HOW MANY PRIMES CAN DIVIDE THE VALUES OF A POLYNOMIAL?

FLORIAN LUCA AND PAUL POLLACK

For Andrzej Schinzel on his seventy-fifth birthday

ABSTRACT. Let $F(T) \in \mathbb{Z}[T]$ be a nonconstant polynomial. We prove a result concerning the maximal order of $\Omega(F(n))$, where $\Omega(\cdot)$ denotes the total number of prime factors (counting multiplicity). In the case when F has only simple roots, the result asserts that

$$\limsup_{n\to\infty} \frac{\Omega(F(n))}{\log n} = \frac{1}{\log \ell},$$

where ℓ is the least prime for which F has a zero in the ℓ-adic integers $\mathbb{Z}_\ell$. This extends investigations of Erdős and Nicolas, who treated the case $F(T) = T(T+1)$.

1. INTRODUCTION

Let $\Omega(n) := \sum_{p^k \mid n} 1$ denote the number of (positive) prime factors of n, counted with multiplicity. The study of statistical properties of $\Omega(n)$ was a major impetus for the development of probabilistic number theory in the first half of the twentieth century. It is a simple consequence of elementary prime number theory that $\Omega(n)$ behaves like $\log\log n$ on average. Hardy and Ramanujan [HR17] showed that this average behavior is typical by demonstrating that $\Omega(n) \sim \log\log n$ as $n \to \infty$ along a set of asymptotic density 1. This result was refined in celebrated work of Erdős and Kac [EK40], who proved that $\Omega(n)$ possesses a Gaussian distribution with mean and variance $\log\log n$. In contrast with the depth of these authors' work, the minimal and maximal orders of $\Omega(n)$ are trivial to determine: $\Omega(n) = 1$ for prime n, while $\Omega(n) = \frac{\log n}{\log 2}$ when n is a power of 2.

Let $F(T) \in \mathbb{Z}[T]$ be a fixed polynomial. One can ask for the average, normal, minimal, and maximal orders of $\Omega(F(n))$. The first two questions have been satisfactorily resolved (see, e.g., [Hal56] for an analogue of the Erdős–Kac theorem in this context). The third question is in general very difficult; to take a famous example, we expect that if $F(T) = T(T+2)$, then $\Omega(F(n)) = 2$ infinitely often, but we are still far from proving this. Probably the following is true:

2010 *Mathematics Subject Classification.* Primary 11N32; Secondary 11N37, 11J68.
Key words and phrases. Hypothesis H, subspace theorem, number of prime factors.

Hypothesis H′. *Let $F(T)$ be a nonzero polynomial with integer coefficients. Let $D := \gcd_{n\in\mathbb{Z}}\{F(n)\}$ be the greatest fixed divisor of F. Then*

$$\liminf_{n\to\infty} \Omega(F(n)) = r + \Omega(D),$$

where r is the number of monic irreducible factors of F in $\mathbb{Q}[T]$, counted with multiplicity.

We show in §2 that Hypothesis H′ is equivalent to Schinzel's well-known Hypothesis H [SS58] concerning simultaneous prime values of polynomials. This equivalence, and its proof, are similar in flavor to Schinzel's own argument [Sch62] that his Hypothesis H implies a conjecture of Bunyakovsky.

The primary purpose of this note is to give a satisfactory answer to the the remaining, fourth question: What is the maximal order of $\Omega(F(n))$? Erdős and Nicolas [EN80] considered this problem when $F(T) = T(T+1)$, so that $\Omega(F(n)) = \Omega(n) + \Omega(n+1)$. Trivially, $\Omega(F(n)) \le 2\frac{\log(n+1)}{\log 2}$. But these authors showed [EN80, Théorème 3] that in fact,

$$\Omega(n(n+1)) \le (1+o(1))\frac{\log n}{\log 2} \qquad (\text{as } n\to\infty).$$

