_k, b_{k-1}, \ldots, b_0$ of $H(x)$ in terms of the coefficients $c_n, c_{n-1}, \ldots, c_0$ of the nth Euler polynomial. The latter are given in Lemma 2.6(e). Hence

$$b_{k-1} = -\frac{k}{2}, \quad b_{k-2} = -\frac{(t-1)k^2}{8}, \quad b_{k-3} = \frac{1}{4}\binom{k}{3} + \frac{(t-1)k^2(k-2)}{16}. \tag{2.6}$$

Substituting these values in (2.5), we obtain

$$\binom{k}{4} > \frac{(t-1)k^2(k-2)(k-3)}{16}, \tag{2.7}$$

which implies $t \leq 1$, contradicting our assumption. Since k is even, we conclude $k = 2$ and hence $t = n/2$. Now Lemma 2.4 implies that this decomposition is equivalent to (1.1).

In the case when $H(1-x) = -H(x)$ and $G(x) = G(-x)$ one can deduce that k is odd, t is even,

$$G(x) = x^t + a_{t-2}x^{t-2} + \cdots + a_2x^2 + a_0$$

and

$$E_n(x) = G(H(x)) = G_1(H_1(x)),$$

where $G_1(x) = x^{t/2} + a_{t-2}x^{t/2-1} + \cdots + a_2x + a_0$, $H_1(x) = H(x)^2$. But then $H_1(x) = H_1(1-x)$ and we can use the above argument to get a contradiction provided that $\deg(G_1(x)) = t/2 \geq 2$. In the remaining case $t = 2$ we have $G(x) = x^2 + a_0$ and so

$$E_n(x) = H(x)^2 + a_0. \tag{2.8}$$

By Theorem 3.2 below on simple zeros of shifted Euler polynomials, (2.8) holds only if $n = 6$. But a simple calculation shows that $E_6(x)$ is not of the form (2.8).

Case 2: *n is odd.* Then k and t are also odd and $G(H(1-x)) = -G(H(x))$. Lemma 2.4 implies $H(1-x) = -H(x)$. Furthermore, Lemma 2.6 and decomposition (2.4) yield

$$2x^n = E_n(x) - E_n(-x) = G(H(x)) - G(H(-x)),$$

from which we deduce that $H(x) - H(-x)$ divides $2x^n$ in $\mathbb{Q}[x]$. Hence, $H(x) - H(-x) = qx^l$ with $q \in \mathbb{Q}$ and $l \leq n$. By expanding $H(x) - H(-x)$ we obtain $l = k$, $q = 2$ and $b_{k-2} = 0$, which together with (2.6) implies $t = 1$ or $k = 0$, contradicting the assumption $k, t \geq 2$. Hence, Euler polynomials with odd index are indecomposable. ∎

3. Finiteness result for $-1^k + 2^k - \cdots + (-1)^x x^k = g(y)$. For the proof of Theorem 1.2 we need some auxiliary results. The first one is a complete ineffective finiteness criterion for diophantine equations of the form $f(x) = g(y)$ which is due to Bilu and Tichy [7].

We say that the equation $f(x) = g(y)$ has *infinitely many rational solutions with bounded denominator* if there exists a positive integer λ such that $f(x) = g(y)$ has infinitely many rational solutions x, y satisfying $\lambda x, \lambda y \in \mathbb{Z}$. Clearly if $f(x) = g(y)$ does not have infinitely many rational solutions with bounded denominator, then it has only finitely many integer solutions.

