Publ. Math. Debrecen
79/3-4 (2011), 623–636
DOI: 10.5486/PMD.2011.5035

On the simple zeros of shifted Euler polynomials

By CSABA RAKACZKI (Miskolc)

Dedicated to Professor K. Győry on the occasion of his 70th birthday

Abstract. In this paper we prove that the shifted Euler polynomial $E_n(x) + b$ ($n \geq 7$) has always three simple zeros for arbitrary non-zero complex number b.

1. Introduction

The investigation of integer and rational solutions of polynomial equations in two unknowns plays a central role in the theory of diophantine equations. The so-called superelliptic equations constitute a very important class of equations from the point of view of applications. These equations are of the form

$$f(x) = dy^n, \tag{1}$$

where $f(x)$ is a polynomial with integral coefficients, $d \neq 0$ and $n \geq 2$ are given integers and x, y are unknown integers. If $n = 2$ then equation (1) is called hyperelliptic equation. After the results of Mordell, Siegel and others, in 1964 LeVeque [4] gave a finiteness criteria for the number of solutions of equation (1). His result is ineffective in the sense that the proof does not provide any algorithm to find the solutions. In 1969 A. Baker [1] gave effective estimates for linear forms in logarithms of algebraic numbers. Using his estimates Baker was the first to give an effective upper bound for the size of the solutions of equation (1) in

Mathematics Subject Classification: 11D41, 11B68.
Key words and phrases: Euler polynomials, higher degree equations.
The author was supported, in part, by Grants K75566 and F68872 from HNFSR, and by the Hungarian Academy of Sciences.

the case when the polynomial $f(x)$ has at least three simple zeros. Later, this result was generalized by Brindza, who also gave an effective version of LeVeque's result. The theorem of Brindza [3] is the following:

Theorem (Brindza (1984))**.** *Let*

$$f(x) = a_0x^N + \cdots + a_N = a_0 \prod_{i=1}^{m} (x - \alpha_i)^{r_i}$$

be a polynomial in $\mathbb{Z}[x]$ *with* $a_0 \neq 0$ *and* $\alpha_i \neq \alpha_j$ *for* $i \neq j$*. Further, let* $d \neq 0$*,* $n > 1$ *be integers and* $q_i = n/(n, r_i)$*,* $i = 1, 2, \ldots, m$*. Suppose that* $(q_1, q_2, \ldots, q_m)$ *is not a permutation of* $(q, 1, \ldots, 1)$ *or* $(2, 2, 1, \ldots, 1)$*, where* $q \geq 1$*. Then the superelliptic equation*

$$f(x) = dy^n \quad \text{in } x, y \in \mathbb{Z}$$

has only finitely many solutions and all these can be effectively determined.

An easy consequence of this result is that the hyperelliptic equation $f(x) = dy^2$ has only finitely many effectively computable integer solutions x, y provided that the polynomial $f(x)$ has at least three zeros with odd multiplicities.

In this paper we investigate the simple zeros of the shifted Euler polynomial $E_n(x) + b$, where $b \in \mathbb{C}$ and the n-th Euler polynomial $E_n(x)$ is defined by the following generating series:

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

The Euler polynomials are closely connected with the alternating sums of powers of consecutive integers. More precisely, the alternating power sums $T_k(n) = \sum_{r=0}^{n} (-1)^r r^k = -1^k + 2^k - 3^k + \cdots + (-1)^n n^k$ can be expressed in the following way:

$$T_k(n) = \frac{E_k(0) + (-1)^n E_k(n+1)}{2}, \quad k \in \mathbb{N}.$$

Theorem 1. *Let* $n \geq 7$ *be an integer and* $b \in \mathbb{C}$*. Then the shifted Euler polynomial* $E_n(x) + b$ *has at least three simple zeros.*

We remark that $E_6(x) - 1 = (x^2 - x - 1)^3$. Combining our theorem with the result of Brindza we can deduce the next effective result.

Theorem 2. *Let* $F(x) \in \mathbb{Q}[x]$ *be a polynomial with at least one root of odd multiplicity. Then the hyperelliptic equation*

$$F(E_n(x)) = y^2 \tag{2}$$

has only finitely many integer solutions x*,* y *which can be effectively determined, provided that* $n \geq 7$*.*

2. Auxiliary results

The Euler numbers E_n may be defined by the generating function:

$$\frac{2e^{t/2}}{e^t+1} = \sum_{n=0}^{\infty} \frac{E_n}{n!} \left(\frac{t}{2}\right)^n.$$

In the first lemma we list some properties of Euler polynomials which will be often used in the text, sometimes without special reference.

