On the largest prime factor of the Mersenne numbers

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

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

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

Abstract

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

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

is convergent for each constant $\alpha < 1/2$, which gives a more precise form of a result of C. L. Stewart of 1977.
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, 10, 11, 12, 14, 15, 16]). For example, the best known lower bound

\[
P(2^n - 1) \geq 2^n + 1, \quad \text{for } n \geq 13
\]

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

C. L. 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 in [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

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

for some real parameter \( \alpha \).

Our result is:

**Theorem 1.** The series \( \sigma_\alpha \) 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 C. L. 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 $\alpha$. We use the letters $p$ and $q$ to denote prime numbers. Finally, for a subset $A$ of positive integers and a positive real number $x$ we write $A(x)$ for the set $A \cap [1, x]$.

3 Motivation

In [16], C. L. Stewart 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 $\kappa$.

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

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

the assertion A above, taken with $f(n) = (\log n)\varepsilon$ for fixed some small positive $\varepsilon < 1 - \alpha$, motivates our Theorem [1]. However, since C. L. Stewart [16] gives no analysis of the exceptional set in the assertion A (that is, of the size
of the set of numbers $n \leq x$ 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 the 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 the $ABC$-conjecture implies that $P(2^n - 1) > n^{2-\varepsilon}$ for all $\varepsilon > 0$ once $n$ is sufficiently large with respect to $\varepsilon$. 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 are directly suitable for our purpose. However, another criterion, implicit in the work of C. L. Stewart [16] and which we present as Lemma 2 below (see also Lemma 3 in [10]), plays an important role in our proof.

**Lemma 2.** Let $n \geq 2$, and let $d_1 < \cdots < d_\ell$ be all $\ell = 2^{\omega(n)}$ divisors of $n$ such that $n/d_i$ is square-free. Then for all $n > 6$,

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

where

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

The proof of C. L. Stewart [16] of Lemma 2 uses the original lower bounds for linear forms in logarithms of algebraic numbers due to Baker. It is
interesting to notice that following [16] (see also [10, Lemma 3]) but using instead the sharper lower bounds for linear forms in logarithms due to E. M. 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 $n$ arranged in increasing order and let

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

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

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

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

**Lemma 3.** The bound

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

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

Next we address the structure of integer with $\Delta_0(n) \leq z$. 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 $\Delta_0(n) \leq z$ if and only if for each $i \leq k$, the inequality

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

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 $\Delta(m) \leq z$, where $m = n/p_1^{e_1}$. Remarking that $p_1 \leq z$, we also conclude that $\Delta(n) \leq z$. \qed
5 Proof of Theorem \ref{thm1}

We put $E = \{ n : \tau(n) \geq (\log n)^3 \}$. To bound $\#E(x)$, let $x$ be large and $n \leq x$. We may assume that $n > x/(\log x)^2$ since there are only at most $x/(\log x)^2$ positive integers $n \leq x/(\log x)^2$. Since $n \in E(x)$, we have that $\tau(n) > (\log(x/\log x))^3 > 0.5(\log x)^3$ for all $x$ sufficiently large. Since

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

(see \cite[Theorem 320]{1}), we get that

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

By the Primitive Divisor Theorem (see \cite{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,

$$\sum_{n \in E(x)} \frac{(\log n)^\alpha}{P(2^n - 1)} \leq \sum_{n \in E(x)} \frac{(\log n)^\alpha}{n} \leq 1 + \int_2^x \frac{(\log t)^\alpha}{t} d\#E(t)$$

$$\leq 1 + \frac{\#E(x)}{x} + \int_2^x \frac{\#E(t)(\log t)^\alpha}{t^2} dt$$

$$\ll 1 + \int_2^x \frac{dt}{t(\log t)^{2-\alpha}} \ll 1.$$ 

Hence,

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

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

$$\sum_{n \in F} \frac{(\log n)^\alpha}{P(2^n - 1)} \leq \sum_{n \geq 1} \frac{1}{n \log n(\log \log n)^2} < \infty. \quad (3)$$

