

On the Convergence of Series of Reciprocals of Primes Related to the Fermat Numbers

Michal Křížek¹

Mathematical Institute, Academy of Sciences, Žitná 25, CZ-115 67, Prague 1, Czech Republic
E-mail: krizek@math.cas.cz

Florian Luca

Instituto de Matemáticas UNAM, Campus Morelia, Apartado Postal 61 - 3 (Xangari)
CP 58 089, Morelia, Michoacán, Mexico
E-mail: fluca@matmor.unam.mx

and

Lawrence Somer

Department of Mathematics, Catholic University of America, Cardinal Station,
Washington, District of Columbia 20064
E-mail: somer@cua.edu

Communicated by R. C. Vaughan

Received August 14, 2001

We examine densities of several sets connected with the Fermat numbers $F_m = 2^{2^m} + 1$. In particular, we prove that the series of reciprocals of all prime divisors of Fermat numbers is convergent. We also show that the series of reciprocals of elite primes is convergent. © 2002 Elsevier Science (USA)

Key Words: Fermat numbers; elite primes; sum of reciprocals; density.

INTRODUCTION

For any integer $m \geq 0$, let $F_m = 2^{2^m} + 1$ be the m th Fermat number. It is well known that F_m is prime for $m \leq 4$, but there is no other m for which F_m is known to be prime. A lot of information about the Fermat numbers F_m can be found in the new book [4].

Throughout this paper, we use p and q to denote prime numbers. For a subset A of all positive integers and any real number x we let

¹To whom correspondence should be addressed.

$A(x) := A \cap [0, x]$. We denote by P the set of all primes for which there exists m such that p divides F_m . By a well-known result of Goldbach (see, e.g., [4]), any two distinct Fermat numbers are coprime. Thus, every member $p \in P$ divides a unique Fermat number.

The first question that we address in this paper concerns the convergence of the sum of the reciprocals of P . We recall that in [4, Chap. 7], we have shown that P is of relative asymptotic density zero as a subset of all the prime numbers. In 1955, Golomb (see [3]) asked if the series

$$\sum_{p \in P} \frac{1}{p} \quad (1)$$

is convergent. We will give a positive answer to this question. We begin with the following upper bound on the size of the set $P(x)$.

THEOREM 1.

$$|P(x)| = O\left(\frac{\sqrt{x}}{\log x}\right) \quad \text{as } x \rightarrow \infty. \quad (2)$$

From Theorem 1, we immediately derive the following corollary. Let D be the set of all positive integers d for which there exists m such that d divides F_m .

COROLLARY 1. *Let $\lambda > \frac{1}{2}$. Then both the series*

$$\sum_{p \in P} \frac{1}{p^\lambda} \quad (3)$$

and

$$\sum_{d \in D} \frac{1}{d^\lambda} \quad (4)$$

are convergent.

We note that the convergence of series (3) at $\lambda = 1$ answers in the affirmative Golomb's question from [3].

We recall that in [4, Chap. 7] we proved that D is of asymptotic density zero as a subset of all positive integers, but we did not provide an upper bound for $|D(x)|$. In particular, the result from [4, Chap. 7] does not imply the convergence of series (4). While as we will see, the convergence of (4) is a consequence of the convergence of (3), we next give an upper bound for $|D(x)|$ which independently implies the convergence of (4) for any $\lambda > \frac{1}{2}$.

THEOREM 2.

$$|D(x)| = O\left(\frac{\sqrt{x} \log \log x}{\log x}\right) \quad \text{as } x \rightarrow \infty. \quad (5)$$

We next give a result in a different spirit from that of Corollary 1, which in a sense is also stronger than the convergence of series (1). For any prime number $p \in P$, let $\alpha(p)$ be the exponent to which p appears in the prime factorization of the (unique) Fermat number F_m which is a multiple of p . We have the following result.

THEOREM 3. *The series*

$$\sum_{p \in P} \frac{\alpha(p)}{p} \quad (6)$$

is convergent.

The next question we address concerns the so-called elite primes. We shall first briefly recall this notion. In testing whether or not a given Fermat number F_m is prime, one usually employs Pepin's Test (cf. [6]). This test asserts the following:

PEPIN'S TEST. *Let $m > 0$ and let $a > 1$ be any quadratic non-residue modulo F_m . Then F_m is prime if and only if*

$$a^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

For the proof, see [4]. For example, the number $a = 3$ has the property that a is a quadratic non-residue modulo F_m for $m > 0$, and therefore $a = 3$ can be used to test the primality of F_m for all $m > 0$. In [1], Aigner introduced the notion of an *elite prime*, as being a prime number p such that p is a quadratic non-residue modulo F_m for all but finitely many values of m . That is, the elite primes are precisely the prime numbers p for which one can apply Pepin's Test with $a = p$ in order to decide the primality of F_m for all but finitely many values of m . Aigner found only 14 elite primes below 35×10^6 , the first few ones being 3, 5, 7, 41, 15 361, ... and the largest one below 35×10^6 being 14 172 161. Since there are so few elite primes in a relatively large range, Aigner asked whether the set of elite primes is infinite. While we were unable to answer this question, we can at least show that the elite primes are really "elite" in the sense that there are relatively few of them. Our exact result is the following. Let E be the set of all elite primes.

