ACTA ARITHMETICA
XLII (1983)

On polynomials taking small values at integral arguments

by

ROBERTO DVORNICICH 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 x_0 such that the equation $F(x_0, y) = 0$ has an integral solution y_0, where $F \in \boldsymbol{Q}[X, Y]$, then there exists a polynomial $g \in \boldsymbol{Q}[X]$ such that $F\big(x, g(x)\big) = 0$ identically.

Suppose now that the values of the polynomial $f(x)$ 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 $f \in \boldsymbol{Z}[X]$ has positive leading coefficient and degree at least two, then the condition

$$f(n) = b^k + o(n), \quad n \in \boldsymbol{N} \setminus \mathscr{E}$$

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

$$f(x) = \big(g(x)\big)^k + a$$

identically, for some $g \in \boldsymbol{Z}[X]$ and $a \in \boldsymbol{Z}$.

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 $F(x, y) = y^k - f(x)$ has, for fixed x_0, not just an integral zero, but a good approximation to zero, i.e.

$$|F(x_0, y_0)| = |y_0^k - f(x_0)| = |R_1| = o(y_0^{k-1}) = o\left(\left|\frac{\partial F}{\partial y}(x_0, y_0)\right|\right).$$

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

$$|F(x_0, y)| = o\left(\sup_{|\xi - y| \leqslant 1} \left|\frac{\partial F}{\partial y}(x_0, \xi)\right|\right) \quad \text{for } x_0 \to \infty$$

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 kth power,

$$\|x\|_k = \min_{m \in \mathbf{Z}} |x - m^k|$$

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

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

$$\|g\|_k = \min_{h \in \boldsymbol{C}[X]} \deg(g - h^k).$$

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

$$\mathscr{A}(N) = \{a \in \mathscr{A},\ 0 \leqslant a \leqslant N\}$$

and

$$\overline{d}(\mathscr{A}) = \limsup_{N \to \infty} \frac{|\mathscr{A}(N)|}{N}, \qquad \underline{d}(\mathscr{A}) = \liminf_{N \to \infty} \frac{|\mathscr{A}(N)|}{N}$$

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

Our results are the following:

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

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

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

$$\overline{d}(\mathscr{A} \setminus \mathscr{B}) = 0 \tag{2}$$

and

$$|F(b, P(b))| \leqslant |F(b, y(b))| \quad \text{for all } b \in \mathscr{B}. \tag{3}$$

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

$$f(a) = y^k(a) + o\left(y^{k-1}(a)\right), \quad a \to \infty \tag{4}$$

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

$$\|D^k f(n)\|_k \sim c \cdot n^{\|f\|_k} \quad \text{for all } n \in \boldsymbol{N},$$

where $c > 0$.

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 $F(x, y) = y^k - f(x)$, condition (1) cannot be replaced by

$$|F(a, y(a))| \ll \sup_{|\xi - y(a)| \leqslant 1} \left|\frac{\partial F}{\partial y}(a, \xi)\right|.$$

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

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

where $y(n) \leqslant \xi \leqslant \lambda_n$, 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

$$|F(a, y(a))| = o\left(\left|\frac{\partial F}{\partial y}(a, y(a))\right|\right). \tag{1a}$$

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

$$F(x, y) = x(y - x)^2 + 1.$$

It is easily seen that (1) is satisfied with $y(a) = a$ for all $a \in \boldsymbol{N}$, while, for any choice of $y(a)$, (1a) is not true.

4. We observe that the sup in (1) may be taken over any neighborhood of $y(n)$ of fixed length. In fact let P be any polynomial of degree k. From Newton's interpolation formula it follows that

$$\sup_{|x|<\delta}|P(x)| \leqslant \sup_{|x|<A}|P(x)| \leqslant C\sup_{|x|<\delta}|P(x)|$$

where $A \geqslant \delta > 0$ and C depends only on A, δ, 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

$$|(\mathscr{A}\setminus\mathscr{B})(N)| \ll Ng(N). \tag{2a}$$

To prove this consider

$$F(x,y) = (y^2-x)(xy-x^3+1).$$

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

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

(ii) $\sum_{k\leqslant\sqrt{x}} kr(k) > xg^{1/2}(x)+x^{3/4}$.

