ARCHIVUM MATHEMATICUM (BRNO)
Tomus 54 (2018), 119–125

POLYNOMIALS WITH VALUES WHICH ARE POWERS OF INTEGERS

Rachid Boumahdi and Jesse Larone

Abstract. Let P be a polynomial with integral coefficients. Shapiro showed that if the values of P at infinitely many blocks of consecutive integers are of the form $Q(m)$, where Q is a polynomial with integral coefficients, then $P(x) = Q(R(x))$ for some polynomial R. In this paper, we show that if the values of P at finitely many blocks of consecutive integers, each greater than a provided bound, are of the form m^q where q is an integer greater than 1, then $P(x) = (R(x))^q$ for some polynomial $R(x)$.

1. Introduction

Several authors have studied the integer solutions of the equation

$$y^m = P(x)$$

where $P(x)$ is a polynomial with rational coefficients, and $m \geq 2$ is an integer. If P is an irreducible polynomial of degree at least 3 with integer coefficients, then the above equation is called a hyperelliptic equation if $m = 2$ and a superelliptic equation otherwise.

In 1969, Baker [1] gave an upper bound on the size of integer solutions of the hyperelliptic equation when $P(x) \in \mathbb{Z}[x]$ has at least three simple zeros, and for the superelliptic equation when $P(x) \in \mathbb{Z}[x]$ has at least two simple zeros.

Using a refinement of Baker's estimates and a criterion of Cassels concerning the shape of a potential integer solution to $x^p - y^q = 1$, Tijdeman [11] proved in 1976 that Catalan's equation $x^p - y^q = 1$ has only finitely many solutions in integers $p > 1$, $q > 1$, $x > 1$, $y > 1$.

Suppose that $y^m - P(x)$ is irreducible in $\mathbb{Q}[x, y]$ where P is monic and $\gcd(m, \deg P) > 1$. Under these conditions, Masser [6] considered the equation $y^m = P(x)$ in the particular case $m = 2$ and $\deg P = 4$. In particular, setting $P(x) = x^4 + ax^3 + bx^2 + cx + d$ where $P(x)$ is not a perfect square, it was shown that for $H \geq 1$ and $X(H)$ defined as the maximum of $|x|$ taken over all integer solutions of all equations $y^2 = P(x)$ with $\max\{|a|, |b|, |c|, |d|\} \leq H$, there are absolute constants $k > 0$ and K such that $kH^3 \leq X(H) \leq KH^3$. Walsh [13] later

2010 *Mathematics Subject Classification*: primary 13F20.
Key words and phrases: integer-valued polynomial.
Received July 25, 2017, revised January 2018. Editor R. Kučera.
DOI: 10.5817/AM2018-2-119

obtained an effective bound on the integer solutions for the general case. Poulakis [7] described an elementary method for computing the solutions of the equation $y^2 = P(x)$, where P is a monic quartic polynomial which is not a perfect square. Later, Szalay [10] established a generalization for the equation $y^q = P(x)$, where P is a monic polynomial and q divides $\deg P$.

Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_r$ are the roots of $P(x)$ with respective multiplicities $e_1, e_2, \ldots, e_r$. Given an integer $m \geq 3$, we define, for each $i = 1, \ldots, r$,

$$m_i = \frac{m}{(e_i, m)} \in \mathbb{N}.$$

It has been shown by LeVeque [5] that the superelliptic equation $y^m = P(x)$ can have infinitely many solutions in $\mathbb{Q}$ only if $(m_1, m_2, \ldots, m_r)$ is a permutation of either $(2, 2, 1, \ldots, 1)$ or $(t, 1, 1, \ldots, 1)$ with $t \geq 1$. In 1995, Voutier [12] gave improved bounds for the size of solutions (x_0, y_0) to the superelliptic equation with $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Q}$ under the conditions of LeVeque.

Given a polynomial $P(x) \in \mathbb{Z}[x]$ and an integer $q \geq 2$, it is then natural to ask when the equation

$$y^q - P(x) = 0$$

will have infinitely many solutions (x_0, y_0) with $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Q}$. It is clear that this will immediately be the case when $P(x) = \big(R(x)\big)^q$ for some polynomial $R(x) \in \mathbb{Q}[x]$. Indeed, this serves as our motivation.