THEOREM 4.

$$|E(x)| = O\left(\frac{x}{(\log x)^2}\right) \quad \text{as } x \rightarrow \infty. \quad (7)$$

Since $\pi(x) \sim O(\frac{x}{\log x})$ for $x \rightarrow \infty$, it follows that E has relative density zero as a subset of all the prime numbers. Moreover, estimate (7) above tells us that if E happens to be infinite, then there must exist a constant c such that $p_n > cn(\log n)^2$ holds for all $n \geq 1$, where p_n stands for the n th element of the set E . In particular, from Theorem 4, we immediately get the following corollary.

COROLLARY 2. *The series*

$$\sum_{p \in E} \frac{1}{p} \quad (8)$$

is convergent.

THE PROOFS

Throughout this section, we use c_1, c_2, \dots to denote computable positive constants which are absolute, and C_1, C_2, \dots to denote positive constants (which are not necessarily computable).

Proof of Theorem 1. We first recall that by the well-known Lucas's Theorem (see [4, Chap. 6]), if $p \mid F_m$ and $m \geq 2$, then $p \equiv 1 \pmod{2^{m+2}}$. For any $n \geq 0$ we let

$$S_n = \{p \in P \mid p = 2^n k + 1 \text{ for some odd } k\}. \quad (9)$$

It is clear that the sets S_n partition P . We see that $S_0 = \emptyset$, $S_1 = \{3\}$, $S_2 = \{5\}$, $S_3 = \emptyset$, $S_4 = \{17\}$, $S_5 = S_6 = \emptyset$, $S_7 = \{641, 6\,700\,417\}$, etc. For $n \geq 3$, it follows that if $p \in S_n$ then $p \mid F_m$ for some $m \geq 2$, and hence, by Lucas's Theorem, it follows that $n \geq m + 2$. In particular,

$$\prod_{p \in S_n} p \leq \prod_{m=0}^{n-2} F_m < F_{n-1},$$

where the product on the left-hand side is equal to 1 when the set S_n is empty. Since $p \geq 2^n + 1$ for all $p \in S_n$, it follows that

$$(2^n + 1)^{|S_n|} < 2^{2^{n-1}} + 1,$$

and thus,

$$|S_n| < \frac{\log(2^{2^{n-1}} + 1)}{\log(2^n + 1)} < \frac{2^{n-1}}{n}. \quad (10)$$

In the last inequality of (10), we used the property that

$$\frac{\log(y+1)}{\log(x+1)} < \frac{\log y}{\log x} \quad \text{holds for all } y > x > 1, \quad (11)$$

with $y = 2^{2^{n-1}}$ and $x = 2^n$. The fact that (11) holds is a consequence of the property that the function $\log(x+1)/\log x$ is decreasing for $x > 1$.

Inequality (10) now tells us that

$$\sum_{j=1}^n |S_j| = 2 + \sum_{j=3}^n |S_j| < 2 + \sum_{j=3}^n \frac{2^{j-1}}{j} \leq c_1 \frac{2^n}{n} \quad \text{for } n \geq 3, \quad (12)$$

where $c_1 = \frac{4}{3}$. Let $x \geq 4$ and choose n such that

$$2^n \leq \sqrt{x} < 2^{n+1}. \quad (13)$$

In particular, both inequalities

$$2^n > \frac{\sqrt{x}}{2} \quad (14)$$

and

$$n \leq c_2 \log x < n + 1 \quad (15)$$

hold with $c_2 = \frac{1}{2 \log 2}$. With this choice of n , by inequalities (12)–(15), it follows that the number of primes $p \in P$ which are in some S_j for some $j \leq n$ is at most

$$\sum_{j=1}^n |S_j| < c_1 \frac{2^n}{n} < c_3 \frac{\sqrt{x}}{\log x} = O\left(\frac{\sqrt{x}}{\log x}\right) \quad \text{as } x \rightarrow \infty. \quad (16)$$

It remains to bound the cardinality of the set of those $p \in P(x)$ for which $p \in S_j$ for some $j > n$. But in this case, $p \equiv 1 \pmod{2^{n+1}}$. According to a result of Montgomery and Vaughan [5], we know that the number of primes not exceeding x which are congruent to $1 \pmod{2^{n+1}}$ is

$$\pi(x; 1, 2^{n+1}) < \frac{2x}{\phi(2^{n+1}) \log(x/2^{n+1})} = \frac{x}{2^{n-1} \log(x/2^{n+1})}, \quad (17)$$

where ϕ is the Euler totient function. We now use inequalities (13) and (14), to conclude that the right-hand side of (17) is bounded above by

$$\pi(x; 1, 2^{n+1}) < \frac{x}{2^{n-1} \log(x/2^{n+1})} < \frac{4\sqrt{x}}{\log(\sqrt{x}/2)} = O\left(\frac{\sqrt{x}}{\log x}\right) \quad \text{as } x \rightarrow \infty. \quad (18)$$

Theorem 1 follows now from (16) and (18). ■

Proof of Corollary 1. The convergence of series (3) is an immediate consequence of Theorem 1, while the convergence of series (4) follows from the convergence of series (3) and the following slightly more general result.

