Bull. London Math. Soc. 37 (2005) 809–817
doi:10.1112/S0024609305004923

PRIME DIVISORS OF SHIFTED FACTORIALS

FLORIAN LUCA AND IGOR E. SHPARLINSKI

ABSTRACT

For any positive integer n we let $P(n)$ be the largest prime factor of n. We improve and generalize several results of P. Erdős and C. Stewart on $P(n!+1)$. In particular, we show that $\limsup_{n\to\infty} P(n!+1)/n \geqslant 2.5$, which improves their lower bound of $\limsup_{n\to\infty} P(n!+1)/n > 2$.

1. *Introduction*

For any positive integer $k > 1$ we denote by $P(k)$ the largest prime factor of k and by $\omega(k)$ the number of distinct prime divisors of k. We also set $P(1) = 1$ and $\omega(1) = 0$.

It is trivial to see that $P(n! + 1) > n$. Erdős and Stewart [**1**] have shown that

$$\limsup_{n\to\infty} \frac{P(n!+1)}{n} > 2.$$

Here, we improve their result by showing that the above upper limit is at least 2.5. It has also been proved in [**1**] that the inequality

$$P(n!+1) > n + (1+o(1))\frac{\log n}{\log\log n}$$

holds for large values of n, where, as throughout the paper, all logarithms are natural.

Here, we show that the above inequality can be both improved and generalized. We also remark that under the ABC conjecture, Murty and Wong [**6**] show that the above inequality can be strengthened to

$$P(n!+1) > (1+o(1))n\log n.$$

We generalize such results by considering the arithmetic structure of the sequence $n! + f(n)$, where f is a nonzero polynomial with integer coefficients.

Our main results are the following theorems.

THEOREM 1. *Let $f(X) \in \mathbb{Z}[X]$ be nonzero. Then*

$$\limsup_{n\to\infty} \frac{P(n!+f(n))}{n} \geqslant \frac{5}{2}.$$

THEOREM 2. *Let $f(X) \in \mathbb{Z}[X]$ be nonzero. Then*

$$P(n!+f(n)) > n + \left(\frac{1}{4}+o(1)\right)\log n.$$

Received 29 September 2003; revised 1 December 2004.

2000 *Mathematics Subject Classification* 11A05, 11A07, 11J86.

These improvements are based on several new elements, such as bounds for the number of solutions of congruences with $n! + f(n)$, which could be of independent interest.

We remark that introducing a polynomial shift makes the problem more difficult and thus more interesting. For example, several facts which are 'for free' for the sequence $n!+1$, such as $P(n!+1) > n$, are not immediately obvious for the sequence $n! + f(n)$, while some others do not hold any more.

Another new ingredient is the use of lower bounds for linear forms in p-adic logarithms, which we apply in the form given by Yu [**8**].

With some minor modifications, our approach also works for a much wider class of sequences of the form $n! + u(n)$. For example, in [**3**], we obtain similar results for the prime divisors of $n! + 2^n - 1$. These results however, require bringing in some additional arguments.

Throughout this paper, we use the Vinogradov symbols $\gg$, $\ll$ and $\asymp$ as well as the Landau symbols O and o with their regular meanings.

2. *Bounding the number of solutions of some equations and congruences*

Here we obtain some upper bounds on the number of solutions of various equations and congruences involving factorials and polynomials. They play a crucial role in our arguments and probably are of independent interest as well.

LEMMA 3. *Let $f(X) \in \mathbb{Z}[X]$ be nonzero. Then there exists n_0, depending only on f, such that the equation*

$$f(n)(n+1)\dots(n+k) - f(n+k) = 0$$

does not have any integer solutions (n, k) with $n \geqslant n_0$ and $k \geqslant 1$.

