On values of $d(n!)/m!$, $\phi(n!)/m!$ and $\sigma(n!)/m!$

by Daniel Baczkowski, Michael Filaseta, Florian Luca and Ognian Trifonov

1 Introduction

In [5], the third author established that for a fixed $r \in \mathbb{Q}$, there are only a finite number of positive integers n and m for which $f(n!) = r \cdot m!$ where f is one of the arithmetic functions d (the number of divisors function), ϕ (Euler's ϕ-function), or σ (the sum of the divisors function). In this paper, we establish a generalization of these results. A similar result that we do not address here was given by the third author and I. Shparlinski [6] for the function τ, that is Ramanujan's tau function. Denoting by $\omega(n)$ the number of distinct prime divisors of n, the following is an easily stated consequence of our main results.

Theorem 1. *Let f denote one of the arithmetic functions d, ϕ or σ, and let k be a fixed positive integer. Then there are at most finitely many positive integers n, m, a and b such that*

$$b \cdot f(n!) = a \cdot m!, \quad \gcd(a, b) = 1 \quad \textit{and} \quad \omega(ab) \le k. \tag{1}$$

Alternatively, Theorem 1 is asserting that the total number of distinct primes dividing the numerator and denominator of the fraction obtained by reducing the quotient $f(n!)/m!$ tends to infinity as the product nm tends to infinity.

For the proof of Theorem 1, we note that it suffices to show that (1) implies that there is a positive integer $N = N(k)$ such that the inequality $n \le N$ holds. In fact, once $n \le N$ is established, we can deduce that the left-hand side of the first equation in (1) has a bounded number of distinct prime factors (depending only on k). This then implies that m is bounded and, hence, that there are only a finite number of possibilities for the value of $a/b = f(n!)/m!$. Given that $\gcd(a, b) = 1$, we can then deduce that there are only a finite number of possibilities for the quadruple (n, m, a, b).

We will establish results considerably stronger than Theorem 1 for each of the arithmetic functions given there. Our argument for the case $f = \sigma$ will be more involved than our arguments for $f = d$ and $f = \phi$. This is due to the difficulty in estimating the number of large distinct prime divisors of $\sigma(n!)$. We are therefore able to more easily prove the cases when $f = d$ and $f = \phi$.

Theorem 2. *There are at most finitely many positive integers a, b, n and m such that*

$$b \cdot d(n!) = a \cdot m!, \quad \gcd(a, b) = 1, \quad \omega(b) \le m^{1/4} \quad \textit{and} \quad P_0(a) \le \frac{\log n}{22}, \tag{2}$$

where $P_0(a)$ denotes the least prime not dividing a.

2000 Mathematics Subject Classification: 11A25 (11N05).

The second and fourth authors were supported by the National Science Foundation. The second author was also supported by the National Security Agency. The third author was supported by SEP-CONACyT 46755.

Theorem 3. *There are at most finitely many positive integers a, b, n and m, with $n > 1$, such that*

$$b \cdot \phi(n!) = a \cdot m!, \quad \gcd(a,b) = 1 \quad \textit{and} \quad \max\{\omega(a), \omega(b)\} \le \frac{n}{7\log n}. \tag{3}$$

Theorem 4. *Fix $\varepsilon > 0$. Then there are at most finitely many positive integers a, b, n and m such that*

$$b \cdot \sigma(n!) = a \cdot m!, \quad \gcd(a,b) = 1, \quad \omega(ab) \le n^{0.2-\varepsilon}. \tag{4}$$

These three results are meant to reflect the flavor of what the arguments produce. Regarding Theorem 2, the bounds on $\omega(b)$ and $P_0(a)$ can be sharpened slightly and altered to the extent that one can weaken (or strengthen) the bound for $\omega(b)$ if one wants to improve (or is willing to weaken, respectively) the bound for $P_0(a)$.

Although the bound on $\max\{\omega(a), \omega(b)\}$ in Theorem 3 is not sharp, by considering $m = \lfloor n/2 \rfloor$ and a and b having prime factors from $[2, n/2]$, it is not difficult to see that one cannot, for any $\varepsilon > 0$, replace the estimate $\max\{\omega(a), \omega(b)\} \le n/(7\log n)$ with $\omega(ab) \le n/\big((2-\varepsilon)\log n\big)$. In particular, the bound is within a constant factor of being best possible.

As with Theorem 1, one can reduce establishing Theorem 2, 3 or 4 to showing that there is a positive integer N for which $n \le N$. To see this, suppose such an N exists. In the case of Theorem 2, we deduce that the number of distinct primes dividing the left-hand side of the first equation in (2) is at most a function of N plus $m^{1/4}$. In the case of Theorems 3 and 4, we deduce that the number of distinct prime factors on the left-hand side of the first equation in (3) and (4), respectively, is bounded by a function of N. As the number of distinct prime divisors of $m!$ is $\gg m/\log m$ by the Prime Number Theorem (or simply a Chebyshev estimate), we obtain that in any case m is bounded, and we deduce as before that there are at most a finite number of quadruples (n, m, a, b).