In 1913, Grösch solved a problem proposed by Jentzsch [4], showing that if a polynomial $P(x)$ with integral coefficients is a square of an integer for all integral values of x, then $P(x)$ is the square of a polynomial with integral coefficients. Kojima [4], Fuchs [2], and Shapiro [9] later proved more general results. In particular, Shapiro proved that if $P(x)$ and $Q(x)$ are polynomials of degrees p and q respectively, which are integer-valued at the integers, such that $P(n)$ is of the form $Q(m)$ for infinitely many blocks of consecutive integers of length at least $p/q + 2$, then there is a polynomial $R(x)$ such that $P(x) = Q(R(x))$.

Recall that the height of a polynomial

$$P(x) = a_p x^p + a_{p-1} x^{p-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$$

is defined by

$$H(P) = \max_{i=0,\ldots,p} |a_i|$$

where $|a_i|$ denotes the modulus of $a_i \in \mathbb{C}$ for each $i = 0, \ldots, p$. We will prove the following result:

Theorem 1. *Let $P(x) = a_p x^p + a_{p-1} x^{p-1} + \cdots + a_0$ be a polynomial with integral coefficients where $a_p > 0$, and let $q \geq 2$ be an integer that divides p. Suppose that there exist integers m_i, $i = 0, 1, \ldots, p/q + 1$, such that $P(n_0 + i) = {m_i}^q$ for some consecutive integers $n_0, n_0 + 1, \ldots, n_0 + p/q + 1$ where*

$$n_0 > 1 + (p/q + 1)!\, p q^{p/q+1} H(P)^{p/q+2} \prod_{j=2}^{p/q+2} (jp - j + 1)^2 .$$

Set $M := \sum_{i=0}^{p/q+1} \binom{p/q+1}{i} |m_{p/q+1-i}|$. *If there exist at least* M *more blocks of such consecutive integers* n_k+i, $i = 0, \dots, p/q+1$, *such that* $n_k > n_{k-1}+p/q+1$ *for each* $k = 1, \dots, M$ *and* $P(n_k+i) = m_{k,i}^q$ *for all* $k = 1, \dots, M$ *and* $i = 0, \dots, p/q+1$ *for some integers* $m_{k,i}$, *then there exists a polynomial* $R(x)$ *such that* $P(x) = (R(x))^q$.

2. Preliminaries

Let $P(x)$ and $Q(x)$ be non-zero polynomials with integral coefficients of degrees p and q respectively. The following properties are easily verified:

(i) $H(P) \geq 1$

(ii) $H(P') \leq pH(P)$

(iii) $H(P+Q) \leq H(P) + H(Q)$

(iv) $H(PQ) \leq (1+p+q)H(P)H(Q)$

The first and second properties are trivial, while the third follows immediately from the triangle inequality. The last property follows by noting that the coefficient of x^k in the product of $a_px^p + a_{p-1}x^{p-1} + \cdots + a_0$ and $b^qx^q + b_{q-1}x^{q-1} + \cdots + b_0$ is given by $\displaystyle\sum_{i+j=k} a_ib_j$, where the number of summands is at most $\lceil (p+q)/2 \rceil + 1 \leq 1+p+q$.

We recall a result which can be found in Rolle [8].

Lemma 1. *Let* $f(x) \in \mathbb{R}[x]$ *be a monic polynomial. If* $t \geq 1 + H(f)$, *then* $f(t) > 0$.

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. The result follows from writing $f(t)$ as

$$f(t) = t^{n-1}\Big(t + \Big(a_{n-1} + \frac{a_n - 2}{t} + \cdots + \frac{a_0}{t^{n-1}}\Big)\Big),$$

since from $t > 1$, we deduce that

$$\Big| a_{n-1} + \frac{a_{n-2}}{t} + \cdots + \frac{a_0}{t^{n-1}} \Big| \leq \sum_{i=0}^{n-1} |a_i|(1/t)^{n-1-i} \leq H(f)\frac{t}{t-1} < t\,,$$

and we conclude that $t + \big(a_{n-1} + \frac{a_n-2}{t} + \cdots + \frac{a_0}{t^{n-1}}\big)$ is positive. □

We will also require the following lemma, which is implicit in the proof of the sole lemma in [9].

