Publ. Math. Debrecen
71/1-2 (2007), 95–100

On the set of the largest prime divisors

By IGOR E. SHPARLINSKI (Sydney) and DANIEL SUTANTYO (Sydney)

Abstract. In this paper we obtain lower bounds on the set of the largest prime divisors $P(a(n))$ of various sequences $a(n)$ for $n \le x$. In particular we obtain such results for polynomial sequences and for linear recurrence sequences.

1. Introduction

For an integer k we use $P(k)$ to denote the largest prime divisor of k (we also put $P(0) = 0$ and $P(\pm 1) = 1$).

Give an integer-valued sequence $\mathcal{A} = (a(n))_{n=1}^{\infty}$ and a real positive x, we denote

$$\mathcal{S}_{\mathcal{A}}(x) = \{P(a(n)) : n \le x\}.$$

Certainly studying the size and other properties of $P(a(n))$ for various sequences $\mathcal{A}$ is a classical number theoretic question, which has been studied for various sequences including shifted primes, polynomials and linear recurrence sequences, for example, see [1], [3], [7]–[9], [11]–[17] and references therein. On the other hand, the question about the cardinality of set $\mathcal{S}_{\mathcal{A}}(x)$ appears to be new. We however mention a result of [10] about

$$\{P(a_1 + \cdots + a_k) : a_i \in \mathcal{A}_i,\ i = 1, \ldots, k\}$$

where $\mathcal{A}_1, \ldots, \mathcal{A}_k$ are k arbitrary sufficiently dense sets of integers.

It also follows immediately from the result of [2] that for the sequence $\mathcal{P}_a = (\ell(n) + a)_{n=1}^{\infty}$ of consecutive shifted prime numbers (where $\ell(n)$ denotes the nth

Mathematics Subject Classification: 11N25, 11N64.
Key words and phrases: largest prime divisor, polynomials, recurrence sequences; products of primes.

prime) the corresponding set $\mathcal{S}_{\mathcal{P}_a}(x)$ consists of all primes in the interval $[1, x^\gamma]$ for any $\gamma < 17/33$.

Throughout the paper, any implied constants in the symbols 'O', '$\ll$' and '$\gg$' may depend (where obvious) on the sequence $\mathcal{A}$ and are absolute otherwise. We recall that the statements $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$ for positive functions A and B.

2. Auxiliary results

We employ some well known results on the distribution of the values of the largest prime divisor for various sequences.

For a given nonconstant polynomial $g(X) \in \mathbb{Z}[X]$, we use $\psi_g(x, y)$ to denote the number of positive integers $n \le x$ with $P(g(n)) \le y$, that is,

$$\psi_g(x, y) = \#\{n \le x : P(g(n)) \le y\}.$$

We have the following bound from [18], which in turn improves some results from [5]:

Lemma 1. *Let $g(X) \in \mathbb{Z}[X]$ be a polynomial of degree $\deg g = k \ge 2$ having t irreducible divisors over $\mathbb{Z}$. Then, for any fixed $\varepsilon > 0$ and all sufficiently large x, we have*

$$\psi_g(x, y) \le \frac{(t+\varepsilon)^{\lfloor v \rfloor} x}{k(k-1)^{\lfloor v \rfloor - 1} v^{\lfloor v \rfloor}}$$

for $y = x^{1/v}$, and $1 \le v \le \sqrt{\log x/(2+\varepsilon)}$.

Let $\mathcal{U} = (u(n))_{n=1}^{\infty}$ be a linear recurrence sequence of integers satisfying a homogeneous linear recurrence relation

$$c_k u(n+k) + c_{k-1} u(n+k-1) + \cdots + c_0 u(n) = 0, \qquad k = 1, 2, \ldots,$$

with the characteristic polynomial

$$c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[X].$$

where $c_k \ne 0$ and $c_0 \ne 0$. We recall that $\mathcal{U}$ is called *non-degenerate* if $\alpha_i^s \ne \alpha_j^s$, $1 \le i < j \le m$, $s = 1, 2, \ldots$, where $\alpha_1, \ldots, \alpha_m$ are pairwise distinct roots of the characteristic polynomial.

For an integer q and a real x we denote by $R_{\mathcal{U}}(x, q)$ the number of positive integers $n \le x$ with $u(n) \equiv 0 \pmod q$. We need the following bound from [11].

Lemma 2. *If the linear recurrent sequence* $\mathcal{U} = (u(n))_{n=1}^{\infty}$ *is non-degenerate then for any integer* $q \ge 2$ *and real* $x \ge 0$,

$$R_{\mathcal{U}}(x, q) \ll x/\log q + 1.$$

Let $\mathcal{L}$ be an arbitrary set of primes and let $A_{\mathcal{U}}(\mathcal{L}, x)$ be the number of $n \le x$ such that $u(n)$ is composed only out of primes from $\mathcal{L}$. The following bound is given in [12].