Theorem 3.1 (Bilu and Tichy, 2000). *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following assertions are equivalent:*

- *The equation $f(x) = g(y)$ has infinitely many rational solutions with bounded denominator.*
- *$f(x) = \varphi(f_1(\lambda(x)))$ and $g(x) = \varphi(g_1(\mu(x)))$, where $\lambda(x)$, $\mu(x) \in \mathbb{Q}[x]$ are some linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with bounded denominator.*

There are five kinds of standard pairs over $\mathbb{Q}$ and they are listed in the following table. Note $a, b \in \mathbb{Q} \setminus \{0\}$, $q, s, t \in \mathbb{N}$, $r \in \mathbb{Z}^+$, $q(x) \in \mathbb{Q}[x] \setminus \{0\}$

and $D_s(x,a)$ is the sth Dickson polynomial defined by

$$D_s(x,a) = \sum_{i=0}^{\lfloor s/2 \rfloor} \frac{s}{s-i}\binom{s-i}{i}(-a)^i x^{s-2i}. \tag{3.1}$$

Kind	Explicit form of (f_1, g_1) or switched pair (g_1, f_1)	Parameter restrictions
first	$(x^t, ax^r q(x)^t)$	$0 \le r < t$, $(r,t) = 1$, $r + \deg q(x) > 0$
second	$(x^2, (ax^2+b)q(x)^2)$	–
third	$(D_s(x,a^t), D_t(x,a^s))$	$(s,t) = 1$
fourth	$(a^{-s/2}D_s(x,a), b^{-t/2}D_t(x,b))$	$(s,t) = 2$
fifth	$((ax^2-1)^3, 3x^4-4x^3)$	–

Now, the theorem of Bilu and Tichy can be summarized as follows: the equation $f(x) = g(y)$ with $f, g \in \mathbb{Q}[x]$ has infinitely many integer solutions x, y if up to certain transformations on the set of polynomials with rational coefficients, the pairs of polynomials (f,g) belong to one of five well understood families.

We will make an extensive use of the following theorem from [15].

THEOREM 3.2 (Rakaczki, 2011). *Let $m \ge 7$ be an integer. Then the shifted Euler polynomial $E_m(x) + b$ has at least three simple zeros for every complex number b.*

The following theorem is a classical effective result of Baker [2] related to hyperelliptic equations.

THEOREM 3.3 (Baker, 1969). *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial having at least three simple roots. Then all the solutions $x, y \in \mathbb{Z}$ of the equation $f(x) = y^2$ satisfy $\max\{|x|, |y|\} \le C$, where C is an effectively computable constant depending only on the coefficients of f.*

For $P(x) \in \mathbb{C}[x]$, a complex number c is said to be an *extremum* if $P(x) - c$ has multiple roots. If $P(x) - c$ has s multiple roots, the *type* of c is the tuple $(\alpha_1, \dots, \alpha_s)$ of multiplicities of its roots in increasing order. Obviously, $s < \deg P$, $(\alpha_1, \dots, \alpha_s) \ne (1, \dots, 1)$ and $\alpha_1 + \cdots + \alpha_s = \deg P$.

The following result concerns Dickson polynomials defined by (3.1). The proof can be found in [5, Proposition 3.3].

THEOREM 3.4. *For $a \ne 0$ and $k \ge 3$, $D_k(x,a)$ has exactly two extrema $\pm 2a^{k/2}$. If k is odd, then both are of type $(1, 2, \dots, 2)$. If k is even, then $2a^{k/2}$ is of type $(1, 1, 2, \dots, 2)$ and $-2a^{k/2}$ is of type $(2, \dots, 2)$.*

What follows is a technical lemma which will be needed in the proof of Theorem 1.2. Everywhere below, $c, u \in \mathbb{Q} \setminus \{0\}$ and $d, v \in \mathbb{Q}$.

LEMMA 3.5. *The polynomial $E_n(cx+d)$ is neither of the form ux^q+v with $q \geq 3$, nor of the form $uD_k(x,a)+v$, where $D_k(x,a)$ is the kth Dickson polynomial with $k>4$ and $a \in \mathbb{Q}\setminus\{0\}$.*

Proof. Suppose that $E_n(cx+d) = ux^q+v$, where $q \geq 3$. Since $\deg E_n(x) = n$ we have $q=n$. The number of roots, as well as the root multiplicities, of an algebraic equation in variable x remain unchanged if we replace x by a linear polynomial in x, so it follows that the polynomial $(E_n(x)-v)' = nE_{n-1}(x)$ has a zero of multiplicity at least $q-1$. This is not possible due to Lemma 2.6(d).

