Bull. Aust. Math. Soc. **79** (2009), 455–463
doi:10.1017/S0004972709000033

ON THE LARGEST PRIME FACTOR OF THE MERSENNE NUMBERS

KEVIN FORD, FLORIAN LUCA and IGOR E. SHPARLINSKI✉

(Received 7 August 2008)

Abstract

Let $P(k)$ be the largest prime factor of the positive integer k. In this paper, we prove that the series

$$\sum_{n\ge 1} \frac{(\log n)^\alpha}{P(2^n-1)}$$

is convergent for each constant $\alpha < 1/2$, which gives a more precise form of a result of C. L. Stewart ['On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers', *Proc. London Math. Soc.* **35**(3) (1977), 425–447].

2000 *Mathematics subject classification*: primary 11B83, 11N25.
Keywords and phrases: primes, Mersenne numbers, applications of sieve methods.

1. Main result

Let $P(k)$ be the largest prime factor of the positive integer k. The quantity $P(2^n-1)$ has been investigated by many authors (see [1, 3, 4, 10–12, 14–16]). For example, the best-known lower bound

$$P(2^n-1) \ge 2n+1 \quad \text{for } n \ge 13$$

is due to Schinzel [14]. No better bound is known even for all sufficiently large values of n.

Stewart [15, 16] gave better bounds provided that n satisfies certain arithmetic or combinatorial properties. For example, he showed in [16], and this was also proved independently by Erdős and Shorey [4], that

$$P(2^p-1) > cp \log p$$

holds for all sufficiently large prime numbers p, where $c > 0$ is an absolute constant and log is the natural logarithm. This was an improvement upon a previous result of

his from [15] with $(\log p)^{1/4}$ instead of $\log p$. Several more results along these lines are presented in Section 3.

Here, we continue to study $P(2^n - 1)$ from a point of view familiar to number theory which has not yet been applied to $P(2^n - 1)$. More precisely, we study the convergence of the series

$$\sigma_\alpha = \sum_{n \geq 1} \frac{(\log n)^\alpha}{P(2^n - 1)} \tag{1}$$

for some real parameter α.

THEOREM 1. *The series σ_α is convergent for all $\alpha < 1/2$.*

The rest of the paper is organized as follows. We introduce some notation in Section 2. In Section 3 we comment on why Theorem 1 is interesting and does not immediately follow from already known results. In Section 4 we present a result due to Stewart [16] which plays a crucial role in our argument. Finally, in Section 5, we give a proof of Theorem 1.

2. Notation

In what follows, for a positive integer n, we use $\omega(n)$ for the number of distinct prime factors of n, $\tau(n)$ for the number of divisors of n and $\varphi(n)$ for the Euler function of n. We use the Vinogradov symbols $\gg$, $\ll$ and $\asymp$ and the Landau symbols O and o with their usual meaning. The constants implied by them might depend on α. We use the letters p and q to denote prime numbers. Finally, for a subset $\mathcal{A}$ of positive integers and a positive real number x, we write $\mathcal{A}(x)$ for the set $\mathcal{A} \cap [1, x]$.

3. Motivation

Stewart [16] proved the following two statements:

A. If $f(n)$ is any positive real-valued function which is increasing and $f(n) \to \infty$ as $n \to \infty$, then the inequality

$$P(2^n - 1) > \frac{n(\log n)^2}{f(n) \log \log n}$$

holds for all positive integers n except for those in a set of asymptotic density zero.

B. Let $\kappa < 1/\log 2$ be fixed. Then the inequality

$$P(2^n - 1) \geq C(\kappa) \frac{\varphi(n) \log n}{2^{\omega(n)}}$$

holds for all positive integers n with $\omega(n) < \kappa \log \log n$, where $C(\kappa) > 0$ depends on κ.

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

Since for every fixed $\varepsilon > 0$ we have

$$\sum_{n\ge 2} \frac{\log\log n}{n(\log n)^{1+\varepsilon}} < \infty,$$

assertion **A** above, taken with $f(n) = (\log n)^{\varepsilon}$ for some fixed small positive $\varepsilon < 1 - \alpha$, motivates our Theorem 1. However, since Stewart [16] gives no analysis of the exceptional set in assertion **A** (that is, of the size of the set of numbers $n \le x$ such that the corresponding estimate fails for a particular choice of $f(n)$), this alone does not lead to a proof of Theorem 1.

