Diophantine equations for second order recursive sequences of polynomials

ANDREJ DUJELLA (Zagreb) and ROBERT F. TICHY (Graz)

Abstract

Let B be a nonzero integer. Let define the sequence of polynomials $G_n(x)$ by

$$G_0(x) = 0, \quad G_1(x) = 1, \quad G_{n+1}(x) = xG_n(x) + BG_{n-1}(x), \quad n \in \mathbf{N}.$$

We prove that the diophantine equation $G_m(x) = G_n(y)$ for $m, n \geq 3$, $m \neq n$ has only finitely many solutions.

1 Introduction

The study of polynomial diophantine equations $f(x) = g(y)$ is a classical topic in number theory. The essential question is whether this equation has finitely or infinitely many solutions in rational integers x and y. Due to the classical theorem of Siegel the finiteness problem can be solved by decomposition of $F(x, y) = f(x) - g(y)$ in irreducible factors and showing that no factor defines a curve of genus 0 and with at most 2 points at infinity. Of course this method is ineffective in the sense that it does not give bounds for the size of the solutions (x, y). However, for special equations $F(x, y) = 0$ effective results are known, for instance in the hyperelliptic case A. BAKER [1] has shown that the equation $F(x, y) = y^n - f(x) = 0$ has only finitely many effectively computable solutions (x, y) in rational integers. Various further effective versions of this result were obtained by SPRINDŽUK, TRELINA, BRINDZA, POULAKIS, VOUTIER and BUGEAUD; see [13, 5] for references.

The general polynomial equation $F(x, y) = f(x) - g(y) = 0$ has been studied by several authors. DAVENPORT, LEWIS and SCHINZEL [6] obtained a finiteness condition which is too restrictive for several applications.

Schinzel [12, Theorem 8] obtained a completely explicit finiteness criterion under the assumption $(\deg f, \deg g) = 1$. Recently, particular types of equations have been studied by Beukers, Shorey and Tijdeman [2] and by Kirschenhofer, Pethő and Tichy [10].

M. Fried investigated the finiteness problem for polynomial equations $F(x, y) = 0$ from various points of views in a series of fundamental papers [7, 8, 9]. He gave in [9, Corollary after Theorem 3] a new and very general finiteness condition.

Recently, Bilu and Tichy [4] obtained a finiteness criterion for polynomial diophantine equations $f(x) = g(y)$, which is much more explicit than the previous ones. It turns out to be more convenient to study a slightly more general problem. We say that the equation $F(x, y) = 0$ has infinitely many rational solutions with a bounded denominator if there exists a positive integer Δ such that $F(x, y) = 0$ has infinitely many solutions $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ with integral Δx and Δy.

To formulate the finiteness criterion, we have to define five types of standard pairs $(f(x), g(x))$.

In what follows a and $b \in \mathbf{Q}\backslash\{0\}$, m and n are positive integers, and $p(x)$ is a non-zero polynomial (which may be constant).

A standard pair of the first kind is

$$(x^m, ax^r p(x)^m)$$

or switched, $(ax^r p(x)^m, x^m)$ where $0 \le r < m$, $(r, m) = 1$ and $r + \deg p(x) > 0$.

A standard pair of the second kind is

$$(x^2, (ax^2 + b)p(x)^2)$$

(or switched).

Denote by $D_m(x, a)$ the m-th Dickson polynomial, defined by

$$D_m(z + a/z, a) = z^m + (a/z)^m \ .$$

A standard pair of the third kind is

$$(D_m(x, a^n), D_n(x, a^m)) \ ,$$

where $\gcd(m, n) = 1$.

A standard pair of the fourth kind is

$$\left(a^{-m/2} D_m(x, a), -b^{-n/2} D_n(x, b)\right) \ ,$$

where $\gcd(m, n) = 2$.

A standard pair of the fifth kind is

$$((ax^2 - 1)^3, 3x^4 - 4x^3)$$

(or switched).