From now on, we assume that $n \not\in E \cup F$. For a given $n$, we let

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

and

$$D^+(n) = \max\{ d \in D(n) \}.$$
Since \( P(2^n - 1) \geq d(n)n + 1 \), we have
\[
D^+(n) \leq (\log n)^{1+\alpha} (\log \log n)^2.
\]  

(4)

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

\[
S_L = \sum_{x_{L-1} \leq n \leq x_L} \frac{(\log n)^\alpha}{P(2^n - 1)} \leq L^\alpha \sum_{d \leq L^{1+\alpha}(\log L)^2} \sum_{n \in \mathcal{H}_{d,L}} \frac{1}{nd + 1}
\]

(5)

\[
< \frac{L^\alpha}{x_{L-1}} \sum_{d \leq L^{1+\alpha}(\log L)^2} \frac{\# \mathcal{H}_{d,L}}{d} \ll \frac{L^\alpha}{x_{L}} \sum_{d \leq L^{1+\alpha}(\log L)^2} \frac{\# \mathcal{H}_{d,L}}{d}.
\]

We now estimate \( \# \mathcal{H}_{d,L} \). We let \( \varepsilon > 0 \) to be a small positive number depending on \( \alpha \) 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

\[
\# \mathcal{D}(n) > \frac{1}{M} (\log n)^{\alpha + \epsilon} (\log \log n)^2 > \frac{1}{M} L^{\alpha + \epsilon}(\log L)^2,
\]

where \( M = M(\varepsilon) \) is some positive integer depending on \( \varepsilon \) to be determined later. Since \( D^+(n) \leq L^{1+\alpha}(\log L)^2 \), 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 \( i = 1, \ldots, M-1 \). For fixed \( d_0, k_1, \ldots, k_{M-1} \), by the Brun sieve (see, for example, Theorem 2.3 in [5]),

\[
\# \{ n \in [x_{L-1}, x_L] : d_i n + 1 \text{ is a prime for all } i = 1, \ldots, M \}
\]

\[
\ll \frac{x_L}{(\log(x_L))^M} \prod_{p \mid d_1 \cdots d_M} \left( 1 - \frac{1}{p} \right)^{-M} \ll \frac{x_L}{L^M} \left( \frac{\prod_{i=1}^M d_i}{\varphi(\prod_{i=1}^M d_i)} \right)^M
\]

(6)

\[
\ll \frac{x_L (\log L)^M}{L^M},
\]

where we have used that \( \varphi(m)/m \gg 1/\log \log y \) in the interval \([1, y]\) with \( y = y_L = L^{1+\alpha}(\log L)^2 \) (see [7] Theorem 328). Summing up the inequality (6) for all \( d_0 \leq L^{1+\alpha}(\log L)^2 \) and all \( k_1, \ldots, k_{M-1} \leq L^{1-\varepsilon} \), we get that the number of \( n \in \mathcal{I}_{d,L} \) is at most

\[
\# \mathcal{I}_{d,L} \ll \frac{x_L (\log L)^{M+1}L^{1+\alpha}(\log L)^{M-1}(1-\varepsilon)}{L^M} = \frac{x_L (\log L)^{M+2}}{L^{(M-1)\varepsilon-\alpha}}.
\]

(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
\[
\#I_{d,L} \ll \frac{x_L}{L^2}.
\]

We now deal with the set \( J_{d,L} \) consisting of the numbers \( n \in \mathcal{H}_{d,L} \) with \#\( D(n) \leq M^{-1} (\log n)^{\alpha+\varepsilon} (\log \log n)^2 \). 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
\[
\log \Delta(n)/\log \log n \ll \#D(n) \ll (\log n)^{\alpha+\varepsilon} (\log \log n)^2.
\]

Thus,
\[
\log \Delta(n) \ll (\log n)^{\alpha+\varepsilon} (\log \log n)^3
\]
\[
\ll (\log x_L)^{\alpha+\varepsilon} (\log \log x_L)^3 \ll L^{\alpha+\varepsilon}(\log L)^3.
\]

Therefore
\[
\Delta_0(n) \leq \Delta(n) \leq z_L,
\]
where
\[
z_L = \exp(cL^{\alpha+\varepsilon}(\log L)^3)
\]
and \( c > 0 \) is some absolute constant.