Lemma 1.

(i) $E_n(x) = (-1)^n E_n(1-x)$;

(ii) $E_n'(x) = nE_{n-1}(x)$;

(iii) *the rational roots of* $E_{2n}(x)$ *are* 0 *and* 1*;*

(iv) *the only rational root of* $E_{2n-1}(x)$ *is* $\frac{1}{2}$*;*

(v) $E_{2m}(x) \in \mathbb{Z}[x]$ *and is monic;*

(vi) $E_n(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{E_k}{2^k} \left(x - \frac{1}{2}\right)^{n-k}$*;*

(vii) $E_5(x)$ *is the only Euler polynomial with a multiple root.*

Proof. See [2]. □

The first property is a symmetry property. The second shows that the Euler polynomials form an Appell sequence. The next two state that the Euler polynomials have no rational root other than 0, 1 and 1/2. From (v) we know that an Euler polynomial of degree even has integer coefficients. Finally, we can see that the Euler polynomials have only simple zeros and they can be written as polynomial in $(x-1/2)$ as in (vi), where $E_k \in \mathbb{Z}$ is the Euler number, $E_0 = 1$, $E_2 = -1$, $E_4 = 5, \ldots$; $E_{2m+1} = 0$, $m \geq 0$. The Euler numbers have extensive application in combinatorial mathematics. Thus many mathematicians have investigated their arithmetic properties. Here we give some useful properties.

Lemma 2. *For any* $k \in \mathbb{N}$ *and* $q \in \mathbb{Z}^+$

$$E_k \equiv \sum_{j=0}^{q-1} (-1)^j (2j+1)^k \pmod{q} \text{ providing } q \nmid 2.$$

Proof. See e.g. [11]. □

Lemma 3. $(-1)^m E_{2m} > 2^{2m+2}$ *for* $m \geq 4$.

Proof. See e.g. [2]. □

Lemma 4. *The following inequalities are satisfied for arbitrary positive integer k.*

$(*)$ $2^{4k}E_{4k}\left(\frac{5}{2}\right) - E_{4k} > 0,$

$(**)$ $2^{4k}E_{4k}(2) - E_{4k} < 0.$

PROOF.

$$\begin{aligned} 2^{4k}E_{4k}\left(\frac{5}{2}\right) - E_{4k} &= 2^{4k}\left(E_{4k}\left(\frac{5}{2}\right) - E_{4k}\left(\frac{1}{2}\right)\right) \\ &= 2^{4k}\left(E_{4k}\left(\frac{5}{2}\right) + E_{4k}\left(\frac{3}{2}\right) - E_{4k}\left(\frac{3}{2}\right) - E_{4k}\left(\frac{1}{2}\right)\right) \\ &= 2^{4k}\left(2\left(\frac{3}{2}\right)^{4k} - 2\left(\frac{1}{2}\right)^{4k}\right) > 0, \qquad (*) \end{aligned}$$

where in the last equality we use the well-known identity (see e.g. [2]): $E_n(x+1) + E_n(x) = 2x^n$, $n \geq 0$. Using $E_{4k}(2) = 2$ and Lemma 3 we get

$$2^{4k}E_{4k}(2) - E_{4k} = 2^{4k+1} - E_{4k} < 2^{4k+1} - 2^{4k+2} < 0. \qquad (**)$$

□

The next lemma is a slightly modified version of a result of BRILLHART [2].

Lemma 5. *$E_{2m}(x) + 2t$ has no multiple roots, $m \geq 1$, $t \in \mathbb{Z}$.*

PROOF. To prove the assertion one can repeat Brillhart's argument with a slight modification. However, for the convenience of the reader we give the full proof here.

We will show that the polynomials $E_{2m}(x) + 2t$ and $E'_{2m}(x)$ are relatively prime. Using the properties of Euler polynomials we have

$$E_{2m}(x) + 2t + xE'_{2m}(x) = (x(E_{2m}(x) + 2t))' \equiv x^{2m} \pmod 2. \qquad (3)$$

Let $d(x)$ be the integral coefficient greatest common divisor of $E_{2m}(x) + 2t$ and $E'_{2m}(x)$, and let $d(x) \equiv d^*(x) \pmod 2$, where the coefficients of $d^*(x)$ are 0 or 1. Then, since $d(x)$ divides the left side of (3), $d^*(x)|x^{2m}$. But then $d^*(x)$ is a power of x by uniqueness of factorization $\pmod 2$. Now $d^*(x)|E'_{2m}(x) \pmod 2$, and since $E'_{2m}(0) \equiv 1 \pmod 2$, $d^*(x) = 1$. But $d(x)$ is monic, being a divisor of $E_{2m}(x) + 2t$. Thus, $d(x) = 1$. □

A polynomial $F(x)$ with complex coefficients will be called *non-degenerate* if it has at least three zeros of odd multiplicities and *degenerate* otherwise.

