Annales Univ. Sci. Budapest., Sect. Comp. 53 (2022) 145–158

PRIMALITY PROOFS WITH ELLIPTIC CURVES: PROBABILISTIC FACTORISATION

Gábor Román (Budapest, Hungary)

Communicated by Jean-Marie De Koninck

(Received August 6, 2022; accepted October 2, 2022)

Abstract. We give an asymptotic for the expected number of complete factorisations of natural numbers of the form $fq \leq n$, utilising probabilistic factorisation methods, where f is a $b(n)$-smooth number, and q is a prime larger than $b(n)$, with $b(n) : \mathbb{N} \to [e, \sqrt{n})$.

1. Introduction

Through the elliptic curve primality proving method, one tries to prove the primality of a probable prime n_0 using a recursive strategy, descending through probable primes $n_1, n_2, \ldots$ until some small number, whose primality can be proven easily, as it is explained in the paper of Atkin and Morain [2]. A crucial point of the recursive step, which deals with probable prime n_i, is the factorisation of certain values into the form fn_{i+1}, where f is a smooth number with known prime divisors, and n_{i+1} is the next probable prime.

In the elliptic curve primality proving method, one main control point is the smoothness bound during this factorisation step, a bound we are going to denote as $b(n)$ for a given natural number n. The authors of article [7] ask what would be the expected number of complete factorisations during this step using different kinds of probabilistic factoring methods, where we cannot guarantee that we find all the prime factors below $b(n)$.

Key words and phrases: Elliptic curve primality proving, smooth number, first category algorithm, probabilistic factoring.
2010 Mathematics Subject Classification: 11Y05.

To achieve good running time, it is crucial to use factorisation methods whose running time is governed by the size of the smallest prime factor of the to-be-factored number. These methods are called first category algorithms.

The most fundamental methods of this category includes the trial division (see for example section 8.1 of [8]), and the batch trial division (see articles [4, 5, 6] and [10]). Note that these algorithms are not probabilistic. Hafner and McCurly gave asymptotics for the function $F(n,t,A)$, which denotes the number of integers $m \leq n$, which can be completely factored by algorithm A in at most t arithmetic operations involving integers of $O(\ln n)$ bits (see article [11]). Here A can be a single factorization method or the combination of multiple ones. By arithmetic operations the authors mean a comparison, assignment; computation of the binary representation arising from an addition, subtraction, multiplication, division (giving both remainder and quotient); or an application of the Euclidean algorithm. They gave the following theorem in the case when only the trial division method is applied with the Adleman–Pomerance–Rumely primality test, see article [1].

Theorem 1.1. *If t satisfies*

$$\frac{t}{(\ln n)^{C \ln\ln\ln n}} \to \infty$$

for some positive constant C and $\ln n/\ln t \to \infty$ then

$$F(n,t,A) \sim e^{\gamma}\frac{n}{\ln n}\ln t \tag{1.1}$$

when A is the trial division method combined with the Adleman–Pomerance–Rumely primality test, where γ is the Euler–Mascheroni constant.

When A is a probabilistic algorithm, then $F(n,t,A)$ denotes the number of integers $m \leq n$ for which A will factor m in at most t operations with probability at least $1/2$. For a more rigorous definition, see the original paper. By applying the Solovay–Strassen probabilistic primality test (see articles [25] and [26]), Hafner and McCurly got the following result.

Theorem 1.2. *If t satisfies*

$$\frac{t}{(\ln n)^2 \ln\ln n} \to \infty$$

and $\ln n/\ln t \to \infty$ then

$$F(n,t,A) \sim e^{\gamma}\frac{n}{\ln n}\ln t \tag{1.2}$$

when A is the trial division method combined with the Solovay–Strassen probabilistic primality test.

Using the Miller–Rabin probabilistic primality test (see articles [17] and [20]) one can deduce a similar result by following the article of Hafner and McCurly [11]. The only difference is in the hidden constants, because the probability 1/2 of success can be achieved with fewer witnesses in the case of the Miller–Rabin test, than in the case of the Solovay–Strassen test.

The other methods of interest are Pollard's ρ method [19], Pollard's $p-1$ algorithm [18], Williams' $p+1$ algorithm [28], and the Lenstra elliptic curve factorisation method [15]. Hafner and McCurly gave the following theorem for the case when the trial division method is combined with the elliptic curve factorisation method (see article [11]).