In this respect, given that the distribution of positive integers n having a fixed number of prime factors $K < \kappa \log\log n$ is very well understood starting with the work of Landau and continuing with the work of Hardy and Ramanujan [6], it may seem that assertion **B** is more suitable for our purpose. However, this is not quite so either since most n have $\omega(n) > (1-\varepsilon)\log\log n$ and for such numbers the lower bound on $P(2^n - 1)$ given by **B** is only of the shape $\varphi(n)(\log n)^{1-(1-\varepsilon)\log 2}$, and this is not enough to guarantee the convergence of series (1) even with $\alpha = 0$.

Conditionally, Murty and Wang [11] have shown that the ABC conjecture implies that $P(2^n - 1) > n^{2-\varepsilon}$ for all $\varepsilon > 0$ once n is sufficiently large with respect to ε. This certainly implies the conditional convergence of series (1) for all fixed $\alpha > 0$. Murata and Pomerance [10] have proved, under the generalized Riemann hypothesis for various Kummerian fields, that the inequality $P(2^n - 1) > n^{4/3}/\log\log n$ holds for almost all n, but they did not give explicit upper bounds on the size of the exceptional set either.

4. Main tools

As we have mentioned in Section 3, neither assertion **A** nor **B** of Section 3 is directly suitable for our purpose. However, another criterion, implicit in the work of Stewart [16] and which we present as Lemma 2 below (see also [10, Lemma 3]), plays an important role in our proof.

LEMMA 2. *Let $n \ge 2$, and let $d_1 < \cdots < d_\ell$ be all $\ell = 2^{\omega(n)}$ square-free divisors of n. Then for all $n > 6$,*

$$\#\{p \mid 2^n - 1 : p \equiv 1 \pmod n\} \gg \frac{\log(2 + \Delta(n)/\tau(n))}{\log\log P(2^n - 1)},$$

where

$$\Delta(n) = \max_{i=1,\dots,\ell-1} d_{i+1}/d_i.$$

Stewart's [16] proof of Lemma 2 uses the original lower bounds for linear forms in logarithms of algebraic numbers due to Baker. It is interesting to note that following [16] (see also [10, Lemma 3]), but using instead the sharper lower bounds

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

for linear forms in logarithms due to Matveev [9], does not seem to lead to any improvement of Lemma 2.

Let $1 = d_1 < d_2 < \cdots < d_{\tau(n)} = n$ be all the divisors of n and let

$$\Delta_0(n) = \max_{i \le \tau(n)-1} d_{i+1}/d_i.$$

Note that $\Delta_0(n) \le \Delta(n)$.

We need the following result of Saias [13] on the distribution of positive integers n with 'dense divisors'. Let

$$\mathcal{G}(x, z) = \{n \le x : \Delta_0(n) \le z\}.$$

LEMMA 3. *The bound*

$$\#\mathcal{G}(x, z) \asymp x \frac{\log z}{\log x}$$

holds uniformly for $x \ge z \ge 2$.

Next we address the structure of integers with $\Delta_0(n) \le z$. In what follows, as usual, an empty product is, by convention, equal to 1.

LEMMA 4. *Let* $n = p_1^{e_1} \cdots p_k^{e_k}$ *be the prime number factorization of a positive integer* n, *such that* $p_1 < \cdots < p_k$. *Then* $\Delta_0(n) \le z$ *if and only if, for each* $i \le k$, *the inequality*

$$p_i \le z \prod_{j<i} p_j^{e_j}$$

holds.

PROOF. The necessity is clear since otherwise the ratio of the two consecutive divisors

$$\prod_{j<i} p_j^{e_j} \quad \text{and} \quad p_i$$

is larger than z.

The sufficiency can be proved by induction on k. Indeed, for $k = 1$ it is trivial. By the induction assumption, we also have $\Delta_0(m) \le z$, where $m = n/p_1^{e_1}$. Remarking that $p_1 \le z$, we also conclude that $\Delta_0(n) \le z$. □