Now we set $\mathscr{A} = \boldsymbol{N}$ and

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

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

$$|F(n,y(n))| < |F(n,P(n))|$$

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

$$\mathscr{A}\setminus\mathscr{B} \supset \bigcup_{k\geqslant k_0}[k^2-kr(k), k^2+kr(k)]$$

whence

$$|(\mathscr{A}\setminus\mathscr{B})(x)| \geqslant \sum_{k\leqslant\sqrt{x}} kr(k)+O(\sqrt{x}) \geqslant xg^{1/2}(x)+x^{3/4}$$

thus contradicting (2a).

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

LEMMA. *Let d be a positive integer and $f \in \boldsymbol{C}[X^{1/d}]$. Assume that there exists a sequence $\mathscr{A} \subset \boldsymbol{N}$ with $\bar{d}(\mathscr{A}) > 0$ such that*

$$\|f(a)\| \to 0 \quad \text{as } a \in \mathscr{A}.$$

Then $f \in \boldsymbol{Q}[X]$.

Proof. We write $f(x) = a_0x^{k/d}+a_1x^{(k-1)/d}+\ldots+a_k$, $a_0 \neq 0$, and set, for fixed d, $l(f) = a_0$, $\delta(f) = k$.

First we note that necessarily $\delta(f) \equiv 0 \pmod d$, since otherwise the sequence $\{f(n), n \in \boldsymbol{N}\}$ would be uniformly distributed mod 1 (see [7], p. 382, 8. Anwendung for a proof); similarly, we also obtain that $l(f) \in \boldsymbol{Q}$ ([7], p. 380, 5. Anwendung).

Now suppose that $f \in \boldsymbol{C}[X^{1/d}]$ satisfies the hypotheses of the lemma; but $f \notin \boldsymbol{Q}[X]$. Then we may certainly write

$$f(x) = \varphi(x)/q+g(x)$$

where $q \in \boldsymbol{N}$, $\varphi \in \boldsymbol{Z}[X]$, and either $l(g) \notin \boldsymbol{Q}$ or $\delta(g) \not\equiv 0 \pmod d$. Pick a congruence class $\{c+q\boldsymbol{N}\} \bmod q$ such that $\mathscr{A}' = \mathscr{A}\cap\{c+q\boldsymbol{N}\}$ has $\bar{d}(\mathscr{A}') > 0$. Set $g_1(x) = g(x)+\varphi(c)/q$; then, if $a' \in \mathscr{A}'$ we have trivially

$$\|f(a')\| = \|g_1(a')\| \to 0$$

a contradiction, since either $l(g_1) \notin \boldsymbol{Q}$ or $\delta(g_1) \not\equiv 0 \pmod d$. ∎

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

$$F(x,y) = Q(x)\prod_{i=1}^{D}(y-\alpha_i(x))$$

where

$$\alpha_i(x) = \sum_{v=0}^{\infty} a_{iv}x^{(k_i-v)/d}, \quad a_{i0} \neq 0, \quad i = 1,\ldots,D,$$

for some $k_i \in \boldsymbol{Z}$, $d \in \boldsymbol{N}$, the series being convergent outside a sufficiently large circle. Applying this to our polynomial F, we first show that

$$\min_j |y(a)-\alpha_j(a)| \to 0 \quad \text{for } a \in \mathscr{A}. \tag{5}$$

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

$$\Big|\prod_{i=1}^{D}(y(a)-\alpha_i(a))\Big| = o\Big(\sup_{|\xi-y(a)|\leqslant 1}\Big|\sum_{i=1}^{D}\prod_{j\neq i}(\xi-\alpha_j(a))\Big|\Big) = o\Big(\sup_{|\xi-y(a)|\leqslant 1}\max_{1\leqslant i\leqslant D}\prod_{j\neq i}|\xi-\alpha_j(a)|\Big). \tag{6}$$