Theorem 1.3. *Let $\theta > 5/6$. If $t \geq \ln^4 n$ and $\ln t = o(\ln^\theta n)$, then*

$$F(n,t,A) \geq e^\gamma \frac{n}{\ln n} \left(\ln \frac{t}{\ln n} \right)^{1/\theta} (1 + o(1)) \tag{1.3}$$

where A is a combination of the trial division and the elliptic curve method combined with the Solovay–Strassen probabilistic primality test.

The authors note that Lenstra's conjecture would allow one to prove this theorem with any $\theta > 1/2$. For more information on Lenstra's conjecture, see articles [15] and [11]. Furthermore the analysis using the Adleman–Pomerance–Rumely, or Miller–Rabin tests instead of the Solovay–Strassen test is very similar.

Hafner and McCurly also state that the analysis of Pollard's ρ method, Pollard's $p-1$ method, and Williams' $p+1$ method is more complicated, but they expect the results to fall in between those of trial division and the elliptic curve method.

Now we give a model for the expected number of complete factorisations of numbers $m \leq n$ having form $m = fq$, where f is $b(n)$ smooth, and q is a prime larger than $b(n)$. This model will supply us with asymptotics similar to expressions (1.1), (1.2), or (1.3).

Taking one of the above mentioned probabilistic factorisation methods, one can say that it will successfully identify a prime factor with a given probability in a given time, which time depends on the size of the prime factor. We present a few articles regarding the factorisation probability of these methods. The factorisation probability of Pollard's ρ method is partially investigated in articles [3] and [21]. Kruppa examined the factoring probability of $p-1$, $p+1$, and elliptic curve factorisation methods in his thesis, see [14]. A factoring probability for the later method can also be found in the original article of Lenstra, see [15].

One also needs to apply a primality test, which will succeed also with a given probability. When the primality test is deterministic, then this probability is 1,

otherwise when the test is probabilistic, then this probability is strictly between 0 and 1.

Assuming that the event of factorisation, and the event of primality test are independent, we can express the overall probability of identifying a prime factor as α, which will be the product of the above mentioned probabilities. (Or one can work with probabilities $\alpha_{\min} \le \alpha \le \alpha_{\max}$ instead of just α.)

Having such probability α, the probability of acquiring the prime factors of a number $m \le n$ will be $\alpha^{\omega(m)-1}$, assuming that the identifications of the different primes are independent events. Here $\omega(m)$ denotes the number of distinct prime factors of m, with the convention $\omega(1) = 1$. To get the expected number of completely factored $m \le n$, we need to sum these $\alpha^{\omega(m)-1}$ probabilities for those m, for which $P_2(m) \le b(n)$. Here, $P_i(m)$ denotes the ith largest prime factor of m, for m having at least i prime factors.

Now we state our result.

Claim 1.4. *We have*

$$\sum_{\substack{1\le m\le n\\ P_2(m)\le b(n)\\ \omega(m)>1}} \alpha^{\omega(m)-1} = \Theta\left(\frac{n}{\ln n}\ln^{\alpha} b(n)\right),$$

where $\alpha \in (0,1)$, *and* $b : \mathbb{N} \to [e, \sqrt{n})$.

2. Proofs

First we briefly summarise the strategy of the proof of Claim 1.4. We are going to split the sum in the claim based on the values of the function ω, gaining a finite number of separate sums. After this, the summands can be extracted from these sums as

$$\alpha^{k-1} \sum_{\substack{1\le m\le n\\ P_2(m)\le b(n)\\ \omega(m)=k}} 1$$

where we are going to bound the value of the remaining sum. The traditional notation for the number of positive integers not greater than n, which have exactly k different prime divisors is $\pi_k(n)$ or $\pi(n,k)$. Now we introduce the notations

$$\pi^*_{i,\theta(n)}(n,k) := \sum_{\substack{1\le m\le n\\ P_i(m)\le n^{\theta(n)}\\ \omega(m)=k}} \mu^2(m) \quad \text{and} \quad \pi_{i,\theta(n)}(n,k) := \sum_{\substack{1\le m\le n\\ P_i(m)\le n^{\theta(n)}\\ \omega(m)=k}} 1$$

where $1 \leq i \leq k$. We are going to bound $\pi^*_{2,\theta(n)}(n,k)$ and $\pi_{2,\theta(n)}(n,k)$, when $k \geq 2$, based on the proof techniques presented by Hardy, and Ramanujan in their article [12]. (Note that they've used the notation $\pi_k(n)$ for the count of positive *square-free* integers not greater than n, which have k different prime divisors; and the notation $\varpi_k(n)$ for the previously mentioned $\pi_k(n)$.) We denote the binary logarithm of a number x as $\log_2 x$.

