Separatum

ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXII.

SECTIO MATEMATICAE

TAMÁS HERENDI and ATTILA PETHŐ

Trinomials, which are divisible by quadratic polynomials

EGER, 1994

Trinomials, which are divisible by quadratic polynomials

TAMÁS HERENDI and ATTILA PETHŐ*

Abstract. The reducibility of the trinomials in the form $x^n - Bx^k - A$ are examined. It is shown, that among the trinomials in the same class (i.e. some of the parameters A,B,k and n are fixed) there are only finitely many wich has quadratic factor.

1. Introduction

Let us consider the trinomial $x^n - Bx^k - A$. Ribenboim [4] has shown that if $k = 1$ then for a fixed n and B there exist only finitely many A for which the trinomial is divisible by a quadratic polynomial and similarly if n and A is fixed then there exist only finitely many B for which the trinomial has a quadratic factor. He used in the proof elementary steps only.

Schinzel in [5] then presented a much more general result in which he proved among others that for fixed A there exist only finitely many n, k, B for which the trinomial is divisible by any polynomial. He could prove similar result for fixed B too. His proof is however not an elementary one.

We are also able to generalize Ribenboim's result extending his proof but keeping its elementaryness. Our result is less general than Schinzel's result. We prove the following theorems:

Theorem 1. Let be given $k \in N$ and $A \in \mathbf{Z} \setminus \{0\}$, then

(a) there exist only finitely many, effectively determinable polynomials in the form $x^n - Bx^k - A$, where $n \in N$, $B \in \mathbf{Z} \setminus \{0\}$ and $\gcd(k, n, 12) = 1$, for which

$$x^2 - bx - a \mid x^n - Bx^k - A$$

with $a, b \in \mathbf{Z}$.

(b) if $\gcd(k, n, 12) \geq 2$ where $n \in N$ then there exist only finitely many effectively determinable polynomials in the form $x^n - Bx^k - A$, where $B \in Z \setminus \{0\}$ for which $x^2 - bx - a | x^n - Bx^k - A$ for an $a, b \in Z$ pair.

* Research (partially) supported by Hungarian National Foundation for Scientific Research, grant No. 1641.

Theorem 2. Let be given $n, k \in N$ and $B \in \mathbf{Z} \setminus \{0\}$ then

(a) if $\gcd(n, k, 12) = 1$ and $n-k > 4$ then there exist only finitely many $A \in \mathbf{Z}$ for which $x^2 - bx - a \mid x^n - Bx^k - A$ for an $a, b \in \mathbf{Z}$ pair;

(b) if $\gcd(n, k, 12) \geq 2$ and $n - k > 4$ then there exist infinitely many $A \in \mathbf{Z}$ for which $x^2 - bx - a \mid x^n - Bx^k - A$ for an $a, b \in \mathbf{Z}$ pair, but except for finitely many values all the possible values of A is explicitely expressable as a series.

Remark. Using properties of curves of genus at least 1, we were able to handle the case $n - k < 4$ too. As Schinzel's result are more general and our proof is not elementary, we omit the details.

2. Auxiliary results

Let the polynomial sequence $\{F_n(x)\}_{n=0}^{\infty}$ be defined as follows: $F_0(x) = F_1(x) = 1$, and if $n \geq 2$ then $F_n(x) = F_{n-1}(x) + x \cdot F_{n-2}(x)$.

Let define the polynomial sequence $\{f_n(x, y)\}_{n=0}^{\infty}$ as $f_n(x, y) = y^{\left[\frac{n}{2}\right]} \cdot F_n\left(\frac{x}{y}\right)$.

Remark. From Lemma 2 you can see that $f_n(x, y)$ is really a polynomial and not a rational function.

Lemma 1. The series $\{F_n(x)\}_{n=0}^{\infty}$ has for any $1 \leq k < n$ the following properties:

(a) $F_n(x) \cdot F_{k-1}(x) = F_{n-1}(x) \cdot F_k(x) - (-1)^k \cdot x^k \cdot F_{n-k-1}(x)$;

(b) $F_n(x) = F_{n-k}(x) \cdot F_k(x) + x \cdot F_{n-k-1}(x) \cdot F_{k-1}(x)$.

PROOF. We prove only property (a), because the proof of (b) is similar. Let $k = 1$. Then $n \geq 2$. The equality in this case is true because

$$F_n(x) \cdot F_0(x) = F_{n-1}(x) \cdot F_1(x) + x \cdot F_{n-2}(x),$$

where $F_0(x) = F_1(x) = 1$, and this is exactly the defining equation of F_n if $n > 2$.