Lemma 3. *If the linear recurrent sequence* $\mathcal{U} = (u(n))_{n=1}^{\infty}$ *is non-degenerate then for any set* $\mathcal{L}$ *of* $r = \#\mathcal{L}$ *primes and real* $x \ge 0$,

$$A_{\mathcal{U}}(\mathcal{L}, x) \ll r(\log x)^2.$$

For an integer q and a real x we denote by $T(x, q)$ the number positive integers $n \le x$ with $n! + 1 \equiv 0 \pmod q$. We need the following bound which is a partial case of a more general estimate from [9].

Lemma 4. *For any prime* p *and real* x *with* $p > x \ge 1$, *we have*

$$T(x, p) \ll x^{2/3}.$$

Let $\mathcal{V} = (v(n))$ where

$$v(n) = \prod_{j=1}^{n} \ell(n) + 1 \qquad (1)$$

and $\ell(n)$ denotes the nth prime. For a prime p and a real x, let $W(x, p)$ be the number of positive integers $n \le x$ such that $v(n) \equiv 0 \pmod p$. We have the following bound which is a special case of a more general result from [6].

Lemma 5. *For any prime* p *and real* $x \ge 3$, *we have*

$$W(x, p) \ll x \frac{\log \log x}{\log x}.$$

3. Main results

We now derive lower bounds for the sets $\mathcal{S}_{\mathcal{A}}(x)$ for various sequences $\mathcal{A}$. We start with polynomial sequences.

Theorem 6. *Let $g(X) \in \mathbb{Z}[X]$ be polynomial of degree $k \ge 2$ which does not split completely over $\mathbb{Z}$. Then for the sequence $\mathcal{G} = (g(n))_{n=1}^{\infty}$ we have*

$$\#\mathcal{S}_{\mathcal{G}}(x) \gg \frac{x}{4k^2} - 1.$$

Proof. We partition the set of integers $n \le x$ into the set $\mathcal{N}_1$ consisting of those $n \le x$ such that $P(g(n)) \le x$, and $\mathcal{N}_2$ consisting of those $n \le x$ such that $P(g(n)) > x$.

Since $g(X)$ does not split over $\mathbb{Z}$ we see that the number t of its irreducible divisors satisfies $t \le k - 1$. It immediately follows from from Lemma 1, applied with $\varepsilon = 1/2$ and $v = 1$, that for a sufficiently large x,

$$\#\mathcal{N}_1 \le \frac{k - 1/2}{k} x.$$

Hence

$$\#\mathcal{N}_2 \ge x - \#\mathcal{N}_1 - 1 = \frac{x}{2k} - 1.$$

Let $\mathcal{Q} = \{P(g(n)) : n \in \mathcal{N}_2\}$. Then for some $p \in \mathcal{Q}$ and $p \ge x$, the congruence

$$g(n) \equiv 0 \pmod p, \qquad n \in \mathcal{N}_2,$$

has at least $\#\mathcal{N}_2/\#\mathcal{Q}$ solutions. On the other hand, there can be at most $k(x/p + 1)$ solutions to this congruence. Therefore we have

$$\frac{\#\mathcal{N}_2}{\#\mathcal{Q}} \le k\left(\frac{x}{p} + 1\right) \le 2k.$$

This leads us to the inequality

$$\#\mathcal{S}_{\mathcal{G}}(x) \ge \#\mathcal{Q} \ge \frac{\#\mathcal{N}_2}{2k} > \frac{x}{4k^2} - 1$$

and the result now follows. □

Clearly, one can easily improve the constant $1/4k^2$. It is also clear that if $g(X)$ splits completely over $\mathbb{Z}$ then $\#\mathcal{S}_{\mathcal{G}}(x) \ll x/\log x$ and one can easily prove a matching lower bound.

Theorem 7. *Let $\mathcal{U} = (u(n))_{n=1}^{\infty}$ be a non-degenerate linear recurrent sequence. Then*

$$\#\mathcal{S}_{\mathcal{U}}(x) \gg \log x.$$

Proof. Let $y = x/(\log x)^2$. We partition the set of integers $n \le x$ into the set $\mathcal{M}_1$ consisting of those $n \le x$ such that $P(u(n)) \le y$, and $\mathcal{M}_2$ consisting of those $n \le x$ such that $P(u(n)) > y$.

By Lemma 3, applied to the set $\mathcal{L}$ of the first $r = \pi(y) \sim x/(\log x)^3$ primes, we obtain $\#\mathcal{M}_1 \ll x/\log x$. Thus $\#\mathcal{M}_2 = (1 + o(1))x$.

