On Rough and Smooth Neighbors

William D. Banks, Florian Luca, and Igor E. Shparlinski

Department of Mathematics
University of Missouri
Columbia, MO 65211 — USA
bbanks@math.missouri.edu

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Department of Computing
Macquarie University
Sydney, NSW 2109 — Australia
igor@ics.mq.edu.au

Received: November 2, 2005
Accepted: June 19, 2006

ABSTRACT

We study the behavior of the arithmetic functions defined by

$$\mathcal{F}(n) = \frac{P^+(n)}{P^-(n+1)} \quad \text{and} \quad \mathcal{G}(n) = \frac{P^+(n+1)}{P^-(n)} \qquad (n \ge 1),$$

where $P^+(k)$ and $P^-(k)$ denote the largest and the smallest prime factors, respectively, of the positive integer k.

Key words: smallest prime divisor, largest prime divisor.

2000 Mathematics Subject Classification: 11N25, 11N64.

Introduction

For every integer $n \ge 2$, let $P^+(n)$ and $P^-(n)$ denote the largest and the smallest prime factors of n, respectively; put $P^+(1) = 1$ and $P^-(1) = \infty$. An integer n is said to be *y-smooth* if $P^+(n) \le y$, and it is said to be *z-rough* if $P^-(n) > z$.

There are several papers in the literature which study smoothness properties of consecutive integers. In certain ranges, upper and lower bounds have been obtained on the number of positive integers $n \le x$ for which $P^+(n(n+1)) \le y$, and other similar questions have been studied; see, for example, [4, 5, 10, 15]. The arithmetic function

$$\mathcal{H}(n) = \frac{P^+(n)}{P^+(n+1)} \qquad (n \geq 1)$$

has been investigated in [3, 6]; in particular, it is known (see [6]) that for every $\varepsilon > 0$ there exists $\delta > 0$ such that the inequalities

$$n^{-\delta} \leq \mathcal{H}(n) \leq n^{\delta}$$

hold for at most εx positive integers $n \leq x$. The distribution of integers n for which $P^+(n) < P^+(n+1)$ (that is, $\mathcal{H}(n) < 1$) and that of integers n such that $P^+(n) > P^+(n+1)$ have also been studied, as well as analogous questions about the possible orderings among the three primes $P^+(n)$, $P^+(n+1)$, and $P^+(n+2)$; see [3, 6]. These results suggest that the values of $P^+(n)$ and $P^+(n+1)$ are essentially independent.

In this paper, we introduce and study the arithmetic functions

$$\mathcal{F}(n) = \frac{P^+(n)}{P^-(n+1)} \qquad \text{and} \qquad \mathcal{G}(n) = \frac{P^+(n+1)}{P^-(n)} \qquad (n \geq 1),$$

for which we obtain a variety of results with a similar flavor; our results suggest that the values of $P^+(n)$ and $P^-(n \pm 1)$ are essentially independent; that is, the smoothness of n does not affect the roughness of its neighbors $n \pm 1$.

We show that for almost all positive integers n, the values $\mathcal{F}(n)$ and $\mathcal{G}(n)$ are "large" in a certain sense. This is consistent with our intuition: Since the set of y-smooth integers $s \leq x$ is much smaller than the set of y-rough integers $r \leq x$ over a wide range in the xy-plane (see [14, chapters III.5 and III.6]), for "random" integers s, r it is likely that $P^+(s)$ is much larger than $P^-(r)$. Our results show that the same result is true when s and r are neighbors, that is, when $|s - r| = 1$.

Although $\mathcal{F}(n)$ and $\mathcal{G}(n)$ tend to be large, the value sets $\mathcal{F}(\mathbb{N})$ and $\mathcal{G}(\mathbb{N})$ are quite dense in the set of all positive real numbers. In particular, both value sets contain *all* fractions of the form $p/q > 1$ and *almost all* fractions of the form $p/q < 1$, where p and q are prime numbers. On the other hand, we show that for every prime p, there are infinitely many primes $q > p$ such that $p/q \notin \mathcal{F}(\mathbb{N})$, and we expect the same statement to hold for $\mathcal{G}(\mathbb{N})$ as well.