Lemma 2.1. *Let $\theta : \mathbb{N} \to (0, 1/2)$ be a function. Assume that there exists a natural number n_0, such that the inequalities $1/\log_2 n \leq \theta(n) < 1/2$ hold for every $n \geq n_0$. Then there is an absolute constant C, such that the inequality*

$$\sum_{p \leq n^{\theta(n)}} \frac{1}{p \ln(n/p)} < \frac{C + \ln\ln n^{\theta(n)}}{\ln n} \tag{2.1}$$

holds for every $n \geq n_0$.

Proof. This proof is a slightly modified version of a certain part of the proof of Lemma A in article [12]. Let $n \geq n_0$. As in the mentioned proof, we have that

$$\frac{1}{\ln(n/p)} = \frac{1}{\ln n} + \frac{\ln p}{\ln^2 n}\left(1 + \frac{\ln p}{\ln n} + \left(\frac{\ln p}{\ln n}\right)^2 + \cdots\right) < \frac{1}{\ln n} + \frac{2\ln p}{\ln^2 n}$$

because

$$1 + \frac{\ln p}{\ln n} + \left(\frac{\ln p}{\ln n}\right)^2 + \cdots \leq 1 + \theta(n) + \theta(n)^2 + \cdots < 2$$

as the inequalities $p \leq n^{\theta(n)}$ and $\theta(n) < 1/2$ hold. Using this, we have that the sum on the left hand side of inequality (2.1) is less than

$$\frac{1}{\ln n} \sum_{p \leq n^{\theta(n)}} \frac{1}{p} + \frac{2}{\ln^2 n} \sum_{p \leq n^{\theta(n)}} \frac{\ln p}{p} < \frac{C + \ln\ln n^{\theta(n)}}{\ln n}$$

when $n^{\theta(n)} \geq 2$, which is satisfied based on the properties of $\theta(n)$. This is because by Mertens' second theorem, we have

$$\sum_{p \leq n^{\theta(n)}} \frac{1}{p} = \ln\ln n^{\theta(n)} + B_1 + o(1)$$

when $n^{\theta(n)} \geq 2$, where $B_1 = 0.26149\ldots$ is the Mertens constant; and by Mertens' first theorem, we have

$$\sum_{p \leq n^{\theta(n)}} \frac{\ln p}{p} = \theta(n)\ln n + O(1)$$

where the constant term does not exceed 2 in absolute value when $n^{\theta(n)} \geq 2$, see article [16]. ■

Lemma 2.2. *Let $\theta : \mathbb{N} \to (0, 1/2)$ be a function. Assume that there exists a natural number n_0, such that the inequalities $1/\log_2 n \leq \theta(n) < 1/2$ hold for every $n \geq n_0$. Then there are absolute constants c_1 and c_2, such that the inequality*

$$\pi^*_{2,\theta(n)}(n,k) < c_1 \frac{n}{\ln n} \frac{(c_2 + \ln\ln n^{\theta(n)})^{k-1}}{(k-1)!} \tag{2.2}$$

holds for $k \geq 2$, when $n \geq n_0$.

Proof. We are going to prove our statement by using induction, similarly as in the proof of Lemma A in article [12]. Let $n \geq n_0$. One can construct the numbers counted in $\pi^*_{2,\theta(n)}(n,2)$ by selecting a prime $p \leq n^{\theta(n)}$, and multiplying it with a prime q, for which the inequalities

$$n^{\theta(n)} < q \leq n/p$$

hold. But if we multiply a prime p with all primes q, which are less than-, or equal to n/p, then we do an overestimation, so we have that the inequality

$$\pi^*_{2,\theta(n)}(n,2) < \sum_{p \leq n^{\theta(n)}} \pi(n/p) \tag{2.3}$$

holds. There exists a small positive constant c_π, such that the inequality

$$\pi(x) < c_\pi \frac{x}{\ln x} \tag{2.4}$$

holds when $x > 1$, see article [22], so the right hand side of inequality (2.3) is less than

$$c_\pi n \sum_{p \leq n^{\theta(n)}} \frac{1}{p \ln(n/p)} < c_\pi \frac{n}{\ln n}(C + \ln\ln n^{\theta(n)})$$

based on Lemma 2.1. The heart of our inductive reasoning will be the inequality

$$k\pi^*_{2,\theta(n)}(n,k+1) < \sum_{p \leq n^{\theta(n)}} \pi^*_{2,\theta(n)}(n/p,k)$$