It is not difficult to see that Theorems 2, 3 and 4 imply Theorem 1 for $f = \phi$, d, and σ, respectively. To see this, let f be one of these three multiplicative functions. We have already seen that the number of quadruples (n, m, a, b) as in (1) is bounded if n is fixed. In the case that $f = d$, as we will see in the next section, it is also the case that the number of quadruples is bounded if m is fixed and n, a and b are allowed to vary. For n large, if $\omega(ab) \le k$, then the conditions in (3) and (4) are satisfied. For n and m large, if $\omega(ab) \le k$, then the conditions in (2) are satisfied. Hence, Theorems 2, 3 and 4 imply that there are only a finite number of quadruples (n, m, a, b) as in (1).

2 The function d

We establish Theorem 2 (and, hence, Theorem 1 in the case that $f = d$). Recall that it suffices to show that under the conditions of (2), n is bounded. We therefore consider n large and assume that we have a solution (n, m, a, b) to (2) with the goal of obtaining a contradiction. We first show that m must also be large. To establish this, we may suppose $m \le 2n$. Consider a prime $q \le \log^2 n$. Let p be a prime in the interval $(n/q, n/(q-1)]$. Using the logarithmic integral approximation of $\pi(x)$ in the Prime Number Theorem with an appropriate error term gives that the number of such primes is

$$\sim \frac{n}{q(q-1)\log n}.$$

For each such prime p, we have $p > \sqrt{n}$ so that $\nu_p(n!) = \lfloor n/p \rfloor = q - 1$, and we deduce that $q = \nu_p(n!)+1$ is a prime divisor of $d(n!)$. Moreover, for q a prime $\le \log^2 n$, we have that $\nu_q\big(d(n!)\big)$ is at least the number of primes $p \in (n/q, n/(q-1)]$. Thus,

$$\nu_q\big(bd(n!)\big) \ge \nu_q\big(d(n!)\big) \ge \frac{n}{2q(q-1)\log n} \qquad \text{for } q \le \log^2 n. \tag{5}$$

We consider a prime $q \le \log^2 n$ that does not divide a, which exists by the condition on a in (2). As n is large, we deduce from (5) that the left-hand side of the first equation in (2) is divisible by a large power of q. We deduce then that m too must be large. Note that this implies that the number of quadruples (n, m, a, b) as in (2) is bounded if m is fixed as was indicated in the introduction.

We will want a general estimate for the exponent in the highest power of a prime p dividing $n!$. A classical formula is

$$\nu_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Alternatively,

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the base p digits of n (cf. [1]). For this section, we use that the latter formula easily implies $\nu_p(n!) \le (n-1)/(p-1)$. One easily deduces that for n a positive integer and p a prime $\le n$, we have

$$\nu_p(n!) + 1 \le \frac{n-1}{p-1} + 1 \le \frac{2n}{p}.$$

It follows that

$$\log d(n!) = \log \prod_{p \le n} \big(\nu_p(n!) + 1\big) \le \sum_{p \le n} \big(\log 2 + \log n - \log p\big) = \pi(n)\big(\log 2 + \log n\big) - \sum_{p \le n} \log p.$$

Classical Prime Number Theorem estimates imply that the right-hand side above is $< 2n/\log n$. On the other hand, Stirling's formula easily gives that

$$\log(m!) > m \log m - m.$$

Indeed, this last inequality can be seen from

$$e^m = \sum_{j=0}^{\infty} \frac{j^m}{j!} > \frac{m^m}{m!}.$$

For an arbitrary prime p, we use $\nu_p(m!) \le (m-1)/(p-1) < 2m/p$. Hence,

$$\log \prod_{\substack{p \le m \\ p \mid b}} p^{\nu_p(m!)} = \sum_{\substack{p \le m \\ p \mid b}} \nu_p(m!) \log p \le 2m \sum_{\substack{p \le m \\ p \mid b}} \frac{\log p}{p}.$$

If $b \ne 3$, this last sum is no bigger than the sum one obtains with b replaced by the product of the first $\omega(b)$ primes. This allows us to deduce from a direct computation that if $\omega(b) \le 100$, then

$$\sum_{\substack{p \le m \\ p \mid b}} \frac{\log p}{p} \le \frac{3 \log\big(\omega(b) + 1\big)}{2}. \tag{6}$$

For $\omega(b) > 100$, we appeal to (3.13) and (3.23) of [8]. The former implies that the $\omega(b)$th prime is $< 2\omega(b)\log\omega(b)$. The latter implies

$$\sum_{p \le 2\omega(b)\log\omega(b)} \frac{\log p}{p} < \log\omega(b) + \log\log\omega(b) < \frac{3\log\big(\omega(b)\big)}{2},$$

all under the condition $\omega(b) > 100$. In any case, (6) holds independent of the value of $\omega(b)$, and we obtain

$$\log \prod_{\substack{p \le m \\ p \mid b}} p^{\nu_p(m!)} < 3m\log\big(\omega(b)+1\big).$$

From (2), we have $\log\big(\omega(b)+1\big) \le 0.26\log m$. We deduce that the logarithm of the product of the primes (to their multiplicities) on the right-hand side of the first equation in (2) that do not divide b is at least

$$m\log m - m - 0.78\, m\log m > \frac{m\log m}{5},$$

where we have used that m is large. This then is a lower bound for $\log d(n!)$, and we deduce

$$\frac{2n}{\log n} > \frac{m\log m}{5}.$$

As n and m are large, we obtain $m \le 11n/\log^2 n$. Hence,

$$\nu_q(m!) \le \frac{m-1}{q-1} < \frac{11n}{(q-1)\log^2 n}.$$

We obtain from (5) that for each $q \le (\log n)/22$, we have $\nu_q\big(b\, d(n!)\big) > \nu_q(m!)$. We deduce from the first equation in (2) that each prime $\le (\log n)/22$ divides a, contradicting the condition on a in Theorem 2 and, hence, completing the proof.

