J. Aust. Math. Soc. **92** (2012), 155–161
doi:10.1017/S1446788712000237

ON THE EQUATION $f(g(x)) = f(x)h^m(x)$ FOR COMPOSITE POLYNOMIALS

HIMADRI GANGULI and JONAS JANKAUSKAS ✉

(Received 26 November 2010; accepted 1 February 2012)

Communicated by I. E. Shparlinski

Abstract

In this paper we solve the equation $f(g(x)) = f(x)h^m(x)$ where $f(x)$, $g(x)$ and $h(x)$ are unknown polynomials with coefficients in an arbitrary field K, $f(x)$ is nonconstant and separable, $\deg g \geq 2$, the polynomial $g(x)$ has nonzero derivative $g'(x) \neq 0$ in $K[x]$ and the integer $m \geq 2$ is not divisible by the characteristic of the field K. We prove that this equation has no solutions if $\deg f \geq 3$. If $\deg f = 2$, we prove that $m = 2$ and give all solutions explicitly in terms of Chebyshev polynomials. The Diophantine applications for such polynomials $f(x)$, $g(x)$, $h(x)$ with coefficients in $\mathbb{Q}$ or $\mathbb{Z}$ are considered in the context of the conjecture of Cassaigne *et al.* on the values of Liouville's λ function at points $f(r)$, $r \in \mathbb{Q}$.

2010 *Mathematics subject classification*: primary 11B83; secondary 11C08, 11D57, 11N32, 11R09, 12D05, 12E10.

Keywords and phrases: Chebyshev polynomial, composite polynomials, Pell equation, multiplicative dependence.

1. Introduction

The problem investigated in the present paper is motivated by the following question.

QUESTION 1. Do there exist integer polynomials $f(x)$, $g(x)$ and $h(x)$ of degrees

$$\deg f \geq 3, \quad \deg g \geq 2,$$

$f(x)$ separable (and possibly irreducible in $\mathbb{Z}[x]$), such that

$$f(g(x)) = f(x)h^2(x)?$$

This question has been posed in connection with recent work by Borwein *et al.* [2] on the sign changes of *Liouville's lambda function* $\lambda(f(n))$ for the values of integer quadratic polynomials $f(x) \in \mathbb{Z}[x]$ at integer points $n \in \mathbb{Z}$. Recall that for $n \in \mathbb{Z}$, the lambda function $\lambda(n)$ is defined by $\lambda(n) = (-1)^{\Omega(n)}$, where $\Omega(n)$ is the total number of prime factors of n, counted with multiplicity. Alternatively, $\lambda(n)$ is the completely

A visit of the second author to IRMACS Centre, Simon Fraser University was funded by the Lithuanian Research Council (Student research support project).

multiplicative function defined by $\lambda(p) = -1$ for each prime p dividing n. Chowla [4] conjectured that

$$\sum_{n\le x} \lambda(f(n)) = o(x)$$

for any integer polynomial $f(x)$ which is not of the form $f(x) = bg(x)^2$, where $b \in \mathbb{Z}$ and $g(x) \in \mathbb{Z}[x]$. For $f(x) = x$, Chowla's conjecture is equivalent to the prime number theorem and has been proven for linear polynomials $f(x)$, but is open for polynomials of higher degree. The much weaker conjecture of Cassaigne *et al.* [3] is as follows.

Conjecture 2. If $f(x) \in \mathbb{Z}[x]$ and is not of the form of $bg^2(x)$ for some $g(x) \in \mathbb{Z}[x]$, then $\lambda(f(n))$ changes sign infinitely often.

Even this has not been proved unconditionally for polynomials of degree $\deg f \ge 2$.

In the paper [2], it has been proved that the sequence $\lambda(f(n))$ cannot be eventually constant for quadratic integer polynomials $f(x) = ax^2 + bx + c$, provided that at least one sign change occurs for $n > (|b| + (|D| + 1)/2)/2a$, where D is the discriminant of $f(x)$. The proof is based on the solutions of Pell-type equations. In practice, using this conditional result, one can prove Cassaigne's conjecture for any particular integer quadratic $f(x)$, for instance, $f(x) = 3x^2 + 2x + 1$. In contrast, the only examples of degree $\deg f \ge 3$ for which the conjecture has been proven in [3] are $f(x) = \prod_{j=1}^{k}(ax + b_j)$, where $a, b_k \in \mathbb{N}$, b_k are all distinct, $b_1 \equiv \cdots \equiv b_k \bmod a$. No similar examples of irreducible integer polynomials of degree $d \ge 3$ are known. The problem of finding an irreducible example of degree $d = 3$ appears interesting and is probably difficult.