We show that $\Omega(F(n))$ always has maximal order $C\log n$ for some positive constant C. More precisely, factor F as

$$F(T) = \pm\mathrm{Cont}(F)\prod_{i=1}^{k} F_i(T)^{e_i}, \tag{1.1}$$

where $\mathrm{Cont}(F)$ is the *content* of F (the greatest common divisor of its coefficients) and the F_i are distinct irreducible elements of $\mathbb{Z}[T]$, each with positive leading term. We prove the following:

Theorem 1. *Let $F(T) \in \mathbb{Z}[T]$ be a nonconstant polynomial with integer coefficients. Suppose that F is written in the form* (1.1)*. For each $1 \le i \le k$, let ℓ_i be the least prime for which F_i has a root in the ℓ_i-adic integers $\mathbb{Z}_{\ell_i}$. Then*

$$\limsup_{n\to\infty}\frac{\Omega(F(n))}{\log n} = C(F), \quad \text{where} \quad C(F) := \max_{1\le i\le k}\frac{e_i}{\log \ell_i}.$$

In particular, if F has only simple roots, then $C(F) = 1/\log \ell$, where ℓ is the least prime for which F has a zero in $\mathbb{Z}_\ell$.

Our proof is similar in spirit to that of Erdős and Nicolas, but replaces the use of Ridout's version of Roth's theorem with an application of the subspace theorem.

The questions we have raised make sense also for $\omega(F(n))$, where ω counts the number of *distinct* prime factors. However, as observed already by Erdős and Nicolas, here it seems very difficult to prove any nontrivial results about the maximal order. To illustrate the difficulties, call the natural number n *special* if $n(n+1)$ is the product of the first k primes for some k; e.g., $n = 714$ is special, with $k = 7$. Improving the trivial bound

$$\limsup_{n\to\infty} \frac{\omega(n(n+1))}{\log n/\log\log n} \le 2$$

entails showing that there are only finitely many special n. This seems unattackable at present. It may be mentioned that in a 2009 preprint, A. Dąbrowski conjectured that there are precisely 28 solutions to the equation

$$N^2 - 1 = p_1^{a_1} \cdots p_k^{a_k}, \tag{1.2}$$

where N and the a_i are positive integers, and p_i denotes the ith prime. Note that if n is special, then $N = 2n+1$ gives a solution to (1.2). The results of [LN11] imply the truth of Dąbrowski's conjecture for all $k \le 25$.

Notation. Most of our notation is standard or will be explained when needed, so we make only a few brief remarks: We let $|\cdot|$ (without a subscript) denote the usual absolute value on $\mathbb{C}$. For a prime p and a nonzero rational number x, we write $\mathrm{ord}_p(x)$ for the exponent of p in the prime factorization of x. We say that a number n is *y-smooth* if each prime factor of n is bounded by y, and we define the *y-smooth part* of n as its largest y-smooth divisor.

2. Minimal order: The equivalence of Hypotheses H and H′

We begin by recalling the statement of Schinzel's Hypothesis H [SS58]:

Hypothesis H. *Suppose that $G_1(T), \dots, G_k(T) \in \mathbb{Z}[T]$ are irreducible over $\mathbb{Q}$, each with positive leading coefficient. Put $G := \prod_{i=1}^k G_i$. Suppose that G has no fixed prime divisor: for every prime p, there is an integer m_p for which $p \nmid G(m_p)$. Then there are infinitely many natural numbers n for which each $G_i(n)$ is prime.*

It is clear that Hypothesis H′ implies H: We need only apply H′ with $F = \prod_{i=1}^r G_i$ (assuming, as we may, that the G_i are distinct). So we may focus our energies on showing that H implies H′.