We now further split \( J_{d,L} \) into two subsets. Let \( S_{d,L} \) be the subset of \( n \in J_{d,L} \) such that \( P(n) < x_L^{1/\log L} \). From known results concerning the distribution of smooth numbers (see the corollary to Theorem 3.1 of [2], or [8], [17], for example),
\[
\#S_{d,L} \leq \frac{x_L}{L^{1+o(1)} \log \log L} \ll \frac{x_L}{L^2},
\]

Let \( T_{d,L} = J_{d,L} \setminus S_{d,L} \). For \( n \in T_{d,L} \), we have \( n = qm \), where \( q > x_L^{1/\log L} \) is a prime. Fix \( m \). Then \( q < x_L/m \) is a prime such that \( qdm + 1 \) is also a prime. By the Brun sieve again,
\[
\#\{ q \leq x_L/m : q, qdm + 1 \text{ are primes} \}
\ll \frac{x_L}{m(\log(x_L/m))^2} \left( \frac{md}{\varphi(md)} \right) \ll \frac{x_L(\log L)^3}{L^2m}.
\]

where in the above inequality we used the minimal order of the Euler function in the interval \( [1, x_LL^{1+\alpha}(\log L)^2] \) together with the fact that
\[
\log(x_L/m) \geq \frac{\log x_L}{\log L} = \frac{L}{\log L}.
\]
We now sum up estimate (10) over all the allowable values for \( m \).

An immediate consequence of Lemma 4 is that since \( \Delta_0(t) \leq z_L \), we also have \( \Delta_0(m) \leq z_L \) for \( m = n/P(n) \). Thus, \( m \in \mathcal{G}(x_L, z_L) \). Using Lemma 3 and partial summation, we immediately get

\[
\sum_{m \in \mathcal{G}(x_L, z_L)} \frac{1}{m} \leq \int_2^{x_L} \frac{d(#G(t, z_L))}{t} \leq \frac{#G(x_L, z_L)}{x_L} + \int_2^{x_L} \frac{#G(t, z_L)}{t^2} dt
\]

\[
\ll \frac{\log z_L}{L} + \log z_L \int_2^{x_L} \frac{dt}{t \log t}
\]

\[
\ll \log z_L \log \log x_L \ll L^{\alpha + \epsilon}(\log L)^4,
\]

as \( L \to \infty \). Thus,

\[
\#T_{d, L} \ll \frac{x_L(\log L)^3}{L^2} \sum_{m \in \mathcal{M}_{d, L}} \frac{1}{m} \ll \frac{x_L(\log L)^7 L^{\alpha + \epsilon}}{L^2} \ll \frac{x_L}{L^{2-\alpha - 2\epsilon}},
\]

(11)

when \( L \) is sufficiently large. Combining estimates (3), (9) and (11), we get that

\[
\#H_{d, L} \leq \#J_{d, L} + \#S_{d, L} + \#T_{d, L} \ll \frac{x_L}{L^{2-\alpha - 2\epsilon}}.
\]

(12)

Thus, returning to series (3), we get that

\[
S_L \leq \sum_{d \leq L^{1+\alpha(\log L)^2}} \frac{1}{L^{2-2\alpha - 2\epsilon}} \ll \frac{\log L}{L^{2-2\alpha - 2\epsilon}}.
\]

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

\[
\sum_{n \geq 1} \frac{(\log n)^\alpha}{P(2^n - 1)} \ll 1 + \sum_{L} \frac{\log L}{L^{2-2\alpha - \epsilon}} < \infty,
\]

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. Journ. Math. (Oxford)* 48 (1917), 76-92.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., 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; English translation *Izv. Math.* 64 (2000), 1217–1269.

[10] L. Murata and C. Pomerance, ‘On the largest prime factor of a Mersenne number’, *Number theory CRM Proc. Lecture Notes vol.36*, Amer. Math. Soc., Providence, RI, 2004, 209–218.

[11] 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.

[12] C. Pomerance, ‘On primitive divisors of Mersenne numbers’, *Acta Arith.* 46 (1986), no. 4, 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 (1974/75), no. 4, 427–433.

[16] C. L. Stewart, ‘On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers’, *Proc. London Math. Soc.* (3) 35 (1977), 425–447.

[17] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.