For $n > 1$, L_n denotes the cardinality of the set of non-zero complex numbers b for which the shifted Euler polynomial $E_n(x) + b$ is degenerate. In 2008 we proved [10] that there is at most one complex number for which the shifted Euler polynomial is degenerate.

Lemma 6 (Rakaczki (2008))**.** *We have $L_3 = L_4 = 2$. Further, if $n \geq 5$ is an odd positive integer then $L_n = 0$ while in case when $n \geq 6$ is even then $L_n \leq 1$.*

In the same paper we proved the following result.

Lemma 7. *If b is a non-zero complex number for which the polynomial $E_{2m}(x) + b$ is of the form $g(x)f(x)^2$, where $g(x), f(x) \in \mathbb{C}[x]$ are monic, $\deg(g(x)) = 2$, then $g(x) = x^2 - x + c$ for some complex number c. Further, $f(1-x) = (-1)^{m-1} f(x)$ for $m \geq 3$.*

In 1913, S. Ramanujan [8], [9] asked whether there were other solutions to the diophantine equation

$$x^2 + 7 = 2^n,$$

sometimes called the Ramanujan–Nagell equation, besides the known ones, namely, $n = 3$, 4, 5, 7, and 15. These correspond to $x = 1$, 3, 5, 11, and 181. This problem was again posed by W. Ljunggren [5] in 1943. It was first solved by T. Nagell [6], [7], who showed that the above mentioned are the only five solutions, thus establishing Ramanujan's question in the negative.

Lemma 8 (Nagell)**.** *All positive integer solutions x, n of the equation*

$$x^2 + 7 = 2^n \tag{4}$$

are

$$(n, x) = (3, 1),\ (4, 3),\ (5, 5), (7, 11) \text{ and } (15, 181).$$

3. Proofs

Proof of Theorem 1. Since $(E_n(x) + b)' = nE_{n-1}(x)$, the polynomial $E_n(x) + b$ ($n \geq 7$) may have zeros of multiplicity at most 2 by (vii). In case when n is odd the assertion of our result follows from Lemma 6. Now suppose that $n = 2m$ is even and there exists a complex number b for which the shifted Euler polynomial of even degree does not have three simple zeros. Then there are two possibilities. The first one is that the shifted polynomial is a square polynomial, the second is that it is a square polynomial multiplied by a quadratic polynomial:

(a) $E_{2m}(x)+b=F(x)^2$,

(b) $E_{2m}(x)+b=G(x)F(x)^2$,

where $F(x), G(x) \in \mathbb{C}[x]$ and $\deg(G(x))=2$. It is not too hard to see that in both cases the greatest common divisor of the shifted polynomial $E_{2m}(x)+b$ and its derivative is the polynomial $F(x)$ whose degree is m or $m-1$. The following equations come from the euclidean algorithm:

$$\begin{aligned}
&E_{2m}(x)+b=(x-1/2)E_{2m-1}(x)+s_1(x)\\
&E_{2m-1}(x)=t_1(x)s_1(x)+s_2(x)\\
&s_1(x)=t_2(x)s_2(x)+s_3(x)\\
&\quad\vdots\\
&s_{k-3}(x)=t_{k-2}(x)s_{k-2}(x)+s_{k-1}(x)\\
&s_{k-2}(x)=t_{k-1}(x)s_{k-1}(x)+s_k(x)\\
&s_{k-1}(x)=t_k(x)s_k(x)+s_{k+1}(x)
\end{aligned}$$