5. Proof of Theorem 1

We put $\mathcal{E} = \{n : \tau(n) \ge (\log n)^3\}$. To bound $\#\mathcal{E}(x)$, let x be large and $x/(\log x)^2 < n \le x$. Since $n \in \mathcal{E}(x)$, we have that $\tau(n) > (\log(x/(\log x)^2))^3 > 0.5(\log x)^3$ for all x sufficiently large. Since

$$\sum_{n \le x} \tau(n) = O(x \log x)$$

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

(see [7, Theorem 320]), we get that

$$\#\mathcal{E}(x) \ll \frac{x}{(\log x)^2}.$$

By the primitive divisor theorem (see [1], for example), there exists a prime factor $p \equiv 1 \pmod{n}$ of $2^n - 1$ for all $n > 6$. Then, by partial summation,

$$\begin{aligned}\sum_{n\in\mathcal{E}(x)} \frac{(\log n)^\alpha}{P(2^n-1)} &\le \sum_{n\in\mathcal{E}(x)} \frac{(\log n)^\alpha}{n} \le 1 + \int_2^x \frac{(\log t)^\alpha}{t} d\#\mathcal{E}(t)\\ &\le 1 + \frac{\#\mathcal{E}(x)}{x} + \int_2^x \frac{\#\mathcal{E}(t)(\log t)^\alpha}{t^2} dt\\ &\ll 1 + \int_2^x \frac{dt}{t(\log t)^{2-\alpha}} \ll 1.\end{aligned}$$

Hence,

$$\sum_{n\in\mathcal{E}} \frac{(\log n)^\alpha}{P(2^n-1)} < \infty. \tag{2}$$

We now let $\mathcal{F} = \{n : P(2^n - 1) > n(\log n)^{1+\alpha}(\log\log n)^2\}$. Clearly,

$$\sum_{n\in\mathcal{F}} \frac{(\log n)^\alpha}{P(2^n-1)} \le \sum_{n\ge 1} \frac{1}{n\log n(\log\log n)^2} < \infty. \tag{3}$$

From now on, we assume that $n \notin \mathcal{E} \cup \mathcal{F}$. For a given n, we let

$$\mathcal{D}(n) = \{d : dn + 1 \text{ is a prime factor of } 2^n - 1\},$$

and

$$D^+(n) = \max\{d \in \mathcal{D}(n)\}.$$

Since $P(2^n - 1) = D^+(n)n + 1$,

$$D^+(n) \le (\log n)^{1+\alpha}(\log\log n)^2. \tag{4}$$

Assume that L is large. Clearly, for $n \in [e^{L-1}, e^L]$, $D^+(n) \le L^{1+\alpha}(\log L)^2$. We let $\mathcal{H}_{d,L}$ be the set of $n \in [e^{L-1}, e^L]$ such that $D^+(n) = d$. We then note that by partial summation

$$\begin{aligned}S_L = \sum_{\substack{e^{L-1}\le n\le e^L\\ n\notin\mathcal{E}\cup\mathcal{F}}} \frac{(\log n)^\alpha}{P(2^n-1)} &\le L^\alpha \sum_{d\le L^{1+\alpha}(\log L)^2} \sum_{n\in\mathcal{H}_{d,L}} \frac{1}{nd+1}\\ &< \frac{L^\alpha}{e^{L-1}} \sum_{d\le L^{1+\alpha}(\log L)^2} \frac{\#\mathcal{H}_{d,L}}{d} \ll \frac{L^\alpha}{e^L} \sum_{d\le L^{1+\alpha}(\log L)^2} \frac{\#\mathcal{H}_{d,L}}{d}.\end{aligned} \tag{5}$$

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

We now estimate $\#\mathcal{H}_{d,L}$. We let $\varepsilon > 0$ to be a small positive number depending on α which is to be specified later. We split $\mathcal{H}_{d,L}$ in two subsets as follows.

Let $\mathcal{I}_{d,L}$ be the set of $n \in \mathcal{H}_{d,L}$ such that

$$\#\mathcal{D}(n) > ML^{\alpha+\varepsilon}(\log L)^2,$$

where M is some positive integer depending on ε to be determined later. Since $D^+(n) \le L^{1+\alpha}(\log L)^2$, there exists an interval of length $L^{1-\varepsilon}$ which contains at least M elements of $\mathcal{D}(n)$. Let them be $d_0 < d_1 < \cdots < d_{M-1}$. Write $k_i = d_i - d_0$ for $i = 1, \dots, M-1$. For fixed $d_0, k_1, \dots, k_{M-1}$, by the Brun sieve (see, for example, [5, Theorem 2.3]),

$$\begin{aligned}
&\#\{n \in [e^{L-1}, e^L] : d_i n + 1 \text{ is a prime for all } i = 1, \dots, M\} \\
&\ll \frac{e^L}{L^M} \prod_{p \mid d_1 \cdots d_M} \left(1 - \frac{1}{p}\right)^{-M} \ll \frac{e^L}{L^M} \left(\frac{\prod_{i=1}^M d_i}{\varphi(\prod_{i=1}^M d_i)}\right)^M \\
&\ll \frac{e^L (\log\log(L^{3M}))^M}{L^M} \ll \frac{e^L (\log\log L)^M}{L^M},
\end{aligned} \tag{6}$$