Proof. Let x_0 be the largest real zero of f and let $d = \deg f$. We may assume that $n > x_0 + 1$, so that $f(n) \neq 0$ and also $f(n) \asymp n^d$. Then, for each solution (n, k) of the above equation, we have

$$(k+1)^d > \left(1 + \frac{k}{n}\right)^d \gg \left|\frac{f(n+k)}{f(n)}\right| = (n+1)\dots(n+k) > k! \geqslant 2^{k-1},$$

which certainly implies that $k \leqslant K$ with some $K = O(1)$. It remains to note that for each fixed integer $k \geqslant 1$, the equation

$$f(n)(n+1)\dots(n+k) - f(n+k) = 0$$

is a polynomial equation of degree exactly $d + k$ in n, and therefore has at most $d + k$ solutions. Choosing n_0 to be larger than $x_0 + 1$ and the absolute value of any of the solutions of this last equation for all $k \leqslant K$, we obtain the result. □

For a given integer-valued function f and integers $y \geqslant 0$, $x \geqslant y + 1$, and $q \geqslant 1$, we denote by $\mathcal{T}_f(y, x, q)$ the set of solutions of the congruence

$$\mathcal{T}_f(y, x, q) = \{n \mid n! + f(n) \equiv 0 \pmod q,\ y + 1 \leqslant n \leqslant x\},$$

and put $T_f(y, x, q) = \#\mathcal{T}_f(y, x, q)$. We also define

$$\mathcal{T}_f(x, q) = \mathcal{T}_f(0, x, q) \quad \text{and} \quad T_f(x, q) = T_f(0, x, q).$$

LEMMA 4. *Let $f(X) \in \mathbb{Z}[X]$ be nonzero. For any prime p and integers x and y with $p > x \geqslant y + 1 \geqslant 1$, we have*

$$T_f(y, x, p) \ll (x - y)^{2/3}.$$

Proof. We assume that p is larger than the absolute value of the leading coefficient of f, otherwise there is nothing to prove. Let $z > 0$ be a parameter to be chosen later. Then

$$\mathcal{T}_f(y, x, p) = \mathcal{U}_1 \cup \mathcal{U}_2,$$

where

$$\mathcal{U}_1 = \{n \in \mathcal{T}_f(y, x, p) \mid |n - m| > z \text{ for all } m \neq n,\ m \in \mathcal{T}_f(y, x, p)\},$$

and $\mathcal{U}_2 = \mathcal{T}_f(y, x, p) \backslash \mathcal{U}_1$.

We observe that $\#\mathcal{U}_1 \ll (x - y)/z$. Assume now that $n \in \mathcal{U}_2$. Then there exists a nonzero integer k with $|k| \leqslant z$, such that both $n! + f(n)$ and $(n + k)! + f(n + k)$ are multiples of p. This implies the congruence

$$f(n)(n + 1) \dots (n + k) - f(n + k) \equiv 0 \pmod{p}.$$

Since p is relatively prime to the leading coefficient of f, for each fixed k, the above congruence is a nontrivial polynomial congruence in n modulo p of degree $d + k$. Summing up over all the values of k with $|k| \leqslant z$, we get $\#\mathcal{U}_2 \ll z^2$. Thus,

$$T_f(y, x, p) = \#\mathcal{U}_1 + \#\mathcal{U}_2 \ll (x - y)/z + z^2,$$

and choosing $z = \lfloor (x - y)^{1/3} \rfloor$, we get the desired inequality. □

For any $n \geqslant p$ with $n! + f(n) \equiv 0 \pmod{p}$, we have $f(n) \equiv 0 \pmod{p}$; hence

$$T_f(p, x, p) \ll x/p. \tag{1}$$

LEMMA 5. *Let $f(X) \in \mathbb{Z}[X]$ be nonzero. For any integers $q \geqslant 2$ and $x \geqslant y + 1 \geqslant 1$, we have*

$$T_f(y, x, q) \leqslant \frac{\log x}{\log q} \left(1 + O\left(\frac{\log x}{\log q}\right)\right)(x - y) + O(1).$$

Proof. Assume that $T_f(y, x, p) \geqslant n_0 + 1$, where n_0 is the constant of Lemma 3, otherwise there is nothing to prove. Then, there exist integers $n \geqslant n_0$ and k, with

$$k \leqslant \frac{x - y}{T_f(y, x, p) - n_0} \quad \text{and} \quad y + 1 \leqslant n < n + k \leqslant x,$$

and such that q divides both $n! + f(n)$ and $(n + k)! + f(n + k)$. In particular, q divides $|f(n)(n + 1) \dots (n + k) - f(n + k)|$, and this last number is nonzero because $n \geqslant n_0$. Thus,

$$q \leqslant |f(n)(n + 1) \dots (n + k) - f(n + k)|;$$

therefore

$$\begin{aligned} \log q &\leqslant \log\left(|f(n)(n + 1) \dots (n + k) - f(n + k)|\right) \\ &\leqslant (k + O(1)) \log x \\ &= \left(\frac{x - y}{T_f(y, x, p) + O(1)} + O(1)\right) \log x, \end{aligned}$$

which finishes the proof. □

In particular,

$$T_f(y,x,q) \ll \frac{(x-y)\log x}{\log q} + 1. \tag{2}$$

Indeed, for $x \leqslant q$ the above inequality follows from Lemma 5, otherwise it is trivial.