THEOREM **1** *(*BILU-TICHY *[4].) Let $f(x), g(x) \in \mathbf{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent.*

(a) The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.

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

It is the aim of the present paper to show how this criterion can be applied to a special family of polynomials defined by a second order linear recurring relation.

Let B be a nonzero integer. Then we define a sequence of polynomials $G_n(x)$ of degree $n - 1$ by

$$G_0(x) = 0, \;\; G_1(x) = 1, \;\; G_{n+1}(x) = xG_n(x) + BG_{n-1}(x), \;\; n \in \mathbf{N}. \qquad (1.1)$$

For $B = 1$ this gives the well-known family of Fibonacci polynomials.

THEOREM **2** *For $m, n \geq 3$, $m \neq n$ the diophantine equation*

$$G_n(x) = G_m(y) \qquad (1.2)$$

has only finitely many solutions.

In Section 2 we will collect some useful facts on polynomials defined by second order linear recurrences. In Section 3 we will completely describe all decompositions of polynomials G_n. Section 4 is devoted to standard pairs of the first, second and fifth kind and Section 5 to standard pairs of the third and fourth kind. We will show that polynomials given by (1.1) cannot yield standard pairs, and so by Theorem 1 we immediately obtain Theorem 2. In the concluding Section 6 we will establish some effective results for special equations $G_n(x) = G_m(y)$.

2 Second order recursive sequences of polynomials

In this section we will collect some useful facts on the polynomials $G_n(x)$ defined in (1.1). Let us recall that the Fibonacci polynomials $F_n(x)$ are the special case of $G_n(x)$ for $B = 1$, and the Chebyshev polynomials of the second kind $U_n(x)$ are defined by

$$U_0(x) = 1, \quad U_1(x) = 2x, \quad U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x) \quad (n \in \mathbf{N}).$$

LEMMA **1** *We have for all* $n \in \mathbf{N}$*:*

$$G_n(x) = F_n\left(\frac{x}{\sqrt{B}}\right) B^{\frac{n-1}{2}} = U_{n-1}\left(\frac{ix}{2\sqrt{B}}\right)(-i\sqrt{B})^{n-1} \tag{2.1}$$

$$G_n(x) = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} B^j x^{n-2j-1} \tag{2.2}$$

Proof. Relation (2.1) follows directly from the definition of the sequences (G_n), (F_n) and (U_n), while (2.2) follows from (2.1) and the well-known expansion of Fibonacci polynomials (see e.g. [3]). ∎

For $m = 1, 2, \ldots$ put $H_m(x) = G_{2m+1}(\sqrt{x})$. Then by (2.2) we have

$$H_m(x) = \sum_{j=0}^{m} \binom{2m-j}{j} B^j x^{m-j}.$$

3 Indecomposability of polynomials G_n

A polynomial $P \in \mathbf{C}[x]$ is called *indecomposable* (over $\mathbf{C}$) if $P = P_1 \circ P_2$, $P_1, P_2 \in \mathbf{C}[x]$ implies $\deg P_1 = 1$ or $\deg P_2 = 1$.

Two decompositions of P, say $P = P_1 \circ P_2$ and $P = Q_1 \circ Q_2$ are *equivalent* if there exist a linear function L such that $Q_1 = P_1 \circ L$, $Q_2 = L^{-1} \circ P_2$ (see [12, pp. 14–15]).

Motivated by Theorem 1, in this section we consider the question of decomposability of polynomials G_n. The complete answer will be given in Proposition 1 below.

For a polynomial $f \in \mathbf{C}[x]$ and a complex number γ, put

$$\delta(f, \gamma) := \deg \gcd(f - \gamma, f').$$

LEMMA **2** *Let B be a nonzero complex number. If n is even, then $\delta(G_n, \gamma) \leq 1$ for any $\gamma \in \mathbf{C}$. If n is odd, then $\delta(G_n, \gamma) \leq 2$ for any $\gamma \in \mathbf{C}$.*

Proof. By relation (2.1) it is clear that it suffices to prove the statement of the lemma for U_{n-1} instead of G_n.