Let $F(T) \in \mathbb{Z}[T]$ be a nonzero polynomial for which we wish to establish the conclusion of Hypothesis H′. We can assume that F is nonconstant and that $\mathrm{Cont}(F) = 1$. Hence, we may write $F = \prod_{i=1}^k F_i(T)^{e_i}$, where each $F_i(T)$ is nonconstant, irreducible over $\mathbb{Z}$, and possesses a positive leading coefficient. Let $D = \gcd_{n\in\mathbb{Z}}\{F(n)\}$; we must prove that

$$\liminf_{n\to\infty} \Omega(F(n)) = \Omega(D) + r, \quad \text{where} \quad r := \sum_{i=1}^{k} e_i.$$

It is easy to prove that $\Omega(F(n)) \geq \Omega(D)+r$ for all large n. Indeed, since $D \mid F(n) = \prod_{i=1}^{k} F_i(n)^{e_i}$, there is a factorization $D = \prod_{i=1}^{k} D_i$ where each $D_i \mid F_i(n)^{e_i}$. Then with $D_i' := \prod_p p^{\lceil(\mathrm{ord}_p D_i)/e_i\rceil}$, we have $D_i' \mid F_i(n)$ for all $1 \leq i \leq n$, and so

$$F(n) = \left(\prod_{i=1}^{k} D_i'^{e_i}\right)\left(\prod_{i=1}^{k} (F_i(n)/D_i')^{e_i}\right).$$

The first product contributes at least $\Omega(D)$ prime factors, since $D = \prod D_i \mid \prod D_i'^{e_i}$, and the second product contributes at least $\sum_{i=1}^{k} e_i = r$ primes (for large n). This gives the desired lower bound on $\Omega(F(n))$.

Turning to the upper bound, let $\mathcal{S}$ be the set of primes p for which either $p \mid D$ or $p \leq \deg F$. For each $p \in \mathcal{S}$, choose an integer n_p so that $p^{1+\mathrm{ord}_p(D)} \nmid F(n_p)$. Choose n_0 to satisfy the simultaneous congruences

$$n_0 \equiv n_p \bmod p^{1+\mathrm{ord}_p(D)} \quad \text{for all } p \in \mathcal{S}.$$

With $M := \prod_{p\in\mathcal{S}} p^{1+\mathrm{ord}_p(D)}$, put $\tilde{F}_i(n) = F_i(MT + n_0)$, and set $\tilde{F}(T) = F(MT + n_0)$, so that $\tilde{F}(T) = \prod_{i=1}^{k} \tilde{F}_i(T)^{e_i}$. Since $D \mid M$ and $D \mid F(n_0)$, it is clear that $\tilde{F}(T)/D \in \mathbb{Z}[T]$. Moreover, $\tilde{F}(T)/D$ has no fixed prime divisor: Indeed, $\gcd(\tilde{F}(0)/D, M) = \gcd(F(n_0)/D, M) = 1$ by construction, so that no prime in $\mathcal{S}$ is a fixed divisor of $\tilde{F}(T)$. Moreover, if $p \notin \mathcal{S}$, then the reduction of $\tilde{F}(T)$ modulo p is nonzero and has degree $\leq \deg F < p$, so that again p is not a fixed divisor of $\tilde{F}(T)/D$.

Since $\tilde{F}(T)/D$ has no fixed prime divisor, we have in particular that

$$D = \mathrm{Cont}(\tilde{F}) = \prod_{i=1}^{k} \mathrm{Cont}(\tilde{F}_i)^{e_i}. \tag{2.1}$$

Let $G_i(T) := \tilde{F}_i(T)/\mathrm{Cont}(\tilde{F}_i)$. Since each F_i is irreducible over $\mathbb{Q}$, so is each G_i. In $\mathbb{Z}[T]$, we have (referring back to (2.1))

$$G(T) := \prod_{i=1}^{k} G_i(T) \mid \prod_{i=1}^{k} G_i(T)^{e_i} = \tilde{F}(T)/D;$$

as $\tilde{F}(T)/D$ has no fixed prime divisor, neither does $G(T)$. So by Hypothesis H, there are infinitely many n for which each $G_i(n)$ is prime. For any such n, it is clear that

$$F(Mn + n_0) = \tilde{F}(n) = D \prod_{i=1}^{k} G_i(n)^{e_i}$$

has precisely $\Omega(D) + \sum_i e_i = \Omega(D) + r$ prime factors, as desired.