LEMMA. *Let A be any set of positive integers such that any two distinct members of A are coprime. Let $D(A)$ be the set of all positive integers which divide some member of A and let $P(A)$ be the subset consisting of the prime numbers belonging to $D(A)$. Let $\lambda > 0$. Then the series*

$$\sum_{p \in P(A)} \frac{1}{p^\lambda} \quad (19)$$

and

$$\sum_{d \in D(A)} \frac{1}{d^\lambda} \quad (20)$$

are either both convergent or both divergent.

Proof of the Lemma. It is clear that if (20) is convergent then so is (19), because $P(A) \subseteq D(A)$. Assume now that series (19) is convergent. Since any two distinct members of A are coprime, it follows that series (20) can be rewritten as

$$\sum_{d \in D(A)} \frac{1}{d^\lambda} = 1 + \sum_{\substack{a \in A \\ a > 1}} \sum_{\substack{d \mid a \\ d > 1}} \frac{1}{d^\lambda} = 1 + \sum_{\substack{a \in A \\ a > 1}} \left(\frac{\sigma_\lambda(a)}{a^\lambda} - 1 \right), \quad (21)$$

where for a positive integer n we wrote $\sigma_\lambda(n)$ for the sum of the λ -powers of all the divisors of n . Now clearly the function $\sigma_\lambda(n)/n^\lambda$ is multiplicative, and if p^t is a prime power then

$$\frac{\sigma_\lambda(p^t)}{p^t} = \sum_{k=0}^t \frac{1}{p^{k\lambda}} < \sum_{k \geq 0} \frac{1}{(p^\lambda)^k} = 1 + \frac{1}{p^\lambda - 1}. \quad (22)$$

Thus, using the multiplicativity of the function $\sigma_\lambda(n)/n^\lambda$ and inequality (22), we infer that if n is any positive integer, then

$$\frac{\sigma_\lambda(n)}{n^\lambda} < \prod_{p|n} \left(1 + \frac{1}{p^\lambda - 1}\right) < e^{\sum_{p|n} \frac{1}{p^\lambda - 1}}. \quad (23)$$

For the last inequality in (23), we used the fact that $1 + x < e^x$ for all $x > 0$. With (21), we now get that

$$\sum_{d \in D(A)} \frac{1}{d^\lambda} < 1 + \sum_{\substack{a \in A \\ a > 1}} (e^{\sum_{p|a} \frac{1}{p^\lambda - 1}} - 1). \quad (24)$$

We now notice that the series

$$\sum_{p \in P(A)} \frac{1}{p^\lambda - 1} \quad (25)$$

is convergent. Indeed, this follows from the fact that the ratio between the general term of series (25) and the general term of series (19), i.e., the ratio $(p^\lambda - 1)/p^\lambda$ tends to 1 and series (19) is convergent. Consequently, there exists a constant C_1 such that

$$\sum_{p \in P(A)} \frac{1}{p^\lambda - 1} < C_1. \quad (26)$$

Let $f : [0, C_1] \rightarrow [1, \infty)$ be the function given by

$$f(x) := \begin{cases} \frac{e^x - 1}{x} & \text{for } x \in (0, C_1], \\ 1 & \text{for } x = 0. \end{cases} \quad (27)$$

The function f is certainly continuous on the closed and bounded interval $[0, C_1]$, and therefore it is bounded. Thus, there exists a constant C_2 such that

$$e^x - 1 < C_2 x \quad \text{holds for all } x \in [0, C_1]. \quad (28)$$

Using formulae (26) and (28), we get that

$$e^{\sum_{p|a} \frac{1}{p^\lambda - 1}} - 1 < C_2 \sum_{p|a} \frac{1}{p^\lambda - 1} \quad (29)$$

holds for all $a \in A$. From inequalities (24), (29) and (26), together with the fact that any two members of A are coprime, we obtain

$$\begin{aligned} \sum_{d \in D(A)} \frac{1}{d^\lambda} &< 1 + \sum_{\substack{a \in A \\ a > 1}} \left(e^{\sum_{p|a} \frac{1}{p^\lambda - 1}} - 1 \right) < 1 + C_2 \sum_{\substack{a \in A \\ a > 1}} \sum_{p|a} \frac{1}{p^\lambda - 1} \\ &= 1 + C_2 \sum_{p \in P(A)} \frac{1}{p^\lambda - 1} < 1 + C_1 C_2, \end{aligned} \quad (30)$$

which shows that (20) is convergent. The Lemma is therefore proved. ■

We now notice that the above Lemma implies that series (4) is convergent. Indeed, this follows from the Lemma, the convergence of series (3), and from the fact that the set $A = \{F_m \mid m \geq 0\}$ satisfies the condition that any two of its distinct members are coprime. ■