which holds, because we count the numbers contributing into $\pi^*_{2,\theta(n)}(n,k+1)$ at least k times on the right hand side. Indeed, if a number which we take into account in $\pi^*_{2,\theta(n)}(n,k+1)$ has the form $p_1 p_2 \dots p_k p_{k+1}$, then we will count it

on the right hand side when $p = p_1$, $p = p_2$, and so forth, until $p = p_k$ during the summation. Assuming that inequality (2.2) is true up until k, we get

$$\pi^*_{2,\theta(n)}(n,k+1) < c_\pi \frac{n}{k!} \sum_{p \le n^{\theta(n)}} \frac{1}{p\ln(n/p)} (C + \ln\ln(n/p)^{\theta(n)})^{k-1} <$$
$$< c_\pi n \frac{(C + \ln\ln n^{\theta(n)})^{k-1}}{k!} \sum_{p \le n^{\theta(n)}} \frac{1}{p\ln(n/p)} <$$
$$< c_\pi \frac{n}{\ln n} \frac{(C + \ln\ln n^{\theta(n)})^k}{k!}$$

based on Lemma 2.1. ■

Lemma 2.3. *There exists a natural number n_1, such that the inequality*

$$k\sqrt[k]{n} < \sqrt{n}$$

holds when $2 < k < \log_2 n$, and $n \ge n_1$.

Proof. Based on the requirements imposed on k, we have that the inequality

$$\frac{k}{n^{1/2-1/k}} < \frac{\log_2 n}{n^{1/6}}$$

holds, where the right hand side is less than 1 when n is big enough, because the numerator grows slower than the denominator. ■

Lemma 2.4. *Let $\theta : \mathbb{N} \to (0, 1/2)$ be a function. Assume that there exists a natural number n_0 such that the inequalities $1/\log_2 n \le \theta(n) < 1/2$ hold for every $n \ge n_0$. Then there are absolute constants c_1 and c_2, such that the inequality*

$$\pi_{2,\theta(n)}(n,k) < c_1 \frac{n}{\ln n} \frac{(c_2 + \ln\ln n^{\theta(n)})^{k-1}}{(k-1)!} \tag{2.5}$$

holds for $k \ge 2$, when $n \ge \max(n_0, n_1)$, where n_1 is from Lemma 2.3.

Proof. We are going to prove this statement by using induction, as in the proof of Lemma B in article [12]. Let $n \ge \max(n_0, n_1)$. First, we are going to give an upper found for $\pi_{2,\theta(n)}(n,2)$. We introduce the values β_i, which overestimate the count of numbers of the form $p^i q^j \le n$, where p and q are distinct primes, $p \le n^{\theta(n)} < q$, $i \ge 1$ is fixed, and $j \ge 1$. To simplify the discussion, we also introduce the values $\delta_{i,n} := \min(1/(i+1), \theta(n))$. Based on these, we set

$$\beta_i := \sum_{p \le n^{\delta_{i,n}}} \pi(n/p^i) + \sum_{p \le n^{\delta_{i,n}}} \pi(\sqrt{n/p^i}) + \cdots + \sum_{p \le n^{\delta_{i,n}}} \pi(\sqrt[m_i]{n/p^i})$$

where $m_i := \lfloor \log_2 n - i \rfloor$, because the prime counting function is zero when its argument is less than 2, so we don't have to take more sums into account than m_i. Using these values, we have the inequality

$$\pi_{2,\theta(n)}(n,2) < \beta_1 + \beta_2 + \cdots + \beta_{\lfloor \log_2 n - 1 \rfloor} \tag{2.6}$$

where we do have a finite number of summands on the right hand side of the inequality based on the previous reasoning. Now we are going to bound these β_i, separately in the case when $i = 1$ holds and when $i > 1$ holds.

- First we look at the case $i = 1$. We have

$$\beta_1 = \sum_{p \leq n^{\theta(n)}} \pi(n/p) + \sum_{p \leq n^{\theta(n)}} \pi(\sqrt{n/p}) + \cdots + \sum_{p \leq n^{\theta(n)}} \pi(\sqrt[m_1]{n/p})$$

because $\delta_{1,n} = \theta(n)$. Here, we have a bound for the first sum from the proof of Lemma 2.2. Using inequality (2.4), we have that the remaining sums are less than

$$c_\pi \sum_{p \leq n^{\theta(n)}} 2\frac{\sqrt{n}}{\sqrt{p}\ln(n/p)} + 3\frac{\sqrt[3]{n}}{\sqrt[3]{p}\ln(n/p)} + \cdots + m_1 \frac{\sqrt[m_1]{n}}{\sqrt[m_1]{p}\ln(n/p)}$$