3 The function ϕ

In this section, we establish Theorem 3 (and, hence, Theorem 1 in the case that $f = \phi$). We again consider n large and assume that we have a solution (n, m, a, b) to (3) with the goal of obtaining a contradiction. We begin by using the bound $n/(7\log n)$ on $\omega(b)$. Observe that every prime factor of $\phi(n!)$ is $\le n/2$. Also, using that n is large and the Prime Number Theorem, we have

$$\pi(0.65n) - \pi(0.5n) > \frac{n}{7\log n} \ge \omega(b).$$

It follows that there is a prime $\le 0.65n$ that does not divide $b \cdot \phi(n!)$. As every prime $\le m$ divides the right-hand side of the first equation in (3), we deduce $m < 0.65n$.

Next, we use that $\omega(a) \le n/(7\log n)$. This inequality together with n being large and the Prime Number Theorem imply that there is a prime q satisfying $\sqrt{n} < q \le 0.15n$ that does not divide a. We fix such a q. Observe that the exponent in the largest power of q dividing $\phi(n!)$ is at least $\lfloor n/q \rfloor - 1 > (n/q) - 2$. Since $m < n$ so that $q > \sqrt{n} > \sqrt{m}$, the exponent in the largest power of q dividing $m!$ is $\lfloor m/q \rfloor \le m/q$. As $q \nmid a$, we have a contradiction to the first equation in (3) if

$$\frac{n}{q} - 2 \ge \frac{m}{q}.$$

Given that $m < 0.65n$ and $q \le 0.15n$, we have

$$\frac{n}{q} - \frac{m}{q} > \frac{0.35n}{q} > 2.$$

The theorem follows.

4 Preliminaries for the function σ

In this section, we discuss a few preliminary results we will use in our proof of Theorem 1 for $f = \sigma$. We denote by $\Phi_N(x)$ the Nth cyclotomic polynomial. We use the following cyclotomic polynomial identities. Let N be a positive integer, and let p be a prime. Then

$$\Phi_{pN}(x) = \begin{cases} \Phi_N(x^p) & \text{if } p|N \\ \Phi_N(x^p)/\Phi_N(x) & \text{if } p \nmid N. \end{cases} \tag{7}$$

In addition, we use that

$$x^N - 1 = \prod_{d|N} \Phi_d(x). \tag{8}$$

We begin by analyzing the highest power of a given prime q that can divide an expression of the form $a^N - 1$. We have in mind here obtaining information about the prime factorization of $\sigma(n!)$ which involves factors of the form $(p^N - 1)/(p - 1)$. The approach we use takes advantage of the factorization given in (8); hence, we are interested in estimates for $\nu_q\big(\Phi_d(a)\big)$. We use the notation $\mathrm{ord}_q(a)$ for the order of a modulo q. The next result, at least for the most part, is fairly well-known. We give a proof that is motivated in part by a 1905 paper by L. E. Dickson [2].

Lemma 1. *Let q be a prime, and let a and N be integers with $N \ge 1$. Write $N = q^r M$ where r and M are integers with $r \ge 0$ and $q \nmid M$. Then $q|\Phi_N(a)$ if and only if $M = \mathrm{ord}_q(a)$. Also, if $r \ge 1$ and $N > 2$, then $q^2 \nmid \Phi_N(a)$.*

Proof. To prove the first assertion, let $s = \mathrm{ord}_q(a)$. First, consider the case that $M = s$. We obtain from (8) that

$$\prod_{d|M} \Phi_d(a) \equiv a^M - 1 \equiv 0 \pmod{q}.$$

If $q|\Phi_d(a)$ for some d, then $a^d \equiv 1 \pmod{q}$ so that $M|d$ (since $M = \mathrm{ord}_q(a)$). We deduce that the only factor on the left that can be divisible by q is $\Phi_M(a)$. Hence, $q|\Phi_M(a)$. Observe that (7) implies

$$\Phi_N(x) \equiv \Phi_M(x)^{q^{r-1}(q-1)} \pmod{q}. \tag{9}$$

Setting $x = a$, we deduce $q|\Phi_N(a)$.

Assume now that $q|\Phi_N(a)$ and $M \ne s$. We want to obtain a contradiction. Since $q|\Phi_N(a)$, we have $a^M \equiv a^N \equiv 1 \pmod{q}$. We deduce $a \not\equiv 0 \pmod{q}$, $s|M$ and, hence, $s < M$. It follows that $(x^s-1)\Phi_M(x)$ is a factor of x^M-1. The definition of s implies $x-a$ is a factor of x^s-1 modulo q. From (9) and $q|\Phi_N(a)$, we have that $x-a$ is a factor of $\Phi_M(x)$ modulo q. We obtain that $x^M-1\equiv(x-a)^2g(x) \pmod q$ for some $g(x)\in\mathbb{Z}[x]$. One obtains a contradiction by taking derivatives and setting $x=a$.