Proof of Theorem 2. Since $x^{1/3} = o\left(\frac{\sqrt{x} \log \log x}{\log x}\right)$ for $x \rightarrow \infty$, it follows that it suffices to count the cardinality of the set $D_1(x)$ of all members of $D(x)$ which are larger than $x^{1/3}$. Let $d \in D_1(x)$ and write

$$d = Qd_1, \quad (31)$$

where Q is the largest prime divisor of d . Let $\Omega(d)$ stand for the total number of prime divisors of d (including multiplicity). Obviously,

$$Q^{\Omega(d_1)+1} = Q^{\Omega(d)} \geq d > x^{1/3},$$

and hence

$$Q > x^{\frac{1}{3(\Omega(d_1)+1)}}. \quad (32)$$

Moreover, we have

$$x \geq d = Qd_1,$$

and therefore both inequalities

$$Q \leq \frac{x}{d_1} \quad (33)$$

and

$$\frac{x}{d_1} \geq Q > x^{\frac{1}{3(\Omega(d_1)+1)}} \quad (34)$$

hold. Let c_1 be a positive constant such that

$$|P(x)| < c_1 \frac{\sqrt{x}}{\log x} \quad (35)$$

holds for all $x > e$. The existence of the constant c_1 above is guaranteed by Theorem 1. Notice that since $Q \geq 3$, it follows, by (33), that $x/d_1 \geq 3 > e$. As $Q \in P$, inequalities (33)–(35) tell us that

$$\begin{aligned} |D_1(x)| &< \sum_{d_1 \in D(x/3)} \left| P\left(\frac{x}{d_1}\right) \right| < c_1 \sum_{d_1 \in D(x/3)} \sqrt{\frac{x}{d_1}} \cdot \frac{1}{\log(x/d_1)} \\ &< c_2 \frac{\sqrt{x}}{\log x} \sum_{d_1 \in D(x)} \frac{\Omega(d_1) + 1}{\sqrt{d_1}}, \end{aligned} \quad (36)$$

where $c_2 = 3c_1$. Since $k < 2^{k/2}$ holds for all positive integers $k > 4$, it follows that $\Omega(d_1) + 1 < 1.1 \times \sqrt{2} \times 2^{\Omega(d_1)/2}$. Inequality (36) now implies that

$$|D_1(x)| < c_3 \frac{\sqrt{x}}{\log x} \left(1 + \sum_{\substack{d_1 \in D(x) \\ d_1 > 1}} \sqrt{\frac{2^{\Omega(d_1)}}{d_1}} \right), \quad (37)$$

with $c_3 = \sqrt{2}c_2$. We now use the fact that every number $d_1 \in D(x)$ divides a unique Fermat number F_m . Notice that since $d_1 \equiv 1 \pmod{2^{m+1}}$, it follows that for $d_1 \in D(x)$ and $d_1 > 1$, we must have $2^{m+1} < x$, hence $m < c_4 \log x$, where $c_4 = 1/\log 2$. It now follows easily that (37) implies

$$|D_1(x)| < c_3 \frac{\sqrt{x}}{\log x} \left(1 + \sum_{m < c_4 \log x} \sum_{\substack{d_1 | F_m \\ 1 < d_1 \leq x}} \sqrt{\frac{2^{\Omega(d_1)}}{d_1}} \right). \quad (38)$$

Obviously, the function

$$g(n) := \sum_{d|n} \sqrt{\frac{2^{\Omega(d)}}{d}}, \quad \text{for } n \geq 1 \quad (39)$$

is multiplicative. For every $x > 1$ write

$$g(n, x) := \sum_{\substack{d|n \\ d \leq x}} \sqrt{\frac{2^{\Omega(d)}}{d}}. \quad (40)$$

From the multiplicativity of $g = g(n)$, it follows that

$$g(n, x) \leq \prod_{\substack{p^\alpha \parallel n \\ p \leq x}} g(p^\alpha). \quad (41)$$

But clearly, for any odd number p ,

$$g(p^\alpha) = \sum_{j=0}^{\alpha} \left(\frac{2}{p}\right)^{j/2} < \sum_{j \geq 0} \left(\frac{2}{p}\right)^{j/2} = 1 + \frac{1}{\sqrt{p/2} - 1} < 1 + \frac{c_5}{\sqrt{p}}. \quad (42)$$

Thus, for odd n and uniformly in $x > 1$, we have

$$g(n, x) < \prod_{\substack{p \mid n \\ p \leq x}} \left(1 + \frac{c_5}{\sqrt{p}}\right) < \exp \left(c_6 \sum_{\substack{p \mid n \\ p \leq x}} \frac{1}{\sqrt{p}} \right). \quad (43)$$

For any $m \geq 0$ let

$$h(m, x) := \sum_{\substack{p \mid F_m \\ p < x}} \frac{1}{\sqrt{p}}. \quad (44)$$

Denote by $\omega(F_m)$ the number of different prime divisors of F_m . It is easy to see that $\omega(F_m) < 2^m/m$. Indeed, this follows by noticing that since $2^{m+1} + 1 \leq p$ holds for all prime divisors p of F_m , one has

$$(2^{m+1} + 1)^{\omega(F_m)} \leq \prod_{p \mid F_m} p \leq F_m = 2^{2^m} + 1.$$