Take b as a parameter. In $s_1(x)$ x^0 is the largest power whose coefficient depends on the parameter b. Let $s_k(x)$ be the first polynomial whose the leading coefficient depends on b. It follows from the algorithm that the coefficients of the polynomials $t_1(x)$, $t_2(x), \dots, t_{k-1}(x)$ do not depend on the parameter b. Indeed, if the coefficients of $t_1(x)$ depend on b then one of the coefficients of $E_{2m-1}(x)$ also depends on b which is not possible. Suppose that we have already proved that the polynomials $t_1(x), t_2(x), \dots, t_{i-1}(x)$ do not depend on b for some $i \in \{2, \dots, k-1\}$. Let t_i and s_i denote the degrees of polynomials $t_i(x)$ and $s_i(x)$, respectively. Then in $s_1(x)$, x^0, in $s_2(x)$, x^{t_1}, in $s_i(x)$, $x^{t_1+\dots+t_{i-1}}$ is the largest power whose coefficient depends on the parameter b. Assume that $t_i(x)$ depends on b. Since $s_{i+1} < s_i$ by the euclidean algorithm we get that the coefficient of x^{s_i+j} depends on b in $s_{i-1}(x)$. Here j denotes the largest exponent for which the coefficient of the power x^j depends on b in $t_i(x)$. But in $s_{i-1}(x)$, $x^{t_1+\dots+t_{i-2}}$ is the largest power which depends on b. We get from the above that

$$t_1+\dots+t_{i-2} \geq s_i+j \geq s_i \geq s_{k-1}.$$

Since the leading coefficient of $s_{k-1}(x)$ does not depend on b, it is obvious that $s_{k-1} \geq \deg(\gcd(E_{2m}(x)+b, E_{2m-1}(x))) \geq m-1$.

Comparing the degrees of polynomials of the algorithm we obtain that

$$2m = 1+\sum_{j=1}^{i-2} t_j + s_{i-2} \geq 1+s_i+s_{i-2} \geq 3+2s_i \geq 3+2(m-1) = 2m+1.$$

This contradiction shows that $t_i(x)$ does not depend on b for $i = 1, 2, \ldots, k-1$. Hence we have that every coefficient of the polynomials $s_1(x), \ldots, s_k(x)$ is of the form $u + vb$, where u, v are rational numbers, and

$$s_k = t_1 + \cdots + t_{k-1}.$$

In case $s_k(x) \equiv 0$ we have that all coefficients $u+vb$ of $s_k(x)$ are zero. This means that b must be a rational number.

If $s_k(x) \not\equiv 0$ then

$$2m = 1 + t_1 + \cdots + t_{k-1} + t_k + s_k \geq 2 + 2s_k, \text{ that is } m - 1 \geq s_k. \tag{5}$$

From (5) we obtain that $s_k = m - 1$ and $s_{k+1}(x)$ must be identically zero polynomial for some parameter b since otherwise the degree of the greatest common divisor would be less than $m - 1$. Comparing again the degrees of polynomials of the euclidean algorithm we can deduce that

$$2m = 1 + t_1 + \cdots + t_{k-1} + s_{k-1} = 1 + s_k + s_{k-1} = 1 + (m-1) + s_{k-1} \tag{6}$$

and

$$s_{k-1} = t_k s_k. \tag{7}$$

It follows from (6) and (7) that $s_{k-1} = m$, $t_k = 1$ and the coefficient of x^{m-1} in $s_{k-1}(x)$ does not depend on b because otherwise $t_1 + \cdots + t_{k-2} = m - 1 = s_k = t_1 + \cdots + t_{k-1}$. Thus we get that

$$s_{k-1}(x) = u_m x^m + u_{m-1} x^{m-1} + \sum_{i=0}^{m-2} (u_i + v_i b) x^i$$

and

$$s_k(x) = \sum_{j=0}^{m-1} (U_j + V_j b) x^j,$$

where $u_m \neq 0$, u_{m-1}, u_i, v_i, U_j, V_j are rational numbers for $i = 0, \ldots, m-2$, $j = 0, \ldots, m-1$. The remainder when $s_{k-1}(x)$ is divided by $s_k(x)$ is of the from

$$s_{k+1}(x) = \sum_{i=0}^{m-2} \frac{h_i(b)}{(U_{m-1} + V_{m-1} b)^2} x^i,$$

where $h_i(x) \in \mathbb{Q}[x]$ are not all identically zero polynomials of degree at most 3 for $i = 0, \ldots, m-2$. If $s_{k+1}(x)$ is identically zero polynomial for some complex number b then b is a root of all polynomials $h_i(x)$, $i = 0, \ldots, m-2$. But if b is

not rational then any algebraic conjugate of b is also a root of polynomials $h_i(x)$. This means that in this case there are at least two complex numbers, b and its algebraic conjugate, for which the shifted Euler polynomials have no three zeros with odd multiplicities. However, this is not possible by Lemma 6. Thus we get that b must be rational.