3. Maximal order

3.1. **The lower bound.** It is simple to prove that $\Omega(F(n))$ is occasionally *at least* as large as predicted here: Fix $1 \le i \le r$ so that the ratio $e_i/\log \ell_i$ is maximal. Write $e = e_i$ and $\ell = \ell_i$ (to ease notation). For each natural number j, choose $n_j \in [\ell^j, 2\ell^j)$ so that $F_i(n_j) \equiv 0 \pmod{\ell^j}$. Then the n_j tend to infinity and

$$\Omega(F(n_j)) \ge e \cdot \Omega(F_i(n_j)) \ge e \cdot j \ge e \frac{\log(n_j/2)}{\log \ell}.$$

This shows that the lim sup considered in Theorem 1 is at least as large as predicted.

3.2. **The upper bound.** To see that the lim sup in Theorem 1 is no larger than predicted, we use a version of Schmidt's subspace theorem due to Schlickewei. First, some terminology. For a nonzero rational number x, its *infinite valuation* is $|x|_\infty = |x|$. *Finite valuations* correspond to prime numbers p, and for such a prime, the *p-adic valuation* of x is taken to be $|x|_p = p^{-\mathrm{ord}_p(x)}$. Put $\mathcal{M}_\mathbb{Q} = \{p : p \text{ prime}\} \cup \{\infty\}$. Such valuations are sometimes called *normalized* since the product formula

$$\prod_{v \in \mathcal{M}_\mathbb{Q}} |x|_v = 1 \qquad \text{holds for all} \qquad x \in \mathbb{Q}^*. \tag{3.1}$$

Often one extends these valuations to all algebraic numbers. A canonical way to do this is the following. Let $\mathbb{K}$ be an algebraic number field of degree d over $\mathbb{Q}$. The infinite valuations v of $\mathbb{K}$ are in correspondence with the embeddings $\sigma\colon \mathbb{K} \hookrightarrow \mathbb{C}$. If σ is real and $x \in \mathbb{K}$, then $|x|_v = |\sigma(x)|^{1/d}$, whereas if σ is complex non-real then $|x|_v = |\sigma(x)|^{2/d}$. Finite valuations of $\mathbb{K}$ are in correspondence with prime ideals π in $\mathcal{O}_\mathbb{K}$. More precisely, say π is a prime ideal in $\mathbb{K}$ of norm $N_{\mathbb{K}/\mathbb{Q}}(\pi) = p^f$. Then $|x|_v = p^{-c_v \mathrm{ord}_\pi(x)}$, where $c_v = f/d$, and $\mathrm{ord}_\pi(x)$ is the exponent at which the prime ideal π appears in the factorization of the fractional ideal $x\mathcal{O}_\mathbb{K}$ generated by x inside $\mathbb{K}$. Put $\mathcal{M}_\mathbb{K}$ for the set of all valuations of $\mathbb{K}$. Then one checks easily that the formula

$$\prod_{v \in \mathcal{M}_\mathbb{K}} |x|_v = 1 \qquad \text{holds for all} \qquad x \in \mathbb{K}^*. \tag{3.2}$$

Let $m \ge 2$ be given, and let $\mathcal{S}$ be a finite subset of $\mathcal{M}_\mathbb{K}$ containing all the infinite valuations. Assume that for each $v \in \mathcal{S}$ we are given a system of m linearly independent linear forms $L_{v,i}(\mathbf{x})$ in $\mathbf{x} = (x_1, \dots, x_m)$ with coefficients in $\mathbb{K}$. Using $x_i^{(j)}$ $(1 \le j \le d)$ for the conjugates of x_i, put

$$\|\mathbf{x}\| := \max_{\substack{1 \le i \le m \\ 1 \le j \le d}} |x_i^{(j)}|.$$