3. *Proof of Theorem* 1

Assuming that the statement of the theorem is false, we see that there exist two constants $\lambda < 5/2$ and μ such that the inequality $P(n! + f(n)) < \lambda n + \mu$ holds for all positive integers n. It is also convenient to assume that $\lambda > 1$. For a sufficiently large positive integer x we consider the product

$$W = \prod_{1 \leqslant n \leqslant x} \max\{|n! + f(n)|, 1\},$$

and let $Q = P(W)$. Note that W and Q depend on x but hereafter, where obvious, we do not include this dependence in our notation. By the Stirling formula,

$$\max\{|n! + f(n)|, 1\} = n \log n + O(n);$$

therefore

$$\log W = \frac{1}{2} x^2 \log x + O(x^2). \tag{3}$$

For a prime p, we denote by $s_p(x)$ the largest p-adic order of the integer $\max\{1, n! + f(n)\}$ for $n \leqslant x$. We also denote by $r_p(x)$ the p-adic order of W. Hence,

$$r_p(x) = \sum_{1 \leqslant s \leqslant s_p(x)} T_f(x, p^s), \tag{4}$$

and therefore, by (3) and (4), we deduce that

$$\sum_{\substack{p \mid W \\ p \leqslant Q}} \log p \sum_{1 \leqslant s \leqslant s_p(x)} T_f(x, p^s) = \log W = \frac{1}{2} x^2 \log x + O(x^2). \tag{5}$$

We let $\mathcal{M}$ be the set of all possible pairs (p, s) which occur on the left-hand side of (5), that is,

$$\mathcal{M} = \{(p,s) \mid p \mid W,\ p \leqslant Q,\ 1 \leqslant s \leqslant s_p(x)\},$$

so that (5) can be written as

$$\sum_{(p,s) \in \mathcal{M}} T_f(x, p^s) \log p = \frac{1}{2} x^2 \log x + O(x^2). \tag{6}$$

We now introduce subsets $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3 \in \mathcal{M}$, which possibly overlap, and whose contribution to the sums on the left-hand side of (6) is $o(x^2 \log x)$. After this, we study the contribution of the remaining set $\mathcal{L}$.

(i) Let $\mathcal{E}_1$ be the set of pairs $(p, s) \in \mathcal{M}$ with $p \leqslant x/\log x$. By (2), we have

$$\begin{aligned} \sum_{(p,s) \in \mathcal{E}_1} T_f(x, p^s) \log p &\ll x \log x \sum_{(p,s) \in \mathcal{E}_1} \frac{1}{s} + \sum_{(p,s) \in \mathcal{E}_1} \log p \\ &\ll x \log x \sum_{p \leqslant x/\log x} \log(s_p(x) + 1) + \sum_{p \leqslant x/\log x} s_p(x) \log p \\ &\ll x^2, \end{aligned}$$

because $s_p(x) \ll x \log x / \log p$.

(ii) Let $\mathcal{E}_2$ be the set of pairs $(p,s) \in \mathcal{M}$ with $s \geqslant x/(\log x)^2$. Again by (2), and by the inequality $s_p(x) \ll x \log x/\log p$, we have

$$\begin{aligned}\sum_{(p,s)\in\mathcal{E}_2} T_f(x,p^s)\log p &\ll x\log x \sum_{(p,s)\in\mathcal{E}_2} \frac{1}{s} + \sum_{(p,s)\in\mathcal{E}_2} \log p \\ &\ll x\log x \sum_{p\leqslant Q} \sum_{x/(\log x)^2 \leqslant s \leqslant s_p(x)} \frac{1}{s} + \sum_{p\leqslant Q} s_p(x)\log p \\ &\ll x\pi(Q)\log x \log\log x \ll x^2 \log\log x,\end{aligned}$$

because $Q = O(x)$ by our assumption.