Lemma 2. *Let* $f(x)$ *be a branch of an algebraic function, real and regular for all* $x > x_0$ *for some* x_0, *and satisfying* $|f(x)| < Cx^\alpha$ *where* $C > 0$ *and* $\alpha > 0$. *Then* $\lim_{x\to\infty} f^{(r+1)}(x) = 0$, *where* r *is the least integer greater than or equal to* α.

We now establish a bound on the zeros of a particular class of algebraic functions.

Lemma 3. *Let* $P(x)$ *be a polynomial of degree* p *with integral coefficients, and let* $f(x)$ *be a branch of the algebraic function defined by the equation* $y^q = P(x)$ *where* q *is an integer greater than* 1. *For any integer* $k \geq 2$, $R_k(x) = q^kf(x)^{kq-1}f^{(k)}(x)$ *is a polynomial with integral coefficients such that* $\deg R_k \leq k(p-1)$ *and* $H(R_k) \leq (k-1)!\,pq^{k-1}H(P)^k\prod_{j=2}^k(jp-j+1)^2$.

Proof. Differentiating $f^q = P$ with respect to x, we obtain $qf^{q-1}f' = P'$. We have $\deg P' = p-1$ and $H(P') \leq pH(P)$. We now consider $R_k = q^k f^{kq-1} f^{(k)}$ and prove the result by induction on k.

For the base case $k = 2$, we differentiate $qf^{q-1}f' = P'$ with respect to x to obtain

$$qf^{q-1}f'' + q(q-1)f^{q-2}f'f' = P''\,.$$

Multiplying both sides of this equation by qf^q, we obtain

$$\begin{aligned} q^2 f^{2q-1} f'' + (q-1)(qf^{q-1}f')(qf^{q-1}f') &= qf^q P'' \\ q^2 f^{2q-1} f'' + (q-1)P'P' &= qPP''\,, \end{aligned}$$

so that

$$R_2 = q^2 f^{2q-1} f'' = qPP'' - (q-1)P'P'\,.$$

We then have

$$\begin{aligned} \deg R_2 &\leq \max\{p + \deg P'', \deg P' + \deg P'\} \\ &= \max\{p + (p-1) - 1, p-1+p-1\} \\ &= 2(p-1)\,, \end{aligned}$$

and

$$\begin{aligned} H(R_2) &\leq qH(PP'') + (q-1)H(P'P') \\ &\leq q(1 + p + \deg P'')H(P)H(P'') + q(1 + \deg P' + \deg P')H(P')H(P') \\ &\leq q(1 + p + p - 2)H(P)[\deg P' H(P')] + q(1 + 2p - 2)[pH(P)]^2 \\ &\leq q(2p-1)H(P)(p-1)[pH(P)] + q(2p-1)[pH(P)]^2 \\ &= pq(2p-1)H(P)^2[(p-1) + p] \\ &= pqH(P)^2(2p-1)^2\,. \end{aligned}$$

Therefore, the result holds for the base case.

We now assume that the result holds for some integer $k \geq 2$. Differentiating $R_k = q^k f^{kq-1} f^{(k)}$ with respect to x yields

$$q^k f^{kq-1} f^{(k+1)} + q^k(kq-1)f^{kq-2}f'f^{(k)} = {R_k}'\,.$$

Multiplying both sides of the equation by qf^q, we obtain

$$\begin{aligned} q^{k+1} f^{[k+1]q-1} f^{(k+1)} + (kq-1)[qf^{q-1}f'][q^k f^{kq-1} f^{(k)}] &= qf^q {R_k}' \\ q^{k+1} f^{[k+1]q-1} f^{(k+1)} + (kq-1)P'R_k &= qP{R_k}', \end{aligned}$$

so that

$$R_{k+1} = q^{k+1} f^{[k+1]q-1} f^{(k+1)} = qP{R_k}' - (kq-1)P'R_k\,.$$

By hypothesis, we have $\deg R_k \le k(p-1)$. Thus,

$$\begin{aligned}\deg R_{k+1} &\le \max\{p+\deg {R_k}', \deg P' + \deg R_k\}\\ &= \max\{p+\deg R_k - 1, p-1+\deg R_k\}\\ &= p-1+\deg R_k\\ &\le p-1+k(p-1)\\ &= (k+1)(p-1)\,.\end{aligned}$$