where we have used the fact that $\varphi(m)/m \gg 1/\log\log y$ in the interval $[1, y]$ with $y = (L^{1+\alpha}(\log L)^2)^M < L^{3M}$ (see [7, Theorem 328]). Summing the inequality (6) for all $d_0 \le L^{1+\alpha}(\log L)^2$ and all $k_1, \dots, k_{M-1} \le L^{1-\varepsilon}$, we get

$$\#\mathcal{I}_{d,L} \ll \frac{e^L (\log L)^{M+2} L^{1+\alpha} L^{(M-1)(1-\varepsilon)}}{L^M} = \frac{e^L (\log L)^{M+2}}{L^{(M-1)\varepsilon-\alpha}}. \tag{7}$$

We now choose M to be the least integer such that $(M-1)\varepsilon > 2 + \alpha$, and with this choice of M we get that

$$\#\mathcal{I}_{d,L} \ll \frac{e^L}{L^2}. \tag{8}$$

We now deal with the set $\mathcal{J}_{d,L}$ consisting of the numbers $n \in \mathcal{H}_{d,L}$ with $\#\mathcal{D}(n) \le ML^{\alpha+\varepsilon}(\log L)^2$. To these, we apply Lemma 2. Since $\tau(n) < (\log n)^3$ and $P(2^n - 1) < n^2$ for $n \in \mathcal{H}_{d,L}$, Lemma 2 yields

$$\log \Delta(n) / \log\log n \ll \#\mathcal{D}(n) \ll L^{\alpha+\varepsilon}(\log L)^2.$$

Thus,

$$\log \Delta(n) \ll L^{\alpha+\varepsilon}(\log L)^3.$$

Therefore

$$\Delta_0(n) \le \Delta(n) \le z_L,$$

where

$$z_L = \exp(cL^{\alpha+\varepsilon}(\log L)^3)$$

and $c > 0$ is some absolute constant.

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

We now further split $\mathcal{J}_{d,L}$ into two subsets. Let $\mathcal{S}_{d,L}$ be the subset of $n \in \mathcal{J}_{d,L}$ such that $P(n) < e^{L/\log L}$. From known results concerning the distribution of smooth numbers (see the corollary to [2, Theorem 3.1], or [8, 17], for example),

$$\#\mathcal{S}_{d,L} \le \frac{e^L}{L^{(1+o(1))\log\log L}} \ll \frac{e^L}{L^2}. \tag{9}$$

Let $\mathcal{T}_{d,L} = \mathcal{J}_{d,L} \setminus \mathcal{S}_{d,L}$. For $n \in \mathcal{T}_{d,L}$, we have $n = qm$, where $q > e^{L/\log L}$ is a prime. Fix m. Then $q < e^L/m$ is a prime such that $qdm + 1$ is also a prime. By the Brun sieve again,

$$\begin{aligned}&\#\{q \le e^L/m : q,\ qdm+1 \text{ are primes}\}\\ &\quad\ll \frac{e^L}{m(\log(e^L/m))^2}\left(\frac{md}{\varphi(md)}\right) \ll \frac{e^L(\log L)^3}{L^2 m},\end{aligned} \tag{10}$$

where in the above inequality we used the minimal order of the Euler function in the interval $[1, e^L L^{1+\alpha}(\log L)^2]$ together with the fact that

$$\log(e^L/m) \ge \frac{L}{\log L}.$$

We now sum estimate (10) over all the allowable values for m.

An immediate consequence of Lemma 4 is that since $\Delta_0(n) \le z_L$, then $\Delta_0(m) \le z_L$ for $m = n/P(n)$. Thus, $m \in \mathcal{G}(e^L, z_L)$. Using Lemma 3 and partial summation, we immediately get

$$\begin{aligned}\sum_{m\in\mathcal{G}(e^L,z_L)} \frac{1}{m} &\le \int_2^{e^L} \frac{d(\#\mathcal{G}(t,z_L))}{t} \le \frac{\#\mathcal{G}(e^L,z_L)}{e^L} + \int_2^{e^L} \frac{\#\mathcal{G}(t,z_L)}{t^2}dt\\ &\ll \frac{\log z_L}{L} + \log z_L \int_2^{e^L} \frac{dt}{t\log t}\\ &\ll \log z_L \log L \ll L^{\alpha+\varepsilon}(\log L)^4.\end{aligned}$$