Let now $k > 2$ and suppose that for every $0 < i < k$ the equality holds. We know that

$$\text{(I)} \qquad F_n(x) \cdot F_k(x) = F_n(x) \cdot (F_{k-1}(x) + x \cdot F_{k-2}(x))$$

$$\text{(II)} \qquad F_{n-1}(x) \cdot F_k(x) = F_{n-1}(x) \cdot (F_{k-1}(x) + x \cdot F_{k-2}(x))$$

and

$$(-1)^k \cdot x^{k-1} \cdot F_{n-k+1}(x) = (-1)^k \cdot x^{k-1} \cdot (F_{n-k}(x) + x \cdot F_{n-k-1}(x)),$$

which is equal to

$$\text{(III)} \quad (-1)^k \cdot x^k \cdot F_{n-k-1}(x) = (-1)^k \cdot x^{k-1} \cdot (F_{n-k+1}(x) + x \cdot F_{n-k}(x)).$$

Let consider the sum: I − II + III:

$$F_n(x)\cdot F_k(x) - F_{n-1}(x)\cdot F_k(x) + (-1)^k\cdot x^k\cdot F_{n-k-1}(x) =$$
$$F_n(x)\cdot F_{k-1}(x) - F_{n-1}(x)\cdot F_{k-1}(x) - (-1)^k\cdot x^{k-1}\cdot F_{n-k}(x) +$$
$$x\cdot(F_n(x)\cdot F_{k-2}(x) - F_{n-1}(x)\cdot F_{k-1}(x) + (-1)^k\cdot x^{k-2}\cdot F_{n-k+1}(x)).$$

The right hand side of this equation is equal to zero by the induction hypothesis, so the equality holds for k too.

Lemma 2.

(a) The polynomial $F_n(x)$ has degree $\left[\frac{n}{2}\right]$ and its roots are $-\frac{\xi_{n+1}^j}{(\xi_{n+1}^j+1)^2}$, where $1\le j\le\left[\frac{n}{2}\right]$ and ξ_{n+1} is a $n+1$-th primitive root of unity;

(b) $F_n(x)$ has a rational root if and only if $\gcd(n+1,12)\ge 3$.

PROOF.

(a) By definition we have $F_0(x)=F_1(x)=1$, so $\deg(F_0(x))=\left[\frac{0}{2}\right]$ and $\deg(F_1(x))=\left[\frac{1}{2}\right]$. Let $n\ge 2$ and suppose that $\deg(F_k(x))=\left[\frac{k}{2}\right]$ if $k<n$. It is easy to see that the leading coeffitient of $F_k(x)$ is positive. So

$$\deg(F_n(x)) = \deg(F_{n-1}(x)+x\cdot F_{n-2}(x)) =$$
$$= \max(\deg(F_{n-1}(x)), \deg(F_{n-2}(x))+1) = \left[\frac{n}{2}\right].$$

Let $\{u_m\}_{m=0}^{\infty}$ be a recurrence sequence with the definition: $u_m \doteq r\cdot u_{m-1} + s\cdot u_{m-2}$, where $r,s\neq 0, r^2+4s\neq 0$ and $|u_0|+|u_1|>0$. Then $u_m = a\cdot\alpha^m + b\cdot\beta^m (m=0,1,2,\ldots)$, where α,β is the two different roots of the polynomial $z^2-r\cdot z-s$ and $a=\frac{u_0\cdot\beta-u_1}{\beta-\alpha}$, $b=\frac{u_1-u_0\cdot\alpha}{\beta-\alpha}$ (see e. g. [2]). Let suppose now that t is a root of $F_n(x)$ and define $\{u_m\}_{m=0}^{\infty}$ by the following recurrence:

$$u_0=u_1=1 \quad\text{and}\quad u_m := u_{m-1}+t\cdot u_{m-2} \quad\text{if}\quad m\ge 2.$$

It is clear that $F_m(t)=u_m$ $(m=0,1,2,\ldots)$, and if $t\neq -\frac{1}{4}$ then

$$u_m = \frac{\sqrt{1+4t}-1}{2\sqrt{1+4t}}\cdot\left(\frac{1-\sqrt{1+4t}}{2}\right)^m + \frac{\sqrt{1+4t}+1}{2\sqrt{1+4t}}\cdot\left(\frac{1+\sqrt{1+4t}}{2}\right)^m =$$
$$\frac{1}{\sqrt{1+4t}}\cdot\left(\left(\frac{1+\sqrt{1+4t}}{2}\right)^{m+1} - \left(\frac{1-\sqrt{1+4t}}{2}\right)^{m+1}\right).$$

By the choice of t we have $0=F_n(t)=u_n$ which means

$$\left(\frac{1+\sqrt{1+4t}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{1+4t}}{2}\right)^{n+1} = 0,$$

i. e.

$$\left(\frac{1+\sqrt{1+4t}}{2}\right)^{n+1} = \left(\frac{1-\sqrt{1+4t}}{2}\right)^{n+1}.$$