Now assume that $E_n(cx+d) = uD_k(x,a)+v$ and $n \geq 7$. Then

$$k=n \quad \text{and} \quad D_n(x,a) \pm 2a^{n/2} = \frac{1}{u}(E_n(cx+d) - v \pm 2ua^{n/2}).$$

From Theorem 3.2 we infer that $D_n(x,a) \pm 2a^{n/2}$ has at least three simple zeros, contradicting Theorem 3.4. In the cases $n=5$ and $n=6$ a direct calculation shows that $E_n(cx+d)$ cannot be of the form $uD_n(x,a)+v$. We remark that

$$E_4\left(cx+\frac{1}{2}\right) = c^4 D_4\left(x, \frac{3}{8c^2}\right) + \frac{1}{32}. \ \blacksquare$$

Proof of Theorem 1.2. We recall that

$$T_k(n) = -1^k + 2^k - \cdots + (-1)^n n^k = \frac{E_k(0) + (-1)^n E_k(n+1)}{2}. \tag{3.2}$$

Now clearly

$$T_k(2n) = \frac{E_k(0)+E_k(2n+1)}{2} \quad \text{and} \quad T_k(2n-1) = \frac{E_k(0)-E_k(2n)}{2} \tag{3.3}$$

for $k,n \in \mathbb{N}$. Hence we can write (1.2) in the form

$$F_k(x) = g(y), \tag{3.4}$$

where

$$F_k(x) = f(E_k(h(x))) \tag{3.5}$$

with $f(x) = x/2 + E_k(0)/2$ and $h(x) = 2x+1$, or $f(x) = -x/2 + E_k(0)/2$ and $h(x) = 2x$.

We first treat the case when $\deg g = 2$. Then (3.4) transforms into

$$df(E_k(h(x))) = ay^2 + by + c \quad \text{with } a,b,c,d \in \mathbb{Z},\ a,d \neq 0, \tag{3.6}$$

and then simply into

$$uE_k(h(x)) + v = (2ay+b)^2, \tag{3.7}$$

where $u \neq 0$ and v are rational numbers. Combining Theorems 3.3 and 3.2, we infer that (3.7) has only finitely many integer solutions x, y which can be effectively determined, provided that $k \geq 7$.

Now let $\deg g > 2$. Suppose that (3.4) has infinitely many solutions $x \in \mathbb{N}$, $y \in \mathbb{Z}$. Then by Theorem 3.1, there exist $\varphi(x) \in \mathbb{Q}[x]$, linear polynomials $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ and a standard pair $(f_1(x), g_1(x))$ over $\mathbb{Q}$ such that

$$F_k(x) = \varphi(f_1(\lambda(x))) \quad \text{and} \quad g(x) = \varphi(g_1(\mu(x))). \tag{3.8}$$

Since $\deg F_k(x) = k$, from decomposition properties of Euler polynomials (Theorem 1.1) and from (3.5) we see that $\deg \varphi = 1$, $\deg \varphi = k/2$, or $\deg \varphi = k$.

Case 1: $\deg \varphi = k$. Then from (3.8) we get $\deg f_1 = 1$. Therefore $F_k(x) = \varphi(t(x))$, where $t(x) \in \mathbb{Q}[x]$ is a linear polynomial. Hence clearly