For the second assertion, we use that $\Phi_N(x)$ is a factor of

$$\frac{\left(x^{N/q}\right)^q-1}{x^{N/q}-1}=\left(x^{N/q}\right)^{q-1}+\left(x^{N/q}\right)^{q-2}+\cdots+\left(x^{N/q}\right)^2+x^{N/q}+1.$$

Substituting $x=a$ on the left, we see that if $q|\Phi_N(a)$, then necessarily $a^{N/q}\equiv 1 \pmod q$. Writing $a^{N/q}=kq+1$, where $k\in\mathbb{Z}$, observe that the expression on the right with $x^{N/q}$ replaced by $a^{N/q}$ is

$$(kq+1)^{q-1}+(kq+1)^{q-2}+\cdots+(kq+1)+1\equiv q+\frac{kq^2(q-1)}{2} \pmod{q^2}.$$

Since the left-hand side is divisible by $\Phi_N(a)$, we see that if $q\neq 2$, then $q^2\nmid\Phi_N(a)$, as desired.

If $q=2$, in fact a stronger assertion is true. In this case, $q^2\nmid\Phi_N(a)$ independent of whether $q|N$. To see this, note that for every prime p, we have $\Phi_p(1)=p$. From (7), $\Phi_N(1)=p$ if N is a power of a prime p and $\Phi_N(1)=1$ if N is an integer with more than one distinct prime factor. Also, $N>1$ implies $\Phi_N(0)=1$. Hence, $\Phi_N(a)\equiv 1 \pmod 2$ if N is not a power of 2 or if a is even. If $N=2^r$ with $r\geq 2$ and if a is odd, then

$$\Phi_N(a)\equiv\Phi_{2^r}(a)\equiv a^{2^{r-1}}+1\equiv 2 \pmod 4.$$

Thus, in any case, $4\nmid\Phi_N(a)$ for $N>2$. □

The following consequence of Lemma 1 is worth noting.

Corollary 1. *Let q be a prime, and let a and N be integers with $N>2$. If $q|\Phi_N(a)$, then either $q\equiv 1 \pmod N$ or we have that both q is the largest prime factor of N and $q^2\nmid\Phi_N(a)$.*

The condition $N>2$ in each of the above results is important as $\Phi_2(a)=a+1$ can clearly, for the right choice of a, be divisible by an arbitrarily large power of 2.

Lemma 2. *Let q be an odd prime, and let j and ℓ be positive integers. Let $f(x)=x^\ell+x^{\ell-1}+\cdots+x+1$. Then $f(x)$ has $\leq\gcd\left(\phi(q^j),\ell+1\right)$ distinct roots modulo q^j. Furthermore, $f(x)$ has $\leq 2\gcd\left(\phi(2^j),\ell+1\right)$ distinct roots modulo 2^j.*

Proof. Observe that $(x-1)f(x)=x^{\ell+1}-1$. Let $N=\ell+1$. The lemma follows from the fact (cf. [4], page 45) that $x^N\equiv 1 \pmod{q^j}$ has exactly $\gcd\left(\phi(q^j),N\right)$ roots modulo q^j if q is odd or $q=2$ and $j\in\{1,2\}$ and has exactly 1 or $2\gcd\left(2^{j-2},N\right)$ roots modulo 2^j if $j\geq 3$ depending on whether N is odd or even, respectively. □

In regards to Lemma 2, we will only be using that the number of distinct roots of $f(x)$ modulo q^j is $\ll\gcd\left(\phi(q^j),\ell+1\right)$, and we could easily get away with only concerning ourselves with odd primes q. The above lemma will, however, allow us not to worry about the parity of q in our lemmas.

We will also make use of the following version of the Brun-Titchmarsh inequality (cf. [7]).

Lemma 3. *Let x and y be positive real numbers, and let h and k be integers with $1 \le k < y \le x$. The number of primes in the interval $(x, x+y]$ that are h modulo k is*

$$\le \frac{2y}{\phi(k)\log(y/k)}.$$

5 The function σ

In this section, we establish Theorem 1 in the case that $f = \sigma$. To avoid confusion with our use of d when talking about divisors of n and the number of divisors function d discussed earlier in this paper, we use here the notation $\sigma_0(n)$ (i.e., the sum of the divisors of n each raised to the power 0) for the number of divisors of n. We also use the notations $f(n) \lesssim g(n)$ and $f(n) \gtrsim g(n)$ to denote $f(n) \le \big(1+o(1)\big)g(n)$ and $f(n) \ge \big(1+o(1)\big)g(n)$, respectively. All asymptotic estimates in this section using $\lesssim$ or $\gtrsim$ will be with respect to n.

Lemma 4. *Let q be a prime, and let a and N be integers with $a > 1$ and $N > 0$. Then*

$$\nu_q\big(a^N - 1\big) \le \frac{\log N + \mathrm{ord}_q(a)\log a + \log(a+1)}{\log q},$$

where the term $\log(a+1)$ in the numerator is only necessary in the case $q = 2$.

Proof. To obtain our result, we estimate the power of q dividing each factor on the right of $a^N - 1 = \prod_{d|N} \Phi_d(a)$. Writing $N = q^r M$ where r is a nonnegative integer and M is a positive integer relatively prime to q, we observe that each divisor of N can be written uniquely in the form $q^j d$ where j is a nonnegative integer $\le r$ and d is a divisor of M. In other words,

$$a^N - 1 = \prod_{j=0}^{r} \prod_{d|M} \Phi_{q^j d}(a).$$

Setting $d' = \mathrm{ord}_q(a)$, Lemma 1 implies that the only factors on the right that are divisible by q are of the form $\Phi_{q^j d'}(a)$. We consider the factors on the right with $j \ge 1$ and $j = 0$ separately.