The functional equation

$$U_{n-1}(\cos x) = \frac{\sin nx}{\sin x} \tag{3.1}$$

shows that U_{n-1} has $n-1$ distinct real roots

$$\alpha_k := \cos(\pi k/n) \qquad (k = 1, \dots, n-1).$$

By Rolle's theorem, the derivative U'_{n-1} has $n-2$ real roots $\beta_1, \dots, \beta_{n-2}$, satisfying $\alpha_k > \beta_k > \alpha_{k+1}$.

Put $\gamma_k := U_{n-1}(\beta_k)$. We claim that

$$\gamma_k = \gamma_l \iff k = l \qquad \text{if } n \text{ is even,} \tag{3.2}$$

$$\gamma_k = \gamma_l \iff (k = l \quad \text{or} \quad k + l = n-1) \qquad \text{if } n \text{ is odd.} \tag{3.3}$$

The polynomial U'_{n-1} is even for even n and odd for odd n. Hence its roots are symmetrical with respect to the origin:

$$\beta_k = -\beta_{n-1-k} \qquad (k = 1, \dots, n-2). \tag{3.4}$$

Further, the functional equation (3.1) implies that γ_k is the maximum of the function $|(\sin nx)/\sin x|$ on the interval $[k\pi/n, (k+1)\pi/n]$. Hence for $1 \leq k \leq (n-2)/2$ we have $1/(\sin(k+1)\pi/n) < |\gamma_k| < 1/(\sin k\pi/n)$. This implies that

$$|\gamma_k| > |\gamma_{k+1}| > 1 \qquad (1 \leq k \leq (n-4)/2). \tag{3.5}$$

Assume that n is even. Then

$$|\gamma_1| > |\gamma_2| > \cdots > |\gamma_{(n-2)/2}|\,. \tag{3.6}$$

Also, the polynomial U_{n-1} is odd, which yields

$$\gamma_k = -\gamma_{n-1-k} \qquad (1 \leq k \leq n-2). \tag{3.7}$$

Together, (3.6) and (3.7) imply (3.2).

Now assume that n is odd. In this case

$$|\gamma_1| > |\gamma_2| > \cdots > |\gamma_{(n-3)/2}| > 1 = |\gamma_{(n-1)/2}|,$$

$$\gamma_k = \gamma_{n-1-k} \qquad (1 \le k \le n-2),$$

which proves (3.3).

If $\delta(U_{n-1}, \gamma) > 0$, then γ is equal to one of the numbers γ_k. Hence, when n is even, (3.2) implies that $\delta(U_{n-1}, \gamma) \le 1$ for any $\gamma \in \mathbf{C}$.

If n is odd, then (3.3) implies that $\delta(U_{n-1}), \gamma) \le 2$ for any $\gamma \in \mathbf{C}$. ■

Lemma **3** *Let $f \in \mathbf{C}[x]$ and let $f = p \circ q$, where p and q are polynomials. Then there exists $\gamma \in \mathbf{C}$ with $\delta(f, \gamma) \ge \deg q$.*

Proof. Let α be a root of p' and put $\gamma = p(\alpha)$. Then both the polynomials $f - \gamma$ and f' are divisible by $q - \alpha$. This proves the lemma.

■

Proposition **1** *The polynomial G_n is indecomposable for even n. If n is odd then (up to equivalence) the only decomposition of G_n is $G_n(x) = H_{(n-1)/2}(x^2)$. In particular, H_m is indecomposable for any m.*

Proof. If n is even, then Lemmas 2 and 3 imply that G_n is indecomposable.

