On polynomials taking small values at integral arguments

by

ROBERTO Dvorčíček and UMBERTO ZANNIER (Pisa)

1. Introduction. It is well known (see for example [5], problems 114, 190) that a polynomial with integral coefficients whose values at integers are kth powers is in fact the kth power of a polynomial with integer coefficients.

This theorem has been generalized and improved in various directions (see for instance [2], [4], [6]). In particular, Davenport-Lewis-Schinzel have shown that if every arithmetical progression contains an integer \( a \) such that the equation \( F(a, y) = 0 \) has an integral solution \( y \), where \( F \in \mathbb{Q}[X, Y] \), then there exists a polynomial \( g \in \mathbb{Q}[X] \) such that \( F(x, g(x)) = 0 \) identically.

Suppose now that the values of the polynomial \( f(a) \) are not just kth powers, but, in some sense, “near” to kth powers: what can then be said about the polynomial \( f \)? Is it “near” to the kth power of a polynomial?

A question of this kind was positively answered by Matthews [3], who showed that if \( f \in \mathbb{Z}[X] \) has positive leading coefficient and degree at least two, then the condition

\[
f(n) = b^n + o(n), \quad n \in \mathbb{N}\setminus \mathcal{S}
\]

where \( b^n \) is the integral kth power nearest to \( f(n) \) and \( \mathcal{S} \) is a sufficiently small set, implies

\[
f(a) = (g(a))^k + a
\]

identically, for some \( g \in \mathbb{Z}[X] \) and \( a \in \mathbb{Z} \).

More generally we observe that, if \( a \) is a positive integer, then there exists an integer \( b \) such that

\[
a = b^k + R
\]

where \( R \ll b^{k-1} \). Then our question becomes interesting when “near” to a kth power means that \( f(n) = b^k + R_1 \) where \( R_1 \) grows less rapidly than \( b^{k-1} \)
We may formulate these conditions assuming that the polynomial $F(x, y) = g^k - f(x)$ has, for fixed $x_0$, not just an integral zero, but a good approximation to zero, i.e.,

$$|F(x_0, y_0)| \leq |y_0^k - f(x_0)| = |E_1| = o(y_0^{k-1}) = o\left(\left|\frac{\partial F}{\partial y}(x_0, y_0)\right|\right).$$

In the direction of [2], we have then a natural generalization (see Remark 2 below) of this problem assuming that, for all $x_0$ in some set, the inequality

$$|F(x_0, y)| = o\left(\sup_{|t| < 1} \left|\frac{\partial F}{\partial y}(x_0, \xi)\right|\right)$$

for $x_0 \to \infty$

has an integral solution $y_0$. We shall show by entirely elementary means that these assumptions lead in fact to the expected consequences.

Before stating our results we introduce some notation. If $x$ is a real number and $k$ is a positive integer, $\|x\|_k$ shall denote the distance of $x$ from the nearest $k$th power,

$$\|x\|_k = \min_{n \in \mathbb{Z}} |x - n^k|$$

setting, as usual, $\|x\| = \|x\|_1$.

In analogy with this, we shall write, for $g \in C[X]$,

$$\|g\|_k = \min_{x \in C(X)} \deg(x - g^k).$$

Further, if $\mathcal{A}$ is any finite set, let $|\mathcal{A}|$ denote the number of its elements, while if $\mathcal{A}$ is a sequence of integers, we set

$$\mathcal{A}(N) = \{a \in \mathcal{A}, 0 \leq a \leq N\}$$

and

$$\mathcal{A}(\mathcal{A}) = \limsup_{N \to \infty} \frac{|\mathcal{A}(N)|}{N}, \quad \mathcal{A}(\mathcal{A}) = \liminf_{N \to \infty} \frac{|\mathcal{A}(N)|}{N}$$

calling these numbers upper, resp. lower, asymptotic density of $\mathcal{A}$.