Then the $\mathfrak{p}$-adic subspace theorem of Schlickewei [Sch77] (in the formulation of [Sch91, Theorem 1D, p. 177]) says the following:

Theorem A. *For each $\varepsilon > 0$, the solutions $\mathbf{x} \in \mathcal{O}_{\mathbb{K}}^m$ of the inequality*

$$\prod_{v \in \mathcal{S}} \prod_{i=1}^{m} |L_{v,i}(\mathbf{x})|_v < \|x\|^{-\varepsilon} \tag{3.3}$$

lie in finitely many proper subspaces of $\mathbb{K}^m$.

The proof of the upper-bound assertion of Theorem 1 is based on the following lemma:

Lemma 1. *Let $F(T) \in \mathbb{Z}[T]$ be a polynomial of degree $d \ge 1$ with only simple roots. Fix $Z > 0$. For each natural number n for which $F(n) \ne 0$, write $F(n) = UV$, where U is the Z-smooth part of F. Given $\epsilon > 0$, we have $U > n^{1+\epsilon}$ for only finitely many natural numbers n.*

Proof of Lemma 1. We can assume that $d \ge 2$, otherwise there is nothing to prove. We can also assume that F is monic. To see this, write c_d for the leading coefficient of F. Replacing F with $-F$ if necessary, we can assume that $c_d > 0$. Then $c_d^{d-1} F(T) = G(c_d T)$ for some monic G of the same degree as F (still with only simple roots), and the lemma holds for F provided that it holds for G.

Let $\mathbb{K}$ be the splitting field of F and write

$$F(T) = (T - \theta_1)(T - \theta_2) \cdots (T - \theta_d).$$

Let $\mathcal{N}$ be the set of n such that $F(n) = UV$, with $U > n^{1+\varepsilon}$ and Z-smooth. Since $F(T)$ is monic, the numbers $\theta_1, \dots, \theta_d$ are all in $\mathcal{O}_{\mathbb{K}}$. Put $m = 2$, $\mathbf{x} = (x_1, x_2)$. We shall take $x_1 = n - \theta_1$ and $x_2 = n - \theta_2$. We take $\mathcal{S}$ to be the finite subset of $\mathcal{M}_{\mathbb{K}}$ consisting of the following valuations:

(i) all the infinite valuations of $\mathbb{K}$;
(ii) all the finite valuations of $\mathbb{K}$ sitting above some prime number $p \le Z$.

To define the forms $L_{v,i}(\mathbf{x})$ for $v \in \mathcal{S}$ and $i = 1, 2$, it is helpful to introduce the notion of *type*. Let $\mathcal{P}$ be the set of finite valuations of $\mathcal{S}$. To each $n \in \mathcal{N}$ we associate a type function $f \colon \mathcal{P} \to \{1, 2, \dots, d\}$, as follows: Let $\pi \in \mathcal{P}$. For each $1 \le i \le d$, write

$$(n - \theta_i)\mathcal{O}_{\mathbb{K}} = \pi^{e_i} I_{i,\pi},$$

where $I_{i,\pi}$ is an ideal of $\mathcal{O}_{\mathbb{K}}$ coprime to π and e_i is a nonnegative integer. We define $f(\pi) \in \{1, 2, \ldots, d\}$ as that index i for which e_i is as large as possible, choosing arbitrarily among the possibilities if more than one such i exists. The number of possible types is finite. So to show that $\mathcal{N}$ is finite, it suffices to show that there are only finitely many n having a fixed type f.