In addition to their intrinsic interest as natural analogues of the arithmetic function $\mathcal{H}(n)$, the functions $\mathcal{F}(n)$ and $\mathcal{G}(n)$ also exhibit interesting links with some famous sets of positive integers, such as the Fermat and Mersenne primes.

1. Notation

Throughout the paper, any implied constants in symbols 'O,' '$\ll$,' and '$\gg$' are absolute unless specified otherwise. We recall that, for positive functions U and V, the statements $U = O(V)$, $U \ll V$, and $V \gg U$ are all equivalent to the assertion that $U \leq cV$ holds with some constant $c > 0$.

In what follows, the letters ℓ, p, q and r (with or without subscripts) always denote prime numbers, k, m and n always denote positive integers, and x is always a positive real number. As usual, we let $\pi(x)$ denote the number of primes $p \le x$.

Finally, for any real number $x > 0$ and integer $k \ge 1$, we denote by $\log_k x$ the k-th iterate of the function $\log x = \max\{\ln x, 1\}$, where $\ln x$ is the natural logarithm.

2. Value sets

Let $\mathcal{F}(\mathbb{N})$ and $\mathcal{G}(\mathbb{N})$ denote the collection of values taken by $\mathcal{F}(n)$ and $\mathcal{G}(n)$, respectively, as n varies over the set of natural numbers $\mathbb{N}$. The following result shows that the intersection $\mathcal{F}(\mathbb{N}) \cap \mathcal{G}(\mathbb{N})$ contains every fraction of the form p/q, where p, q are primes with $p > q$:

Theorem 2.1. *For any two primes $p > q$, there exist integers $m, n \in \mathbb{N}$, with*

$$\max\{m, n\} \le \exp\left(p + o(p)\right) \qquad \text{as} \quad p \to \infty,$$

such that

$$\mathcal{F}(m) = \mathcal{G}(n) = p/q.$$

Proof. Let $\mathcal{L} = \{\text{primes } \ell \le p \ : \ \ell \ne q\}$, and put

$$L = \prod_{\ell \in \mathcal{L}} \ell.$$

Let M be the unique integer such that $1 \le M < q$ and $LM \equiv 1 \pmod q$, and put

$$m = (q-1)LM \qquad \text{and} \qquad n = (q+1)LM - 1.$$

Since $p \ge q + 1 > M$, it is clear that $P^+(m) = P^+(n+1) = p$. On the other hand, it is easy to see that $q \mid m + 1$ and $q \mid n$, whereas

$$m + 1 \equiv 1 \pmod \ell \qquad \text{and} \qquad n \equiv -1 \pmod \ell \qquad (\ell \in \mathcal{L});$$

therefore, $P^-(m+1) = P^-(n) = q$. Combining these results, it follows that $\mathcal{F}(m) = \mathcal{G}(n) = p/q$.

By the *Prime Number Theorem*, we also have the bound

$$\max\{m, n\} < (q+1)LM \le (q^2-1)L < q \prod_{\ell \le p} \ell = \exp(p + o(p)), \tag{1}$$

and this finishes the proof. □

Remark 2.2. Using explicit bounds from [12] for the product of the primes $\ell \le p$, one can derive from (1) an entirely explicit version of Theorem 2.1 with a specific function of p in the exponent rather than $p + o(p)$.

Remark 2.3. A minor modification to the construction of Theorem 2.1 allows one to build infinitely many m and n with $\mathcal{F}(m) = \mathcal{G}(n) = p/q$ when $p > q$. On the other hand, the equation $\mathcal{H}(m) = p/q$ has only finitely many solutions m since by a classical result of C. Siegel [13] it is known that $P^+(n(n+1)) \to \infty$ as $n \to \infty$. (See also [9] for the currently best known effective lower bound of the type $P^+(n(n+1)) \gg \log_2 n \log_3 n / \log_4 n$.)

In contrast with Theorem 2.1, the value set $\mathcal{F}(\mathbb{N})$ does not contain every fraction of the form p/q with $p < q$ (see Theorem 2.5 below), and we expect the same to be true for $\mathcal{G}(\mathbb{N})$. However, the next result implies that *almost all* such fractions occur in the intersection $\mathcal{F}(\mathbb{N}) \cap \mathcal{G}(\mathbb{N})$.