From now we suppose that $b = \frac{p}{q}$, $p,\ q \neq 0 \in \mathbb{Z}$, $\gcd(p,q) = 1$. From (v), (ii) of Lemma 1 we know that $E_{2m}(x) = x^{2m} + a_{2m-1}x^{2m-1} + \cdots + a_1 x \in \mathbb{Z}[x]$ is a polynomial with integer coefficients and $E'_{2m}(x) = 2mE_{2m-1}(x)$. Further, from (vi) we can see that the denominators of the coefficients of $E_{2m-1}(x)$ are powers of two. If we write the integer $2m$ as a product of a power of two 2^t and an odd integer r ($2m = 2^t r$) then from the previous observation we obtain that $2^t E_{2m-1}(x) = \sum_{i=0}^{2m-1} c_i x^i$ is also a polynomial with integer coefficients. Since $E_{2m}(x) + b$ has multiple roots the resultant of the polynomials $E_{2m}(x) + b$ and $2^t E_{2m-1}(x)$ is zero. This resultant is equal to the following determinant of order $4m - 1$:

$$\operatorname{Res}\left(E_{2m}(x) + b, 2^t E_{2m-1}(x)\right)$$

$$= \begin{vmatrix}
1 & a_{2m-1} & a_{2m-2} & \dots & a_2 & a_1 & b & 0 & 0 & \dots & 0 \\
0 & 1 & a_{2m-1} & \dots & a_3 & a_2 & a_1 & b & 0 & \dots & 0 \\
\vdots & & & & & & & & & \vdots & \\
0 & 0 & 0 & \dots & 1 & a_{2m-1} & a_{2m-2} & a_{2m-3} & & \dots & b \\
2^t & c_{2m-2} & c_{2m-3} & \dots & c_1 & c_0 & 0 & 0 & & \dots & 0 \\
0 & 2^t & c_{2m-2} & \dots & c_2 & c_1 & c_0 & 0 & & \dots & 0 \\
0 & 0 & 2^t & \dots & c_3 & c_2 & c_1 & c_0 & & \dots & 0 \\
\vdots & & & & & & & & & \vdots & \\
0 & 0 & 0 & \dots & 0 & 2^t & c_{2m-2} & c_{2m-3} & & \dots & c_0
\end{vmatrix}.$$

The above determinant is a polynomial in b with integer coefficients of degree $2m - 1$ and leading coefficient 2^{2tm}. Since the rational number b is a root of this polynomial, the denominator q of b satisfies

$$q | 2^{2tm}, \tag{8}$$

that is q is a power of two.

After this we turn to the investigation of case (a). We have that $E_{2m}(x) + b$ is a square polynomial. We can assume that

$$qE_{2m}(x) + p = f(x)^2 = b_{2m}x^{2m} + \cdots + b_1 x + b_0 \tag{9}$$

is a square of a primitive polynomial $f(x) = d_m x^m + \cdots + d_1 x + d_0$. The polynomial $f(x) \in \mathbb{Z}[x]$ is called primitive if the greatest common divisor of its coefficients is 1. The Euler polynomial $E_{2m}(x)$ can be given explicitly about the origin as

$$E_{2m}(x) = \sum_{k=0}^{2m} \binom{2m}{k} E_k(0) x^{2m-k}. \tag{10}$$

Using the fact that 0 is a root of any Euler polynomial of degree even (cf. (iii)) we can deduce from (9) and (10) that

$$0 = b_{2i} = d_i^2 + 2d_{2i}d_0 + \cdots + 2d_{i+1}d_{i-1}, \quad m-1 \geq i \geq 1,$$

hence we get that $d_1, d_2, \ldots, d_{m-1}$ are even integers. If $q = 1$ then $d_m = \pm 1$. Further, from the above and Lemma 5 we have that $p \equiv d_0 \equiv 1 \pmod 2$,

$$f(1) = d_m + d_{m-1} + \cdots + d_0 \equiv d_m + d_0 \equiv 0 \pmod 2$$

and

$$(f(1))^2 = E_{2m}(1) + p = p \equiv 1 \pmod 2$$

which is a contradiction. This means that $q > 1$.