which is less than

$$c_\pi \sqrt{n} \sum_{p \leq n^{\theta(n)}} \frac{1}{\sqrt{p}\ln(n/p)} + \frac{1}{\sqrt[3]{p}\ln(n/p)} + \cdots + \frac{1}{\sqrt[m_1]{p}\ln(n/p)} \tag{2.7}$$

based on Lemma 2.3. Removing the prime roots from the denominators, and using the fact that inequality $m_1 < C_1 \ln n$ holds for some constant C_1, we have that expression (2.7) is less than

$$c_\pi C_1 \sqrt{n} \ln n \sum_{p \leq n^{\theta(n)}} \frac{1}{\ln(n/p)} < \frac{c_\pi C_1}{(1-\theta(n))} \sqrt{n} \sum_{p \leq n^{\theta(n)}} 1$$

because $\ln(n/p) \geq (1-\theta(n)) \ln n$. Using inequality (2.4) again, we have that the right hand side is less than

$$\frac{c_\pi^2 C_1}{(1-\theta(n))\theta(n)} \frac{n^{1/2+\theta(n)}}{\ln n} = O\left(\frac{n}{\ln n}\right)$$

because of the requirements concerning $\theta(n)$.

- Now we look at the case $i > 1$. As in the case of the previous item, we are going to look at the first sum in β_i, then handle the remaining

sums separately. Based on $p \leq n^{\delta_{i,n}}$, when $1/(i+1) \leq \theta(n)$, then the inequalities

$$\ln \frac{n}{p^i} \geq \ln \frac{n}{n^{i/(i+1)}} \geq \frac{\ln n}{i+1}$$

hold, otherwise when $\theta(n) < 1/(i+1)$, then the inequalities

$$\ln \frac{n}{p^i} \geq (1 - i\theta(n)) \ln n > \left(1 - \frac{i}{i+1}\right) \ln n = \frac{\ln n}{i+1}$$

hold. Based on these and inequality (2.4), we have

$$\sum_{p \leq n^{\delta_{i,n}}} \pi(n/p^i) < c_\pi n \sum_{p \leq n^{\delta_{i,n}}} \frac{1}{p^i \ln(n/p^i)} < c_\pi (i+1) P(i) \frac{n}{\ln n}$$

where $P(s)$ is the prime zeta function, defined as $\sum_p p^{-s}$ for $\Re(s) > 1$. Using inequality (2.4), we have that the remaining sums in β_i are less than

$$c_\pi \sum_{p \leq n^{\delta_{i,n}}} 2 \frac{\sqrt{n}}{\sqrt{p^i} \ln(n/p^i)} + 3 \frac{\sqrt[3]{n}}{\sqrt[3]{p^i} \ln(n/p^i)} + \cdots + m_i \frac{\sqrt[m_i]{n}}{\sqrt[m_i]{p^i} \ln(N/p^i)}$$

which is less than

$$c_\pi \sqrt{n} \sum_{p \leq n^{\delta_{i,n}}} \frac{1}{\sqrt{p^i} \ln(n/p^i)} + \frac{1}{\sqrt[3]{p^i} \ln(n/p^i)} + \cdots + \frac{1}{\sqrt[m_i]{p^i} \ln(n/p^i)} \tag{2.8}$$

because of Lemma 2.3. Removing the prime roots from the denominators, and using the fact that inequality $m_i < C_i \ln N$ holds for some constant C_i, we have that expression (2.8) is less than

$$c_\pi C_i \sqrt{n} \ln n \sum_{p \leq n^{\delta_{i,n}}} \frac{1}{\ln(n/p^i)} < \frac{c_\pi C_i}{(1 - i\delta_{i,n})} \sqrt{n} \sum_{p \leq n^{\delta_{i,n}}} 1$$

where the right hand side is less than

$$\frac{c_\pi^2 C_i}{(1 - i\delta_{i,n})\delta_{i,n}} \frac{n^{1/2+\delta_{i,n}}}{\ln n} = O\left(\frac{n^{5/6}}{\ln n}\right)$$

based again on inequality (2.4).