Theorem 2.4. *For every pair of primes (p, q) such that $p < q \le x$, with at most $o\big(\pi(x)^2\big)$ possible exceptions, there exist integers $m, n \in \mathbb{N}$, with*

$$\max\{m, n\} \le \exp(\exp(q + o(q))) \qquad \text{as} \quad q \to \infty,$$

such that

$$\mathcal{F}(m) = \mathcal{G}(n) = p/q.$$

Proof. Let $y = \sqrt{\log x}$. We exclude from consideration any pair of primes (p, q) for which $p \le q/y$; clearly, there are at most

$$\pi(x)\,\pi(x/y) \ll \frac{x}{\log x}\,\frac{(x/y)}{\log(x/y)} \ll \frac{x^2}{(\log x)^{2.5}} = o(\pi(x)^2)$$

such pairs with $p < q \le x$. We also exclude those pairs (p, q) for which

$$\max\{P^+(q-1), P^+(q+1)\} > q/y.$$

To estimate the number of such pairs, we apply *Brun's method* (see, for example, [8, Theorem 2.3]) to deduce that for every positive integer a, each of the linear forms $a\ell + 1$ and $a\ell - 1$ take prime values for at most

$$N_a(x) \ll \frac{x}{\varphi(a)\log^2(x/a)} \ll \frac{x\log_2 a}{a\log^2(x/a)}$$

primes $\ell \le x/a$, where $\varphi(\cdot)$ is the Euler function. In the above estimate, we have used the bound $a/\varphi(a) \ll \log_2 a$, which holds uniformly for all $a \ge 1$. If $p < q \le x$ and $P^+(q \pm 1) > q/y$, then $q = a\ell \mp 1$ for some integer $a < 2y$ and prime $\ell \le (x+1)/a$; hence, there are at most

$$\pi(x)\sum_{a<2y} 2N_a(x+1) \ll \pi(x)\,\frac{x\log y\,\log_2 y}{\log^2 x} \ll \pi(x)^2\,\frac{\log_2 x\,\log_3 x}{\log x} = o(\pi(x)^2)$$

such pairs of primes (p, q).

Now, fix one of the remaining pairs (p, q). Let $\mathcal{L} = \{\text{primes } \ell \le p\}$ and $\mathcal{R} = \{\text{primes } r : p < r < q\}$, and put

$$m = (q-1)L^{(q-1)R} \qquad \text{and} \qquad n = (q+1)L^{(q-1)R} - 1,$$

where

$$L = \prod_{\ell \in \mathcal{L}} \ell \qquad \text{and} \qquad R = \prod_{r \in \mathcal{R}} (r-1).$$

Since $P^+(q \pm 1) \le q/y < p$, we have $P^+(m) = P^+(n+1) = p$. We claim that $P^-(m+1) = P^-(n) = q$ (and consequently, $\mathcal{F}(m) = \mathcal{G}(n) = p/q$). Indeed, using *Fermat's Little Theorem*, we have

$$m \equiv -L^{(q-1)R} \equiv -1 \pmod{q},$$

hence, $q \mid m+1$. Similarly,

$$n \equiv L^{(q-1)R} - 1 \equiv 0 \pmod{q},$$

thus, $q \mid n$. On the other hand, as $(r-1) \mid R$ for each prime $r \in \mathcal{R}$, Fermat's Little Theorem also implies that

$$m + 1 = (q-1)L^{(q-1)R} + 1 \equiv q \not\equiv 0 \pmod{r},$$

and

$$n = (q+1)L^{(q-1)R} - 1 \equiv q \not\equiv 0 \pmod{r},$$

thus, $r \nmid (m+1)n$. Finally, since $\ell \mid L$ for every $\ell \in \mathcal{L}$, it is clear that $\ell \nmid (m+1)n$, and the claim is proved.