(iii) Let $\mathcal{E}_3$ be the set of pairs $(p,s) \in \mathcal{M}\backslash\mathcal{E}_1$ with $s \leqslant p^{1/3}$. By Lemma 4, and by the inequality $s_p(x) \ll x\log x$, we have

$$\begin{aligned}\sum_{(p,s)\in\mathcal{E}_3} T_f(x,p^s)\log p &\ll \sum_{p\leqslant Q} p^{1/3} T_f(x,p)\log p \\ &\ll \sum_{p\leqslant Q} p^{1/3}\left(p^{2/3} + x/p\right)\log p \\ &\ll \sum_{p\leqslant Q} p\log p \ll x\pi(Q)\log x \ll x^2.\end{aligned}$$

We now put $\mathcal{L} = \mathcal{M}\backslash(\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3)$. The above estimates, together with (6), show that

$$\sum_{(p,s)\in\mathcal{L}} T_f(x,p^s)\log p = \frac{1}{2}x^2\log x + O(x^2\log\log x). \tag{7}$$

We now remark that because by our assumption $P(n!+f(n)) \leqslant \lambda n + \mu$ for $n \leqslant x$, we see that $T_f(x,p^s) = T_f(\lfloor (p-\mu)/\lambda \rfloor, x, p^s)$. Defining $x_p = \min\{x,p\}$, we have, by (1),

$$\begin{aligned}T_f(\lfloor (p-\mu)/\lambda\rfloor, x, p^s) &= T_f(\lfloor (p-\mu)/\lambda\rfloor, x_p, p^s) + T_f(x_p, x, p^s) \\ &\leqslant T_f(\lfloor (p-\mu)/\lambda\rfloor, x_p, p^s) + T_f(x_p, x, p) \\ &\leqslant T_f(\lfloor (p-\mu)/\lambda\rfloor, x_p, p^s) + O(x/p).\end{aligned}$$

We also see that for every pair $(p,s) \in \mathcal{L}$, we have $\log x_p = o(s\log p)$. Therefore, by Lemma 5, we get

$$T_f(\lfloor (p-\mu)/\lambda\rfloor, x_p, p^s) \leqslant (1+o(1))|x_p - p/\lambda|\frac{\log x}{s\log p} + O(1).$$

Combining the above inequalities, we obtain

$$\begin{aligned}&\sum_{(p,s)\in\mathcal{L}} T_f(x,p^s)\log p \\ &\quad\leqslant \sum_{(p,s)\in\mathcal{L}} \left((1+o(1))|x_p - p/\lambda|\frac{\log x}{s} + O\left(\log p + \frac{x\log p}{p}\right)\right).\end{aligned} \tag{8}$$

Recalling the definition of $\mathcal{E}_1$ and $\mathcal{E}_2$, we obtain

$$\sum_{(p,s)\in\mathcal{L}} \log p \ll \frac{x}{\log^2 x}\sum_{p\leqslant Q}\log p \ll \frac{x}{\log x}\pi(Q) = o(x^2),$$

and also

$$\sum_{(p,s)\in\mathcal{L}} \frac{\log p}{p} \ll \frac{x}{\log^2 x} \sum_{x/\log x\leqslant p\leqslant Q} \frac{\log p}{p}$$
$$\ll \frac{x}{\log^2 x}\left(\log(Q) - \log\left(\frac{x}{\log x}\right)\right) \ll \frac{x\log\log x}{\log^2 x} = o(x),$$

by the Mertens formula (see [**7**, Theorem 3.1 of Chapter 1]). Therefore, taking (7) and (8) into account, we conclude that

$$\sum_{(p,s)\in\mathcal{L}} |x_p - p/\lambda|\frac{1}{s} = \left(\frac{1}{2} + o(1)\right)x^2. \tag{9}$$

On the other hand, recalling again the definition of the sets $\mathcal{E}_1$ and $\mathcal{E}_2$, we see that $s < x/\log x \leqslant p$ for every pair $(p,s) \in \mathcal{L}$. From this, and from the definition of the set $\mathcal{E}_3$, we obtain

$$\sum_{(p,s)\in\mathcal{L}} |x_p - p/\lambda|\frac{1}{s} \leqslant \sum_{p\leqslant Q} |x_p - p/\lambda| \sum_{p^{1/3}\leqslant s\leqslant p} \frac{1}{s}$$
$$= \left(\frac{2\log x}{3} + o(1)\right)\sum_{p\leqslant Q} |x_p - p/\lambda|.$$