From this we get

$$(1) \qquad \left(1+\sqrt{1+4t}\right) = \xi_{n+1}^{j} \cdot \left(1-\sqrt{1+4t}\right),$$

where ξ_{n+1} is a $n+1$-th primitive root of unity, and $1 \leq j \leq n$. Also $j \neq \frac{n+1}{2}$ (if it is integer), because in this case $1+\sqrt{1+4t} = \sqrt{1+4t}-1$ would hold which is impossible. From equation (1) we obtain $t = -\frac{\xi_{n+1}^{j}}{\left(\xi_{n+1}^{j}+1\right)^2}$.
The next question is how many different values t can have. If $j = 0$ then $t = -\frac{1}{4}$ and it is easy to see that $F_m\left(-\frac{1}{4}\right) \neq 0$ for any $m = 0, 1, 2, \ldots$. Further $-\frac{\xi_{n+1}^{i}}{\left(\xi_{n+1}^{i}+1\right)^2} = -\frac{\xi_{n+1}^{j}}{\left(\xi_{n+1}^{j}+1\right)^2}$, where $0 \leq i, j < n+1$ and $i \neq j$ if and only if $i+j = n+1$. It means that t has at most $\left[\frac{n}{2}\right]$ different values. We know that $\deg\left(F_n(x)\right) = \left[\frac{n}{2}\right]$ which implies that $F_n(x) = \prod_{j=1}^{\left[\frac{n}{2}\right]} \left(x + \frac{\xi_{n+1}^{j}}{\left(\xi_{n+1}^{j}+1\right)^2}\right)$.

(b) $F_n(x)$ has a rational root if and only if $-\frac{\xi_{n+1}^{j}}{\left(\xi_{n+1}^{j}+1\right)^2} = \frac{p}{q}$ for $j \in \left\{1, 2, \ldots, \left[\frac{n}{2}\right]\right\}$, $p, q \in Z$, $q \neq 0$. This is equivalent to $0 = p \cdot \left(\xi_{n+1}^{j}+1\right)^2 + q \cdot \xi_{n+1}^{j} = p \cdot \left(\xi_{n+1}^{j}\right)^2 + (q+2p)\xi_{n+1}^{j} + p$. Hence ξ_{n+1}^{j} has to be a root of the polynomial $px^2 + (q+2p)x + p$, i.e. ξ_{n+1}^{j} is rational or a quadratic algebraic number. But it is known that if ξ is a k-th primitive root of unity, then its degree is $\varphi(k)$, where $\varphi(k)$ is the Euler-function. $\varphi(k) \leq 2$ if and only if $k \in \{1, 2, 3, 4, 6\}$. From the proof of (a) it is clear that $k > 2$. If $k = 3$ then $t = -1$, if $k = 4$ then $t = -\frac{1}{2}$ and if $k = 6$ then $t = -\frac{1}{3}$. As ξ_{n+1}^{j} is primitive k -th root of unity if $n+1 = j-k$, thus $F_n(x)$ has a rational root if and only if $3 \mid n+1$ or $4 \mid n+1$, i.e. $\gcd(n+1, 12) \geq 3$.

In the next step some properties of the series $\{f_n(x,y)\}_{n=-\infty}^{\infty}$ are presented.

Lemma 3. The series $\{f_n(x,y)\}_{n=-\infty}^{\infty}$ has the property

$$\delta_{0n} \cdot f_n(x,y) = y^{n-1 \bmod 2} \cdot f_{n-1}(x,y) + x \cdot f_{n-2}(x,y) \text{if} n \in \mathbf{Z},$$

where

$$\delta_{0n} = \begin{cases} 0, & \text{if } n \neq 0 \\ 1, & \text{if } n = 0. \end{cases}$$

3. Basic lemmata

The following lemma generalizes a result of Ribenboim [4] and it is basic for the proofs of the theorems.

Lemma 4.

Let $n \geq 2$, $1 \leq k < n$ and $a, b, A, B \in \mathbf{Z}$. If $x^2 - bx - a$ divides $x^n - Bx^k - A$ then

$$B \cdot b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2) = b^{n-1 \bmod 2} \cdot f_{n-1}(a, b^2).$$

Further if

(a) $b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2) = 0$ then $b^{n-1 \bmod 2} \cdot f_{n-1}(a, b^2) = 0$ and

$$A = a \cdot \left(b^{n-2 \bmod 2} \cdot f_{n-2}(a, b^2) - B \cdot b^{k-2 \bmod 2} \cdot f_{k-2}(a, b^2)\right).$$

(b) otherwise

$$a \mid A, \qquad B = \frac{b^{n-1 \bmod 2} \cdot f_{n-1}(a, b^2)}{b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2)}$$

and

$$A = a^k(-1)^k \frac{b^{n-k-1 \bmod 2} \cdot f_{n-k-1}(a, b^2)}{b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2)}.$$

PROOF.