Our results are the following:

**Theorem.** Let $F \in R[X, Y]$. Assume that $\mathcal{A}$ is a sequence of natural numbers with $\mathcal{A}(\mathcal{A}) > 0$ such that, for all $a \in \mathcal{A}$ we find integers $y(a)$ satisfying

$$|F(a, y(a))| = o\left(\sup_{|t| < 1} \left|\frac{\partial F}{\partial y}(a, \xi)\right|\right).$$

Then there exist a polynomial $P$ with rational coefficients and a sequence $\mathcal{A} \subset \mathcal{A}$ such that

$$\mathcal{A}(\mathcal{A} \setminus \mathcal{A}) = 0$$

and

$$|F(b, P(b))| \leq |F(b, y(b))| \quad \text{for all } b \in \mathcal{A}.$$

**Corollary.** Let $f \in R[X]$ and $\mathcal{A}$ a sequence of positive integers such that $\mathcal{A}(\mathcal{A}) > 0$. Assume that, for all $a \in \mathcal{A}$, we have

$$x = y^k(a) + o(y^{k-1}(a)), \quad a \to \infty$$

for some integers $y(a)$. Then there exists an integer $D$ such that

$$\|D^k f(n)\|_n \sim e^{-n^{1/1}} \quad \text{for all } n \in \mathcal{A},$$

where $e > 0$.

2. **Remarks.**

1. Replacing condition (1) by

$$F(a, y(a)) = 0$$

we obtain the same conclusion as in the above mentioned theorem of Davenport–Lewis–Schinzel. However there exist sequences with positive upper asymptotic density which do not intersect infinitely many arithmetical progressions, and conversely, so neither statement may be directly derived from the other.

2. As observed in the introduction for the particular case when $F(x, y) = g^k - f(x)$, condition (1) cannot be replaced by

$$|F(a, y(a))| \leq \sup_{|t| < 1} \left|\frac{\partial F}{\partial y}(a, \xi)\right|.$$

In fact, suppose that $F(n, y)$ has a real zero $\lambda$, for all sufficiently large $n$. Then, setting $y(n) = [\lambda n]$, we have

$$|F(n, y(n))| = |y(n) - \lambda| \left|\frac{\partial F}{\partial y}(n, \xi)\right| \leq \left|\frac{\partial F}{\partial y}(n, \xi)\right|$$

where $y(n) \leq \xi \leq \lambda$, but the conclusion is in general not true.

3. In the particular case $F(x, y) = y^k - f(x)$, the sup condition in (1) may be substituted with the simpler

$$|F(a, y(a))| = o\left(\left|\frac{\partial F}{\partial y}(a, y(a))\right|\right).$$

In the general case, however, this would lead to a weaker theorem. To see this consider the polynomial

$$F(x, y) = x(y - a)^2 + 1.$$
4. We observe that the sup in (1) may be taken over any neighborhood of \( g(n) \) of fixed length. In fact let \( P \) be any polynomial of degree \( k \). From Newton’s interpolation formula it follows that

\[
\sup_{|x| < \delta} |P(x)| \leq \sup_{|x| < \delta} |P(x)| \leq C \sup_{|x| < \delta} |P(x)|
\]

where \( A \geq \delta > 0 \) and \( C \) depends only on \( A \), \( \delta \), \( k \).

5. We point out that (2) is essentially best possible, in the sense that, given any function \( g(N) \) which tends to zero, one cannot improve (2) to

\[
(2a) \quad |A \Delta \Delta(N)| \leq Ng(N).
\]

To prove this consider

\[
F(x, y) = (y^2 - x)(xy - x^2 + 1).
\]

Choose now, as is certainly possible, a function \( r(k) \) such that

(i) \( r(k) \to 0 \) as \( k \to \infty \),

(ii) \( \sum_{k \leq r(k)} kr(k) > a^2 \xi^2(a) + a^3 \).

Now we set \( \mathcal{A} = \mathbb{N} \) and

\[
y(n) = \begin{cases} 
   k & \text{if } |n - k^2| \leq kr(k), \\
   n^2 & \text{otherwise}.
\end{cases}
\]

It is not difficult to verify that for every polynomial \( P \) the inequality

\[
|F(n, y(n))| < |F(n, P(n))|
\]

holds whenever \( |n - k^2| \leq kr(k) \) and \( n \) is large enough; moreover the conditions of our theorem are clearly fulfilled in view of (i). Now, recalling the meaning of \( \mathcal{A} \), this means that

\[
\mathcal{A} \Delta \Delta = \bigcup_{k \geq r(k)} [k^2 - kr(k), k^2 + kr(k)]
\]

whence

\[
|\mathcal{A} \Delta \Delta(x)| \geq \sum_{k \leq r(k)} kr(k) + O(1) \geq ax^2 + ax^3
\]

thus contradicting (2a).