Therefore,

$$\omega(F_m) < \frac{\log(2^{2^m} + 1)}{\log(2^{m+1} + 1)} < \frac{2^m}{m+1} < \frac{2^m}{m}. \quad (45)$$

By writing now all prime divisors p of F_m in the form $2^{m+1}k + 1$ for some positive integer k , we get

$$\begin{aligned} h(m, x) &\leq \sum_{p \mid F_m} \frac{1}{\sqrt{p}} < \sum_{k=1}^{\omega(F_m)} \frac{1}{\sqrt{2^{m+1}k + 1}} < \frac{1}{2^{m/2}} \sum_{1 \leq k \leq \frac{2^m}{m}} \frac{1}{\sqrt{k}} \\ &< \frac{1}{2^{m/2}} \left(1 + \int_1^{\frac{2^m}{m}} \frac{dx}{\sqrt{x}} \right) = \frac{1}{2^{m/2}} \left(1 + 2\sqrt{x} \Big|_{x=1}^{x=\frac{2^m}{m}} \right) < \frac{c_7}{\sqrt{m}}. \end{aligned} \quad (46)$$

In particular, it follows that $h(m, x)$ tends to zero with m and uniformly in $x > 1$. From inequality (43) and the arguments employed in the proof of Corollary 1, it follows that there exists a constant $c_8 > 1$ such that the inequality

$$g(F_m, x) < \exp(c_6 h(m, x)) < 1 + c_8 h(m, x) \quad (47)$$

holds for all $m \geq 0$ and all $x \geq 1$. With (38), we get

$$\begin{aligned} |D_1(x)| &< c_3 \frac{\sqrt{x}}{\log x} \left(1 + \sum_{m < c_4 \log x} (g(F_m, x) - 1) \right) \\ &< c_9 \frac{\sqrt{x}}{\log x} \left(1 + \sum_{m < c_4 \log x} h(m, x) \right) \\ &\leq c_9 \frac{\sqrt{x}}{\log x} \left(1 + \sum_{p \in P(x)} \frac{1}{\sqrt{p}} \right). \end{aligned} \quad (48)$$

In inequality (48), we took $c_9 = c_3 c_8$ and for the right-most inequality (48) we used the fact that any two Fermat numbers are coprime.

Now let $3 = p_1 < p_2 < \dots < p_t < \dots$ be all the prime numbers in P . Estimate (2) implies that there exists a constant c_{10} such that $p_t > c_{10}(t \log t)^2$ holds for all $t \geq 2$. In particular,

$$\frac{1}{\sqrt{p_t}} < \frac{c_{11}}{t \log t} \quad (49)$$

is valid for all $t \geq 2$, where $c_{11} = 1/\sqrt{c_{10}}$. With (49), we obviously have

$$\begin{aligned} \sum_{p \in P(x)} \frac{1}{\sqrt{p}} &< \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{5}} + \frac{1}{\sqrt{17}} + \sum_{4 \leq t \leq x} \frac{1}{\sqrt{p_t}} < c_{12} + c_{11} \sum_{4 \leq t \leq x} \frac{1}{t \log t} \\ &< c_{12} + c_{11} \int_3^x \frac{dt}{t \log t} \\ &= c_{12} + c_{11} \log \log t \Big|_{t=3}^{t=x} = c_{13} + c_{11} \log \log x, \end{aligned} \quad (50)$$

where $c_{12} = 1/\sqrt{3} + 1/\sqrt{5} + 1/\sqrt{17}$ and $c_{13} = c_{12} - \log \log 3$. Clearly, (48) and (50) imply

$$|D_1(x)| < c_{14} \frac{\sqrt{x} \log \log x}{\log x}, \quad (51)$$

which concludes the proof of Theorem 2. ■

Proof of Theorem 3. For the convergence of series (6), we use the following lower bound for a linear form in two p -adic logarithms due to Bugeaud and Laurent [2]. In what follows, for a given prime number p and a given non-zero integer n we use $\mu_p(n)$ to denote the exponent to which p appears in the prime factorization of n .

BUGEAUD–LAURENT THEOREM. *Let p be a prime number, a_1, a_2, b_1, b_2 be positive integers such that $a_1 a_2$ is coprime to p and $a_1^{b_1} - a_2^{b_2} \neq 0$. Let A and B be two positive integers such that $|A| \geq \max(a_1, a_2)$ and $B \geq \max(b_1, b_2, 2)$, and let g be the smallest positive integer such that $a_1^g \equiv a_2^g \equiv 1 \pmod{p}$. Then there exists c_1 such that*

$$\mu_p(a_1^{b_1} - a_2^{b_2}) < c_1 \frac{pg}{(p-1)(\log p)^4} (\log A)^2 (\log B)^2. \quad (52)$$