$$F_k(t^{-1}(x)) = \varphi(t(t^{-1}(x))) = \varphi(x). \tag{3.9}$$

From (3.5), (3.8) and (3.9) we obtain

$$g(x) = \varphi(g_1(\mu(x))) = F_k(t^{-1}(g_1(\mu(x)))) = f(E_k(p(x))),$$

where $p(x) = h(t^{-1}(g_1(\mu(x)))) \in \mathbb{Q}[x]$. Hence (3.4) may have infinitely many solutions $x \in \mathbb{N}$, $y \in \mathbb{Z}$ only if $g(x) = f(E_k(p(x)))$, where $p(x) = \tau(g_1(\mu(x)))$ with $\tau(x), \mu(x) \in \mathbb{Q}[x]$ linear polynomials and $(f_1(x), g_1(x))$ a standard pair over $\mathbb{Q}$ with $\deg f_1 = 1$. In this particular case, (3.4) is of the form

$$F_k(x) = F_k(p(y)) \quad \text{in integers } x \in \mathbb{N},\ y \in \mathbb{Z}. \tag{3.10}$$

Obviously, if $p(y) \in \mathbb{N}$ for infinitely many integers y, we have infinitely many solutions $x \in \mathbb{N}$, $y \in \mathbb{Z}$ of (3.4). For example, one can take an arbitrary polynomial $p(x) \in \mathbb{Z}^+[x]$.

Case 2: $\deg \varphi = 1$. Let $\varphi(x) = \varphi_1 x + \varphi_0$, where $\varphi_1, \varphi_0 \in \mathbb{Q}$ and $\varphi_1 \neq 0$. From (3.8) it follows that

$$F_k(\lambda^{-1}(x)) = \varphi(f_1(x)) = \varphi_1 f_1(x) + \varphi_0, \tag{3.11}$$

and (3.5) yields

$$f(E_k(h(\lambda^{-1}(x)))) = F_k(\lambda^{-1}(x)) = \varphi_1 f_1(x) + \varphi_0. \tag{3.12}$$

Since $f(x), h(x), \lambda^{-1}(x) \in \mathbb{Q}[x]$ are linear polynomials, we have

$$E_k(cx + d) = u f_1(x) + v \quad \text{for some } c, d, u, v \in \mathbb{Q}, \quad c, u \neq 0. \tag{3.13}$$

Now we study the five types of standard pairs over $\mathbb{Q}$.

First, consider the case when $(f_1(x), g_1(x))$ in (3.8) is a standard pair over $\mathbb{Q}$ of the first kind. From (3.13), either $E_k(cx+d) = ux^t + v$, or $E_k(cx+d) = uax^r q(x)^t + v$, where $0 \leq r < t$, $(r, t) = 1$ and $r + \deg q(x) > 0$. In the former case we get a contradiction by Lemma 3.5 since $k = t \geq 3$. In the latter case, Theorem 3.2 yields $\deg g = t \leq 2$, a contradiction.

Let now $(f_1(x), g_1(x))$ be of the second kind. Then either $E_k(cx + d) = ux^2 + v$, or $E_k(cx+d) = u(ax^2+b)q(x)^2 + v$. The former case is not possible since $k \geq 7$, and the latter since Theorem 3.2 applies.

Next, let $(f_1(x), g_1(x))$ be of the third or fourth kind. Then by (3.13) it follows that

$$E_k(cx+d) = uD_k(x,w) + v, \tag{3.14}$$

where $w = a^t$ or $w = a$. However, from Lemma 3.5 we obtain a contradiction since $k \geq 7$.

Finally, it is easy to see that $(f_1(x), g_1(x))$ cannot be of the fifth kind either because $k \geq 7$.

Case 3: $\deg \varphi = k/2$. Obviously, in this case $k = 2s$ is even and $\deg f_1 = 2$. From (3.5) and (3.8) we see that

$$E_k(x) = f^{-1}(\varphi(f_1(\tau(x)))), \tag{3.15}$$

where $\tau(x) = cx+d$ is a linear polynomial in $\mathbb{Q}[x]$. Since $\deg f_1 = 2$ and $k \geq 7$ we have a nontrivial decomposition of $E_k(x)$ in (3.15). By Theorem 1.1, this decomposition is equivalent to the decomposition $E_k(x) = \widetilde{E}_s((x-1/2)^2)$, so there exists a linear polynomial $u(x) = u_1 x + u_0$ such that

$$\varphi(x) = f(\widetilde{E}_s(u(x))) \quad \text{and} \quad u(f_1(\tau(x))) = (x-1/2)^2, \tag{3.16}$$

which together with (3.8) implies that (3.4) may have infinitely many integer solutions only if

$$g(x) = f(\widetilde{E}_s(q(x))), \quad \text{where} \quad q(x) = u(g_1(\mu(x))). \tag{3.17}$$

Now again we study the five types of standard pairs over $\mathbb{Q}$.