As in the proof of Theorem 6 we conclude that there is a prime $p > y$ such that the congruence

$$u(n) \equiv 0 \pmod{p}, \qquad n \in \mathcal{M}_2,$$

has at least $\#\mathcal{M}_2/\#\mathcal{R}$ solutions, where $\mathcal{R} = \{P(u(n)) : n \in \mathcal{M}_2\}$. Using Lemma 2, we derive

$$\frac{\#\mathcal{M}_2}{\#\mathcal{R}} \ll \frac{x}{\log p} + 1 \ll \frac{x}{\log y} \ll \frac{x}{\log x}$$

and the result now follows. □

Theorem 8. *Let* $\mathcal{F} = (n! + 1)_{n=1}^{\infty}$. *Then*

$$\#\mathcal{S}_{\mathcal{F}}(x) \ge x^{1/3}.$$

Proof. Clearly, there is a prime p such that the congruence

$$n! + 1 \equiv 0 \pmod{p}, \qquad 1 \le n \le x,$$

has at least $\lfloor x \rfloor/\#\mathcal{S}_{\mathcal{F}}(x)$ solutions. We have two possible cases; one when $p > x$, and the second when $p \le x$. If $p > x$, we can apply Lemma 4 directly. If $p \le x$, we see that $P(n!+1) = p$ only when $n < p$, and we can use Lemma 4 with $x = p$. Therefore

$$\frac{\lfloor x \rfloor}{\#\mathcal{S}_{\mathcal{F}}(x)} \ll \min\{x^{2/3}, p^{2/3}\} \ll x^{2/3}$$

and the result now follows. □

Theorem 9. *Let* $\mathcal{V} = (v(n))_{n=1}^{\infty}$ *where* $v(n)$ *is given by* (1). *We have*

$$\#\mathcal{S}_{\mathcal{V}}(x) \ge \frac{\log x}{\log\log x}.$$

Proof. As before, we note that there is a prime p such that the congruence

$$v(n) \equiv 0 \pmod{p}, \qquad 1 \le n \le x,$$

has at least $\lfloor x \rfloor/\#\mathcal{S}_{\mathcal{V}}(x)$ solutions. Using Lemma 5, we finish the proof. □

References

[1] R. C. Baker and G. Harman, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331–361.

[2] W. D. Banks and I. E. Shparlinski, On values taken by the largest prime factor of shifted primes, *J. Aust. Math. Soc.* (*to appear*).

[3] G. Everest, A. J. van der Poorten, I. E. Shparlinski and T. B. Ward, Recurrence sequences, *Amer. Math. Soc.* (2003).

[4] H. Halberstam and H.-E. Richert, Sieve Methods, *Academic Press*, *London*, 1974.

[5] N. A. Hmyrova, On polynomials with small prime divisors, II, *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 1367–1372.

[6] E. Levieil, F. Luca and I. Shparlinski, Bounding the number of solutions of some congruences, *Bol. Soc. Matem. Mexicana* **11** (2005), 3057–3073.

[7] F. Luca, Divisibility properties of binary recurrent s equences, *Bull. Lond. Math. Soc.* **37** (2005), 809–817.

[8] F. Luca, Arithmetic properties of members of a binary recurrence sequence, *Acta Arith.* **109** (2003), 81–107.

[9] F. Luca and I. Shparlinski, Prime divisors of shifted factorials, *Bull. Lond. Math. Soc.* **37** (2005), 809–817.

[10] A. Sárközy and C. L. Stewart, On divisors of sums of integers, I, *Acta. Math. Hung.* **48** (1986), 147–154.

[11] I. E. Shparlinski, The number of different prime divisors of recurrence sequences, *Matem. Zametki* = *Math. Notes* **42** (1987), 494–507 (in *Russian*).

[12] I. E. Shparlinski, Some arithmetic properties of recurrence sequences, *Matem. Zametki* **47** (1990), 612–617 (in *Russian*).

[13] V. G. Sprindzuk, Classical Diophantine equations, Lecture Notes in Math, vol. 1559, *Springer-Verlag*, 1993.

[14] C. L. Stewart, On divisors of terms of linear recurrence sequences, *J. Reine Angew. Math.* **333** (1982), 12–31.

[15] C. L. Stewart, On the greatest prime factor of terms of a linear recurrence sequence, *Rocky Mountain J. Math.* **15** (1985), 599–608.

[16] C. L. Stewart, On the greatest prime factor of integers of the form $ab+1$, *Periodica Math. Hung.* **43** (2001), 81–91.

[17] C. L. Stewart, On the greatest and least prime factors of $n!+1$, II, *Publ. Math. Debrecen* **65** (2004), 461–480.

[18] N. M. Timofeev, Polynomials with small prime divisors, Taškent. Gos. Univ., Naučn. Trudy No. 548, Voprosy Mat., *Taškent*, 1977, 87–91 (in *Russian*).

IGOR E. SHPARLINSKI
DEPARTMENT OF COMPUTING
MACQUARIE UNIVERSITY
SYDNEY, NSW 2109
AUSTRALIA

E-mail: igor@ics.mq.edu.au

DANIEL SUTANTYO
DEPARTMENT OF COMPUTING
MACQUARIE UNIVERSITY
SYDNEY, NSW 2109
AUSTRALIA

E-mail: daniels@ics.mq.edu.au

(Received November 10, 2005; revised February 16, 2006)