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

$$\min_j |y(a_k)-\alpha_j(a_k)| \geqslant \delta$$

It follows that

$$\prod_{j\neq i}|\xi-a_j(a_k)|\leqslant\prod_{j\neq i}\{|\xi-y(a_k)|+|y(a_k)-a_j(a_k)|\}$$

$$\leqslant\prod_{j\neq i}\left\{|y(a_k)-a_j(a_k)|\left(1+\frac{1}{\delta}\right)\right\}\leqslant\frac{1}{\delta}\left(1+\frac{1}{\delta}\right)^{D-1}\prod_{j=1}^{D}|y(a_k)-a_j(a_k)|$$

and this contradicts (6). Write now

$$a_i(x)=\sum_{v=0}^{k_i}a_{iv}x^{(k_i-v)/d}+\sum_{v=1}^{\infty}a_{i,k_i+v}x^{-v/d}=P_i(x^{1/d})-O(x^{-1/d}).$$

From (5) we derive immediately

$$\min_j|y(a)-P_j(a^{1/d})|=o(1)\quad\text{for } a\in\mathscr{A}. \tag{7}$$

Rearranging eventually the indices, suppose that

$$R_i(x)=P_i(x^{1/d})\in\boldsymbol{Q}[X]\quad\text{for } i=1,\dots,D_1$$

(this set may possibly be empty), and

$$R_i(x)\notin\boldsymbol{Q}[X]\quad\text{for } i=D_1+1,\dots,D.$$

From the lemma it follows that the minimum in (7) can be attained at $i\geqslant D_1+1$ only on a sequence $\mathscr{A}'\subset\mathscr{A}$ with $\bar{d}(\mathscr{A}')=0$. This implies in particular that $D_1\geqslant 1$. We show that, for large $b\in\mathscr{A}\setminus\mathscr{A}'$,

$$\min_{i\leqslant D_1}|y(b)-R_i(b)|=0. \tag{8}$$

In fact let r be a common denominator for all the coefficients of the R_i's. Fix $b\in\mathscr{A}\setminus\mathscr{A}'$; then either (8) is true or

$$\min_{i\leqslant D_1}|y(b)-R_i(b)|\geqslant 1/r,$$

but this is inconsistent for large b in view of our definition of $\mathscr{A}'$. Next define an order relation in $\boldsymbol{C}[X]$ by

$$P_1\prec P_2\quad\text{iff}\quad|P_1(m)|\leqslant|P_2(m)|\text{ for all sufficiently large } m\in\boldsymbol{N}.$$

Then it is clear that, for every pair of polynomials P_1, P_2, at least one of the relations $P_1\prec P_2$, $P_2\prec P_1$ holds. Choose then R_j, with $j\leqslant D_1$, such that $F(x,R_j(x))$ is minimum with respect to $\prec$. Now we are finished: in fact, set $\mathscr{B}=\mathscr{A}\setminus(\mathscr{A}'\cup[1,L])$, where L is large; then, for $b\in\mathscr{B}$ we have

$$|F(b,R_j(b))|\leqslant\min_{i\leqslant D_1}|F(b,R_i(b))|\leqslant|F(b,y(b))|$$

the last inequality being a consequence of (8); moreover

$$\bar{d}(\mathscr{A}\setminus\mathscr{B})\leqslant\bar{d}(\mathscr{A}')+\bar{d}([1,L])=0.$$

Proof of Corollary. Applying the theorem to $F(x,y)=y^k-f(x)$, which obviously satisfies (1), we obtain the existence of a polynomial $P\in\boldsymbol{Q}[X]$ such that

$$|f(n)-P^k(n)|=o(P^{k-1}(n)) \tag{9}$$

for all n in some infinite sequence $\mathscr{B}$, whence for all $n\in\boldsymbol{N}$. Setting

$$R(x)=f(x)-P^k(x)$$

we contend that

$$\|f\|_k=\deg R\leqslant\frac{k-1}{k}\deg f-1. \tag{10}$$

In fact from (9) we derive

$$\|f\|_k\leqslant\deg R\leqslant\frac{k-1}{k}\deg f-1. \tag{11}$$

Now choose $S\in\boldsymbol{C}[X]$ such that $\deg(f-S^k)=\|f\|_k$; (10) will be proved by showing that $S^k=P^k$. Assume the contrary; then

$$\deg(S^k-P^k)=\deg\prod_{v=0}^{k-1}(S-e^{2\pi iv/k}P)\geqslant(k-1)\deg P\geqslant\frac{k-1}{k}\deg f$$

while it follows from (11) that

$$\deg(S^k-P^k)=\deg(\{S^k-f\}+\{f-P^k\})\leqslant\frac{k-1}{k}\deg f-1$$

and we have a contradiction.