By the Prime Number Theorem, we have the estimates

$$L \le \exp(p + o(p)) \qquad \text{and} \qquad R \le \exp(q + o(q)),$$

and the theorem follows. □

The following result shows that $\mathcal{F}(\mathbb{N})$ does not include all fractions of the form p/q with $p < q$:

Theorem 2.5. *For every prime p, let*

$$\mathcal{Q}_p = \{\textit{primes } q : p/q \notin \mathcal{F}(\mathbb{N})\}.$$

Then,

$$\#\{q \le x : q \in \mathcal{Q}_p\} \gg \pi(x),$$

where the implied constant depends only on p. Moreover,

$$\min_{q \in \mathcal{Q}_p} \{q\} \le \exp(O(p)).$$

Proof. For a fixed prime p, let q be a prime such that:

(i) every prime $\ell \le p$ is a quadratic residue modulo q;

(ii) -1 is a quadratic nonresidue modulo q.

We claim that $q \in \mathcal{Q}_p$. Indeed, if $n \ge 1$ is an integer for which $P^+(n) = p$, property (i) implies that n is a quadratic residue modulo q. But then the equation $P^-(n+1) = q$ is not possible, for otherwise $n \equiv -1 \pmod q$ is a quadratic nonresidue by (ii).

To construct examples of such primes q, let $N = 4\prod_{\ell \le p} \ell$, and let a be the congruence class modulo N determined by the conditions $a \equiv 7 \pmod 8$ and $a \equiv (-1)^{(\ell-1)/2} \pmod \ell$ for $2 < \ell \le p$; then every prime $q \equiv a \pmod N$ satisfies (i) and (ii), and we obtain the first statement of the theorem. The second statement follows from the bound $N \le \exp(p + o(p))$ and Linnik's theorem. □

Since $+1$ is always a quadratic residue modulo q, the method of Theorem 2.5 cannot be used to prove the analogous statement for the set $\mathcal{G}(\mathbb{N})$. However, numerical evidence suggests that such a statement is likely to be true.

Question 2.6. *Does an analogue of Theorem 2.5 hold if the value set $\mathcal{F}(\mathbb{N})$ is replaced by $\mathcal{G}(\mathbb{N})$?*

It follows from the classical results of H. Hasse that the set of primes which divide some element of the sequence $\{2^k + 1 \ : \ k = 1, 2, 3, \dots\}$ has relative asymptotic density $2/3$ in the set of all prime numbers (see [2] for an exhaustive survey of results of this kind). This immediately implies that

$$\#\bigl\{\text{primes } q \le x \ : \ 2/q \notin \mathcal{F}(\mathbb{N})\bigr\} \ge (1/3 + o(1))\,\pi(x).$$

A slight modification of this argument also works for $\mathcal{G}(\mathbb{N})$ and in fact using some results of [11] one can show that

$$\#\bigl\{\text{primes } q \le x \ : \ 2/q \notin \mathcal{G}(\mathbb{N})\bigr\} = (1 + o(1))\,\pi(x).$$

Question 2.7. *Is it true that the lower bound*

$$\#\bigl\{\textit{prime pairs } (p,q) \textit{ with } p < q \le x \ : \ p/q \notin \mathcal{F}(\mathbb{N})\bigr\} \ge x^{1+\delta}$$

holds for some absolute constant $\delta > 0$ and all sufficiently large values of x?

3. Distribution of values

Theorem 3.1. *If $F = \mathcal{F}$ or $F = \mathcal{G}$, then for any $\varepsilon > 0$ the following estimate holds:*

$$\#\{n \le x \ : \ F(n) \le x^{1/u}\} \ll \frac{x \log_2 x}{\log x \log_3 x} + x \exp(-(1-\varepsilon)\,u \log u),$$

where the implied constant in the $\ll$-symbol depends only on ε.