Next we study the case when q is not 1. It is obvious from (9) that $q = 2^k$ is a power of two with even exponent k. Since p and q are coprime we know that p is an odd integer. From the fact that an Euler polynomial of degree even is a polynomial with integer coefficient we obtain from (9) that

$$2^k | b_{2m}, b_{2m-1}, \ldots, b_1.$$

Since $p = d_0^2 \equiv 1 \pmod 2$ and $2^k | b_1 = 2d_0 d_1$ one can see that $2^{k-1} | d_1$. Suppose that we have shown that

$$2^{k-1} | d_1, \ldots, d_i \quad \text{for some } i \in \{1, 2, \ldots, m-1\}.$$

From the observation that

$$b_{i+1} = \begin{cases} 2d_{i+1}d_0 + 2d_i d_1 + \cdots + 2d_{\frac{i+2}{2}} d_{\frac{i}{2}}, & \text{if } i \text{ even}, \\ 2d_{i+1}d_0 + 2d_i d_1 + \cdots + 2d_{\frac{i+3}{2}} d_{\frac{i-1}{2}} + d_{\frac{i+1}{2}}^2, & \text{if } i \text{ odd}, \end{cases} \tag{11}$$

we can deduce that $2^{k-1} | d_{i+1}$ too. But $d_m = \pm\sqrt{q} = \pm 2^{k/2}$, thus $k \leq 2$.

After this we have to investigate only one remaining case, namely when $q = 4$ and p is odd. Substitute $x = 0$, 2 and 3 into the equality

$$4E_{2m}(x) + p = f(x)^2$$

and use that $E_{2m}(2) = 2$ and $E_{2m}(3) = 2(2^{2m} - 1)$. We can infer that $p = f(0)^2$ is a square, $8 + f(0)^2 = f(2)^2$ and $8(2^{2m} - 1) + p = f(3)^2$. From the last two equations we have that $p = f(0)^2 = 1$ and

$$2^{2m+3} = f(3)^2 + 7. \tag{12}$$

Applying now Lemma 8 to equation (12) one can compute that $n = 2m \leq 12$. In the cases $2m = 6$, 8, 10 and 12 we can check directly that $4E_{2m}(x) + p$ is not a square polynomial.

Next consider the case (b). We would like to prove that if $b = p/q$ is a rational number, where $q > 0, p \in \mathbb{Z}, (p, q) = 1$, then the shifted Euler polynomial $E_{2m}(x) + b$ is not of the form

$$E_{2m}(x) + b = G(x)F(x)^2. \tag{b}$$

Assume that (b) is true for some monic polynomials $G(x), F(x) \in \mathbb{C}[x]$. Since b is rational we have that $G(x), F(x) \in \mathbb{Q}[x]$. Further, we know from Lemma 7 that $G(x) = x^2 - x + u/v$, where $v > 0, u \in \mathbb{Z}$, $(u, v) = 1$, and if m is even then $F(1/2) = 0$ so in this case $b = -E_{2m}(1/2) = -E_{2m}/2^{2m}$. If m is odd then we have $q|2^{2m}$ by (8). Thus, $q = 2^k$ for $0 \leq k \leq 2m$.

Every polynomial with rational coefficients can be written uniquely as a product of a rational number and a primitive polynomial. Hence we can assume that

$$2^k E_{2m}(x) + p = (vx^2 - vx + u)f(x)^2 = (vx^2 - vx + u) \sum_{i=0}^{2m-2} b_i x^i, \tag{13}$$

where $f(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a primitive polynomial. Let c_i denote the coefficient of the power x^i on the right side. Then

$$c_i = \begin{cases} vb_{2m-2}, & \text{if } i = 2m \\ -vb_{2m-2} + vb_{2m-3}, & \text{if } i = 2m-1 \\ ub_i - vb_{i-1} + vb_{i-2}, & \text{if } 2 \leq i \leq 2m-2 \\ ub_1 - vb_0, & \text{if } i = 1 \\ ub_0, & \text{if } i = 0. \end{cases} \tag{14}$$

From (13) we get that $2^k = vb_{2m-2}$ and so $v|2^k$. It is easy to see that 2^k divides all coefficients on the left side of (13) except the constant term. This means that

$$2^k|c_1, c_2, \ldots, c_{2m},$$

hence $v|(ub_i - vb_{i-1} + vb_{i-2})$ for $i = 2, \ldots, 2m-2$ and $v|(ub_1 - vb_0)$. That is,

$$v|b_1, \ldots, b_{2m-2}. \tag{15}$$

Suppose that we have inductively proved that

$$v^j|b_{2j-1}, b_{2j} \ldots, b_{2m-2} \quad \text{for some } j \in \{1, 2, \ldots, m-2\}. \tag{16}$$

