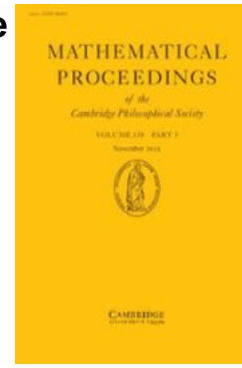

Polynomials which are near to *k*-th powers

K. R. Matthews

Mathematical Proceedings of the Cambridge Philosophical Society / Volume 61 / Issue 01 / January 1965, pp 1 - 5
DOI: 10.1017/S0305004100038561, Published online: 24 October 2008

PROCEEDINGS OF THE
Cambridge Philosophical Society

VOL. 61 JANUARY 1965 PART 1

Proc. Camb. Phil. Soc. (1965), **61**, 1
Printed in Great Britain

Polynomials which are near to k-th powers

BY K. R. MATTHEWS
Trinity College, Cambridge

(*Received* 30 *July* 1964)

1. Let $f(x)$ be a polynomial of degree $n \geqslant 2$ with integral coefficients, the highest coefficient being positive. It is well known that if $f(x)$ is an exact k-th power for all sufficiently large integers x, where $k \geqslant 2$, then $f(x) = g(x)^k$ identically, where $g(x)$ is another polynomial with integral coefficients. (See Pólya and Szegö (4), section 8, problems 114, 190; also Davenport, Lewis and Schinzel (1), where other references are given.) The main purpose of this note is to prove that if we suppose only that

$$f(x) = y^k + o(x) \tag{1}$$

as $x \to \infty$ through integral values, where y^k denotes for each x the integral k-th power nearest to $f(x)$, then

$$f(x) = (g(x))^k + A \tag{2}$$

identically, where A is a constant integer.

In these results it is not necessary to suppose that the hypothesis applies for *all* large integers x. We shall say that a sequence

$$x_1 < x_2 < x_3 < \dots$$

of positive integers is *thin* if, for some integer $M > 0$ and some $\alpha > 0$, we have

$$x_{j+M} - x_j > x_j^{\alpha} \tag{3}$$

for all sufficiently large j. Then for the first result it suffices if the positive integers x for which $f(x) = y^k$ do not form a thin sequence, relative to certain values of M and α which depend only on n and k. This is an easy deduction from the work of Dörge, and occurs later as Lemma 2. For the second result we have to make a somewhat stronger hypothesis, namely that (1) holds for all x except for a set whose number up to X, say $N(X)$, satisfies

$$N(X) = o(X^{1/k}). \tag{4}$$

Stated formally, our result is as follows.

THEOREM. *Let $f(x)$ be a polynomial of degree $n \geqslant 2$ with integral coefficients and highest coefficient positive, and let $k \geqslant 2$ be an integer. Suppose that for any $\epsilon > 0$ the inequality*

$$|f(x) - y^k| < \epsilon x, \tag{5}$$

where y^k is the integral k-th power nearest to $f(x)$, holds for all positive integers x apart from exceptions whose number up to X satisfies (4). *Then $f(x)$ is identically of the form* (2), *where $g(x)$ is a polynomial with integral coefficients.*

The proof depends on the quantitative form of Hilbert's Irreducibility Theorem given by Dörge (2), (3), and on a use of expansions of algebraic functions of x in powers of x^{-1} which is similar to the use made in the theory of Diophantine equations. (See Th. Skolem (5), chapter 6, section 1.)

2. LEMMA 1. *Let $F(x, y)$ be a polynomial with integral coefficients which is irreducible over the rationals. Then the sequence of positive integers x for which $F(x, y)$, considered as a polynomial in y, is reducible over the rationals is thin; that is, this sequence satisfies* (3) *for certain values of M and α. These values depend only on the degree of F.*

This is the principal result of the second paper of Dörge cited above.

LEMMA 2. *Let $f(x)$ be a polynomial of degree $n \geqslant 2$ with integral coefficients and highest coefficient positive, which is not identically of the form $g(x)^k$, where $g(x)$ is a polynomial with integral coefficients and $k \geqslant 2$. Then the sequence of positive integers x for which $f(x)$ is an integral k-th power is a thin sequence, for values of M and α which depend only on n and k.*

Proof. We factorize $f(x) - y^k$ into polynomials which are irreducible over the rationals:

$$f(x) - y^k = F_1(x, y) F_2(x, y) \ldots F_h(x, y); \tag{6}$$

we can suppose, by Gauss's lemma, that the factors have integral coefficients. Assume first that each factor is of degree 2 at least in y.

If x_0 is any integer for which $f(x_0) = y_0^k$, where y_0 is an integer, then there is some i such that $F_i(x_0, y)$ has the factor $y - y_0$, and this is a proper factor. For each i the sequence of positive integers x for which $F_i(x, y)$ has a proper factor is a thin sequence, by Lemma 1. Further, it is easily seen that the union of h thin sequences is itself thin, and this holds for values of the parameters M and α which depend only on the parameters of the given sequences and on h. Since $h \leqslant \frac{1}{2}k$, the conclusion holds for values of M and α which depend only on n and k.