If n is odd, then Lemmas 2 and 3 imply that in any decomposition $G_n = p \circ q$ we have $\deg q = 2$. Further, $p(q(-x)) = U_{n-1}(-x) = U_{n-1}(x) = p(q(x))$ implies $q(-x) = q(x)$. Hence $q(x) = ax^2 + b$ for some $a, b \in \mathbf{C}$. Therefore the decomposition $G_n = p \circ q$ is equivalent to the decomposition $G_n(x) = H_{(n-1)/2}(x^2)$. ■

Corollary **1** *Let $m, n \ge 3$ and $m \ne n$. Then there does not exist a polynomial $P(x) \in \mathbf{C}[x]$ such that*

$$G_n(x) = G_m(P(x)).$$

Proof. Assume that $G_n(x) = G_m(P(x))$. Then, by Proposition 1, n is odd and the decomposition $G_m(P(x))$ is equivalent to $H_{(n-1)/2}(x^2)$. Hence $n = 2m - 1$ and

$$H_{m-1}(x) = G_m(ax + b), \tag{3.8}$$

for some $a, b \in \mathbf{C}$. From (3.8) we have

$$G_{2m-1}(\sqrt{x}) = G_m(ax + b)$$

and therefore

$$G_{2m-1}(x) = G_m(ax^2 + b). \tag{3.9}$$

Relations (3.9) and (2.2) imply

$$x^{2m-2} + (2m-3)Bx^{2m-4} + \cdots B^{m-1} \tag{3.10}$$
$$= (ax^2 + b)^{m-1} + (m-2)B(ax^2 + b)^{m-3} + \cdots . \tag{3.11}$$

We have $a^{m-1} = 1$, and we may assume that $a = 1$. The comparison of $[x^{2m-4}]$ in (3.10) gives

$$(m-1)b = (2m-3)B, \tag{3.12}$$

while the comparison of $[x^{2m-6}]$ gives

$$\binom{m-1}{2} b^2 + (m-2)B = \binom{2m-4}{2} B^2. \tag{3.13}$$

Combining (3.12) and (3.13) we obtain (for $m \neq 2$)

$$2(m-1)B = (1-2m)B^2,$$

which implies $B = 0$ or $B = -1 + \frac{1}{2m-1}$, a contradiction. ■

4 Standard pairs of the first, second and fifth kind

4.1 Standard pair of the first kind: $(x^q,\, ux^r p(x)^q)$

We have $G_n(ax+b) = \varphi(x^q)$. If $q \geq 3$ then Proposition 1 implies that φ is linear, say $\varphi(x) = e_1 x + e_0$. The comparison of the coefficients of x^{n-2} and x^{n-3} in

$$(ax+b)^{n-1} + (n-2)B(ax+b)^{n-3} + \cdots = e_1 x^q + e_0$$

gives $b = 0$ and $(n-2)Ba^{n-3} = 0$, a contradiction.

Assume now that $q = 2$. Then $G_n(ax+b) = \varphi(x^2)$ and $G_m(cx+d) = \varphi(ux^r p^2(x))$, where $r = 0$ or 1. If φ is not linear, then $\varepsilon = \deg(x^r p^2(x)) = 1$ or 2. If $\varepsilon = 2$ then $m = n$, a contradiction, and if $\varepsilon = 1$ then $G_n(x) = G_n(P(x))$, where $P(x) \in \mathbf{Q}[x]$ and $\deg P = 2$, contradicting Corollary 1.

Hence φ is linear and $n = 3$. From $G_3(ax+b) = (ax+b)^2 + B = e_1 x^2 + e_0$, it follows $b = 0$, $e_1 = a^2$ and $e_0 = B$. Therefore we have $G_m(cx+d) = a^2 ux^r p^2(x) + B$ and

$$G_m(x) = (ex+f)P^2(x) + B, \tag{4.1}$$

where $e, f \in \mathbf{Q}$, $P(x) \in \mathbf{Q}[x]$. By Corollary 1 we have $e \neq 0$, and therefore m is even. Relation (4.1) implies that $P(x)$ divides $G(x) - B$ and $G'(x)$. From Lemma 2 we have $\deg P = 1$ and therefore $m = 4$. However, it is easy to check that the polynomial $G_4(x) - B = x^3 + 2Bx - B$ has no multiple roots for $B \neq 0, -\frac{27}{32}$.