We now explain how the composition identity in Question 1 could be of use to prove that $\lambda(f(n))$ or $\lambda(f(-n))$ is not eventually constant for cubic polynomials $f(x)$. Assume that the leading coefficient of $g(x)$ is positive. Since $\deg g \ge 2$, there exists a positive integer n_0 such that $g(n) > n$ for integers $n > n_0$. Suppose that there exist two integers $k_0, l_0 > n_0$ such that $\lambda(f(k_0)) = -\lambda(f(l_0))$. Then $\lambda(f(k_j))$ and $\lambda(f(l_j))$ also differ in sign for infinite sequences of integers k_j and l_j, defined by $k_{j+1} = g(k_j)$ and $l_{j+1} = g(l_j)$, $j \ge 0$, since $\lambda(f(g(n))) = \lambda(f(n))$ follows by the composition identity.

Unfortunately, the answer to Question 1 is negative. In the next section we prove a general result which holds for polynomials with coefficients in an arbitrary field K. Our result shows that one cannot prove the conjecture for cubic polynomials $f(x)$ by using the composition identity in Question 1. We also refer to [6], where a certain composition identity was used to investigate multiplicative dependence of integer values of quadratic integer polynomials, and [5] for further results in this direction.

2. Main result

The main result of this paper is the following theorem.

Theorem 3. *Let $m \ge 2$ be an integer not divisible by the characteristic of the field K. Suppose that $f(x) \in K[x]$ is nonconstant and separable, and the polynomial $g(x)$ has a* *nonzero derivative and* $\deg g \geq 2$. *Then the equation*

$$f(g(x)) = f(x)h^m(x)$$

holds if and only if one of the following conditions holds:

(i) $f(x) = ax + b$ *where* $a, b \in K$, $a \neq 0$, *and* $g(x) = (x + b/a)\, h^m(x) - b/a$;

(ii) $f(x) = ax^2 + bx + c$ *where* $a, b, c \in K$, $a \neq 0$, *and* $m = 2$, *and for some* $n \geq 1$,

$$g(x) = \frac{1}{2a}\left(\pm T_n\left(\frac{2ax+b}{\sqrt{D}}\right)\sqrt{D} - b\right), \quad h(x) = \pm U_{n-1}\left(\frac{2ax+b}{\sqrt{D}}\right),$$

$T_n(x)$ *and* $U_n(x)$ *being Chebyshev polynomials of the first and second kind, and* D *being the discriminant* $b^2 - 4ac$ *of* $f(x)$.

We remark that the condition on the separability of $f(x)$ cannot be weakened in Theorem 3, as may be seen by taking $f(x) = g(x) = x(x-1)^m$ in $\mathbb{Q}[x]$. Further, the requirement that $g(x)$ has a nonzero derivative for fields K of nonzero characteristic cannot be weakened. Indeed, consider the simple example where $f(x) = x^d - 1$ and $g(x) = x^{p^l}$ in $\mathbb{F}_p[x]$. Moreover, if the characteristic p divides the nonzero exponent m in the equation $f(g(x)) = f(x)h^m(x)$, then one can write $h^m(x) = h_1^{m/p}(x^p) = h_2^{m/p}(x)$, where $h_2(x)$ is a polynomial with coefficients in K.

Recall that for a field K of characteristic other than 2, the *Chebyshev polynomials* $T_n(x) \in K[x]$ of the *first kind* are defined by the linear recurrence of order two,

$$T_0(x) = 1, \quad T_1(x) = x \quad \text{and} \quad T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x). \tag{1}$$

Similarly, the Chebyshev polynomials of the *second kind* $U_n(x) \in K[x]$ are defined by the recurrence

$$U_0(x) = 1, \quad U_1(x) = 2x \quad \text{and} \quad U_{n+2}(x) = 2xU_{n+1}(x) - U_n(x). \tag{2}$$

The polynomials $T_n(x)$ and $U_n(x)$ contain only even powers of x for even n and odd powers of x for odd n. Thus, the coefficients of $g(x)$ and $h(x)$ in Theorem 3(ii) lie in K if n is odd and in $K(\sqrt{D})$ if n is even. Chebyshev polynomials have many other remarkable properties; see, for instance, [12]. They play a key role in the theorems of Ritt on decompositions of polynomials [13]. In addition, Chebyshev polynomials are related to permutation polynomials over finite fields called Dickson polynomials [8]. In our proof, the following property of Chebyshev polynomials will be useful.