First, consider the case when $(f_1(x), g_1(x))$ is of the first kind. Since $\deg f_1 = 2$, if $f_1(x) = x^t$ we have $(f_1(x), g_1(x)) = (x^2, axq(x)^2)$. From (3.16), we infer that $u(x) = x/c^2$ and

$$g(x) = f\left(\widetilde{E}_s\left(\frac{a\mu(x)q(\mu(x))^2}{c^2}\right)\right), \tag{3.18}$$

which we can write as $g(x) = f(\widetilde{E}_s(\delta(x)p(x)^2))$, where $\delta(x), p(x) \in \mathbb{Q}[x]$ and $\deg \delta(x) = 1$. Now (3.4) turns into

$$f(\widetilde{E}_s((h(x)-1/2)^2)) = f(\widetilde{E}_s(\delta(y)p(y)^2)). \tag{3.19}$$

If $\delta(y)$ is the square of a rational number for infinitely many integers y, and for these y, $\sqrt{\delta(y)}\,p(y) + 1/2$ are all positive even integers or all positive odd integers, then $x = \sqrt{\delta(y)}\,p(y)/2 \pm 1/4$, y are solutions of (3.4), respectively. For example, let $\delta(x) = x$, $r(x)$ be a polynomial which takes a positive odd integer value for every $x \in \mathbb{N}$ and $p(x) = r(x) - 1/2$. Then for every positive integer k the pairs of integers $x = ((4k+3)r((4k+3)^2) - 2k - 1)/2$, $y = (4k+3)^2$ and $x = ((4k+1)r((4k+1)^2) - 2k - 1)/2$, $y = (4k+1)^2$ are solutions of (3.4).

Since $0 \le r < t$, $(r,t) = 1$ and $r + \deg q(x) > 0$, if the two components are switched, that is, when $(f_1(x), g_1(x)) = (ax^r q(x)^t, x^t)$, there are two possibilities: either

(i) $r = 0$, $t = 1$ and $\deg q(x) = 2$, or
(ii) $r = 2$, $t \ge 3$ odd and $q(x)$ is a constant polynomial.

In the former case, we have $g_1(x) = x$ and thus

$$g(x) = f(\widetilde{E}_s(u(\mu(x)))) = f(\widetilde{E}_s(\delta(x)p(x)^2)) \quad \text{with } p(x) \equiv 1. \tag{3.20}$$

In the latter case, from (3.16) we deduce that $f_1(x) = bx^2$ and $u(x) = x/(bc^2)$, where $b \in \mathbb{Q} \setminus \{0\}$. Then

$$g(x) = f\left(\widetilde{E}_s\left(\frac{(\mu(x))^t}{bc^2}\right)\right) = f(\widetilde{E}_s(\gamma\delta(x)^t)), \tag{3.21}$$

where $\gamma = 1/(bc^2)$, $\delta(x) = \mu(x)$. Now (3.4) is of the form

$$f(\widetilde{E}_s((h(x) - 1/2)^2)) = f(\widetilde{E}_s(\gamma\delta(y)^t)). \tag{3.22}$$

If there are infinitely many integers y for which $\sqrt{\gamma\delta(y)^t} + 1/2$ are all positive even integers or all positive odd integers, then $x = \sqrt{\gamma\delta(y)^t}/2 \pm 1/4$, y are solutions of (3.4), respectively. For example, let $\gamma = 1/4$, $\delta(x) = x$, $t \ge 3$ odd. Then, for $k \in \mathbb{N}$, the pairs of integers $x = ((4k-1)^t + 1)/4$, $y = (4k-1)^2$ and $x = ((4k+1)^t - 1)/4$, $y = (4k+1)^2$ are solutions of (3.22).