Observe that

$$r \le \frac{\log N}{\log q}.$$

We apply Lemma 1 to $\Phi_{q^j d}(a)$, noting that the case $q^j d \le 2$ below requires separate consideration. We obtain

$$\begin{aligned}\nu_q\Big(\prod_{j=1}^{r}\prod_{d|M}\Phi_{q^j d}(a)\Big) &\le \nu_q\Big(\prod_{j=1}^{r}\Phi_{q^j d'}(a)\Big) + \frac{\log(a+1)}{\log q} \\ &\le r + \frac{\log(a+1)}{\log q} \le \frac{\log N + \log(a+1)}{\log q}.\end{aligned}$$

Also,

$$\nu_q\Big(\prod_{d|M}\Phi_d(a)\Big) = \nu_q\big(\Phi_{d'}(a)\big) \le \frac{\log(a^{d'} - 1)}{\log q} < \frac{d' \log a}{\log q}.$$

The lemma follows. ∎

Lemma 5. *Let q be a prime number, j a positive integer, and $L \geq 1$. Then*

$$\sum_{\ell \leq L} \frac{\gcd(\phi(q^j), \ell)}{\ell^2} \ll \log\log(q+1).$$

Before going to the proof, we make some observations. First, the wording of the above lemma is somewhat awkward but appropriate for our needs. A cleaner statement would be to take the sum on the left to be an infinite series and then to assert that the series converges and its value is $O\big(\log\log(q+1)\big)$. The implied constant here (and in the lemma) is absolute. The reason for using $\log\log(q+1)$ instead of $\log\log q$ is simply to handle the case $q = 2$ where $\log\log q$ is negative.

Proof. Notice that for a positive integer r,

$$\sum_{\ell \leq L} \frac{\gcd(r, \ell)}{\ell^2} = \sum_{t|r} \sum_{\substack{\ell \leq L \\ \gcd(r,\ell)=t}} \frac{t}{\ell^2} = \sum_{t|r} \sum_{\substack{s \leq L/t \\ \gcd(r/t,s)=1}} \frac{1}{s^2 t} \leq \zeta(2) \sum_{t|r} \frac{1}{t} = \zeta(2)\frac{\sigma(r)}{r}.$$

When $r = \phi(q^j) = q^{j-1}(q-1)$, the right-hand side above is

$$< \zeta(2)\frac{\sigma(q-1)}{q-1} \sum_{i=0}^{\infty} \frac{1}{q^i} \ll \log\log(q+1)$$

since $\sigma(N) \ll N \log\log N$. □

Lemma 6. *Let r be a positive integer, $L \geq 1$, and $\mathcal{M} = \min\{r, L\}$. Then*

$$\sum_{\ell \leq L} \ell \gcd(r, \ell) \leq L^2 \sum_{\substack{d \leq \mathcal{M} \\ d|r}} \frac{\phi(d)}{d}.$$

Moreover, if $K \geq 1$, then

$$\sum_{\ell \leq q^2 \log_q n} \ell \gcd(\phi(q^K), \ell) \leq 3q^4 (\log_q n)^2 \sigma_0(q-1) + (\log_q n)^9,$$

where q is a prime and $\log_q n$ denotes the logarithm of n to the base q (i.e., $\log_q n = \log n / \log q$).

Proof. Using the fact that $\sum_{d|N} \phi(d) = N$, we have

$$\sum_{\ell \leq L} \ell \gcd(r, \ell) = \sum_{\ell \leq L} \ell \sum_{d|\gcd(r,\ell)} \phi(d) = \sum_{\substack{d \leq \mathcal{M} \\ d|r}} \sum_{\substack{\ell \leq L \\ d|\ell}} \ell\phi(d)$$

$$= \sum_{\substack{d \leq \mathcal{M} \\ d|r}} \sum_{t \leq L/d} td\phi(d) \leq L^2 \sum_{\substack{d \leq \mathcal{M} \\ d|r}} \frac{\phi(d)}{d}.$$

Now, let $r = \phi(q^K) = q^{K-1}(q-1)$ and $L = q^2 \log_q n$. If $q > \log_q n$, then the sum on the right-hand side above is

$$\leq \sum_{\substack{d < q^3 \\ d|q^2(q-1)}} \frac{\phi(d)}{d} \leq \sigma_0\big(q^2(q-1)\big) \leq 3\sigma_0(q-1).$$

In the case that $q \le \log_q n$, we easily have

$$\sum_{\ell \le L} \ell \gcd(r, \ell) \le \sum_{\ell \le L} \ell^2 \le L^3 = q^6 (\log_q n)^3 \le (\log_q n)^9.$$

The lemma follows. □

Lemma 7. *If $0 < \epsilon < 1/5$ and q is a prime $\le n^{1/5-\epsilon}$, then*

(i) $$\nu_q\big(\sigma(n!)\big) \ll \frac{n \log\log(q+1)}{q \log n}.$$

If $0 < \delta < 1/3$ and q is a prime, then

(ii) $$\nu_q\Bigg(\prod_{n^{1-\delta} < p \le n} \sigma\big(p^{\nu_p(n!)}\big)\Bigg) \ll \frac{n \log\log(q+1)}{q} + \frac{n^{3\delta} \log n}{\log q}.$$