PROPOSITION 4. *Suppose that the characteristic of the field* K *is not equal to* 2. *Then all the solutions of the Pell equation*

$$P^2(x) - (x^2 - 1)Q^2(x) = 1$$

in the ring $K[x]$ *are given by*

$$P(x) = \pm T_n(x) \quad \text{and} \quad Q(x) = \pm U_{n-1}(x),$$

where $T_n(x)$ *and* $U_n(x)$ *are Chebyshev polynomials of the first and second kind, respectively.*

The equation that appears in Proposition 4 is a special case of a general polynomial Pell equation, $P(x)^2 - D(x)Q^2(x) = 1$. Solutions to general Pell equations in polynomials over complex number field $K = \mathbb{C}$ were investigated by Pastor [11]. Dubickas and Steuding [7] gave an elementary algebraic proof for arbitrary field K. The proof of Proposition 4 can be found in [7]. Alternative proofs (in the case where $K = \mathbb{C}$) are given in [1, 11].

3. Proof of Theorem 3

In this section we prove Theorem 3.

Proof. Set $d = \deg f$. Let $a \in K$ and $b \in K$ be the leading coefficients of polynomials $f(x)$ and $g(x)$; then $ab \neq 0$. Suppose that L is the field extension of K generated by the roots of the three polynomials $f(x)$, $x^m - 1$ and $x^m - b$. Then

$$f(x) = a \prod_{\alpha \in V(f)} (x - \alpha). \tag{3}$$

Here $V(f) \subset L$ denotes the set of the roots of the polynomial $f(x)$. The composition equation $f(g(x)) = f(x)h^m(x)$ factors in $L[x]$ into

$$a \prod_{\alpha \in V(f)} (g(x) - \alpha) = a \prod_{\alpha \in V(f)} (x - \alpha)h^m(x), \tag{4}$$

and one can cancel a on both sides. Observe that distinct factors $g(x) - \alpha$ on the left-hand side of (4) are relatively prime in $L[x]$ since their difference is a nonzero constant. We claim that at most one factor $g(x) - \alpha$ may be relatively prime to $f(x)$ if $m \geq 2$ and the characteristic of K does not divide m. Indeed, suppose that $g(x) - \beta$, where $\beta \in V(f)$ and $\beta \neq \alpha$, is another such factor. Then both $g(x) - \alpha$ and $g(x) - \beta$ divide $h^m(x)$, so $g(x) - \alpha$ and $g(x) - \beta$ must be the mth powers of polynomials $u(x)$ and $v(x)$ in $L[x]$ which divide $h(x)$, say, $g(x) - \alpha = u^m(x)$ and $g(x) - \beta = v(x)^m$ (note that $u(x)$ and $v(x)$ belong to $L[x]$ since the field L contains all roots of $f(x)$ and the mth roots of the leading coefficient b of the polynomial $g(x)$). Then $u(x)^m - v(x)^m = \beta - \alpha$ is a nonzero constant polynomial. On the other hand,

$$u^m(x) - v^m(x) = \prod_{j=0}^{m-1} (u(x) - \zeta^j v(x)),$$

where ζ is a primitive mth root of unity in L and at least one of the polynomials $u(x) - \zeta^j v(x)$ has degree greater than orequal to one, which is impossible.

Now, suppose that $V(f) = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$. Let V_j be the set containing all distinct common roots of the polynomial $g(x) - \alpha_j$ and the polynomial $f(x)$,

$$V_j = V(g(x) - \alpha_j) \cap V(f).$$

Then $g(x) - \alpha_j = f_j(x)u_j(x)$, where $u_j(x) \in L[x]$ and

$$f_j(x) = \prod_{\alpha \in V_j} (x - \alpha).$$

Note that $f_j(x)$ are all separable and coprime in $L[x]$. Since $f(x)$ is also separable, the equation (4) implies that