Furthermore,

$$\sum_{p\leqslant Q} |x_p - p/\lambda| = \sum_{p\leqslant x}(p - p/\lambda) + \sum_{x<p\leqslant Q} |x - p/\lambda|$$
$$= \left(\frac{1}{2} + o(1)\right)x\pi(x) + x(\pi(Q) - \pi(x)) - \left(\frac{1}{2\lambda} + o(1)\right)Q\pi(Q)$$
$$\leqslant \left(\frac{1}{2} + \lambda - 1 - \frac{\lambda}{2} + o(1)\right)\frac{x^2}{\log x} = \left(\frac{\lambda - 1}{2} + o(1)\right)\frac{x^2}{\log x}.$$

Therefore, by (9), and the last two estimates above, we have

$$\frac{\lambda - 1}{3} + o(1) \geqslant \frac{1}{2},$$

which contradicts the assumption that $\lambda < 5/2$.

4. *Proof of Theorem* 2

For every prime number p and every nonzero rational number r we denote by $\mu_p(r)$ the p-adic order of r.

We assume that n is large enough so that $|f(n)| \geqslant 1$. Then we can write it as

$$f(n) = U(n)V(n), \tag{10}$$

where

$$U(n) = \prod_{p<n^{1/2}} p^{\mu_p(f(n))}, \qquad V(n) = |f(n)|/U(n).$$

If $p \leqslant n^{1/2}$, then we have

$$\mu_p(U(n)) = \mu_p(f(n)) \leqslant \frac{\log|f(n)|}{\log p} \ll \log|f(n)| \ll \log n,$$

while

$$\mu_p(n!) \geqslant \left\lfloor \frac{n}{p} \right\rfloor \geqslant \frac{n}{p} - 1 \geqslant n^{1/2} - 1,$$

and, in particular, $\mu_p(n!) \geqslant 2\mu_p(U(n))$ holds for sufficiently large n. Thus, $U(n)^2 | n!$. Let $d = \deg f$. Then

$$n^{\omega(V(n))/2} \leqslant \prod_{p|V(n)} p \leqslant V(n) \leqslant |f(n)| \ll n^d,$$

and therefore $\omega(V(n)) \leqslant 2d$ holds for large values of n. We now let $W(n) = \gcd(n!, f(n))$, and we assume that

$$n! + f(n) = W(n) p_1^{\alpha_1} \dots p_s^{\alpha_s}, \tag{11}$$

where $p_1 < p_2 < \ldots < p_s$ are distinct primes. As we have remarked, $U(n)^2 | n!$; therefore $\gcd(U(n), p_1 \dots p_s) = 1$. Hence, if $p_\ell < n$ for some $1 \leqslant \ell \leqslant s$, then $p_\ell | V(n)$, and, in particular $\ell \leqslant 2d$. Because

$$\log W(n) \leqslant \log |f(n)| = d \log n + O(1),$$

and by the prime number theorem

$$\sum_{p < (d+1)\log n} \log p = (d + 1 + o(1)) \log n,$$

we conclude that there is a prime $p < (d+1)\log n$ which does not divide $W(n)$.

From (11), we deduce that

$$\mu_p \left(p_1^{\alpha_1} \dots p_s^{\alpha_s} - \frac{f(n)}{W(n)} \right) = \mu_p(n!) \gg \frac{n}{p} \gg \frac{n}{\log n}. \tag{12}$$

On the other hand, using the lower bound for linear forms in p-adic logarithms of Yu [**8**], we derive

$$\mu_p \left(p_1^{\alpha_1} \dots p_s^{\alpha_s} - \frac{f(n)}{W(n)} \right) \ll (400s)^{s+2} \log(s+2) \cdot \frac{p}{\log^2 p} \cdot \Omega \cdot \log B, \tag{13}$$

where

$$B = \max\{3, \alpha_1, \dots, \alpha_s\} \quad \text{and} \quad \Omega = \prod_{i=1}^{s+1} \log A_i$$

with $A_i = \max\{3, p, p_i\}$ for $i = 1, \dots, s$, and $A_{s+1} = \max\{3, p, |f(n)|/W(n)\}$. We can assume that $A_i \leqslant 2n$ for $i = 1, \dots, s$, because otherwise $P(n! + f(n)) \geqslant 2n$ and there is nothing to prove. We also see that $B \leqslant 2n \log n$ holds for all sufficiently large n.