We are now ready to define the forms $L_{v,i}(\mathbf{x})$. If v is infinite, we take $L_{v,1}(\mathbf{x}) = x_1$ and $L_{v,2}(\mathbf{x}) = x_1 - x_2$. It is clear that they are independent. Say that θ_1 has degree $d_1 \mid d$, with minimal polynomial $F_1 \mid F$. For large n,

$$\prod_{v \text{ infinite}} L_{v,i}(\mathbf{x}) = \prod_{v \text{ infinite}} |n - \theta_1|_v \prod_{v \text{ infinite}} |\theta_1 - \theta_2|$$

$$\asymp N_{\mathbb{K}/\mathbb{Q}}(n - \theta_1)^{1/d} = F_1(n)^{1/d_1} \asymp n. \tag{3.4}$$

(The implied constants may depend on F.) In order to proceed to the finite valuations, observe first that for $i = 3, \ldots, d$, we have $n - \theta_i = c_i x_1 + d_i x_2$, where (c_i, d_i) is the unique solution of the system $c_i + d_i = 1$ and $c_i\theta_1 + d_i\theta_2 = \theta_i$. Observe that $d_i \neq 0$, as otherwise $c_i = 1$ and $\theta_1 = c_i\theta_1 = \theta_i$. If now $v \in \mathcal{P}$ corresponds to a prime ideal π, we then take $L_{v,1}(\mathbf{x}) = x_1$ and $L_{v,2}(\mathbf{x}) = x_2$ if $f(\pi) \in \{1, 2\}$, and $L_{v,1}(\mathbf{x}) = x_1$ and $L_{v,2} = c_i x_1 + d_i x_2$ if $f(\pi) = i \geq 3$. In all cases, $L_{v,1}(\mathbf{x})$ and $L_{v,2}(\mathbf{x})$ are independent. It remains to compute $|L_{v,i}(\mathbf{x})|_v$ for $i = 1, 2$. Continuing to denote $f(\pi)$ by i, note that if $j \neq i$, then $e_j \leq e_i$, so that π^{e_j} divides $n - \theta_j$ and $n - \theta_i$. Thus, it also divides $\theta_j - \theta_i$. Hence,

$$\pi^{\sum_{j \neq i} e_j} \mid \prod_{j \neq i} (\theta_j - \theta_i) \mid \Delta(F),$$

where $\Delta(F)$ is the discriminant of F. This shows immediately that

$$|L_{v,1}(\mathbf{x})|_v |L_{v,2}(\mathbf{x})|_v \leq |n - \theta_i|_v \leq \frac{|f(n)|_v}{|\Delta(F)|_v}.$$

Hence,

$$\prod_{\substack{v \in \mathcal{S} \\ v \text{ finite}}} |L_{v,1}(\mathbf{x})|_v |L_{v,2}(\mathbf{x})|_v \leq \prod_{\substack{v \in \mathcal{S} \\ v \text{ finite}}} \frac{|f(n)|_v}{|\Delta(F)|_v} \leq \frac{|\Delta(F)|}{U} \ll \frac{1}{U}. \tag{3.5}$$

Thus, putting together (3.4) and (3.5), we have

$$\prod_{v \in \mathcal{S}} \prod_{i=1}^{2} |L_{v,i}(\mathbf{x})|_v \ll \frac{n}{U} \ll \frac{1}{n^{\varepsilon}} \ll \|x\|^{-\varepsilon}.$$

By Theorem A, all solutions $\mathbf{x}$ are contained in finitely many subspaces of $\mathbb{K}^2$. In other words, there is a positive integer K and K pairs (C_1, D_2), $\ldots$, (C_K, D_K) of numbers in $\mathbb{K}$, not both zero, such that each such solution $\mathbf{x}$ satisfies $C_i x_1 + D_i x_2 = 0$ for some $1 \leq i \leq K$. Take an i with $1 \leq i \leq K$. If $C_i = 0$, then $D_i \neq 0$; thus, $x_2 = 0$ and $n = \theta_2$. Similarly, if $D_i = 0$, then

$x_1 = 0$ and $n = \theta_1$. If neither C_i nor D_i vanishes, then $(n-\theta_1)/(n-\theta_2) = x_1/x_2 = -D_i/C_i$, which uniquely determines n. So there are only finitely many possibilities for n, as desired. □

Completion of the proof of Theorem 1. It remains only to prove the upper bound for the lim sup. For an interval I, let us write $\Omega_I(n) := \sum_{p^k \mid n, p\in I} 1$ for the number of prime power divisors p^k of n with $p \in I$.