Suppose now that one of the $F_i(x, y)$ is of the first degree in y, say

$$F_1(x, y) = G(x) - yH(x),$$

where $G(x)$, $H(x)$ are relatively prime polynomials with integral coefficients. Since

$$f(x)\,(H(x))^k = (G(x))^k$$

identically, $H(x)$ must be a constant, and this constant can be taken to be 1 by Gauss's lemma. Hence $f(x) = G(x)^k$ identically, and this is contrary to hypothesis.

3. *Proof of the theorem.*

Case 1. *Suppose n is a multiple of k*, say $n = kN$. Then

$$f(x) = Rx^{kN} + a_{kN-1}x^{kN-1} + \ldots + a_0,$$

where the coefficients are integers and $R > 0$. We have

$$(f(x))^{1/k} = R^{1/k}x^N + \alpha_{N-1}x^{N-1} + \ldots + \alpha_0 + O(x^{-1})$$

as $x \to \infty$, for certain real numbers $\alpha_{N-1}, \ldots, \alpha_0$. If $R^{1/k}$ is irrational, the famous theorem of Weyl ((6), 326–331)) tells us that the values of the polynomial on the right of the last equation are uniformly distributed (mod 1) as x takes all positive integral values. In this case there is a set of integers x of positive density for which

$$|(f(x))^{1/k} - y| > \tfrac{1}{3}$$

for all integers y. These x have the property that

$$|f(x) - y^k| > C_1 x^{(k-1)N} \geqslant C_1 x$$

from some point onwards, where $C_1 > 0$ is independent of x. Thus the exceptions to (5) have positive density, which is contrary to hypothesis.

We can therefore suppose that R is a kth power. Replacing R by R^k, for convenience of notation, we have

$$f(x) = R^k x^{kN} + a_{kN-1}x^{kN-1} + \ldots + a_0.$$

Now
$$(f(x))^{1/k} = Rx^N + r_{N-1}x^{N-1} + \ldots + r_0 + r_{-1}x^{-1} + \ldots,$$

where the coefficients r_j are rational. The series is absolutely convergent for all sufficiently large x, and the remainder after any particular term $r_j x^j$ is $O(x^{j-1})$ as $x \to \infty$.

Let D be a common denominator for the rational numbers $r_{N-1}, \ldots, r_1$. The fractional part of $(f(Dt))^{1/k}$ is the same as that of

$$r_0 + r_{-1}(Dt)^{-1} + \ldots,$$

and unless r_0 is an integer we have

$$|(f(Dt))^{1/k} - y| > C_2 > 0$$

for all integers y and all large integers t. This again contradicts the hypothesis, since (5) is not satisfied when x is any large multiple of D. Hence r_0 is an integer.

If $r_{-1}, r_{-2}, \ldots,$ are all 0, we get $f(x) = g(x)^k$ identically, where $g(x)$ is a polynomial with rational coefficients, and therefore with integral coefficients by Gauss's lemma. Now let r_{-j} be the first non-zero coefficient with negative suffix. Then $(f(Dt))^{1/k}$ differs from the nearest integer by an amount which is asymptotic to

$$r_{-j}(Dt)^{-j}$$

as $t \to \infty$. Hence
$$f(Dt) - y^k \sim C_3 t^{(k-1)N-j}$$

as $t \to \infty$, where $C_3 \neq 0$. If $(k-1)N - j \geqslant 1$, then (5) is not satisfied when x is any large multiple of D, and again this is contrary to hypothesis. Hence $(k-1)N - j \leqslant 0$, and this implies that

$$|f(Dt) - y^k| < 2|C_3|$$

for all sufficiently large t.

We apply Lemma 2 to each of the polynomials

$$f(Dt) - a,$$

where a takes all integral values satisfying $|a| < 2|C_3|$. If none of these polynomials is identically of the form $g(t)^k$, the sequence of integers t for which any one of them is an integral kth power is a thin sequence. This contradicts the fact that these sequences together include all sufficiently large t.

It follows that for some integer a we have

$$f(Dt)-a = (g(t))^k$$

identically, where $g(t)$ is a polynomial with integral coefficients. Hence

$$f(x)-a = (g_1(x))^k,$$

where $g_1(x)$ has rational, and therefore integral, coefficients. This proves the theorem in Case 1.

Case 2. Suppose that n is not a multiple of k, say $n = kN+l$, where $N \geqslant 0$ and $0 < l < k$. Write

$$f(x) = Rx^n + a_{n-1}x^{n-1} + \ldots + a_0.$$

Then

$$(f(t^k))^{1/k} = R^{1/k}t^n + \alpha_{N-1}t^{n-k} + \ldots + \alpha_0 t^l + O(t^{l-k})$$

as $t \to \infty$. If $R^{1/k}$ is not an integer, it follows from Weyl's theorem, as in Case 1, that there is a sequence of integers t, of positive density, for which

$$|f(t^k)-y^k| > C_4 t^{n(k-1)},$$

where $C_4 > 0$. Since $n(k-1) \geqslant 2(k-1) \geqslant k$, the corresponding integers $x = t^k$ do not satisfy (5). The number of such integers up to X does not satisfy (4), and therefore we have a contradiction to the hypothesis of the theorem. Hence R is a kth power.