Combining the inequalities (12) and (13), we derive

$$\frac{n}{\log n} \ll (400s)^{s+2} \log(s+2) \cdot \frac{\log n}{(\log\log n)^2} \cdot (\log(2n))^{s+2},$$

and therefore

$$(1 + o(1)) \log n \leqslant (s+3)(\log s + \log\log n + O(1)).$$

The above inequality yields

$$s \geqslant \left(\frac{1}{2} + o(1) \right) \frac{\log n}{\log\log n}.$$

As we have seen, $p_s > \ldots > p_{2d+1} > n$; thus

$$\pi(p_s) - \pi(n) \geqslant s - 2d \geqslant \left(\frac{1}{2} + o(1)\right) \frac{\log n}{\log\log n},$$

where as usual $\pi(x)$ is the number of primes $p \leqslant x$. By a classical result of Montgomery and Vaughan [**5**] (see also [**4**, p. 34]), we know that

$$\pi(x+y) - \pi(x) < \frac{2y}{\log y}.$$

Thus,

$$\left(\frac{1}{2} + o(1)\right) \frac{\log n}{\log\log n} \leqslant \frac{2(p_s - n)}{\log(p_s - n)}, \tag{14}$$

which implies the inequality of Theorem 2.

5. *Remarks*

In some cases, such as when $f(X)$ is a constant nonzero polynomial, the constant $1/4$ from the inequality of Theorem 2 can be replaced by $1/2$. Indeed, in this case, $|f(n)|/W(n) = 1$ holds for large n, and since p_i are distinct primes for $i = 1, \ldots, s$, the Kummer condition $[\mathbb{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_s}\right) : \mathbb{Q}] = 2^s$ is fulfilled. In this case, the factor $(s+2)^{s+2}$ from (13) can be replaced by K^s, where K is an absolute constant (see [**8**]), and this saves a factor of 2 in the final estimate (14).

We also note that if $f(X) \in \mathbb{Z}[X]$ is nonzero, then our arguments also show that

$$\omega\left(\prod_{1 \leqslant n \leqslant x} \max\{|n! + f(n)|, 1\}\right) \gg \frac{x}{\log x}$$

holds for any sufficiently large x. Indeed, in the notation of the proof of Theorem 1, we derive from (4) and (2), that

$$r_p(x) \ll \sum_{1 \leqslant s \leqslant s_p(x)} \frac{x \log x}{s \log p} + 1 \ll \frac{x \log x \log(s_p(x)+1)}{\log p} + s_p(x).$$

Since $s_p(x) \ll x \log x / \log p$, we obtain $r_p(x) \ll x(\log x)^2 / \log p$. Thus, for any prime number p,

$$p^{r_p(x)} = \exp\left(O\left(x(\log x)^2\right)\right),$$

which together with (3) implies the desired lower bound.

Finally, we remark that the arguments used in the proof of Lemma 4 have also been used in [**2**] to study several more congruences with factorials.

Acknowledgements. The authors would like to thank Martin Klazar for a careful reading of the manuscript and a number of useful comments. During the preparation of this paper, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459.

References

1. P. Erdős and C. Stewart, 'On the greatest and least prime factors of $n! + 1$', *J. London Math. Soc.* 13 (1976) 513–519.

2. M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Character sums and congruences with $n!$', *Trans. Amer. Math. Soc.* 356 (2004) 5089–5102.

3. F. Luca and I. Shparlinski, 'On the largest prime factor of $n! + 2^n - 1$', *J. Théor. Nombres Bordeaux*, to appear.
4. H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics 227 (Springer, 1991).
5. H. L. Montgomery and R. C. Vaughan, 'The large sieve', *Mathematika* 20 (1973) 119–134.
6. M. R. Murty and S. Wong, 'The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences', *Number theory for the millennium, III* (*Urbana, IL, 2000*) (A. K. Peters, Natick, MA, 2002) 43–54.
7. K. Prachar, *Primzahlverteilung* (Springer, Berlin, 1957).
8. K. Yu, 'p-adic logarithmic forms and group varieties, II', *Acta Arith.* 89 (1999) 337–378.

F. Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
CP 58089
Morelia
Michoacán
México

fluca@matmor.unam.mx

I. E. Shparlinski
Department of Computing
Macquarie University
Sydney
NSW 2109
Australia

igor@ics.mq.edu.au