We use the Bugeaud–Laurent Theorem to bound $\alpha(p)$ for a given prime $p \in P$. Clearly, $\alpha(3) = 1$ and $\alpha(5) = 1$. Suppose now that $p \in S_n$ for some $n \geq 3$. Then $p^{\alpha(p)} \parallel F_m$ for some m such that $m \leq n-2$. In particular,

$$p^{\alpha(p)} \parallel \prod_{m \geq 0}^{n-2} F_m.$$

Consequently,

$$p^{\alpha(p)} \parallel (2^{2^{n-1}} - 1). \quad (53)$$

We now apply the above Bugeaud–Laurent Theorem with $a_1 = 2, a_2 = 1, b_1 = 2^{n-1}, b_2 = 1$. We can obviously take $A = 2, B = 2^{n-1}$ and $g = 2^{m+1}$, where m is such that $p \mid F_m$. Thus, $g \leq 2^{n-1}$. Now (52) implies that

$$\begin{aligned} \alpha(p) = \mu_p(2^{2^{n-1}} - 1) &\leq \frac{c_1 2^{n-1} p}{(p-1)(\log p)^4} (\log 2)^2 (\log(2^{n-1}))^2 \\ &< \frac{c_2 2^{n-1} n^2 p}{(p-1)(\log p)^4}, \end{aligned} \quad (54)$$

where $c_2 = c_1 (\log 2)^4$. Writing $p = 2^n k + 1$ for some $k \geq 1$, we get

$$\alpha(p) < c_2 \frac{2^{n-1} n^2 (2^n k + 1)}{2^n k (\log(2^n k + 1))^4} < c_2 \frac{2^n n^2}{(\log(2^n))^4} = \frac{c_2}{(\log 2)^4} \frac{2^n}{n^2} = c_1 \frac{2^n}{n^2}. \quad (55)$$

We are now ready to prove that series (6) is convergent. Write

$$\sum_{p \in P} \frac{\alpha(p)}{p} = \frac{1}{3} + \frac{1}{5} + \sum_{n \geq 3} \sum_{p \in S_n} \frac{\alpha(p)}{p}, \quad (56)$$

where S_n is defined as in the proof of Theorem 1. Set also

$$b_n := \sum_{p \in S_n} \frac{\alpha(p)}{p}. \quad (57)$$

It suffices to find a good upper bound on b_n . We partition the set S_n into the following two subsets:

$$A_n := \{p \in S_n \mid \alpha(p) \leq 2^n/n^3\} \quad (58)$$

and

$$B_n := \{p \in S_n \mid \alpha(p) > 2^n/n^3\}. \quad (59)$$

Notice that, by inequality (10) and the fact that

$$\frac{2^{n-1}}{n} < 2^n - 2 \quad \text{for } n \geq 3,$$

we have that $|S_n| < 2^n - 2$ for $n \geq 3$. Thus,

$$\begin{aligned} \sum_{p \in A_n} \frac{\alpha(p)}{p} &\leq \frac{2^n}{n^3} \sum_{p \in S_n} \frac{1}{p} \leq \frac{2^n}{n^3} \sum_{k=0}^{2^n-2} \frac{1}{2^n(2k+1)+1} < \frac{2^n}{n^3} \left(\frac{1}{2^n} + \frac{1}{2^n} \sum_{k=2}^{2^n-1} \frac{1}{k} \right) \\ &< \frac{2^n}{n^3} \left(\frac{1}{2^n} + \frac{1}{2^n} \int_1^{2^n} \frac{dx}{x} \right) = \frac{2^n}{n^3} \left(\frac{1}{2^n} + \frac{\log(2^n)}{2^n} \right) = \frac{1}{n^3} + \frac{\log 2}{n^2}. \end{aligned} \quad (60)$$

We now notice that B_n does not contain too many elements. Indeed, since

$$\prod_{p \in B_n} p^{\alpha(p)} \left| \prod_{m=0}^{n-2} F_m, \right.$$

we get that

$$\prod_{p \in B_n} p^{\alpha(p)} < F_{n-1}.$$

Therefore,

$$\sum_{p \in B_n} \alpha(p) \log p < \log F_{n-1}.$$

Since $p \geq 2^n + 1$ and $\alpha(p) > 2^n/n^3$ for all $p \in B_n$, we find that

$$\frac{2^n \log(2^n + 1)}{n^3} |B_n| < \log(2^{2^{n-1}} + 1),$$

or equivalently

$$|B_n| < \frac{\log(2^{2^{n-1}} + 1)}{\log(2^n + 1)} \frac{n^3}{2^n} < \frac{2^{n-1} n^3}{n} \frac{n^2}{2^n} < \frac{n^2}{2} < n^2 - 1. \quad (61)$$

In the above inequality, we applied again inequality (11) with $y = 2^{2^{n-1}}$ and $x = 2^n$. Hence, by (55) and (61), we obtain

$$\begin{aligned} \sum_{p \in B_n} \frac{\alpha(p)}{p} &< \frac{c_1 2^n}{n^2} \sum_{p \in B_n} \frac{1}{p} \leq \frac{c_1 2^n}{n^2} \sum_{k=0}^{n^2-2} \frac{1}{2^n(2k+1)+1} \\ &< \frac{c_1 2^n}{n^2} \left(\frac{1}{2^n} + \frac{1}{2^n} \sum_{k=2}^{n^2-1} \frac{1}{k} \right) < \frac{c_1 2^n}{n^2} \left(\frac{1}{2^n} + \frac{1}{2^n} \int_1^{n^2} \frac{dx}{x} \right) \\ &= \frac{c_1 2^n}{n^2} \left(\frac{1}{2^n} + \frac{\log(n^2)}{2^n} \right) = \frac{c_1}{n^2} + \frac{2c_1 \log n}{n^2}. \end{aligned} \quad (62)$$