Proof. For a fixed integer $a \neq 0$, let

$$F_a(n) = \frac{P^+(n)}{P^-(n+a)} \qquad (n \geq 1-a).$$

Since $\mathcal{F}(n) = F_1(n)$ and $\mathcal{G}(n) = F_{-1}(n+1)$, it suffices to prove the stated inequality for the function $F = F_a$. Let us fix a sufficiently small $\delta > 0$. Put

$$y = x^{1/u}, \qquad v = \min\left\{\frac{u}{1+\delta}, \frac{2\log_2 x}{\log_3 x}\right\}, \qquad \text{and} \qquad z = x^{1/v},$$

and note that $z \geq y^{(1+\delta)}$. Clearly, if $F_a(n) \leq y$, then $P^-(n+a) \geq P^+(n)/y$; hence, either $P^+(n) \leq z$ or $P^-(n+a) > z/y$. For integers of the first type, we use the bound (see, for example, [14, chapter III.5]):

$$\Psi(x,z) \leq x \exp\left(-(1+o(1))\, v \log v\right),$$

where

$$\Psi(x,z) = \#\{n \leq x \ : \ P^+(n) \leq z\},$$

and for integers of the second type, we use the bound (see [14, Chapter III.6]):

$$\Phi(x+a, z/y) \ll \Phi(x, z/y) \ll \frac{x}{\log(z/y)} \leq \frac{xv}{\delta \log x},$$

where

$$\Phi(x, z/y) = \#\{n \leq x \ : \ P^-(n) > z/y\}.$$

Taking a sufficiently small δ, after simple calculations, we obtain the stated result. □

Theorem 3.2. *For a positive real number x, the lower bound*

$$\#\big(\{\mathcal{F}(m) \ : \ m \leq x\} \cap \{\mathcal{G}(n) \ : \ n \leq x\}\big) \gg \frac{x}{\log x}$$

holds.

Proof. This is clear since all fractions of the form $p/2 = \mathcal{F}(p) = \mathcal{G}(p-1)$ with $2 < p \leq x$ are distinct. □

4. Extreme values

Theorem 4.1. *As $x \to \infty$, each of the inequalities*

$$\mathcal{F}(n) \geq n^{7/10}, \quad \mathcal{F}(n) \leq n^{-7/10}, \quad \mathcal{G}(n) \geq n^{7/10}, \quad \text{and} \quad \mathcal{G}(n) \leq n^{-7/10}$$

holds for $x^{1+o(1)}$ positive integers $n \leq x$.

Proof. By a well-known result of R. C. Baker and G. Harman [1], for any fixed integer $a \neq 0$, there exists a constant $C > 0$ such that the cardinality of the set

$$\mathcal{P}_a(x) = \left\{\text{primes } p \le x \ : \ P^+(p-a) \le p^{0.2961}\right\}$$

is bounded below by

$$\#\mathcal{P}_a(x) > \frac{x}{(\log x)^C} = x^{1+o(1)}$$

for all sufficiently large values of x. In particular, we have

$$\mathcal{F}(p-1) = \frac{P^+(p-1)}{p} \le p^{-0.7039} \qquad \text{and} \qquad \mathcal{G}(p-1) = \frac{p}{P^-(p-1)} \ge p^{0.7039}$$

for all $p \in \mathcal{P}_1(x)$, and

$$\mathcal{F}(p) = \frac{p}{P^+(p+1)} \ge p^{0.7039} \qquad \text{and} \qquad \mathcal{G}(p) = \frac{P^+(p+1)}{p} \le p^{-0.7039}$$

for all $p \in \mathcal{P}_{-1}(x)$. The result follows. □

Remark 4.2. Assuming the *Elliott-Halberstam conjecture*, it is clear that the constant $7/10$ can be replaced by $1-\varepsilon$ for any fixed $\varepsilon > 0$.

Remark 4.3. We note that $\mathcal{F}(n) \ge 2/(n+1)$ holds for all $n \ge 2$, and $\mathcal{F}(n) = 2/(n+1)$ if and only if $n+1$ is a *Fermat prime*. Similarly, $\mathcal{G}(n) \ge 2/n$ holds for all $n \ge 2$, and $\mathcal{G}(n) = 2/n$ if and only if n is a *Mersenne prime*.

As a complementary result to Theorem 4.1, we now state the following corollary to Theorem 2.1, which concerns integers n for which $\mathcal{F}(n)$ or $\mathcal{G}(n)$ is close to 1.