Thus,

$$\#\mathcal{T}_{d,L} \ll \frac{e^L(\log L)^3}{L^2} \sum_{m\in\mathcal{M}_{d,L}} \frac{1}{m} \ll \frac{e^L(\log L)^7 L^{\alpha+\varepsilon}}{L^2} < \frac{e^L}{L^{2-\alpha-2\varepsilon}}, \tag{11}$$

when L is sufficiently large. Combining estimates (8), (9) and (11), we get that

$$\#\mathcal{H}_{d,L} \le \#\mathcal{I}_{d,L} + \#\mathcal{S}_{d,L} + \#\mathcal{T}_{d,L} \ll \frac{e^L}{L^{2-\alpha-2\varepsilon}}. \tag{12}$$

Thus, returning to series (5), we get that

$$S_L \le \sum_{d\le L^{1+\alpha}(\log L)^2} \frac{1}{L^{2-2\alpha-2\varepsilon}} \ll \frac{\log L}{L^{2-2\alpha-2\varepsilon}}.$$

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

Since $\alpha < 1/2$, we can choose $\varepsilon > 0$ such that $2 - 2\alpha - 2\varepsilon > 1$ and then the above arguments show that

$$\sum_{n\ge 1} \frac{(\log n)^\alpha}{P(2^n-1)} \ll 1 + \sum_L \frac{\log L}{L^{2-2\alpha-\varepsilon}} < \infty,$$

which is the desired result.

References

[1] G. D. Birkhoff and H. S. Vandiver, 'On the integral divisors of $a^n - b^n$', *Ann. of Math.* (2) **5** (1904), 173–180.

[2] E. R. Canfield, P. Erdős and C. Pomerance, 'On a problem of Oppenheim concerning "factorisatio numerorum" ', *J. Number Theory* **17** (1983), 1–28.

[3] P. Erdős, P. Kiss and C. Pomerance, 'On prime divisors of Mersenne numbers', *Acta Arith.* **57** (1991), 267–281.

[4] P. Erdős and T. N. Shorey, 'On the greatest prime factor of $2^p - 1$ for a prime p and other expressions', *Acta Arith.* **30** (1976), 257–265.

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

[6] G. H. Hardy and S. Ramanujan, 'The normal number of prime factors of an integer', *Quart. J. Math. (Oxford)* **48** (1917), 76–92.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edn (Clarendon Press, Oxford, 1979).

[8] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. de Théorie des Nombres de Bordeaux* **5** (1993), 411–484.

[9] E. M. Matveev, 'An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers II', *Izv. Ross. Akad. Nauk. Ser. Math.* **64** (2000), 125–180; Engl. transl. *Izv. Math.* **64** (2000), 1217–1269.

[10] L. Murata and C. Pomerance, *On the Largest Prime Factor of a Mersenne Number*, Number Theory CRM Proceedings Lecture Notes, 36 (American Mathematical Society, Providence, RI, 2004), pp. 209–218.

[11] R. Murty and S. Wong, 'The ABC conjecture and prime divisors of the Lucas and Lehmer sequences', in: *Number Theory for the Millennium, III,* Urbana, IL, 2000 (A K Peters, Natick, MA, 2002), pp. 43–54.

[12] C. Pomerance, 'On primitive divisors of Mersenne numbers', *Acta Arith.* **46**(4) (1986), 355–367.

[13] E. Saias, 'Entiers à diviseurs denses 1', *J. Number Theory* **62** (1997), 163–191.

[14] A. Schinzel, 'On primitive prime factors of $a^n - b^n$', *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.

[15] C. L. Stewart, 'The greatest prime factor of $a^n - b^n$', *Acta Arith.* **26**(4) (1974/75), 427–433.

[16] ———, 'On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers', *Proc. London Math. Soc.* **35**(3) (1977), 425–447.

[17] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory* (Cambridge University Press, Cambridge, 1995).

KEVIN FORD, Department of Mathematics, The University of Illinois at Urbana-Champaign, Urbana, Champaign, IL 61801, USA
e-mail: ford@math.uiuc.edu

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press

FLORIAN LUCA, Instituto de Matemáticas,
Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au

https://doi.org/10.1017/S0004972709000033 Published online by Cambridge University Press