Let finally $q = 1$. In this case, $G_n(ax + b) = \varphi(x)$ and $G_m(cx + d) = \varphi(up(x))$. Hence, $G_m(x) = G_n(P(x))$, where $P(x) \in \mathbf{Q}[x]$ and $\deg P \geq 2$ (since $m \neq n$). But this is impossible by Corollary 1.

4.2 Standard pair of the second kind: $(x^2,\, (ux^2 + v)p(x)^2)$

We have $G_n(ax + b) = \varphi(x^2)$ and $G_m(cx + d) = \varphi((ux^2 + v)p^2(x))$. Let $\delta = \deg p$. Since $m \neq n$, we see that $\delta \geq 1$. Therefore, by Proposition 1, the polynomial φ is linear and $n = 3$. As in section 4.1, we obtain $\varphi(x) = a^2x + B$. It implies

$$G_m(x) = (ex^2 + fx + g)P^2(x) + B, \tag{4.2}$$

for $e, f, g \in \mathbf{Q}$ and $P(x) \in \mathbf{Q}[x]$.

From section 4.1 it follows that we may assume $e \neq 0$. Relation (4.2) implies that $P(x)$ divides $\gcd(G_m(x) - B, G'_m(x))$. From Lemma 2 we have $\deg P = 1$ or 2, and therefore $m = 5$ or 7.

Assume that $m = 7$. It is easy to check that for $B \neq 0, \pm\sqrt{\frac{\pm\sqrt{28}-1}{7}}$, the polynomial $G_7(x) - B$ has not two distinct multiple roots.

Assume now that $m = 5$. The polynomial $G_5(x) - B$ has a multiple root iff $B = 0$, 1 or $-\frac{4}{5}$. We are interested only in the case $B = 1$. We have

$$F_5(x) = x^4 + 3x^2 + 1 = F_3(x\sqrt{x^2 + 3}) = (x^2 + 3)x^2 + 1,$$

so this is indeed a standard pair of the second kind. However, we can check directly that the equation

$$y^2 + 1 = x^4 + 3x^2 + 1$$

has only finitely many integer solutions (namely, $(x, y) = (\pm 1, \pm 2), (0, 0)$).

4.3 Standard pair of the fifth kind: $((ux^2 - 1)^3,\, (3x^4 - 4x^3))$

From $G_n(ax + b) = \varphi((ux^2 - 1)^3)$ and Proposition 1 it follows that φ is linear. Hence $m = 7$ and $n = 5$. From

$$G_7(ax + b) = e_1(ux^2 - 1)^3 + e_0$$

it follows that $G_n(ax+b) - e_0$ has a triple root $\frac{1}{\sqrt{u}}$. However, this is impossible since we have shown in the proof of Lemma 2 that all roots of U'_{n-1} (and thus of G'_n) are simple.

5 Standard pairs of the third and fourth kind

5.1 Standard pair of the third kind: $(D_s(x,\alpha^t),\ D_t(x,\alpha^s))$

From $G_n(ax+b) = \varphi(D_s(x,\alpha^t))$ and Proposition 1 we conclude that $s=1$ or $s=2$ or φ is linear. The same conclusion for t follows from $G_m(cx+d) = \varphi(D_t(x,\alpha^s))$ and Proposition 1. Since $\gcd(s,t)=1$, and $s=1$ or $t=1$ contradicts Corollary 1, we must have that φ is linear, say $\varphi(x) = e_1x+e_0$.

Assume that $s \geq 5$. Let $\delta = \alpha^t$. We have $D_s(x,\delta) = d_sx^s + d_{s-2}x^{s-2} + \cdots$, where

$$d_{s-2i} = \frac{s\binom{s-i}{i}}{s-i}(-\delta)^i\,,$$

(see [11]).