Since $2^k = vb_{2m-2}$ and $v^j|b_{2m-2}$ we obtain that $v^{j+1}|2^k$. But we know that $2^k|c_i = ub_i - vb_{i-1} + vb_{i-2}$ when $2 \le i \le 2m-2$, hence using (16) we can deduce that

$$v^{j+1}|b_{2j+1}, b_{2j+2}, \ldots, b_{2m-2}$$

and so $v^{m-1}|b_{2m-2}$. From $2^k = vb_{2m-2}$ we get that $v^m|2^k$. As $v > 0$ and $k \le 2m$ it is obvious that $v \in \{1, 2, 4\}$. It follows from the above that we have to investigate the next three remaining cases:

(b1) $v = 1$ and $0 \le k \le 2m$,

(b2) $v = 2$ and $m \le k \le 2m$,

(b3) $v = 4$ and $k = 2m$.

Case (b1): First assume that $v = 1$ and $1 \le k$. Applying (14) and (13) we can infer that

$$2|b_{2m-2}, b_{2m-3}, \ldots, b_1, b_0.$$

But this contradicts our observation that $f(x)^2$ is a primitive polynomial, that is the greatest common divisor of its coefficients is 1. Now suppose that $v = 1$ and $k = 0$. Then p is odd by Lemma 5. Now we can write equation (13) in the form

$$\begin{aligned} E_{2m}(x) + p &= (x^2 - x + u)(x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0)^2 \\ &= (x^2 - x + u)\sum_{i=0}^{2m-2} b_i x^i. \end{aligned} \tag{17}$$

Denote by i the greatest index for which a_i is even. It is trivial that $i \le m-2$. One can observe from (17) that

$$\begin{aligned} b_{2j} &= a_j^2 + 2a_{2j}a_0 + 2a_{2j-1}a_1 + \cdots + 2a_{j+1}a_{j-1}, \\ b_{2j+1} &= 2a_{2j+1}a_0 + 2a_{2j}a_1 + \cdots + 2a_{j+1}a_j, \end{aligned} \tag{18}$$

and so $b_{2i} \equiv 0 \pmod 2$, as well as $b_{2i+2} \equiv 1 \pmod 2$. One can see from (10) and (iii) of Lemma 1 that the coefficient of the power x^{2i+2} is zero on the left side of (17). At the same time on the right side this coefficient is $ub_{2i+2} - b_{2i+1} + b_{2i} \equiv 1 - 0 + 0 \equiv 1 \pmod 2$ which is a contradiction. This means that

$$a_i \equiv 1 \pmod 2, \quad i = 0, 1, \ldots, m-2.$$

If $u \equiv 1 \pmod 4$, then the coefficient $ub_6 - b_5 + b_4$ of x^6 is congruent to $7+6+5 \equiv 2 \pmod 4$ by (18) provided that a_6 exists, that is $2m \geq 14$. But this contradicts the fact that this coefficient is zero on the left side of (17). In case when $u \equiv -1 \pmod 4$ we obtain that $ub_4 - b_3 + b_2 \equiv -5 + 4 + 3 \equiv 2 \pmod 4$, provided $2m \geq 10$. This is again a contradiction. When $2m < 14$ we can easily check that only $E_6(x) - 1$ is the form $(x^2 - x + u)f(x)^2$. In this case $u = -1$ and $f(x) = x^2 - x - 1$.

Case (b2): Denote by i the greatest index for which a_i is odd. It is obvious that $i \leq m - 2$ by (13). From (18) we know that $b_{2i} \equiv 1 \pmod 2$. If $i \geq 1$ then 2^k divides the coefficient of the power x^{2i} on the left side of (13). On the right side this coefficient is $ub_{2i} - 2b_{2i-1} + 2b_{2i-2} \equiv 1 \pmod 2$. This contradiction shows that $a_{m-1}, a_{m-2}, \ldots, a_1$ are even, while a_0 is odd. As $b_1 = 2a_1a_0$ we have $4|b_1$. Since 2^k divides the coefficient of x on the left side of (13) we get that $2^k|ub_1 - 2b_0$. But then $2|b_0 = a_0^2$ which is a contradiction.