Combining (60) and (62), we get

$$b_n < \frac{1}{n^3} + \frac{c_1 + \log 2 + 2c_1 \log n}{n^2}, \quad (63)$$

and now it obvious that

$$\sum_{p \in P} \frac{\alpha(p)}{p} = \frac{1}{3} + \frac{1}{5} + \sum_{n \geq 3} b_n$$

is convergent. ■

Proof of Theorem 4. We start with a large positive real number x and we count how many primes $p \leq x$ can be elite. We may assume that $p \geq \sqrt{x}$ because there are only $o(\sqrt{x}) = O(\frac{x}{(\log x)^2})$ primes which are below \sqrt{x} . For such a prime $p \geq \sqrt{x}$ write

$$p - 1 = 2^{e_p} k_p, \quad (64)$$

where $e_p \geq 1$ and k_p is odd. Let $c_1 = \frac{1}{\log 2}$ and $c_2 > 0$ be an absolute constant to be fixed later. We now notice that but for $O(\frac{x}{(\log x)^2})$ primes $p \leq x$ the inequality

$$e_p < c_1 \log \log x - c_2 \quad (65)$$

holds. Indeed, let $t = \lfloor c_1 \log \log x - c_2 \rfloor$ and assume that p is such that $e_p \geq t$. In particular, p is a prime number which is congruent to 1 mod 2^t . By the result of Montgomery and Vaughan [5], the number of such primes not exceeding x is

$$\pi(x; 1, 2^t) < \frac{2x}{2^{t-1} \log(x/2^t)}. \quad (66)$$

Notice that

$$\sqrt{x} > 2^t \quad (67)$$

is valid for $x > c_3 = e^e$. Indeed, (67) certainly holds if

$$\frac{\log x}{2} > c_1 \log \log x - c_2,$$

which is clearly satisfied when $x > c_3$. In particular, $x/2^t > \sqrt{x}$ for $x > c_3$ and now inequality (66) tells us that

$$\pi(x; 1, 2^t) < \frac{16x}{2^{t+1} \log x} \leq \frac{2^{c_2+4} x}{(\log x)^2} = O\left(\frac{x}{(\log x)^2}\right) \quad \text{as } x \rightarrow \infty. \quad (68)$$

From now on, we look at an elite prime p with $p \leq x$ and $e_p < t$. We now notice that for such p ,

$$k_p = \frac{p-1}{2^{e_p}} > \frac{p-1}{2^t} > \frac{c_4 \sqrt{x}}{\log x} > x^{1/3} \quad \text{for } x > c_5. \quad (69)$$

In inequality (69), we can take $c_4 = 2^{c_2-1}$ and $c_5 > c_3$. We now denote by f_p the multiplicative order of 2 mod k_p . That is, f_p is the smallest positive integer for which $k_p \mid (2^{f_p} - 1)$. In particular, from inequality (69), it follows that

$$2^{f_p} > k_p > x^{1/3}.$$

Hence,

$$f_p > c_6 \log x, \quad (70)$$

where $c_6 = \frac{1}{3 \log 2}$.

So far, we did not say anything about the Fermat numbers F_m . We now bring them into the game by noticing that the sequence $\{F_m\}_{m \geq 0}$ is periodic modulo p for $m \geq e_p$ with period f_p . Indeed, notice that

$$F_m \equiv F_{m+f_p} \pmod{p} \quad \text{for } m \geq e_p \quad (71)$$

is equivalent to

$$2^{2^m(2^f-1)} \equiv 1 \pmod{p}. \quad (72)$$

Since $m \geq e_p$ and $k_p \mid (2^f - 1)$, it follows that $(p - 1) \mid 2^m(2^f - 1)$, and thus the fact that (72) holds follows from Fermat's Little Theorem.

Now, by (71), we find that p is an elite prime if and only if F_m is a quadratic non-residue modulo p for any $m \geq e_p$. Indeed, since F_m is congruent to 1 mod 4 for all $m \geq 1$, it follows, by the law of quadratic reciprocity, that

$$\left(\frac{F_m}{p}\right) = \left(\frac{p}{F_m}\right) \quad \text{holds for all } m \geq 1.$$

Here, for two integers a and b with $b > 1$ odd we use $\left(\frac{a}{b}\right)$ to denote the Jacobi symbol of a with respect to b .