(a) Assume that $x^n - Bx^k - A = (x^2 - bx - a) \cdot p(x)$ with $p(x) = x^{n-2} + c_{n-3}x^{n-3} + c_{n-4}x^{n-4} + \cdots + c_1 x + c_0$. Similarly as in [4] we have the following equations:

$$\begin{aligned}
A &= a \cdot c_0 \\
\delta_{1,k} \cdot B &= a \cdot c_1 + b \cdot c_0 \\
&\vdots \\
\delta_{i,k} \cdot B &= a \cdot c_i + b \cdot c_{i-1} - c_{i-2} \qquad (2) \\
&\vdots \\
\delta_{n-2,k} \cdot B &= a + b \cdot c_{n-3} - c_{n-4} \\
\delta_{n-1,k} \cdot B &= b - c_{n-3}
\end{aligned}$$

where

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Using this we prove that if $1 \leq i \leq n-2$, then

$$c_{n-2-i} = b^{i \bmod 2} \cdot f_i(a,b^2) - Bb^{k-n+i \bmod 2} \cdot f_{k-n-i}(a,b)^2. \tag{3}$$

By (2) it is easy to see that (3) holds for $i = 1, 2$. Let $2 < i \leq n-2$ and suppose that (3) holds for every j with $1 \leq j < i$. Then by (2) we get

$$\begin{aligned} c_{n-2-i} &= a \cdot c_{n-2-(i-2)} + b \cdot c_{n-2-(i-1)} - \delta_{n-i,k} \cdot B \\ &= a \cdot C_1 + b \cdot C_2 - \delta_{n-i,k} \cdot B \\ &= b^{i-2 \bmod 2} \cdot C_3 - B \cdot b^{k-n+i-2 \bmod 2} \cdot C_4 + B \cdot \delta_{n-i,k}, \end{aligned}$$

where

$$\begin{aligned} C_1 &= b^{i-2 \bmod 2} \cdot f_{i-2}(a,b^2) - B \cdot B^{k-n+i-2 \bmod 2} \cdot f_{k-n+i-2}(a,b^2) \\ C_2 &= b^{i-1 \bmod 2} \cdot f_{i-1}(a,b^2) - B \cdot B^{k-n+i-1 \bmod 2} \cdot f_{k-n+i-1}(a,b^2) \\ C_3 &= b^{2(i-1 \bmod 2)} \cdot f_{i-1}(a,b^2) + a \cdot f_{k-n+i-2}(a,b^2) \\ C_4 &= b^{2(k-n+i-1 \bmod 2)} \cdot f_{k-n+i-1}(a,b^2) + a \cdot f_{k-n+i-2}(a,b^2). \end{aligned}$$

From this by Lemma 3 we get (3). Using (2) and (3) we obtain

$$\begin{aligned} 0 &= a \cdot c_1 + b \cdot c_0 - \delta_{1,k} \cdot B \\ &= a \cdot \left(b^{n-3 \bmod 2} \cdot f_{n-3}(a,b^2) - B \cdot b^{k-3 \bmod 2} \cdot f_{k-3}(a,b^2)\right) + \\ &+ b \cdot a \cdot \left(b^{n-2 \bmod 2} \cdot f_{n-2}(a,b^2) - B \cdot b^{k-2 \bmod 2} \cdot f_{k-2}(a,b^2)\right) - \delta_{1,k} \cdot B \\ &= b^{n-3 \bmod 2} \cdot \left(b^{2(n-2 \bmod 2)} \cdot f_{n-2}(a,b^2) + a \cdot f_{n-3}(a,b^2)\right) - \\ &- B \cdot \left(b^{k-3 \bmod 2} \cdot \left(b^{2(k-2 \bmod 2)} \cdot f_{k-2}(a,b^2) + a \cdot f_{k-3}(a,b^2)\right) + \delta_{1,k}\right). \end{aligned}$$

Using Lemma 3 we get

$$0 = b^{n-1 \bmod 2} \cdot f_{n-1}(a,b^2) - B \cdot b^{k-1 \bmod 2} \cdot f_{k-1}(a,b^2), \tag{4}$$

which proves the first assertion. This implies $b^{k-1 \bmod 2} \cdot f_{k-1}(a,b^2) = 0$ if and only if $b^{n-1 \bmod 2} \cdot f_{n-1}(a,b^2) = 0$. By (2) and (3)

$$A = a \cdot \left(b^{n-2 \bmod 2} \cdot f_{n-2}(a,b^2) - B \cdot b^{k-2 \bmod 2} \cdot f_{k-2}(a,b^2)\right). \tag{5}$$

(b) If $b^{k-1 \bmod 2} \cdot f_{k-1}(a,b^2) \neq 0$ then from (4) we get

$$B = \frac{b^{n-1 \bmod 2} \cdot f_{n-1}(a,b^2)}{b^{k-1 \bmod 2} \cdot f_{k-1}(a,b^2)}. \tag{6}$$

and from (5) and (6), using Lemma 1 we obtain $a \mid A$ and

$$A = a^k(-1)^k \frac{b^{n-k-1 \bmod 2} \cdot f_{n-k-1}(a, b^2)}{b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2)}.$$

Lemma 5. Let $k, n \in N$ and $A \in \mathbf{Z} \setminus \{0\}$. Then there exist only finitely many, effectively computable $a, b, B \in \mathbf{Z}$ such that $x^2 - bx - a \mid x^n - Bx^k - A$.