$$a \prod_{j=1}^{d} f_j(x) = f(x), \tag{5}$$

and consequently

$$\prod_{j=1}^{d} u_j(x) = h^m(x). \tag{6}$$

The polynomials $u_j(x)$ are relatively prime, thus $u_j(x) = h_j^m(x)$, $j = 1, \ldots, d$, for some polynomials $h_j(x) \in L[x]$ whose product is equal to $h(x)$ in (6). Let $n_j = \deg f_j$, for $j = 1, \ldots, d$. Without loss of generality, assume that $n_1 \le n_2 \le \cdots \le n_d$. Then $n_1 \ge 0$. Observe that $n_2 \ge 1$ if $n_1 = 0$, since no two factors $g(x) - \alpha_j$ can be coprime with $f(x)$, as noted above. The identity (5) gives

$$n_1 + n_2 + \cdots + n_d = \deg f = d. \tag{7}$$

Since $g(x) = f_j(x)h_j(x)^m + \alpha_j$, one also has $\deg g \equiv n_j \bmod m$. We now consider two cases for $\deg g$ modulo m.

Case 1. Assume that $\deg g \equiv 0 \bmod m$. Then $n_j \ge m$ for $j \ge 2$, hence

$$d \ge m(d-1) \tag{8}$$

by (7). Since $m \ge 2$, one has $d \ge 2d - 2$ which is only possible if $d = 1$ or $d = 2$. Suppose that $d = 2$. Then $m \le 2$ by (8).

Case 2. Assume that $\deg g \not\equiv 0 \bmod m$. Then $n_1 = \cdots = n_d = 1$ by (7). Suppose that $\deg g = sm + 1$, where $s := \deg h_j \ge 1$ for $1 \le j \le d$. Since $h_j^m(x) \mid g(x) - \alpha_j$, the polynomials $h_j^{m-1}(x)$ are (relatively prime) factors of the derivative $g'(x)$. By the conditions of the theorem, $g'(x)$ is a nonzero polynomial, hence

$$ms \ge \deg g' \ge \deg h_1^{m-1} + \cdots + \deg h_d^{m-1} = d(m-1)s$$

and, consequently,

$$m \ge d(m-1). \tag{9}$$

Then $d \le m/(m-1) \le 2$. Suppose that $d = 2$. Then, in addition, (9) gives $m \le 2$.

Thus it remains to consider the cases where $d = 1$ and $d = 2$. If $d = 1$, then the polynomial $f(x)$ is linear, thus $f(x) = ax + b$ where $a, b \in K$ and $a \ne 0$. The equation $f(g(x)) = f(x)h^m(x)$ is equivalent to

$$ag(x) + b = (ax + b)h^m(x),$$

so one simplification solves $g(x)$ and this completes the proof in this case.

Suppose that $d = 2$. Then $f(x) = ax^2 + bx + c$ where $a, b, c \in K$ and $a \ne 0$. Let $D = b^2 - 4ac$; then $D \ne 0$ since $f(x)$ is separable. Further, $m = 2$ by the conditions of Theorem 3 and the degree inequalities in the two cases above. Hence, it suffices

TABLE 1. Examples of polynomials $f(x), g(x), h(x) \in \mathbb{Z}[x]$ in Theorem 3.

$f(x)$	$g(x)$	$h(x)$
x^2+1	$4x^3+3x$	$4x^2+1$
x^2-1	$4x^3-3x$	$4x^2-1$
x^2+2	$2x^3+3x$	$2x^2+1$
x^2-2	$2x^3-3x$	$2x^2-1$
x^2+4	x^3+3x	x^2+1
x^2-4	x^3-3x	x^2-1

to find the polynomials $g(x)$ and $h(x)$ in the equation $f(g(x)) = f(x)h^2(x)$. Since the characteristic of the field K is not equal to 2 by the conditions of Theorem 3, the linear change of variables $x \to x(t)$ defined by

$$x = \frac{t\sqrt{D} - b}{2a}$$

transforms the polynomial $f(x)$ into

$$f(x) = \frac{D}{4a}F(t),$$

where $F(t) = t^2 - 1$. Set

$$G(t) = \frac{1}{\sqrt{D}}\Big(2ag\Big(\frac{t\sqrt{D}-b}{2a}\Big) + b\Big) \quad \text{and} \quad H(t) = h\Big(\frac{t\sqrt{D}-b}{2a}\Big).$$