Write now $P(x)=P_1(x)/D$, where $P_1\in\boldsymbol{Z}[X]$ and, for $n\in\boldsymbol{N}$, pick an integer $g(n)$ such that

$$|D^kf(n)-g^k(n)|=\|D^kf(n)\|_k.$$

We have

$$|D^kf(n)-g^k(n)|\leqslant|D^kf(n)-P_1^k(n)|=o(P_1^{k-1}(n))$$

and thus we obtain

$$|g^k(n)-P_1^k(n)|\leqslant|g^k(n)-D^kf(n)|+|D^kf(n)-P_1^k(n)|=o(P_1^{k-1}(n)).$$

On the other hand

$$|g^k(n)-P_1^k(n)|=\left|\prod_{v=0}^{k-1}(g(n)-e^{2\pi iv/k}P_1(n))\right|\geqslant|g(n)-P_1(n)|\,|P_1(n)|^{k-1}$$

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

$$\|D^k f(n)\|_k = |D^k f(n)-g^k(n)| = |D^k f(n)-P_1^k(n)| \sim c\cdot n^{\|f\|_k}.$$

References

[1] E. Artin, *Algebraic numbers and algebraic functions*, Gordon & Breach Science Publishers, New York 1967.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107–116.

[3] K. R. Matthews, *Polynomials which are near to k-th powers*, Proc. Camb. Phil. Soc. 61 (1965), pp. 1–5.

[4] A. Perelli, U. Zannier, *Una proprietà aritmetica dei polinomi*, Boll. U.M.I. (5) 17-A (1980), pp. 199–202.

[5] G. Pólya, G. Szegö, *Problems and theorems in Analysis*, vol. II, Springer Verlag, Berlin 1976.

[6] P. Ribenboim, *Polynomials whose values are powers*, J. Reine Angew. Math. 268/269 (1974), pp. 34–40.

[7] J. G. Van der Corput, *Diophantische Ungleichungen — I. Zur Gleichverteilung Modulo Eins*, Acta Math. 56 (1931), pp. 373–447.

ISTITUTO DI MATEMATICA "L. TONELLI"
Via F. Buonarroti, 2
56100 Pisa, Italy

SCUOLA NORMALE SUPERIORE
Piazza dei Cavalieri, 7
56100 Pisa, Italy

Received on 16. 7. 1981
and in revised form on 4. 11. 1981 (1261)

ACTA ARITHMETICA
XLII (1983)

Primes in arithmetic progressions

by

E. Fouvry (Talence) and H. Iwaniec (Warszawa)

1. Introduction. Statement of results. Let a and q be coprime integers, $q \geqslant 1$ and for any $x \geqslant 2$ let $\pi(x; q, a)$ be the number of primes $\leqslant x$ congruent to $a \bmod q$. 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 moduli q as large as possible.

The classical prime number theorem of Siegel and Walfisz states that if A is a given positive number and $q \leqslant (\log x)^A$ then

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \operatorname{li} x + O\left(x \exp(-c\sqrt{\log x})\right)$$

where c and the constant implied in the symbol O depend on A alone (not effectively computable if $A \geqslant 2$). A mention should be made of the two conjectures

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \operatorname{li} x + O(x^{1/2+\varepsilon}), \quad \text{Great Riemann Hypothesis (GRH),}$$

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \operatorname{li} x + O(q^{-1/2} x^{1/2+\varepsilon}), \quad \text{H. L. Montgomery's Hypothesis,}$$

the first one giving an asymptotic formula for $q < x^{1/2-2\varepsilon}$ and the latter for $q \leqslant x^{1-3\varepsilon}$ (cf. [15]), neither of these relations is expected to be proved in a 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. Renyi [18] and some others [17], [1] in 1965 E. Bombieri [2] and A. I. Vinogradov [21] proved a mean-value theorem which states, in a form given by Bombieri, that for any $A > 0$ the following holds

$$\sum_{q \leqslant Q} \max_{(a,q)=1} \max_{y \leqslant x} \left| \pi(y; q, a) - \frac{1}{\varphi(q)} \operatorname{li} y \right| \ll x (\log x)^{-A}$$