Proof. Let $e(p) = \nu_p(n!)$, and set $N(p) = e(p) + 1$. We also let $L = \lfloor q^2 \log_q n \rfloor$. We begin by proving the first part of the lemma. We will estimate the contribution of factors of $q \le n^{1/5-\epsilon}$ arising from $\sigma\big(p^{e(p)}\big)$ separately depending on whether $p \le n/L$ or $p > n/L$. In other words, noting that

$$\sigma(n!) = \prod_{p \le n/L} \sigma(p^{e(p)}) \cdot \prod_{n/L < p \le n} \sigma(p^{e(p)}) = \prod_{p \le n/L} \frac{p^{N(p)} - 1}{p-1} \cdot \prod_{n/L < p \le n} \frac{p^{N(p)} - 1}{p-1},$$

we combine estimates for

$$\mathcal{V} = \mathcal{V}(q) = \nu_q\Bigg(\prod_{p \le n/L} \sigma(p^{e(p)})\Bigg) = \nu_q\Bigg(\prod_{p \le n/L} \frac{p^{N(p)} - 1}{p-1}\Bigg)$$

and

$$\mathcal{V}' = \mathcal{V}'(q) = \nu_q\Bigg(\prod_{n/L < p \le n} \sigma(p^{e(p)})\Bigg) = \nu_q\Bigg(\prod_{n/L < p \le n} \frac{p^{N(p)} - 1}{p-1}\Bigg).$$

From Lemma 4, for any prime q we have that

$$\mathcal{V} \ll \sum_{p \le n/L} \frac{\log N(p) + \mathrm{ord}_q(p) \log p}{\log q},$$

where the term $\log(a+1)$ appearing in the numerator of the bound given in Lemma 4 has been absorbed by the implied constant above. We use that $N(p) \le n$, which follows easily from

$$e(p) = \sum_{u=1}^{\infty} \left\lfloor \frac{n}{p^u} \right\rfloor < \sum_{u=1}^{\infty} \frac{n}{p^u} = \frac{n}{p-1} \le n, \tag{10}$$

and that $\mathrm{ord}_q(p)$ divides $\phi(q)$. Since also $\pi(x) \ll x/\log x$, we obtain

$$\mathcal{V} \ll \sum_{p \le n/L} \frac{\log n}{\log q} + \sum_{p \le n/L} \frac{q \log p}{\log q}$$

$$\ll \frac{\pi\big(n/L\big)\log n}{\log q} + \frac{q}{\log q}\sum_{p\le n/L}\log p$$

$$\ll \frac{q\,n}{L\log q} \ll \frac{n}{q\log n}.$$

We divide up our consideration of larger primes p as follows. For each positive integer $\ell < L$, we consider the contribution of q's from $\sigma\big(p^{e(p)}\big)$ with $p \in I_\ell = (n/(\ell+1), n/\ell]$. Fix such an ℓ and a prime $p \in I_\ell$. As n is sufficiently large, the definition of L implies $p > \sqrt{n}$. Since $p \in I_\ell$, we obtain

$$N(p) = \lfloor n/p \rfloor + 1 = \ell + 1.$$

Let $f_\ell(x) = x^\ell + x^{\ell-1} + \cdots + x^2 + x + 1$. Then $\sigma(p^{e(p)}) = f_\ell(p)$. Observe that this polynomial defining $\sigma(p^{e(p)})$ does not change as p varies over the primes in I_ℓ. We now let p vary over the primes in I_ℓ and use that

$$\nu_q\bigg(\sigma\bigg(\prod_{p\in I_\ell} p^{e(p)}\bigg)\bigg) = \sum_{p\in I_\ell}\nu_q\big(f_\ell(p)\big) = \sum_{j\ge 1}\sum_{\substack{p\in I_\ell\\ f_\ell(p)\equiv 0 \pmod{q^j}}} 1. \tag{11}$$

Let $J = \log_q(\log n) + 1$ so that $q^J = q\log n$. For each $\ell < L$, we obtain from $q \le n^{1/5-\epsilon}$ that

$$\frac{|I_\ell|}{q^J} \ge \frac{n}{L^2 q^J} \ge \frac{n}{q^5(\log_q n)^2\log n} \ge \frac{n^{5\epsilon}}{\log_2^3 n} \gg n^\epsilon. \tag{12}$$

We consider the numbers

$$\rho_{j,\ell} = \rho_{j,\ell}(q) = \big|\{t \in \mathbb{Z} : 0 \le t \le q^j - 1,\ f_\ell(t) \equiv 0 \ (\mathrm{mod}\ q^j)\}\big|.$$

For each $a \in \{0, 1, \ldots, q^j - 1\}$ with $j \le J$ and $f_\ell(a) \equiv 0 \pmod{q^j}$, we obtain from Lemma 3 that

$$\pi\big(n/\ell; q^j, a\big) - \pi\big(n/(\ell+1); q^j, a\big) \le \frac{2|I_\ell|}{\phi(q^j)\log\big(|I_\ell|/q^j\big)}.$$