If $G_n(ax+b) = \varphi(D_s(x,\delta))$, then the comparison of $[x^{n-2}]$ implies $b=0$. Comparison of degrees gives $n-1=s$. From $[x^{n-1}]$ we see that $e_1d_s = a^{n-1}$. But $d_s = 1$ and thus $e_1 = a^{n-1}$. From $[x^{n-3}]$ it follows that $e_1d_{s-2} = (n-2)Ba^{n-3}$. Hence, $d_{s-2} = \frac{n-2}{a^2}B$, while from the definition $d_{s-2} = -\delta s$. Since $s>4$, from $[x^{n-5}]$ we obtain

$$e_1d_{s-4} = \binom{n-3}{2}B^2a^{n-5}.$$

Since $d_{s-4} = \frac{\delta^2 s(s-3)}{2}$, we have

$$a^4\delta^2 s(s-3) = B^2(n-3)(n-4),$$

$$(n-2)^2(s-3) = s(n-3)(n-4)$$

and finally

$$(n-2)^2(n-4) = (n-1)(n-3)(n-4),$$

a contradiction.

It follows that $s \leq 4$ and analogously $t \leq 4$. Since $\gcd(s,t)=1$, the only remaining cases are $(s,t) = (4,3)$ or $(3,2)$, i.e. $(m,n) = (5,4)$ or $(4,3)$.

Assume $(m,n) = (5,4)$. We have

$$G_5(ax+b) \;=\; e_1(x^4 - 4\alpha^3x^2 + 2\alpha^6) + e_0, \tag{5.1}$$

$$G_4(cx+d) \;=\; e_1(x^3 - 3\alpha^4x) + e_0. \tag{5.2}$$

It clear that (5.1) and (5.2) imply $b = d = 0$ and hence $e_0 = 0$. Now from (5.1) we obtain $e_1 = a^4$ and $B^2 = 2a^4\alpha^6$, a contradiction.

Assume now that $(m, n) = (4, 3)$. It follows that

$$G_4(ax + b) = e_1(x^3 - 3\alpha^2 x) + e_0, \tag{5.3}$$

$$G_3(cx + d) = e_1(x^2 - 2\alpha^3)^k + e_0. \tag{5.4}$$

We have again $b = d = e_0 = 0$. Now (5.3) and (5.4) imply $B = -\frac{3}{2}\alpha^2 a^2 = -2\alpha^3 c^2 = -2\alpha^3 a^3$ and $B = -\frac{27}{32}$, contradicting our assumption that B is a nonzero integer.

5.2 Standard pair of the fourth kind: $\left(\alpha^{-\frac{s}{2}} D_s(x,\alpha),\ -\beta^{-\frac{t}{2}} D_t(x,\beta)\right)$

From Proposition 1 we conclude that $s = t = 2$ or φ is linear. Since $m \neq n$, we see that φ is linear. We have

$$G_n(ax + b) = e_1\alpha^{-s/2}(d_s x^s + d_{s-2}x^{s-2} + \cdots) + e_0.$$

If $s \geq 6$, then we may repeat the discussion for $s \geq 5$ in section 5.1. After doing that, we may assume that $s \leq 4$ and $t \leq 4$.

Since $\gcd(s, t) = 2$, the only remaining case is $(s, t) = (4, 2)$, i.e. $(m, n) = (5, 3)$. Thus

$$G_5(ax + b) = e_1\Big(\frac{x^4}{\alpha^2} - \frac{4x^2}{\alpha} + 2\Big) + e_0, \tag{5.5}$$

$$G_3(cx + d) = e_1\Big(-\frac{x^2}{\beta} + 2\Big) + e_0. \tag{5.6}$$

It is clear that $b = d = 0$. Since $G_n(0) = G_m(0) = 2e_1 + e_0$, we have $B^2 = B$ and $B = 1$. Hence, $G_5(x) = F_5(x)$ and $G_3(x) = F_3(x)$. As in section 4.2, this is a special pair of the fourth kind, but the equation $F_3(y) = F_5(x)$ has only finitely many solutions.