PROOF. Let $a, b \in \mathbf{Z}$ be such that $b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2) \neq 0$ and $x^2 - bx - a \mid x^n - Bx^k - A$. Then by Lemma 4 (b) $a \mid A$ and

$$0 = A \cdot b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2) - a^k(-1)^k b^{n-k-1 \bmod 2} \cdot f_{n-k-1}(a, b^2). \tag{7}$$

Because of $a \mid A$, a may assume only finitely many different values. Let a be fixed. Then the right hand side of (7) is a polynomial in b, which has only finitely many roots, and the integer roots of it are effectively computable. So there exist only finitely many possibilities for a, b (and they are effectively computable). As $f_{k-1}(a, b^2) \neq 0$, by Lemma 4 (b) B is explicitely determinable from a and b so the numbers of the possible B is also finite and the values of B are effectively computable. Let a, b now be such that $f_{k-1}(a, b^2) = 0$. By Lemma 2 (b)

$$\frac{a}{b^2} \in \left\{-1, -\frac{1}{2}, -\frac{1}{3}\right\}. \tag{8}$$

By Lemma 4 (a) $a \mid A$ and

$$A = a \cdot \left(b^{n-2 \bmod 2} \cdot f_{n-2}(a, b^2) - B \cdot b^{k-2 \bmod 2} \cdot f_{k-2}(a, b^2)\right), \tag{9}$$

where $b^{k-2 \bmod 2} \cdot f_{k-2}(a, b^2) \neq 0$. (Otherwise $b^{i \bmod 2} \cdot f_i(a, b^2) = 0$ would hold for every i and it is possible only when $a, b = 0$.) As $a \mid A$ the cardinality of the possible a-s is finite and by (8) the cardinality of the possible b-s is also finite and effectively computable. Let fix now a and b. Then (9) is a linear equation in B which has only one solution and the solution is explicitely given. So we obtain that B has only finitely many possible values in both cases and they are effectively computable.

By replacing y with y^2 in the definition of $f_n(x, y)$ it is easy to prove the following:

Lemma 6. $y^{n \bmod 2} \cdot f_n(x, y^2) = y^n \cdot F_n\left(\frac{x}{y^2}\right)$.

Lemma 7. Let suppose that $\gcd(n,k)=m$. Then

$$\gcd\left(y^{n-1 \bmod 2}\cdot f_{n-1}\left(x,y^2\right), y^{k-1 \bmod 2}\cdot f_{k-1}\left(x,y^2\right)\right) = \\ = y^{m-1 \bmod 2}\cdot f_{m-1}\left(x,y^2\right)$$

PROOF. By Lemma 2 (a) we know that $F_n(x)$ has $\left[\frac{n}{2}\right]$ different real roots. Let suppose that they are $x_1,\ldots,x_{\left[\frac{n}{2}\right]}$. Then

$$F_n(x)=\mathrm{lc}\left(F_n\right)\cdot\prod_{i=1}^{\left[\frac{n}{2}\right]}\left(x-x_i\right),$$

where $\mathrm{lc}\left(F_n\right)$ is the leading coefficient of F_n, which is 1 if n is even and $n+1$ if n is odd. Then by Lemma 6

$$y^{n \bmod 2}\cdot f_n\left(x,y^2\right)=\mathrm{lc}\left(F_n\right)\cdot\prod_{i=1}^{\left[\frac{n}{2}\right]}\left(x-x_i\cdot y^2\right)\cdot y^{n \bmod 2}.$$

It is clear that $\left(x-x_i\cdot y^2\right)$ is irreducible, and by the unique factorization in a polynomial ring, this is the only possible factorization of $y^{n \bmod 2}\cdot f_n\left(x,y^2\right)$. By Lemma 2(a) $\left(x-t\cdot y^2\right)\mid y^{n-1 \bmod 2}\cdot f_{n-1}\left(x,y^2\right)$ if and only if there exists $j\in\left\{1,\ldots,\left[\frac{n}{2}\right]\right\}$ such that $t=-\frac{\xi_n^j}{\left(\xi_n^j+1\right)^2}$. Of course, then for all $\bar{t}$, conjugate of t, $\left(x-\bar{t}\cdot y^2\right)\mid y^{n-1 \bmod 2}\cdot f_{n-1}\left(x,y^2\right)$.
If t is such that