Based on these calculations, we have that the right hand side of inequality (2.6) is less than

$$c_1 \frac{n}{\ln n} (c_2 + \ln \ln n^{\theta(n)}) + c_3 \frac{n}{\ln n} \sum_{i=2}^{\infty} (i+1) P(i)$$

for some constants c_1, c_2, and c_3. According to the proof of Lemma B in [12], the value of the infinite sum is a constant, so we have shown that inequality (2.5) holds for $k = 2$, when $n \geq \max(n_0, n_1)$. Based on a reasoning like the one found in the proof of Lemma 2.2, this time the inequality

$$k\pi_{2,\theta(n)}(n, k+1) < \sum_{p \leq n^{\delta_{1,n}}} \pi_{2,\theta}(n/p, k) + \sum_{p \leq n^{\delta_{2,n}}} \pi_{2,\theta}(n/p^2, k) + \ldots \tag{2.9}$$

is the base of the induction. Assuming that inequality (2.5) is true up until k, we get that the right hand side of inequality (2.9) is less than

$$c_1 n \frac{(c_2 + \ln\ln n^{\theta})^{k-1}}{k!} \left(\sum_{p \leq n^{\delta_{1,n}}} \frac{1}{p \ln(n/p)} + \sum_{p \leq n^{\delta_{2,n}}} \frac{1}{p^2 \ln(n/p^2)} + \cdots \right)$$

where the value of the first sum inside the parentheses is known due to Lemma 2.1. As in article [12], the remaining sums inside the parentheses can be bounded by $C'/\ln n$ for some constant C'. Note that even if c_2 and the constant inside the parentheses differ, one can still fine-tune the value of c_2, so that the upper bound can be expressed in the form (2.5). ■

Lemma 2.5. *Let $\theta : \mathbb{N} \to (0, 1/2)$ be a function. There is an absolute constant $C > 0$, such that the inequality*

$$\pi_{2,\theta(n)}(n, k) > C \frac{n}{\ln n} \frac{(\ln\ln n^{\theta(n)/2})^{k-2}}{(k-2)!}$$

holds for sufficiently large n, when $2 \leq k \leq \ln\ln n$.

Proof. Let $2 \leq k \leq \ln\ln n$. One can construct the numbers counted in $\pi_{2,\theta(n)}(n, k)$ by taking powers of primes $n^{1-\theta(n)} < p$, and by multiplying the numbers counted in $\pi(n/p^i, k-1)$ with these prime powers. Using the restriction $p < n^{1-\theta(n)/2}$, and only counting the power $i = 1$, we get that the lower estimate

$$\pi_{2,\theta(n)}(n, k) \geq \sum_{n^{1-\theta(n)} < p < n^{1-\theta(n)/2}} \pi(n/p, k-1) \tag{2.10}$$

holds. Based on Sathe [23], and Selberg [24], we have that

$$\pi(n, k) = F(y) \frac{n}{\ln n} \frac{(\ln\ln n)^{k-1}}{(k-1)!} \left(1 + O\left(\frac{1}{\ln\ln n}\right)\right)$$

holds uniformly for $n \geq 3$, and $1 \leq k \leq \varepsilon \ln\ln n$, for any given fixed $\varepsilon > 0$; using $y := k/\ln\ln n$, and

$$F(z) := \frac{1}{\Gamma(z+1)} \prod_p \left(1 + \frac{z}{p-1}\right)\left(1 - \frac{1}{p}\right)^z$$

where the product iterates over the prime numbers. We fix ε to be 1, this way y will be in $(0,1]$. Based on section 6.1 of [27], by setting $s=\sigma+i\tau$, we have that

$$f_s(z) := \prod_p \left(1+\frac{z}{p^s-1}\right)\left(1-\frac{1}{p^s}\right)^z$$

converges absolutely for $\sigma > 1/2$, so the value of F is positive on $(0,1]$. Thus there exists a positive constant c such that

$$\pi(n,k) \geq c\frac{n}{\ln n}\frac{(\ln\ln n)^{k-1}}{(k-1)!}$$

holds for sufficiently large n, when $1 \leq k \leq \ln\ln n$. Based on this, the sum on the right hand side of inequality (2.10) is greater than

$$c\frac{n}{(k-2)!}\sum_{n^{1-\theta(n)}<p<n^{1-\theta(n)/2}}\frac{1}{p\ln(n/p)}(\ln\ln(n/p))^{k-2}$$

which is greater than

$$c\frac{n(\ln\ln n^{\theta(n)/2})^{k-2}}{(k-2)!}\sum_{n^{1-\theta(n)}<p<n^{1-\theta(n)/2}}\frac{1}{p\ln(n/p)}.$$

Based on the proof of Lemma 2.1, this last sum is greater than

$$\frac{1}{\ln n}\sum_{n^{1-\theta(n)}<p<n^{1-\theta(n)/2}}\frac{1}{p}+\frac{1}{\ln^2 n}\sum_{n^{1-\theta(n)}<p<n^{1-\theta(n)/2}}\frac{\ln p}{p}$$

where, based on Mertens' theorems, the first sum is a small constant, and the second sum is greater than $c'/\ln n$ for some c' constant. ■

Now we give our proof for Claim 1.4.