3. Proofs. The following result will play an important role in the sequel.

LEMMA. Let \( d \) be a positive integer and \( f \in \mathbb{C}[x] \). Assume that there exists a sequence \( \mathcal{A} \in \mathbb{N} \) with \( \mathcal{A}(\mathcal{A}) > 0 \) such that

\[
|f(a)| \to 0 \quad \text{as } a \in \mathcal{A}.
\]

Then \( f \in \mathbb{Q}[X] \).

Proof. We write \( f(x) = a_0 + a_2 x^2 + \cdots + a_d x^d \), where \( a_0 \neq 0 \), and set, for fixed \( d \),

\[
I(f) = a_d, \quad \delta(f) = k.
\]

First we note that necessarily \( \delta(f) = 0 \pmod{d} \), since otherwise the sequence \( \{f(n), n \in \mathbb{N}\} \) would be uniformly distributed \( \pmod{1} \) (see [7], p. 382, 8. Anwendung für einen Beweis); similarly, we also obtain that \( I(f) \in \mathbb{Q} \) ([7], p. 380, 5. Anwendung). Now suppose that \( f \in \mathbb{C}[X] \) satisfies the hypotheses of the lemma; but \( f \notin \mathbb{Q}[X] \). Then we may certainly write

\[
f(x) = q(x)|q + g(x)
\]

where \( q \in \mathbb{N}, q \in \mathbb{Z}[X] \), and either \( I(g) \neq 0 \) or \( \delta(g) \neq 0 \pmod{d} \). Pick a congruence class \( \{\equiv qN \pmod{d}\} \) such that \( \mathcal{A} = \mathcal{A}(\{\equiv qN \pmod{d}\}) \) has \( \mathcal{A}(\mathcal{A}') > 0 \). Let \( g_i(x) = g(x) + q_i(x)q \); then, if \( a' \in \mathcal{A} \), we have trivially

\[
\|f(a')\| = \|g_i(a')\| \to 0
\]

a contradiction, since either \( I(g_i) \neq 0 \) or \( \delta(g_i) \neq 0 \pmod{d} \).

We may now begin the proof of the theorem, recalling some basic facts about Puisieux expansions (see for instance [1], pp. 47–52). Let \( F \in \mathbb{C}[X, Y] \) and \( D = \deg_P F \). Then we may write

\[
F(x, y) = Q(x) \prod_{i=1}^{D} (y - a_i(x))
\]

where

\[
a_i(x) = \sum_{j=0}^{\infty} a_{ij} x^j, \quad a_{ij} \neq 0, \quad i = 1, \ldots, D,
\]

for some \( \mathbb{C}, a \in \mathbb{N} \), the series being convergent outside a sufficiently large circle. Applying this to our polynomial \( F \), we first show that

\[
\min_{i \in \mathcal{A}} |y(a) - a_i(a)| \to 0 \quad \text{for } a \in \mathcal{A}.
\]

In fact from hypothesis (1) we have, for large \( a \in \mathcal{A} \),

\[
\left| \prod_{i=1}^{D} (y(a) - a_i(a)) \right| \leq o \left( \sup_{k \in \mathbb{N} \setminus \mathcal{A}} \left| \prod_{i=1}^{D} (\varepsilon - a_i(a)) \right| \right)
\]

\[
= o \left( \sup_{k \in \mathbb{N} \setminus \mathcal{A}} \max_{i \in \mathcal{A}} \left| \varepsilon - a_i(a) \right| \right).
\]