Fix a large real number Z. Write F in the form (1.1). By the choice of ℓ_i, each prime $< \ell_i$ divides $F_i(n)$ to a bounded power. Hence, for large n,

$$\begin{aligned}(3.6)\quad \Omega(F(n)) = \Omega(\mathrm{Cont}(F)) + \\ \sum_{i=1}^{k} e_i \left(\Omega_{[1,\ell_i)}(F_i(n)) + \Omega_{[\ell_i,Z]}(F_i(n)) + \Omega_{(Z,\infty)}(F_i(n))\right) \\ = O(\log n/\log Z) + \sum_{i=1}^{k} e_i \cdot \Omega_{[\ell_i,Z]}(F_i(n)),\end{aligned}$$

where as before we suppress the dependence of the implied constants on F. Let U_i denote the Z-smooth part of $F_i(n)$, so that

$$\Omega_{[\ell_i,Z]}(F_i(n)) \le \frac{\log U_i}{\log \ell_i}. \tag{3.7}$$

We now apply Lemma 1 with $G(T) := \prod_{i=1}^{k} F_i(T)$. Writing $G(n) = UV$, where U is the Z-smooth part of $G(n)$, we find that $U \le n^{1+o(1)}$ as $n \to \infty$, and so

$$\sum_{i=1}^{k} \frac{\log U_i}{\log n} \le 1 + o(1). \tag{3.8}$$

From (3.6), (3.7), (3.8), and the definition of $C(F)$ given in the theorem statement,

$$\begin{aligned}\Omega(F(n)) &\le \log n \sum_{i=1}^{k} \frac{\log U_i}{\log n}\frac{e_i}{\log \ell_i} + O(\log n/\log Z) \\ &\le (C(F) + o(1))\log n + O(\log n/\log Z).\end{aligned}$$

Dividing by $\log n$ and letting $n \to \infty$ gives that $\limsup \Omega(F(n))/\log n \le C(F) + O(1/\log Z)$. Since Z can be taken arbitrarily large, the result follows. □

Acknowledgements

The authors thank Carl Pomerance and Enrique Treviño for useful discussions. This research was conducted while P. P. was supported by NSF award DMS-0802970.

References

[EK40] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742.

[EN80] P. Erdős and J.-L. Nicolas, *Sur la fonction "nombre de facteurs premiers de n"*, Séminaire Delange-Pisot-Poitou, 20e année: 1978/1979. Théorie des nombres, Fasc. 2 (French), Secrétariat Math., Paris, 1980, Exp. No. 32, 19 pp.

[Hal56] H. Halberstam, *On the distribution of additive number-theoretic functions. II*, J. London Math. Soc. **31** (1956), 1–14.

[HR17] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. **48** (1917), 76–92.

[LN11] F. Luca and F. Najman, *On the largest prime factor of x^2-1*, Math. Comp. **80** (2011), 429–435.

[Sch62] A. Schinzel, *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. **7** (1961/1962), 1–8.

[SS58] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum in **5** (1958), 259.

[Sch77] H. P. Schlickewei, *The $\mathfrak{p}$-adic Thue–Siegel–Roth–Schmidt theorem*, Arch. Math. **29** (1977), 267–270.

[Sch91] W. M. Schmidt, *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, vol. 1467, Springer-Verlag, Berlin, 1991.

The John Knopfmacher Centre for Applicable Analysis and Number Theory, University of the Witwatersrand, P.O. Wits 2050, South Africa

Current address: Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México

E-mail address: fluca@matmor.unam.mx

University of British Columbia, Department of Mathematics, 1984 Mathematics Road, Vancouver, British Columbia V6T 1Z2, Canada

E-mail address: twonth@gmail.com