Proof. Fix an $\alpha \in (0,1)$, and a function $b : \mathbb{N} \to [e, \sqrt{n})$. For the extremal order of ω, we have

$$\omega(n) \leq (1+o_n(1))\frac{\ln n}{\ln\ln n}$$

as n keeps to infinity, see section 5.3 in [27]. Based on this, we can do the split

$$\sum_{\substack{1\leq m\leq n\\ P_2(m)\leq n^{\theta(n)}\\ \omega(m)>1}}\alpha^{\omega(m)-1} = \sum_{\substack{1\leq m\leq n\\ P_2(m)\leq n^{\theta(n)}\\ \omega(m)=2}}\alpha + \sum_{\substack{1\leq m\leq n\\ P_2(m)\leq n^{\theta(n)}\\ \omega(m)=3}}\alpha^2 + \cdots + \sum_{\substack{1\leq m\leq n\\ P_2(m)\leq n^{\theta(n)}\\ \omega(m)=\lambda_n}}\alpha^{\lambda_n-1}$$

with a finite λ_n depending on n. Note that the summands are independent of the sums now, so the right hand side is equal to

$$\alpha\pi_{2,\theta(n)}(n,2)+\alpha^2\pi_{2,\theta(n)}(n,3)+\cdots+\alpha^{\lambda_n-1}\pi_{2,\theta(n)}(n,\lambda_n) \tag{2.11}$$

which we are going to bound from above, and from below.

- Based on Lemma 2.4, for sufficiently large n, expression (2.11) is less than

$$c_1 \frac{n}{\ln n} \sum_{k=1}^{\lambda_n - 1} \frac{(\alpha c_2 + \alpha \ln \ln n^{\theta(n)})^k}{k!}$$

where, by using equality

$$\sum_{k=0}^{s-1} \frac{z^k}{k!} = e^z \frac{\Gamma(s,z)}{\Gamma(s)} \tag{2.12}$$

see section 9.2.1 of [9], we get

$$c_1 \frac{n}{\ln n} \left(e^{\alpha c_2 + \alpha \ln \ln n^{\theta(n)}} \frac{\Gamma(\lambda_n, \alpha c_2 + \alpha \ln \ln n^{\theta(n)})}{\Gamma(\lambda_n)} - 1 \right)$$

where the fraction inside the parentheses is the cumulative distribution function of a Poisson distribution with parameter $\alpha c_2 + \alpha \ln \ln n^{\theta(n)}$. (The parameter should be a positive real number, which holds in our case for sufficiently large n.) Because λ_n grows much faster than the parameter, the value of the fraction is close to one for large n. So we have that expression (2.11) is in $O(\theta(n)^\alpha n \ln^{\alpha-1} n)$.

- For a lower bound, we take only $\lambda'_n < \lambda_n$ number of summands from expression (2.11), where λ'_n is defined as $\ln \ln n$, so the indexes $2 \leq k \leq \lambda'_n$ satisfy the requirements of Lemma 2.5. Then we get that expression (2.11) is greater than

$$C\alpha \frac{n}{\ln n} \sum_{k=0}^{\lambda'_n} \frac{(\alpha \ln \ln n^{\theta(n)/2})^k}{k!}$$

by applying Lemma 2.5 on the remaining summands. We can apply equality (2.12) again, to get

$$C\alpha \frac{n}{\ln n} e^{\alpha \ln \ln n^{\theta(n)/2}} \frac{\Gamma(\lambda'_n + 1, \alpha \ln \ln n^{\theta(n)/2})}{\Gamma(\lambda'_n + 1)}$$

where the second fraction is the cumulative distribution function of a Poisson distribution again, for sufficiently large n. As λ'_n still grows faster than the parameter, the value of this fraction is positive for larger n, and we get that expression (2.11) is in $\Omega(\theta(n)^\alpha n \ln^{\alpha-1} n)$.

Taking $\theta(n) := \ln b(n) / \ln n$ in both cases, we get our result. ■

Acknowledgments. The author wishes to thank the reviewer for the thorough reviews and the suggestions.