Replacing R by R^k for convenience, we obtain

$$(f(t^k))^{1/k} = Rt^n + r_{N-1}t^{n-k} + \ldots + r_0 t^l + r_{-1}t^{l-k} + \ldots,$$

where the coefficients r_j are now rational. Let D be a common denominator for $r_{N-1}, \ldots, r_0$. Then the fractional part of $(f(D^k t^k))^{1/k}$ is

$$r_{-1}(Dt)^{l-k} + r_{-2}(Dt)^{l-2k} + \ldots.$$

If $r_{-1}, r_{-2}, \ldots$ are all 0, we obtain

$$f(t^k) = t^{lk}(g(t^k))^k \tag{7}$$

identically, where g has rational, and therefore integral, coefficients. We postpone this case, since we shall encounter it again later.

If r_{-j} is the first non-zero coefficient, we get

$$f(D^k t^k) - y^k \sim C_5 t^{n(k-1)+l-jk}$$

as $t \to \infty$, where $C_5 \neq 0$. Now

$$n(k-1)+l-jk = k(n-N-j).$$

If this exponent is k or more, the integers $x = D^k t^k$ do not satisfy (5), and their number up to X does not satisfy (4), and this is contrary to hypothesis. Hence the exponent is negative or zero, and we get

$$|f(D^k t^k) - y^k| < 2|C_5|$$

for all large t.

Applying Lemma 2 to the polynomials

$$f(D^k t^k) - a, \quad |a| < 2|C_5|,$$

we infer as before that one of these is identically a kth power. Hence

$$f(u^k) - a = (h(u))^k$$

identically, where h has rational, and therefore integral, coefficients. Since we can replace $f(x)$ by $f(x)-a$ without affecting the theorem, we can suppose without loss of generality that $a = 0$. Plainly $h(u)$ is of degree $n = kN + l$. Since all the terms in $h(u)^k$ with exponents not divisible by k must vanish, we easily find that

$$h(u) = u^l g(u^k),$$

where g is a polynomial of degree N with integral coefficients. Hence

$$f(x) = x^l (g(x))^k,$$

and this is the same as the case postponed from (7).

For any fixed z and large x, we have

$$\begin{aligned}(f(x+z))^{1/k} &= x^{l/k}(1+zx^{-1})^{l/k} g(x+z)\\ &= x^{l/k}(q_N(z)\,x^N + \ldots + q_0(z) + q_{-1}(z)\,x^{-1} + \ldots),\end{aligned}$$

where the $q_i(z)$ are polynomials in z with rational coefficients. It is easily verified that

$$q_{-1}(z) = \binom{N + l/k}{N+1} g_N z^{N+1} + \text{lower powers},$$

where g_N is the highest coefficient in $g(x)$.

We choose an integer z for which $q_{-1}(z) \neq 0$. Then

$$(f(t^k + z))^{1/k} = r_N t^{l+kN} + r_{N-1} t^{l+k(N-1)} + \ldots + r_0 t^l + r_{-1} t^{l-k} + \ldots,$$

where the r_j are rational and $r_{-1} \neq 0$. For a suitable positive integer D, we have

$$f(D^k t^k + z)^{1/k} - y \sim C_6 t^{l-k}$$

as $t \to \infty$, where $C_6 \neq 0$. This gives

$$f(D^k t^k + z) - y^k \sim C_7 t^{n(k-1)+l-k}$$

as $t \to \infty$, where $C_7 \neq 0$. Now

$$n(k-1) + l - k \geqslant \begin{cases}(k+1)(k-1) + l - k \geqslant k & \text{if} \quad N > 0,\\ 2(k-1) + 2 - k = k & \text{if} \quad N = 0.\end{cases}$$

Hence the integers $x = D^k t^k + z$ do not satisfy (5), and since they also do not satisfy (4) we have a contradiction to the hypothesis. This completes the proof of the theorem.

The author is indebted to Prof. H. Davenport for suggesting the problem and for preparing the manuscript for publication.

REFERENCES

(1) DAVENPORT, H., LEWIS, D. J. and SCHINZEL, A. Polynomials of certain special types. *Acta Arith.* **9** (1964), 107–116.

(2) DÖRGE, K. Zum Hilbertschen Irreduzibilitätssatz. *Math. Ann.* **95** (1926), 84–97.

(3) DÖRGE, K. Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes. *Math. Ann.* **96** (1927), 176–182.

(4) PÓLYA, G. and SZEGÖ, G. *Aufgaben und Lehrsätze aus der Analysis*, vol. II (Berlin, 1925).

(5) SKOLEM, TH. *Diophantische Gleichungen* (Ergebnisse der Math. v, 4; Berlin, 1938).

(6) WEYL, H. Ueber die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.* **77** (1916), 313–352.