In addition,

$$\begin{aligned}H(R_{k+1}) &\le qH(P{R_k}') + (kq-1)H(P'R_k)\\ &\le kq(1+p+\deg {R_k}')H(P)H({R_k}')\\ &\quad + kq(1+\deg P' + \deg R_k)H(P')H(R_k)\\ &\le kq(p+\deg R_k)H(P)[\deg R_k H(R_k)]\\ &\quad + kq(p+\deg R_k)[pH(P)]H(R_k)\\ &= kq(p+\deg R_k)^2 H(P)H(R_k)\,.\end{aligned}$$

By hypothesis, we have $\deg R_k \le k(p-1)$ and

$$H(R_k) \le (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp-j+1)^2\,.$$

Thus,

$$\begin{aligned}H(R_{k+1}) &\le kq\big(p+k(p-1)\big)^2 H(P)(k-1)\,!pq^{k-1}H(P)^k\prod_{j=2}^{k}(jp-j+1)^2\\ &= k!\,pq^k H(P)^{k+1}\prod_{j=2}^{k+1}(jp-j+1)^2\,,\end{aligned}$$

proving the result. □

Corollary 1. *Let $P(x)$ be a polynomial of degree p with integral coefficients, and let $f(x)$ be a branch of the algebraic function defined by the equation $y^q = P(x)$ where q is an integer greater than 1. If β is a real zero of $f^{(k)}(x)$ for any integer $k \ge 2$ such that $\beta > 1 + H(P)$, then $\beta \le 1 + (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp-j+1)^2$.*

Proof. Let β be a zero of $f^{(k)}(x)$ such that $\beta > 1 + H(P)$. If $f(\beta) = 0$, then $0 = f(\beta)^q = P(\beta)$ and $\beta \le 1 + H(P)$ by Lemma 1. We conclude that β is not a zero of $f(x)$.

Since β must be a zero of the polynomial $R_k = q^k f^{kq-1} f^{(k)}$, we conclude from Lemma 1 and Lemma 3 that

$$\beta \le 1 + H(R_k) \le 1 + (k-1)!pq^{k-1}H(P)^k\prod_{j=2}^{k}(jp-j+1)^2\,,$$

as claimed. □

Defining the difference operator Δ by $\Delta f(x) = f(x+1) - f(x)$ and recursively defining higher order difference operators, we have the following lemma from [3]:

Lemma 4. *Let $k \geq 1$ be an integer. Then* $\Delta^k f(x) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i f(x+k-i)$.

3. Proof of Theorem 1

Proof. Let $x = \phi(y)$ denote the branch of the algebraic function inverse to the polynomial $y = x^q$, that is, $\phi(y) = y^{1/q}$. Then $\phi(y)$ is positive and free of singularities for all $y \geq 0$.

Set $f(x) = \phi(P(x))$. Then $f(x)$ is asymptotically $a_p^{1/q} x^{p/q}$, and $f(n) = \pm m$ for any n such that $P(n) = m^q$.

We show by contradiction that $f(x)$ is a polynomial. Suppose that $f(x)$ is not a polynomial. Then $f^{(p/q+2)}(x)$ is not identically zero. By Corollary 1, any real zero β of $f^{(p/q+2)}(x)$ satisfying $\beta > 1 + H(P)$ must also satisfy

$$\beta \leq 1 + (p/q+1)! pq^{p/q+1} H(P)^{p/q+2} \prod_{j=2}^{p/q+2} (jp - j + 1)^2 .$$

Thus, $f^{(p/q+1)}(x)$ is either monotone decreasing or monotone increasing for

$$x > 1 + (p/q+1)! pq^{p/q+1} H(P)^{p/q+2} \prod_{j=2}^{p/q+2} (jp - j + 1)^2 .$$

Suppose that $f^{(p/q+1)}(x)$ is monotone decreasing. It must then be strictly positive for $x > 1+(p/q+1)\,!pq^{p/q+1} H(P)^{p/q+2} \prod_{j=2}^{p/q+2} (jp-j+1)^2$, since $\lim_{x\to\infty} f^{(p/q+1)}(x) = 0$ by Lemma 2.