References

[1] **Adleman, L.M., C. Pomerance and R.S. Rumely,** On distinguishing prime numbers from composite numbers, *Ann. Math.*, **117(1)** (1983), 173–206.

[2] **Atkin, A.O.L. and F. Morain,** Elliptic curves and primality proving, *Math. Comp.*, **61(203)** (1993), 29–68.

[3] **Bach, E.,** Toward a theory of Pollard's Rho Method, *Inf. Comput.*, **90** (1991), 139–155.

[4] **Bernstein, D.J.,** How to find small factors of integers, Preprint (2002).

[5] **Bernstein, D.J.,** How to find smooth parts of integers, Preprint (2004).

[6] **Bernstein, D.J.,** Fast multiplication and its applications, *Algorithmic Number Theory, MSRI Publications*, **44** (2008), 325–384.

[7] **Bosma, W., E. Cator, A. Járai and Gy. Kiss,** Primality proofs with elliptic curves: Heuristics and analysis, *Annales Univ. Sci. Budapest., Sect. Comp.*, **44** (2015), 3–27.

[8] **Cohen, H.,** *A Course In Computational Algebraic Number Theory*, Springer–Verlag, third, corrected printing (1996).

[9] **Erdélyi, A., editor,** *Higher Transcendental Functions*, Vol. 2, The Bateman Manuscript Project, McGraw-Hill, New York (1953).

[10] **Franke, J., T. Kleinjung, F. Morain and T. Wirth,** Proving the primality of very large numbers with fastECPP, in: *Algorithmic Number Theory. ANTS 2004.*, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, **3076** (2004), 194–207.

[11] **Hafner, J.L. and K.S. McCurley,** On the distribution of running times of certain integer factoring algorithms, *J. Algorithms*, **10(4)** (1989), 531–556.

[12] **Hardy, G.H. and S. Ramanujan,** The normal number of prime factors of a number n, *Quarterly J. Math.*, **48** (1917), 76–92.

[13] **Hildebrand, A. and G. Tenenbaum,** On the number of prime factors of an integer, *Duke Math. J.*, **56(3)** (1988), 471–501.

[14] **Kruppa, A.,** *Speeding up Integer Multiplication and Factorization*, PhD thesis, Université Henri Poincaré - Nancy I, (2010).

[15] **Lenstra, H.W., Jr.,** Factoring integers with elliptic curves, *Ann. Math.*, **126** (1987), 649–673.

[16] **Mertens, F.,** Ein Beitrag zur analytischen Zahlentheorie, *J. reine angew. Math.*, **78** (1874), 46–62.

[17] **Miller, G.L.,** Riemann's hypothesis and tests for primality, *J. Comput. Syst. Sci.*, **13(3)** (1976), 300–317.

[18] **Pollard, J.M.,** Theorems of factorization and primality testing, *Math. Proc. Camb. Philos. Soc.*, **76(3)** (1974), 521–528.

[19] **Pollard, J.M.,** A Monte Carlo method for factorization, *BIT Numer. Math.*, **15(3)** (1975), 331–334.

[20] **Rabin, M.O.,** Probabilistic algorithm for testing primality, *J. Number Theory*, **12(1)** (1980), 128–138.

[21] **Román, G.,** Primality proofs with elliptic curves: factoring with Pollard's ρ method, *Annales Univ. Sci. Budapest., Sect. Comp.*, **48** (2018), 169–179.

[22] **Rosser, J.B. and L. Schoenfeld,** Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6(1)** (1962), 64–94.

[23] **Sathe, L.G.,** On a problem of Hardy and Ramanujan on the distribution of integers having a given number of prime factors, *J. Indian Math. Soc.*, **17** (1953), 63–141.

[24] **Selberg, A.,** Note on a paper by L.G. Sathe, *J. Indian Math. Soc.*, **18** (1954), 83–87.

[25] **Solovay, R.M. and V. Strassen,** A fast Monte-Carlo test for primality, *SIAM J. Comput.*, **6(1)** (1977), 84–85.

[26] **Solovay, R.M. and V. Strassen,** Erratum: A fast Monte-Carlo test for primality, *SIAM J. Comp.*, **7(1)** (1978), 118–118.

[27] **Tenenbaum, G.,** *Introduction to Analytic and Probabilistic Number Theory*, AMS, third edition, (2015).

[28] **Williams, H.C.,** A $p+1$ method of factoring, *Math. Comp.*, **39(159)** (1982), 225–234.

G. Román
Department of Computer Algebra
Eötvös Loránd University
Budapest
Hungary
rogpaai@inf.elte.hu