Now, we consider the $j > J$. Recall that $N(p) = \ell + 1$ for each $p \in I_\ell$. Define

$$K = K_\ell = (\ell+1)\log_q n.$$

We show that K can be used as an upper bound on the j appearing in (11) as follows. Observe that if q^j divides $f_\ell(p)$ for some $p \in I_\ell$, then $N = \ell + 1$ implies that $q^j \le (p^N - 1)/(p-1)$. We deduce that $q^j < p^N$ and, hence,

$$j < N\log_q p \le N\log_q n = (\ell+1)\log_q n = K. \tag{13}$$

Thus, for ℓ fixed, we need only consider the positive integer values of j such that $J < j < K$. For each such j, we proceed as before by counting the number of primes $p \in I_\ell$ such that q^j divides $f_\ell(p)$. For each $j > J$, we simply use that the number of primes $p \in I_\ell$ for which q^j divides $f_\ell(p)$ is

$$\le \rho_{j,\ell}\bigg(\frac{|I_\ell|}{q^j} + 1\bigg).$$

Altogether, we deduce that

$$\mathcal{V}' = \sum_{\ell<L}\sum_{p\in I_\ell}\nu_q\big(f_\ell(p)\big) \le \sum_{\ell<L}\Bigg(\sum_{1\le j\le J}\frac{2|I_\ell|\rho_{j,\ell}}{\phi(q^j)\log\big(|I_\ell|/q^j\big)} + \sum_{J<j<K_L}\frac{|I_\ell|\rho_{j,\ell}}{q^j} + \sum_{J<j<K_\ell}\rho_{j,\ell}\Bigg).$$

We view the right-hand side above as three double sums and estimate each in turn. Note that $|I_\ell| \ll n/(\ell+1)^2$ and, from Lemma 2, we have $\rho_{j,\ell} \le 2\gcd\big(\phi(q^j),\ell+1\big)$. From the estimate in (12) and Lemma 5, we deduce

$$\begin{aligned}\sum_{\ell<L}\sum_{1\le j\le J}\frac{2|I_\ell|\rho_{j,\ell}}{\phi(q^j)\log\big(|I_\ell|/q^j\big)} &\ll \sum_{1\le j\le J}\sum_{\ell<L}\frac{n\gcd\big(\phi(q^j),\ell+1\big)}{\phi(q^j)(\ell+1)^2\log\big(|I_\ell|/q^j\big)}\\ &\ll \sum_{1\le j\le J}\sum_{\ell<L}\frac{n\gcd\big(\phi(q^j),\ell+1\big)}{\phi(q^j)(\ell+1)^2\log n}\\ &\ll \sum_{1\le j\le J}\frac{n\log\log(q+1)}{\phi(q^j)\log n}\\ &\ll \sum_{j=1}^{\infty}\frac{n\log\log(q+1)}{q^j\log n}\\ &\ll \frac{n\log\log(q+1)}{q\log n}.\end{aligned}$$

Recall that $q^J = q\log n$. Hence,

$$\begin{aligned}\sum_{\ell<L}\sum_{J<j<K_L}\frac{|I_\ell|\rho_{j,\ell}}{q^j} &\ll \sum_{J<j<K_L}\sum_{\ell<L}\frac{n\gcd\big(\phi(q^j),\ell+1\big)}{q^j(\ell+1)^2}\\ &\ll \sum_{j>J}\frac{n\log\log(q+1)}{q^j}\\ &\ll \frac{n\log\log(q+1)}{q^J}\\ &\ll \frac{n\log\log(q+1)}{q\log n}.\end{aligned}$$

Recall $K_\ell = (\ell+1)\log_q n$, and observe that

$$\rho_{j,\ell} \le 2\gcd\big(\phi(q^j),\ell+1\big) \le 2\gcd\big(\phi\big(q^{\lfloor K_\ell\rfloor}\big),\ell+1\big).$$

From Lemma 6, we obtain

$$\begin{aligned}\sum_{\ell<L}\sum_{J<j<K_\ell}\rho_{j,\ell} &\ll \sum_{\ell<L}\sum_{J<j<K_\ell}\gcd\big(\phi\big(q^{\lfloor K_\ell\rfloor}\big),\ell+1\big)\\ &\ll \sum_{\ell<L}K_\ell\gcd\big(\phi\big(q^{\lfloor K_\ell\rfloor}\big),\ell+1\big)\end{aligned}$$

$$\ll (\log_q n) \sum_{\ell < L} (\ell+1) \gcd\left(\phi\big(q^{\lfloor K_\ell \rfloor}\big), \ell+1\right)$$

$$\ll q^4 \sigma_0(q-1)(\log_q n)^3 + (\log_q n)^{10}.$$

For fixed $\epsilon > 0$ and $q \leq n^{1/5-\epsilon}$, this sum is $\ll n^{1-\epsilon}/q \ll n/(q \log n)$. Combining the above, we obtain for $q \leq n^{1/5-\epsilon}$ that

$$\nu_q\big(\sigma(n!)\big) = \mathcal{V} + \mathcal{V}' \ll \frac{n \log\log(q+1)}{q\ \log n}.$$

For the second part of the lemma, we can give a similar but simpler argument. We take $L = n^\delta$. We partition the interval I_ℓ into congruence classes of length q^j. For each $\ell < L$, we consider all possible values of $1 \leq j \leq K_\ell$ together. Doing so, we obtain

$$\sum_{\ell < L} \sum_{p \in I_\ell} \nu_q\big(f_\ell(p)\big) \leq \sum_{\ell < L} \sum_{1 \leq j < K_\ell} \rho_{j,\ell} \left(\frac{|I_\ell|}{q^j} + 1 \right) \leq \sum_{1 \leq j < K_L} \sum_{\ell < L} \rho_{j,\ell} \frac{|I_\ell|}{q^j} + \sum_{\ell < L} \sum_{1 \leq j < K_L} \rho_{j,\ell}.$$