Thus, p is a quadratic non-residue modulo F_m if and only if F_m is a quadratic non-residue modulo p . Now if there is an $m \geq e_p \geq 1$ such that F_m is a quadratic residue modulo p , then by (71) it follows that there are infinitely many of them. Therefore, p is a quadratic residue modulo infinitely many Fermat numbers, contradicting the fact that p is elite. Since $e_p < t$, it follows, in particular, that

$$F_t, F_{t+1}, \dots, F_{2t} \quad (73)$$

are all quadratic non-residues modulo p . Notice that the numbers appearing in list (73) are independent of the number p (they depend only on x). We now notice that

$$\prod_{i=0}^t F_{t+i} < x^{1/3} \quad (74)$$

for $x > c_7$. Indeed

$$\prod_{i=0}^t F_{t+i} < \prod_{i=0}^{2t} F_i < 2^{2^{t+1}},$$

and the inequality

$$2^{2^{t+1}} < x^{1/3}$$

is equivalent to

$$(t+1)\log 2 + \log \log 2 < \log \log x - \log 3,$$

which holds if

$$(c_1 \log \log x - c_2 + 1) \log 2 < \log \log x - \log 3 - \log \log 2,$$

which is equivalent to

$$c_2 \log 2 > \log 2 + \log 3 + \log \log 2. \quad (75)$$

Thus, if we choose c_2 such that (75) holds, it follows that (73) holds as well. In particular, all the numbers from list (73) are smaller than p ; hence, any two of them are incongruent modulo p . For $i = 0, 1, \dots, t$ put

$$F_{t+i} = S_i U_i^2, \quad (76)$$

where S_i is square free. It is well-known that no Fermat number is a perfect square. Therefore $S_i > 1$ for all $i = 0, 1, \dots, t$, and since any two Fermat numbers are coprime, it follows that any two of the numbers S_i are coprime as well. The condition that all numbers in list (73) are quadratic non-residues modulo p is equivalent to the fact that

$$\left(\frac{S_i}{p}\right) = -1 \quad \text{for } i = 0, 1, \dots, t. \quad (77)$$

Since every prime divisor of F_m is congruent to 1 mod 4 for any $m \geq 1$, it follows that S_i is congruent to 1 mod 4. Therefore, (77) is equivalent to

$$\left(\frac{p}{S_i}\right) = -1 \quad \text{for } i = 0, 1, \dots, t. \quad (78)$$

For a fixed i , relation (78), the fact that S_i is square free, and the fact that for any odd prime number q there are precisely $(q-1)/2$ quadratic residues modulo q , along with the Chinese Remainder Theorem, together imply that out of all $\phi(S_i)$ arithmetical progressions of the form $a \pmod{S_i}$ with a running through all positive integers smaller than S_i and coprime to S_i , p can belong to precisely $\phi(S_i)/2$ of those. That is, there is a subset A_i of cardinality $\phi(S_i)/2$ of the set of all the positive integers smaller than S_i and coprime to S_i , such that if p satisfies relation (78) for i , then $p \equiv a \pmod{S_i}$ for some $a \in A_i$. Now let $T = \prod_{i=0}^t S_i$. Using the Chinese Remainder Theorem again (because any two of the S_i are coprime), it follows that there are exactly

$$\prod_{i=0}^t \frac{\phi(S_i)}{2} = \frac{\phi(T)}{2^{t+1}} \quad (79)$$

residue classes modulo T which are coprime to T and which can contain the prime number p . However, by the result of Montgomery and Vaughan, for a fixed congruence class modulo T which is coprime to T , the number of primes up to x in this congruence class is at most

$$\frac{2x}{\phi(T)\log(x/T)}. \quad (80)$$

Since by (74)

$$T = \prod_{i=0}^t S_i \leq \prod_{i=0}^t F_{k+i} < x^{1/3},$$

we get that $x/T > x^{2/3}$. Hence, the number of primes up to x in a fixed residue class modulo T does not exceed

$$\frac{3x}{\phi(T)\log x}. \quad (81)$$

Since we have precisely $\phi(T)/2^{t+1}$ such congruence classes modulo T which can contain p , it follows that the totality of such p does not exceed

$$\frac{\phi(T)}{2^{t+1}} \frac{3x}{\phi(T)\log x} = \frac{3x}{2^{t+1}\log x} = O\left(\frac{x}{(\log x)^2}\right) \quad \text{as } x \rightarrow \infty. \quad (82)$$

Theorem 4 is therefore proved. ■

As we have said previously, Corollary 2 is an immediate consequence of Theorem 4.

ACKNOWLEDGMENT

This paper was supported by Grant 201/02/1057 of the Grant Agency of the Czech Republic.

REFERENCES

1. A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatschen Zahlen quadratische Nichtreste sind, *Monatsh. Math.* **101**, No. 2 (1986), 85–93.
2. Y. Bugeaud and M. Laurent, Minoration effective de la distance p -adique entre puissances de nombres algébriques, *J. Number Theory* **61** (1996), 311–342.
3. S. W. Golomb, Sets of primes with intermediate density, *Math. Scand.* **3** (1955), 264–274.
4. M. Křížek, F. Luca, and L. Somer, “17 Lectures on Fermat Numbers,” Springer-Verlag, New York, 2001.
5. H. L. Montgomery and R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), 119–134.
6. P. Pepin, Sur la formule $2^{2^n} + 1$, *C. R. Acad. Sci.* **85** (1877), 329–331.