Corollary 4.4. *Both of the inequalities*

$$|\mathcal{F}(n) - 1| \le (1+o(1))\frac{\log_2 n}{\log n} \qquad \textit{and} \qquad |\mathcal{G}(n) - 1| \le (1+o(1))\frac{\log_2 n}{\log n}$$

hold for infinitely many $n \in \mathbb{N}$.

Proof. By the Prime Number Theorem, there are infinitely many consecutive primes $q < p$ such that

$$|p - q| \le (1+o(1))\log q.$$

By Theorem 2.1, one can find $m, n \in \mathbb{N}$ with $\max\{m,n\} \le \exp(p + o(p))$ such that

$$\mathcal{F}(m) = \mathcal{G}(n) = \frac{p}{q} = 1 + O\left(\frac{\log q}{q}\right) = 1 + O\left(\frac{\log p}{p}\right).$$

Since $p \ge (1+o(1))\max\{\log m, \log n\}$, the result follows. □

Remark 4.5. By the recent breakthrough result of D. A. Goldston, J. Pintz, and C. Y. Yıldırım [7], there are infinitely many consecutive primes $q < p$ for which

$$p = q + O\left(\frac{\log q \log_4 q}{\log_2 q}\right),$$

and this result leads to an obvious improvement in the bound of Corollary 4.4.

Remark 4.6. We observe that

$$|\mathcal{F}(n) - 1| \geq (n+1)^{-1/2} \qquad (n \geq 3). \tag{2}$$

Indeed, if $n+1$ is prime, then $P^+(n) \leq n/2$ and $P^-(n+1) = n+1$. Hence, $\mathcal{F}(n) < 1/2$, and therefore $|\mathcal{F}(n) - 1| > 1/2 \geq (n+1)^{-1/2}$ (since $n+1 \geq 4$). On the other hand, if $n+1$ is composite, then $P^-(n+1) \leq (n+1)^{-1/2}$, and the bound (2) follows from the obvious inequality $|\mathcal{F}(n) - 1| \geq 1/P^-(n+1)$.

We believe that for every $\varepsilon > 0$ there exists n such that

$$|\mathcal{F}(n) - 1| \leq n^{-1/2+\varepsilon}$$

but we do not know how to attack this problem. Perhaps it follows from standard conjectures about the distribution of prime numbers, such as the Elliott-Halberstam conjecture, but our efforts to find such an argument have not been successful.

References

[1] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), no. 4, 331–361.

[2] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551.

[3] A. Balog, *On triplets with descending largest prime factors*, Studia Sci. Math. Hungar. **38** (2001), 45–50.

[4] A. Balog and I. Z. Ruzsa, *On an additive property of stable sets*, Sieve Methods, Exponential Sums, and Their Applications in Number Theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser., vol. 237, Cambridge Univ. Press, Cambridge, 1997, pp. 55–63.

[5] C. Dartyge, G. Martin, and G. Tenenbaum, *Polynomial values free of large prime factors*, Period. Math. Hungar. **43** (2001), no. 1-2, 111–119.

[6] P. Erdős and C. Pomerance, *On the largest prime factors of n and $n+1$*, Aequationes Math. **17** (1978), no. 2-3, 311–321.

[7] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, *Small gaps between primes*, II (2005), preprint.

[8] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, vol. 4, Academic Press, London-New York, 1974.

[9] J. Haristoy, *Équations diophantiennes exponentielles*, Prépublication de l'Institut de Recherche Mathématique Avancée, vol. 2003/29, Université Louis Pasteur, Département de Mathématique, Institut de Recherche Mathématique Avancée, Strasbourg, 2003. Thèse, University of Strasbourg I (Louis Pasteur), Strasbourg, 2003.

[10] A. Hildebrand, *On integer sets containing strings of consecutive integers*, Mathematika **36** (1989), no. 1, 60–70.

[11] F. Pappalardi, *Square free values of the order function*, New York J. Math. **9** (2003), 331–344.

[12] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[13] C. Siegel, *Approximation algebraischer Zahlen*, Math. Z. **10** (1921), no. 3-4, 173–213.

[14] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[15] N. M. Timofeev, *Polynomials with small prime divisors*, Taškent. Gos. Univ. Naučn. Trudy (1977), no. 548 Voprosy Mat., 87–91, 145 (Russian).