$$\left(x-t\cdot y^2\right)\mid y^{n-1 \bmod 2}\cdot f_{n-1}\left(x,y^2\right)$$

and $\left(x-t\cdot y^2\right)\mid y^{k-1 \bmod 2}\cdot f_{k-1}\left(x,y^2\right)$ then there exist $j,i\in\left\{1,\ldots,\left[\frac{n}{2}\right]\right\}$ such that $\frac{\xi_n^j}{\left(\xi_n^j+1\right)^2}=\frac{\xi_k^i}{\left(\xi_k^i+1\right)^2}$ from where we get either $\xi_n^j=\xi_k^i$ or $\xi_n^j=\xi_k^{-i}$. Without loss of generality we can suppose that $\xi_n^j=\xi_k^i$. It is easy to see, if $m=\gcd(n,k)$ then $\left(\xi_n^j\right)^m=\left(\xi_k^i\right)^m$, which means that ξ_n^j is m-th root of unity and so $\left(x-t\cdot y^2\right)\mid y^{m-1 \bmod 2}\cdot f_{m-1}\left(x,y^2\right)$. Reversing, if $\left(x-t\cdot y^2\right)\mid y^{m-1 \bmod 2}\cdot f_{m-1}\left(x,y^2\right)$ then there exists $i\in\left\{1,\ldots,\left[\frac{n}{2}\right]\right\}$ such that $t=-\frac{\xi_k^i}{\left(\xi_k^i+1\right)^2}$, and if $m\mid n$ then there exists $j\in\left\{1,\ldots,\left[\frac{n}{2}\right]\right\}$ such that $\xi_m^i=\xi_n^j$ or $\xi_m^i=\xi_n^{-j}$, which means that $\left(x-t\cdot y^2\right)\mid y^{n-1 \bmod 2}\cdot f_{n-1}\left(x,y^2\right)$. We have $m-1 \bmod 2=1$ if and only if $n-1 \bmod 2=1$ and $k-1 \bmod 2=1$. So if $y\mid y^{n-1 \bmod 2}\cdot f_{n-1}\left(x,y^2\right)$ and $y\mid y^{k-1 \bmod 2}\cdot$

$f_{k-1}(x, y^2)$ then $y \mid y^{m-1 \bmod 2} \cdot f_{m-1}(x, y^2)$ and vice versa. The leading coeffitient of $f_{m-1}(x, y^2)$ is different from 1 if and only if m is even and in this case it is equal to m. But then the leading coeffitient of $f_{n-1}(x, y^2)$ is equal to n and the leading coeffitient of $f_{k-1}(x, y^2)$ is equal to k.

Lemma 8. Let $D = y \cdot (4x + y)$, $U_1 = \frac{2x+y+\sqrt{D}}{2}$ and $U_2 = \frac{2x+y-\sqrt{D}}{2}$. Then

$$f_n(x, y) = \left(\frac{1}{2}\right)^{n+1 \bmod 2} \cdot C,$$

where

$$C = \frac{\left(y + \sqrt{D} \cdot U_1\right)^{n+1 \bmod 2} \cdot U_1^{\left[\frac{n+1}{2}\right]} - \left(y - \sqrt{D} \cdot U_2\right)^{n+1 \bmod 2} \cdot U_2^{\left[\frac{n+1}{2}\right]}}{\sqrt{D}}.$$

PROOF. It is easy to see that $f_n(x, y)$ has the property $F_{n+2}(x, y) = (2x + y) \cdot f_n(x, y) - x^2 \cdot f_{n-2}(x, y)$. From this similarly to the method used in Lemma 2 for $F_n(x)$ we get the statement of the Lemma.

4. Proof of the theorems

Proof of Theorem 1.

(a) Let suppose that $\gcd(k, n) = 1$. At first we show that there exists an effectively computable upper bound for the possible n values. If $A \neq 0$ is given then by Lemma 2 (b) using the definition of $f_n\, b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2) \neq 0$. Then by Lemma 4 (b)

$$a \mid A \quad \text{and} \quad a^{k-1}(-1)^k \frac{b^{n-k-1 \bmod 2} \cdot f_{n-k-1}(a, b^2)}{b^{k-1 \bmod 2} \cdot f_{k-1}(a, b^2)} \mid A.$$

Let assume now that n is given and a is fixed and suppose that $b^2 \geq 4a^2$. Then if we substitute x by a and y by b^2 in Lemma 8, we obtain $D > 0$, $U_1 > a^2$ and $U_2 < 1$. Then there exists M_a constant, such that $\left|f_{k-1}(a, b^2)\right| < \left|M_a b^{k-1}\right|$ if $b \neq 0$ and from Lemma 8 follows that there exists m_a, n_a and $c_a > 0$ such that if $n > n_a$ and $|b| > m_a$ then as $U_1 > \frac{b^2}{2}$

$$f_n(a, b^2) = \left(\frac{1}{2}\right)^{n+1 \bmod 2} \cdot C$$

$$> c_a \cdot \left(\frac{1}{2}\right)^{n+1 \bmod 2} \cdot \frac{\left(b^2 + \sqrt{D} \cdot U_1\right)^{n+1 \bmod 2} \cdot U_1^{\left[\frac{n+1}{2}\right]}}{\sqrt{D}}$$

$$\geq c_a \cdot \left(\frac{1}{2}\right)^{n+1 \bmod 2} \cdot \frac{\left(b^2+\sqrt{D}\right)^{n+1 \bmod 2}}{\sqrt{D}} \cdot b^{n+1}$$
$$> c_a \cdot \frac{1}{2} \cdot b^{n-1}.$$

Hence

$$A > \left| \frac{b^{n-k-1 \bmod 2} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right)} \right|$$
$$> \frac{c_a}{2} \cdot \frac{b^{n-k-2}}{b^k} = b^{n-2k-2}.$$