Assume that (5) does not hold; then there exist an infinite sequence \( \{a_n\} \subset \mathcal{A} \) and \( \delta > 0 \) such that

\[
\min_{i \in \mathcal{A}} |y(a) - a_i(a)| \geq \delta
\]
It follows that
\[
\prod_{j=1}^{\delta} |\xi - a_j(a_k)| \leq \prod_{j=1}^{\delta} \{ |\xi - y(a_k)| + |y(a_k) - a_j(a_k)| \}
\leq \prod_{j=1}^{\delta} \left( |y(a_k) - a_j(a_k)| + \frac{1}{\delta} \right) \leq \frac{1}{\delta} \left( 1 + \frac{1}{\delta} \right)^{\delta - 1} \prod_{j=1}^{\delta} |y(a_k) - a_j(a_k)|
\]
and this contradicts (6). Write now
\[
a_k(a) = \sum_{\delta = 0}^{\infty} a_{\delta} \omega^{\delta - n|\alpha|} + \sum_{\delta = 0}^{\infty} a_{\delta} \omega^{\delta} = P_\delta(w^{1/\delta}) - O(w^{1/\delta}).
\]
From (5) we derive immediately
\[
\min_{i} |y(a) - P_i(w^{1/\delta})| = o(1) \quad \text{for } a \in \mathcal{A}.
\]
Rearranging eventually the indices, suppose that
\[
R_i(a) = P_i(w^{1/\delta}) \in Q[X] \quad \text{for } i = 1, \ldots, D_1
\]
(this set may possibly be empty), and
\[
R_i(a) \not\in Q[X] \quad \text{for } i = D_1 + 1, \ldots, D.
\]
From the lemma it follows that the minimum in (7) can be attained at \(i \geq D_1 + 1\) only on a sequence \(a' \in \mathcal{A} \) with \(d(a') = 0\). This implies in particular that \(D_1 \geq 1\). We show that, for large \(b \in \mathcal{A} \setminus \mathcal{A}'\),
\[
\min_{c \in D_1} |y(b) - R_i(b)| = 0.
\]
In fact let \(r\) be a common denominator for all the coefficients of the \(R_i\)'s. Fix \(b \in \mathcal{A} \setminus \mathcal{A}'\); then either (8) is true or
\[
\min_{c \in D_1} |y(b) - R_i(b)| \geq 1/r,
\]
but this is inconsistent for large \(b\) in view of our definition of \(\mathcal{A}'\). Next define an order relation in \(C[X] \) by
\[
P_1 < P_2 \quad \text{iff } |P_1(m)| < |P_2(m)| \quad \text{for all sufficiently large } m \in N.
\]
Then it is clear that, for every pair of polynomials \(P_1, P_2\), at least one of the relations \(P_1 < P_2, P_2 < P_1\) holds. Choose then \(R_i\) with \(j \leq D_1\), such that \(P_\delta, R_i(a)\) is minimum with respect to \(<\). Now we are finished: in fact, set \(\mathcal{B} = \mathcal{A} \setminus \mathcal{A}' \cup [1, L]\), where \(L\) is large; then, for \(b \in \mathcal{B} \) we have
\[
|F[b, R_i(b)]| = \min_{c \in D_1} |F[b, R_i(b)]| < |F[b, y(b)]|
\]
the last inequality being a consequence of (8); moreover
\[
d(\mathcal{A} \setminus \mathcal{B}) \leq d([1, L]) = 0.
\]
Proof of Corollary. Applying the theorem to \(P(x, y) = y^k - f(x)\), which obviously satisfies (1), we obtain the existence of a polynomial \(P \in Q[X] \) such that
\[
|f(n) - P^k(n)| = o(P^{k-1}(n))
\]
for all \(n\) in some infinite sequence \(\mathcal{B}\), whence for all \(n \in N\). Setting
\[
R(x) = f(x) - P^k(x)
\]
we contend that
\[
|f_n| = \deg R \leq \frac{k - 1}{k} \deg f - 1.
\]
In fact from (9) we derive
\[
|f_n| = \deg R \leq \frac{k - 1}{k} \deg f - 1.
\]
Now choose \(\mathcal{S} \in C[X] \) such that \(\deg (f - \mathcal{S}) = |f_n| \); (10) will be proved by showing that \(\mathcal{S}^k = P^k\). Assume the contrary; then
\[
\deg (\mathcal{S}^k - P^k) = \deg \prod_{\delta = 0}^{k - 1} (\mathcal{S} - \omega^{\delta} P) \geq (k - 1) \deg P \geq \frac{k - 1}{k} \deg f
\]
while it follows from (11) that
\[
\deg (\mathcal{S}^k - P^k) = \deg ((\mathcal{S} - f) + (f - P^k)) < \frac{k - 1}{k} \deg f - 1
\]
and we have a contradiction.