Next suppose that $(f_1(x), g_1(x))$ in (3.8) is of the second kind. If $f_1(x) = (ax^2 + b)q(x)^2$, then $g_1(x) = x^2$ and $q(x)$ is a constant polynomial. Hence

$$g(x) = f(\widetilde{E}_s(u_1\mu(x)^2 + u_0)) = f(\widetilde{E}_s((a\delta(x)^2 + b)p(x)^2)) \tag{3.23}$$

with $a = u_1$, $b = u_0$, $\delta(x) = \mu(x)$ and $p(x) \equiv 1$. When $f_1(x) = x^2$ an easy calculation shows that $u(x) = x/c^2$ and

$$g(x) = f\left(\widetilde{E}_s\left(\frac{(a\mu(x)^2 + b)q(\mu(x))^2}{c^2}\right)\right) = f(\widetilde{E}_s((a\delta(x)^2 + b)p(x)^2)), \tag{3.24}$$

where $p(x) = q(\mu(x))/c$ and $\delta(x) = \mu(x)$. Then (3.4) is of the form

$$f(\widetilde{E}_s((h(x) - 1/2)^2)) = f(\widetilde{E}_s((a\delta(y)^2 + b)p(y)^2)). \tag{3.25}$$

Let $\delta(x) = x$, $r(x)$ be a positive integer valued polynomial and $p(x) = 4r(x) + 1$. Let $a = 1/2$, $b = 1/4$. Then (3.25) has infinitely many integer solutions

$$x = \frac{a_{2n+1}(4r(y)+1)+1}{4},\ y = b_{2n+1}; \quad x = \frac{a_{2n}(4r(y)+1)-1}{4},\ y = b_{2n},$$

respectively, where a_n and b_n are defined by

$$a_n + b_n\sqrt{2} = (3 + 2\sqrt{2})^n,$$

that is,

$$(a_1, b_1) = (3, 2), \quad (a_{n+1}, b_{n+1}) = (3a_n + 4b_n, 2a_n + 3b_n), \quad n \in \mathbb{N}.$$

Let now $(f_1(x), g_1(x))$ be of the third kind. In this case $(f_1(x), g_1(x)) = (D_2(x, a^t), D_t(x, a^2))$ with odd t. Substituting $f_1(x) = D_2(x, a^t) = x^2 - 2a^t$ into (3.16), we obtain $u(x) = (x + 2a^t)/c^2$. Hence

$$g(x) = f\left(\widetilde{E}_s\left(\frac{D_t(\mu(x), a^2) + 2a^t}{c^2}\right)\right). \tag{3.26}$$

From Theorem 3.4 we know that the polynomial $D_t(\mu(x), a^2)/c^2$ has exactly two extrema and those are $\pm 2a^t/c^2$. Since t is odd, both extrema are of the type $(1, 2, \ldots, 2)$. We deduce

$$g(x) = f(\widetilde{E}_s(\delta(x)p(x)^2)),$$

where $\delta(x), p(x) \in \mathbb{Q}[x]$ with $\deg \delta(x) = 1$.

Finally, let $(f_1(x), g_1(x))$ be of the fourth kind. Then $(f_1(x), g_1(x)) = (a^{-1}D_2(x, a), b^{-t/2}D_t(x, b))$ with t even. Using again (3.16), one can deduce that $u(x) = (ax + 2a)/c^2$ and so

$$g(x) = f(\widetilde{E}_s(u(g_1(\mu(x))))) = f\left(\widetilde{E}_s\left(\frac{ab^{-t/2}D_t(\mu(x), b) + 2a}{c^2}\right)\right). \tag{3.27}$$