Because of the monotonity of the exponential function and the finiteness of the number of the possible a-s there exists an upper bound for n depending only on A. Let examine now the case $b^2 < \max\left(4a^2, m_a\right)$. There exist only finitely many b satisfying the inequality. For these values we apply Theorem 3.1 from [2] and get

$$f_n\left(a, b^2\right) > |U_1|^{n-1-c_1 \cdot \log(n-1)} \tag{10}$$

where c_1 is effectively computable and depends finally on a and b. As we have only finitely many possibilities for a and b, c_1 is a constant and for n large enough the exponent in (10) is positive. By a result of Dobrowolski (see in [1]) $|U_1| \geq c_2 > 1$ holds for any quadratic algebraic integers which are not roots of unity, hence by (10) similarly to the previous case n is bounded. So there exist only finitely many possible n-s satisfying the assumptions in the theorem from which using Lemma 5 follows the statment of the theorem.
Suppose now that $\gcd(k, n) > 1$, but $\gcd(k, n, 12) = 1$. If a and b satisfy the assumptions in the theorem then $b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right)$ isn't zero otherwise by Lemma 4 (a) $b^{n-1 \bmod 2} \cdot f_{n-1}\left(a, b^2\right)$ would be zero, which is impossible. Hence

$$A = a^k (-1)^k \frac{b^{n-k-1 \bmod 2} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right)}$$

and the proof of the theorem in this case is the same as in the previous case.

(b) In this case we can divide the possible a, b pairs into two sets. In the first set $b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right) \neq 0$. Similarly to the previous two cases there exist only finitely many solution for B. In the second set $b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right) = 0$. Then by Lemma 4 (a) $b^{n-1 \bmod 2} \cdot f_{n-1}\left(a, b^2\right) = 0$. This is possible if and only if one of the following statements holds:

1. n is even and $b = 0$, or

2. $\frac{a}{b^2}$ is one of the rational roots of $F_{n-1}(x)$.

As $A \neq 0$ by Lemma 4 (a) $a|A$, so in case 1 (k is also even)

$$A = a \cdot \left(b^{n-2 \bmod 2} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{k-2 \bmod 2} \cdot f_{k-2}\left(a, b^2\right)\right)$$

is finitely many linear equation for the possible B -s.

In case 2, as by Lemma 2, $F_{n-1}(x)$ has at most three different rational roots and similarly to the previous case $a|A$, we have only finitely many a, b pairs which satisfies the necessary conditions. By Lemma 3 if $f_{n-1}\left(a, b^2\right) = 0$ then $f_{n-2}\left(a, b^2\right) \neq 0$ so we have again finitely many linear equations for the possible B -s.

Proof of Theorem 2.

(a) Let $a, b, A \in \mathbf{Z}$ such that $x^2 - bx - a \mid x^n - Bx^k - A$. As $B \neq 0$ similarly to Theorem 1 (b) $b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right) \neq 0$. By Lemma 4

$$B \cdot b^{k-1 \bmod 2} \cdot f_{k-1}\left(a, b^2\right) = b^{n-1 \bmod 2} \cdot f_{n-1}\left(a, b^2\right).$$

If we suppose that $b = 0$ then the equation is a polynomial equation for a, which has only finitely many solution in a so the number of possible values for A is also finite (and effectively determinable).

Let suppose now that $b \neq 0$. Then

$$\frac{B \cdot F_{k-1}(\frac{a}{b^2})}{b^{n-k}} = F_{n-1}(\frac{a}{b^2}).$$

As $\deg(F_{k-1}) = \left[\frac{k-1}{2}\right]$ and $\deg(F_{n-1}) = \left[\frac{n-1}{2}\right]$, there exist real numbers M_1, M_2, x_1, x_2 so that if $x > x_1$ then $|F_{k-1}(x)| < M_1 \cdot |x|^{\left[\frac{k-1}{2}\right]}$ and if $x > x_2$ then $|F_{n-1}(x)| > M_2 \cdot |x|^{\left[\frac{n-1}{2}\right]}$ $(M_1, M_2 > 0)$. Let $x_0 = \max(1, x_1, x_2)$ and suppose that $\left|\frac{a}{b^2}\right| > x_0$ then

$$\frac{B \cdot M_1 \cdot \left|\frac{a}{b^2}\right|^{\left[\frac{k-1}{2}\right]}}{|b^{n-k}|} > \frac{B \cdot F_{k-1}(\frac{a}{b^2})}{|b^{n-k}|} = F_{n-1}\left(\frac{a}{b^2}\right) > M_2 \cdot \left|\frac{a}{b^2}\right|^{\left[\frac{n-1}{2}\right]}.$$

As $n - k > 4$ and $\left|\frac{a}{b^2}\right| \geq 1$ we get

$$\frac{B \cdot M_1}{M_2} \geq \frac{B \cdot M_1}{M_2 \cdot |b^{n-k}|} > \left|\frac{a}{b^2}\right|^{\left[\frac{n-1}{2}\right]-\left[\frac{k-1}{2}\right]} \geq \left|\frac{a}{b^2}\right|.$$