Applying the difference operator Δ to $f(x)$ $p/q+1$ times, we find that $\Delta^{p/q+1} f(n_0)$ is an integer. We now apply the Mean Value Theorem repeatedly to obtain a number $c_0 \in (n_0, n_0 + p/q + 1)$ such that $f^{(p/q+1)}(c_0) = \Delta^{p/q+1} f(n_0)$ is an integer.

For each $k = 1, \ldots, M$, we repeat the above process with each block of consecutive integers $n_k + i$, $i = 0, \ldots, p/q+1$, to obtain numbers c_k such that $c_k \in (n_k, n_k + p/q + 1)$ and $f^{(p/q+1)}(c_k) = \Delta^{p/q+1} f(n_k)$ are integers.

By Lemma 4, the integer $f^{(p/q+1)}(c_0) = \Delta^{p/q+1} f(n_0)$ is such that

$$\begin{aligned} |f^{(p/q+1)}(c_0)| &= \left| \sum_{i=0}^{p/q+1} \binom{p/q+1}{i} (-1)^i f(n_0 + p/q + 1 - i) \right| \\ &\leq \sum_{i=0}^{p/q+1} \binom{p/q+1}{i} |m_{p/q+1-i}| \\ &= M . \end{aligned}$$

Since $f^{(p/q+1)}(x)$ is monotone decreasing, $f^{(p/q+1)}(c_k) < f^{(p/q+1)}(c_{k-1})$ for each $k = 1, \ldots, M$. Thus $f^{(p/q+1)}(c_j) \leq M - j$ for $j = 0, \ldots, M$. This implies that

$f^{(p/q+1)}(c_M) \leq 0$, which contradicts $f^{(p/q+1)}(x)$ being strictly positive at

$$c_M > c_0 > n_0 > 1 + (p/q+1)!pq^{p/q+1}H(P)^{p/q+2} \prod_{j=2}^{p/q+2} (jp - j + 1)^2 .$$

Similarly, the case where $f^{(p/q+1)}(x)$ is monotone increasing leads to a contradiction. Therefore, $f(x)$ is a polynomial and $P(x) = f(x)^q$. □

References

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

[2] Fuchs, W.H.J., *A polynomial the square of another polynomial*, Amer. Math. Monthly **57** (1950), 114–116.

[3] Jordan, C., *Calculus of Finite Differences*, Chelsea Publishing Company, New York, N.Y., 1950, 2nd edition.

[4] Kojima, T., *Note on number-theoretical properties of algebraic functions*, Tohoku Math. J. **8** (1915).

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

[6] Masser, D.W., *Polynomial bounds for Diophantine equations*, Amer. Math. Monthly (1980), 486–488.

[7] Poulakis, D., *A simple method for solving the Diophantine equation* $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, Elem. Math. **54** (1) (1999), 32–36.

[8] Rolle, M., *Traité d'algèbre*, Paris, 1690.

[9] Shapiro, H.S., *The range of an integer-valued polynomial*, Amer. Math. Monthly **64** (1957).

[10] Szalay, L., *Superelliptic equations of the form* $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, Bull. Greek Math. Soc. **46** (2002), 23–33.

[11] Tijdeman, R., *On the equation of Catalan*, Acta Arith. **29** (2) (1976), 197–209.

[12] Voutier, P.M., *An upper bound for the size of integral solutions to* $Y^m = f(X)$, J. Number Theory **53** (1995), 247–271.

[13] Walsh, P.G., *A quantitative version of Runge's theorem on Diophantine equations*, Acta Arith. **62** (2) (1992), 157–172.

Laboratoire d'Arithmétique, Codage,
Combinatoire et Calcul Formel,
Université des Sciences et Technologies Houari Boumédiène,
16111, El Alia, Algiers, Algeria
E-mail: r_boumehdi@esi.dz

Département de mathématiques et de statistiques,
Université Laval, Québec,
Canada, G1V 0A6
E-mail: jesse.larone.1@ulaval.ca