6 Effective theorems for $n = 3$ and $n = 5$

THEOREM **3** *For $m \geq 4$ the equation $G_3(y) = G_m(x)$ has only finitely many solutions which are effectively computable.*

Proof. Our equation becomes $y^2 + B = G_m(x)$. By Lemma 2, the polynomial $G_m(x) - B$ has at most one double root if m is even, and at most two double roots if m is odd. Hence, if $m \notin \{4,5,7\}$, then $G_m(x) - B$ has at least three simple roots and the assertion of the theorem follows from Baker's theorem [1].

Furthermore, in section 4.1 we proved that $G_4(x) - B$ has no double roots for a nonzero integer B, and in section 4.2 we proved that the same is true for $G_5(x) - B$ if $B \neq 1$. But for $(m, B) = (5, 1)$ we have the equation $y^2 = x^2(x^2 + 3)$ with the only solutions $(x, y) = (\pm 1, \pm 2)$, $(0, 0)$. In section 4.2 we also proved that for a nonzero integer B the polynomial $G_7(x) - B$ has at most one double root. Therefore it has at least four simple roots, so that Baker's theorem can be applied again. ■

THEOREM **4** *For $m \geq 3$, $m \neq 5$, the equation $G_5(y) = G_m(x)$ has only finitely many solutions which are effectively computable.*

Proof. We have the equation $y^4 + 3By^2 + B^2 = G_m(x)$. By Theorem 3 we may assume that $m \geq 4$. By the substitution $z = 2y^2 + 3B$ we obtain the equation

$$z^2 = 4G_m(x) + 5B^2. \tag{6.1}$$

Consider the polynomial

$$g_m(x) = 4G_m(x) + 5B^2.$$

As in the proof of Theorem 3, applying Lemma 2, we conclude that if $m \notin \{4, 7\}$, then g_m has at least three simple roots.

However, it is easy to check that for a nonzero integer B the polynomials $g_4(x)$ and $g_7(x)$ have no double roots. It follows that in all cases we may apply Baker's theorem. ■

Acknowledgement: The authors wish to express their gratitude to the referee for suggestions on improvement of the original manuscript. In particular, they are pleased to thank the referee for the much simpler proof of Corollary 1. Section 3 is heavily due to his suggestions.

References

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

[2] F. Beukers, T. N. Shorey, R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal product of terms*, in: Number Theory in Progress, Proceedings of Zakopane meeting in honour of A. Schinzel, de Gruyter, Berlin, 1999, pp. 11–26.

[3] M. Bicknell, *Introduction to Fibonacci polynomials and their divisibility properties*, Fibonacci Quart. **8** (1970), 407–420.

[4] Yu. Bilu, R. F. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith., to appear.

[5] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Math. **107** (1997), 187–219.

[6] H. Davenport, D. J. Lewis, A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Math. Oxford Ser. (2) **12** (1961), 304–312.

[7] M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. **17** (1973), 128-146.

[8] M. Fried, *Arithmetical properties of function fields. II. The generalized Schur problem*, Acta Arith. **25** (1973/74), 225-258.

[9] M. Fried, *On a theorem of Ritt and related Diophantine problems*, J. Reine. Angew. Math. **264** (1974), 40-55.

[10] P. Kirschenhofer, A. Pethő, R. F. Tichy, *On analytical and diophantine properties of a family of counting polynomials*, Acta Sci. Math. (Szeged) **65** (1999), 47–59.

[11] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific & Technical, New York, 1993.

[12] A. Schinzel, *Selected Topics in Polynomials*, The University of Michigan Press, Ann Arbor, 1983.

[13] V. G. Sprindžuk, *Classical Diophantine Equations in Two Unknowns* (in Russian), Nauka, Moscow, 1982; English trans.: Lecture Notes in Math. **1559**, Springer-Verlag, 1994.

Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb
Croatia
E-mail: `duje@math.hr`

Institut für Mathematik
Technische Universität Graz
Steyrergasse 30
A-8010 Graz
Austria
E-mail: `tichy@weyl.math.tu-graz.ac.at`