It means that there exists a constant $M_0 > 0$ so that $-M_0 < \frac{a}{b^2} < M_0$ for all the possible $a, b \in \mathbf{Z}$ pairs. Hence there exists $M > 0$ so that $\left|F_{k-1}\left(\frac{a}{b^2}\right)\right| < M$ for all the possible a, b pairs. Or which is the same,

$$\frac{B \cdot M}{|b^{n-k}|} > F_{n-1}\left(\frac{a}{b^2}\right). \tag{11}$$

Let $l = \frac{\min\limits_{i,j}(|x_i - x_j|)}{2}$ where $x_1 \dots x_{\left[\frac{n-1}{2}\right]}$ are the roots of the polynomial $F_{n-1}(x)$. We have $l > 0$ by Lemma 2. If $\min\limits_i \left(\left|x_i - \frac{a}{b^2}\right|\right) \geq l$ then

$$\left|F_{n-1}\left(\frac{a}{b^2}\right)\right| = \prod_{i=1}^{\left[\frac{n-1}{2}\right]} \left|x_i - \frac{a}{b^2}\right| \geq l^{\left[\frac{n-1}{2}\right]},$$

from where it follows that $\frac{B \cdot M}{l^{\left[\frac{n-1}{2}\right]}} \geq \left|b^{n-k}\right|$ and there exist only finitely many $b \in \mathbf{Z}$ which is suitable for this. This together with the fact, that $\frac{a}{b^2}$ is bounded implies that there exist only finitely many possible a, b pair.
Let $\min\limits_i \left(\left|x_i - \frac{a}{b^2}\right|\right) < l$. Obviously among the $\left|x_i - \frac{a}{b^2}\right| < l$ inequalities hold only one. Let suppose that $\left|x_{i_0} - \frac{a}{b^2}\right| < l$. Then

$$\left|F_{n-1}\left(\frac{a}{b^2}\right)\right| \geq l^{\left[\frac{n-3}{2}\right]} \cdot \left|x_{i_0} - \frac{a}{b^2}\right|$$

hence using (11) we get

$$\frac{B \cdot M}{l^{\left[\frac{n-1}{2}\right]} \cdot b^{n-k}} \geq \left|x_{i_0} - \frac{a}{b^2}\right|.$$

As $b \cdot f_{n-1}\left(a, b^2\right) \neq 0$ so $x_{i_0} \neq \frac{a}{b^2}$. We assumed $n - k > 4$, hence the theorem of Roth on approximation of algebraic numbers [3] implies that there exist only finitely many suitable a, b pair for this approximation if i_0 is given. The number of the roots of $F_{n-1}(x)$ are finite so there exist only finitely many possible a, b pair and so there exist only finitely many possible A values.
(b) Let $\gcd(n, k, 12) = m > 1$. Then by Lemma 7

$$\begin{aligned}\gcd\left(y^{n-1 \bmod 2} \cdot f_{n-1}\left(x, y^2\right), y^{k-1 \bmod 2} \cdot f_{k-1}\left(x, y^2\right)\right) \\ = y^{m-1 \bmod 2} \cdot f_{m-1}\left(x, y^2\right).\end{aligned}$$

Hence there exist $g_1(x, y), g_2(x, y) \in \mathbf{Z}[x, y]$ such that

$$y^{n-1 \bmod 2} \cdot f_{n-1}\left(x, y^2\right) = g_1(x, y) \cdot y^{m-1 \bmod 2} \cdot f_{m-1}\left(x, y^2\right),$$

$$y^{k-1 \bmod 2} \cdot f_{k-1}\left(x, y^2\right) = g_2(x, y) \cdot y^{m-1 \bmod 2} \cdot f_{m-1}\left(x, y^2\right).$$

We have by Lemma 4

$$B \cdot g_2(x, y) \cdot y^{m-1 \bmod 2} \cdot f_{m-1}\left(x, y^2\right) = g_1(x, y) \cdot y^{m-1 \bmod 2} \cdot f_{m-1}\left(x, y^2\right).$$

We devide the set of pairs $a, b \in \mathbf{Z}$ into two classes according as
(i) $b^{m-1 \bmod 2} \cdot f_{m-1}\left(a, b^2\right) = 0$;
(ii) $b^{m-1 \bmod 2} \cdot f_{m-1}\left(a, b^2\right) \neq 0$.

In the case (i) by Lemma 2 (b) the values of a, b are explicitely determinable and so the possible values of A are infinitely many but they are explicitely determinable as a series.

In the case (ii) we can simplify the equation by $b^{m-1 \bmod 2} \cdot f_{m-1}\left(a, b^2\right)$ and with the simplified eqation can be solved in the same way as in (a).

References

[1] E. DOBROWOLSKI, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.

[2] T. N. SHOREY and R. TIJDEMAN, Exponential diophantine equations, *Cambridge University Press*, Cambridge · London · New York · New Rochelle · Melbourne · Sydney, (1986).

[3] K. F. ROTH, Rational approximations to algebraic numbers, *Mathematika*, **2** (1955), 1–20.

[4] P. RIBENBOIM, On the factorization of $x^n - Bx - A$, *Enseign. Math.*, **37** (1991), 191–200.

[5] A. SCHINZEL, On reducible polynomials, (to appear).