By straightforward substitution, one can easily check that the map $x \to x(t)$ transforms the composition equation $f(g(x)) = f(x)h^2(x)$ into $(D/4a)F(G(t)) = (D/4a)F(t)H^2(t)$. Cancelling the factor $D/4a$ on both sides, one obtains

$$F(G(t)) = F(t)H^2(t),$$

or, equivalently,

$$G^2(t) - (t^2-1)H^2(t) = 1.$$

By Proposition 4, the solutions to this equation are all of the form $G(t) = \pm T_n(t)$, $H(t) = \pm U_{n-1}(t)$, where $T_n(t)$ and $U_n(t)$ are Chebyshev polynomials of the first and second kind. Application of the inverse map $t \to t(x)$ now yields the result. □

4. Rational and integer examples

Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial with rational coefficients. For $n = 3$ in Theorem 3, one has $T_3(x) = 4x^3 - 3x$ and $U_2(x) = 4x^2 - 1$. By Theorem 3, $f(g(x)) = f(x)h^2(x)$ holds for

$$\begin{aligned} g(x) &= (16a^2x^3 + 24abx^2 + (9b^2 + 12ac)x + 8bc)/D, \\ h(x) &= (16a^2x^2 + 16abx + 3b^2 + 4ac)/D. \end{aligned} \tag{10}$$

Extend the definition of the λ function to the whole set of rationals $\mathbb{Q}$ by complete multiplicativity. Then, using the method outlined in Section 1, one can easily prove the following analogue of Theorem 2 in [2] for the sign changes of λ function at rational points: either $\lambda(f(r))$ is constant for all rational numbers r greater than the largest real root of $g(x) - x$ or it changes sign infinitely many often.

The question of finding all solutions of the composition equation in integer polynomials $f(x)$, $g(x)$, and $h(x)$ is closely related to the solution of the polynomial Pell equations in $\mathbb{Z}[x]$; see [9, 10, 14]. This does not seem to be easy. Examples of such polynomials are $f(x) = x^2 \pm 1$, $f(x) = x^2 \pm 2$, $f(x) = x^2 \pm 4$. The corresponding polynomials $g(x)$ and $h(x)$ with integer coefficients can be found using (10); see Table 1.

References

[1] E. J. Barbeau, *Pell's Equation*, Problem Books in Mathematics (Springer, New York, 2003).
[2] P. Borwein, S. Choi and H. Ganguli, 'Sign changes of the Liouville function on quadratics', *Canad. Math. Bull.*, to appear.
[3] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, 'On finite pseudorandom binary sequences, IV. The Liouville function. II', *Acta Arith.* **95**(4) (2000), 343–359.
[4] S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Mathematics and Its Applications, 4 (Gordon and Breach Science Publishers, New York, 1965).
[5] P. Drungilas and A. Dubickas, 'Multiplicative dependence of shifted algebraic numbers', *Colloq. Math.* **96**(1) (2003), 75–81.
[6] A. Dubickas, 'Multiplicative dependence of quadratic polynomials', *Liet. Mat. Rink.* **38**(3) (1998), 295–303.
[7] A. Dubickas and J. Steuding, 'The polynomial Pell equation', *Elem. Math.* **59**(4) (2004), 133–143.
[8] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edn, Encyclopedia of Mathematics and its Applications, 20 (Cambridge University Press, Cambridge, 1997).
[9] J. McLaughlin, 'Polynomial solutions of Pell's equation and fundamental units in real quadratic fields', *J. London Math. Soc.* (2) **67**(1) (2003), 16–28.
[10] M. B. Nathanson, 'Polynomial Pell's equations', *Proc. Amer. Math. Soc.* **56** (1976), 89–92.
[11] A. V. Pastor, 'Generalized Chebyshev polynomials and the Pell–Abel equation', *Fundam. Prikl. Mat.* **7**(4) (2001), 1123–1145.
[12] T. J. Rivlin, *Chebyshev Polynomials*, 2nd edn, Pure and Applied Mathematics (New York) (Wiley, New York, 1990).
[13] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, 77 (Cambridge University Press, Cambridge, 2000).
[14] W. A. Webb and H. Yokota, 'Polynomial Pell's equation', *Proc. Amer. Math. Soc.* **131**(4) (2003), 993–1006 (electronic).

HIMADRI GANGULI, Department of Mathematics,
Simon Fraser University, 8888 University Drive,
Burnaby, British Columbia, Canada V5A 1S6
e-mail: hganguli@sfu.ca

JONAS JANKAUSKAS, Department of Mathematics and Informatics,
Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
e-mail: jonas.jankauskas@gmail.com