Now, the extrema of the polynomial $ab^{-t/2}D_t(\mu(x), b)/c^2$ are $\pm 2b^{t/2}ab^{-t/2}/c^2 = \pm 2a/c^2$, and the extremum $-2a/c^2$ is of the type $(2, \ldots, 2)$ by Theorem 3.4. Therefore

$$g(x) = f(\widetilde{E}_s(p(x)^2)),$$

where $p(x) \in \mathbb{Q}[x]$. Let $r(x)$ be a positive integer valued polynomial and $p(x) = 2r(x) \mp 1/2$. It is easy to see that the equation

$$f(\widetilde{E}_s((h(x) - 1/2)^2)) = f(\widetilde{E}_s(p(x)^2)) \tag{3.28}$$

has infinitely many integer solutions, for example $(x, y) = (r(k), k)$, where $k \in \mathbb{N}$. Since $\deg f_1 = 2$, clearly $(f_1(x), g_1(x))$ cannot be of the fifth kind. ∎

Acknowledgements. The first-named author was supported by the Austrian Science Fund (FWF): W1230-N13 and NAWI Graz. The second-named author was supported, in part, by the Hungarian Academy of Sciences under OTKA Grant K75566 and the Project TAMOP-4.2.1.B-10/2/KONV-2010-0001, which was supported by the European Union and co-financed by the European Social Fund.

References

[1] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*, Dover, New York, 1972.

[2] A. Baker, *Bounds for solutions of hyperelliptic equations*, Proc. Cambridge Philos. Soc. 65 (1969), 439–444.

[3] A. Bazsó, D. Kreso, F. Luca and Á. Pintér, *On equal values of power sums of arithmetic progressions*, Glas. Mat. 47 (2012), 253–263.
[4] M. A. Bennett, *A superelliptic equation involving alternating sums of powers*, Publ. Math. Debrecen 79 (2011), 317–324.
[5] Y. F. Bilu, *Quadratic factors of $f(x) - g(y)$*, Acta Arith. 90 (1999), 341–355.
[6] Y. F. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér and R. F. Tichy (with an appendix by A. Schinzel), *Diophantine equations and Bernoulli polynomials*, Compos. Math. 131 (2002), 173–188.
[7] Y. F. Bilu and R. F. Tichy, *The diophantine equation $f(x) = g(y)$*, Acta Arith. 95 (2000), 261–288.
[8] J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angew. Math. 234 (1969), 45–64.
[9] K. Dilcher, *On a Diophantine equation involving quadratic characters*, Compos. Math. 57 (1986), 383–403.
[10] F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra 28 (1974), 88–101.
[11] H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. 63 (1941), 249–255.
[12] M. Fried, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. 264 (1973), 40–55.
[13] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. 64 (1942), 389–400.
[14] Cs. Rakaczki, *On the Diophantine equation $S_m(x) = g(y)$*, Publ. Math. Debrecen 65 (2004), 439–460.
[15] Cs. Rakaczki, *On the simple zeros of shifted Euler polynomials*, Publ. Math. Debrecen 79 (2011), 623–636.
[16] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), 51–56; Erratum: ibid., 23 (1922), 431.
[17] J. J. Schäffer, *The equation $1^p + 2^p + 3^p + \cdots + n^p = m^q$*, Acta Math. 95 (1956), 155–189.
[18] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge Univ. Press, 2004.
[19] B. Wyman and M. Zieve, *Two questions on polynomial decomposition*, Quart. J. Math. Oxford 63 (2012), 507–511.

Dijana Kreso
Institut für Analysis und
Computational Number Theory (Math A)
Technische Universität Graz
Steyrergasse 30/II
8010 Graz, Austria
E-mail: kreso@math.tugraz.at

Csaba Rakaczki
Institute of Mathematics
University of Miskolc
H-3515 Miskolc Campus, Hungary
E-mail: matrcs@uni-miskolc.hu

Received on 25.10.2012
and in revised form on 15.4.2013 (7243)