Case (b3): Denote by i the greatest index for which a_i is odd. In this case, similar to case (b2), we have that $a_{m-1}, a_{m-2}, \ldots, a_1$ are even, while a_0 is odd. Now denote by j the greatest index for which $a_j \equiv 2 \pmod 4$. Such an index j exists since otherwise $4|a_1$ and so $8|b_1 = 2a_1a_0$. But 2^{2m} divides the coefficient of x on the left side of (13). On the right side the coefficient of x is equal to $ub_1 - 4b_0 \equiv 4 \pmod 8$. This is impossible. We proceed by studing the coefficient of the power x^{2j} on both sides of (13). On the left side 2^{2m} divides this coefficient. On the right side this is equal to $ub_{2j} - 4b_{2j-1} + 4b_{2j-2}$ which is congruent to 4 (mod 8) if $j > 1$ by (15) and (18). This contradiction shows that j must be 1. We know from Lemma 7 that $f(x) = (-1)^{m-1}f(1-x)$ for $m \geq 3$. This means for even m that $1/2$ is a root of the polynomial $f(x)$, while for odd m we have $f(x) = f(1-x)$ and so

$$f(1) = a_{m-1} + a_{m-2} + \cdots + a_1 + a_0 = a_0 = f(0).$$

In case m odd we have a simple contradiction: $2 \equiv a_{m-1} + a_{m-2} + \cdots + a_1 = 0 \pmod 4$. In case when $m = 2l$ is even we obtain that $p = -2^{4l}E_{4l}(1/2) = -E_{4l}$

by (13). Thus we have to study the equality:

$$2^{4l}E_{4l}(x) - E_{4l} = (4x^2 - 4x + u)f(x)^2. \tag{19}$$

We substitute $x = 2$ and $x = 5/2$ into (19). From Lemma 4 and (19) we infer that $8+u < 0 < 15+u$, which yields $-15 < u < -8$. Since u is odd $u \in \{-9, -11, -13\}$. Inserting $x = 3$ into (19) we obtain that $-2 \equiv uf(3)^2 \pmod 3$ by Lemma 2. But this is a contradiction if $u = -9, -13$. In case when $u = -11$ put $x = 11$ into (19). By Lemma 2 again $-E_{4l} \equiv -\sum_{j=0}^{10}(-1)^j(2j+1)^{4l} \equiv 0 \pmod{11}$ which is impossible if $l \geq 1$. □

Proof of Theorem 2. Let

$$F(x) = a\prod_{i=1}^{t}(x - \alpha_i)^{k_i}$$

be a non-square polynomial with rational coefficients. Since $F(x)$ is not a square we can assume that the exponent k_1 is odd. But in this case we obtain that the polynomial

$$F(E_n(x)) = a\prod_{i=1}^{t}(E_n(x) - \alpha_i)^{k_i}$$

has at least three zeros with odd multiplicities by Theorem 1. Applying the theorem of Brindza we find that there are only finitely many integer solutions x, y of (2). □

Acknowledgments. This research was carried out as part of the TAMOP-4.2.1.B-10/2/KONV-2010-0001 project with support by the European Union, co-financed by the European Social Fund.

References

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439–444.

[2] J. Brillhart, On the Euler and Bernoulli polynomials, *J. Reine Angew. Math.* **234** (1969), 45–64.

[3] B. Brindza, On S-integral solutions of the equation $y^m = f(x)$, *Acta. Math. Hung.* **44** (1984), 133–139.

[4] W. J. LeVeque, On the equation $y^m = f(x)$, *Acta Arith.* **9** (1964), 209–219.

[5] W. Ljunggren, Oppgave nr2, *Norsk. Mat. Tidsskr.* **25** (1943), 29.

[6] T. Nagell, Løsning till oppgave nr2, *Norsk. Mat. Tidsskr.* **30** (1948), 62–64.

[7] T. Nagell, The diophantine equation $x^2 + 7 = 2^n$, *Ark. Mat.* **4** (1961), 185–187.

[8] S. Ramanujan, Question 464, *J. Indian Math. Soc.* **5** (1913), 130.

[9] S. Ramanujan, Collected Papers, *Chelsea Publishing Co., New York*, 1962.

[10] Cs. Rakaczki, On some diophantine results related to Euler polynomials, *Periodica Math. Hung.* **56** (2008), 247–257.

[11] Zhi-Wei Sun, On Euler numbers modulo powers of two, *J. Number Theory* **115** (2005), 371–380.

CSABA RAKACZKI
NUMBER THEORY RESEARCH GROUP
OF THE HUNGARIAN ACADEMY OF SCIENCES
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

AND

INSTITUTE OF MATHEMATICS
UNIVERSITY OF MISKOLC
H-3515 MISKOLC CAMPUS
HUNGARY

E-mail: rcsaba@math.klte.hu, matrcs@uni-miskolc.hu

(Received November 2, 2010; revised February 11, 2011)