Write now \(P(x) = P_\delta(a)/D\), where \(P_\delta \in Z[X] \) and, for \(n \in N\), pick an integer \(g(n)\) such that
\[
|D^k f(n) - g^k(n)| = \|D^k f(n)\|_k.
\]
We have
\[
|D^k f(n) - g^k(n)| \leq |D^k f(n) - P^k_\delta(n)| + o(P^{k-1}_\delta(n))
\]
and thus we obtain
\[
|g^k(n) - P^k_\delta(n)| \leq |g^k(n) - D^k f(n)| + |D^k f(n) - P^k_\delta(n)| = o(P^{k-1}_\delta(n)).
\]
On the other hand
\[
|g^k(n) - P^k_\delta(n)| = \prod_{\delta = 0}^{k - 1} (g(n) - \omega^{\delta} \cdot P_\delta(n)) \geq |g(n) - P_\delta(n)| |P_\delta(n)|^{k - 1}
\]
whence
\[ |P_1(n) - g(n)| = o(1). \]
This implies, for large \( n \), \( P_1(n) = g(n) \). Now the result is achieved, as follows from the relation
\[ \|D^k f(n)\|_\infty = |D^k f(n) - g(n)| = |D^k f(n) - P_1(n)| \sim n^{\delta k}. \]

References


1. Introduction. Statement of results. Let \( a \) and \( q \) be co-prime integers, \( q \geq 1 \) and for any \( x \geq 2 \) let \( \pi(x; q, a) \) be the number of primes \( \leq x \) congruent to \( a \mod q \). One of the basic and important problems in analytic theory of numbers is that of proving an asymptotic formula for \( \pi(x; q, a) \) that would hold, depending on \( x \), for modulus \( q \) as large as possible.

The classical prime number theorem of Siegel and Walfisz states that if \( A \) is a given positive number and \( q \leq (\log x)^A \) then
\[
\pi(x; q, a) = \frac{1}{\varphi(q)} \cdot \log x + O(\exp(-c\sqrt{\log x}))
\]
where \( c \) and the constant implied in the symbol \( O \) depend on \( A \) alone (not effectively computable if \( A \geq 2 \)). A mention should be made of the two conjectures:
\[
\pi(x; q, a) = \frac{1}{\varphi(q)} \cdot \log x + O(x^{\theta_1 + \epsilon}), \quad \text{Great Riemann Hypothesis (GRH)},
\]
\[
\pi(x; q, a) = \frac{1}{\varphi(q)} \cdot \log x + O(q^{-1/2}x^{1/4 + \epsilon}), \quad \text{H. L. Montgomery's Hypothesis},
\]
the first one giving an asymptotic formula for \( q < x^{1/4 - \epsilon} \) and the latter for \( q \leq x^{1/3} \) (cf. [18]), neither of these relations is expected to be proved in the near future.

With the development of Brun's and Selberg's sieve methods it became motivated and popular to investigate statistical results which would hold for "almost all" \( q ")s in wider ranges. After pioneering works of Yu. V. Linnik [13] and A. Rényi [18] and some others [17], [1] in 1965 E. Bombieri [2] and M. I. Vinogradov [21] proved a mean-value theorem which states, in a form given by Bombieri, that for any \( A > 0 \) the following holds
\[
\sum_{\substack{q \leq x \sigma \leq 1 \nu \geq 1 \nu < x}} \max_{\sigma < 1} \max_{\nu \geq 1} \left| \pi(x; q, a) - \frac{1}{\varphi(q)} \log x \right| \leq x(\log x)^{A - 1}
\]