Applying Lemma 2 and Lemma 5 to the first double sum on the right-hand side above and using that $\rho_{j,\ell} \ll \ell$ to the latter, we obtain

$$\nu_q\left(\prod_{n^{1-\delta} < p \leq n} \frac{p^{N(p)} - 1}{p-1} \right) = \sum_{\ell < n^\delta} \sum_{p \in I_\ell} \nu_q\big(f_\ell(p)\big) \ll \frac{n \log\log(q+1)}{q} + \frac{n^{3\delta} \log n}{\log q}.$$

The lemma follows. □

Proof of Theorem 4: Set $c = 1/5 - 2\epsilon$ where $0 < \epsilon < 1/10$. It suffices to show that $\omega(ab) \leq n^c$ has no solutions for n sufficiently large. So assume n is sufficiently large and $\omega(ab) \leq n^c$.

First, we consider the case that $\omega\big(\sigma(n!)\big) \geq 2n^c$. Then there exists $\geq n^c$ distinct primes p dividing $\sigma(n!)$ and not dividing ab. The equation $b \cdot \sigma(n!) = a \cdot m!$ implies that any such prime p must divide $m!$ and, hence, every prime $\leq p$ divides $b \cdot \sigma(n!)$. We deduce that among the first $2n^c$ primes, there is an odd prime q that divides $\sigma(n!)$ and not ab. Note that $q \leq n^{c+\epsilon} \leq n^{1/5-\epsilon}$. Since q does not divide ab, we have

$$\nu_q\big(\sigma(n!)\big) = \nu_q(m!) \geq \frac{m}{q} - 1.$$

Lemma 7 (i) now implies

$$m \ll \frac{n \log\log n}{\log n}. \tag{14}$$

Before proceeding, we note that the case when $\omega\big(\sigma(n!)\big) < 2n^c$ also gives (14). Indeed, in this case we have

$$\frac{m}{\log m} \ll \pi(m) = \omega(m!) \leq \omega\big(b \cdot \sigma(n!)\big) \leq \omega(b) + \omega\big(\sigma(n!)\big) \ll n^c$$

implying that $m \ll n^c \log n$.

Observe that

$$\log \sigma(n!) \geq \log(n!) \sim n \log n$$

and, from (14),

$$\log(m!) \sim m \log m \ll n \log\log n.$$

Hence, $b \cdot \sigma(n!) = a \cdot m!$ implies

$$\log a = \log(b/m!) + \log \sigma(n!) \gtrsim n \log n.$$

Fix $0 < \delta < 1/3$. Also, let

$$a' = \prod_{p \le n^{1-\delta}} \sigma\big(p^{e(p)}\big) \quad \text{and} \quad a'' = \gcd\big(a, \sigma(n!)/a'\big).$$

Clearly, $a \le a'a''$. As a consequence of (10), we have

$$\frac{n}{p} - 1 < e(p) < \frac{n}{p-1}$$

from which we deduce

$$\log a' \lesssim \sum_{p \le n^{1-\delta}} e(p) \log p \sim \big(1-\delta\big) n \log n.$$

Combining the above, we get

$$n \log n \lesssim \log a \le \log a' + \log a'' \lesssim (1-\delta) n \log n + \sum_{q \mid a''} \nu_q(a'') \log q. \tag{15}$$

From Lemma 7,

$$\sum_{q \mid a''} \nu_q(a'') \log q \ll \sum_{\substack{q \mid a'' \\ q \le n^{c+\epsilon}}} \frac{n \log\log n}{q \log n} \log q \; + \sum_{\substack{q \mid a'' \\ q > n^{c+\epsilon}}} \left(\frac{n \log\log(q+1)}{q} \log q + n^{3\delta} \log n \right).$$

For the first sum on the right, we have

$$\sum_{\substack{q \mid a'' \\ q \le n^{c+\epsilon}}} \frac{n \log\log n}{q \log n} \log q \le \frac{n \log\log n}{\log n} \sum_{q \le n^{c+\epsilon}} \frac{\log q}{q} \ll n \log\log n.$$

For the second sum, we use that the number of terms is bounded by $\omega(a)$. We obtain

$$\sum_{\substack{q \mid a'' \\ q > n^{c+\epsilon}}} \frac{n \log\log(q+1)}{q} \log q \le \omega(a) \cdot \frac{n \log\log(n^{c+\epsilon}+1)}{n^{c+\epsilon}} \log n^{c+\epsilon}$$

$$\ll n^c \cdot \frac{n \log\log n}{n^{c+\epsilon}} \log n \ll n^{1-(\epsilon/2)}$$

and

$$\sum_{\substack{q \mid a'' \\ q > n^{c+\epsilon}}} n^{3\delta} \log n \ll \omega(a) n^{3\delta} \log n.$$

Thus,

$$\sum_{q|a''} \nu_q(a'') \log q \ll n \log\log n + n^{1-(\epsilon/2)} + \omega(a) n^{3\delta} \log n.$$

By (15), this last sum must exceed $(1 + o(1))\delta n \log n$. Consequently,

$$\omega(a) n^{3\delta} \log n \gg n \log n.$$

Taking $\delta = 4/15 < 1/3$, the left-hand side is $\ll n$ and we reach the desired contradiction. Hence, the theorem is complete. $\square$

References

[1] G. Bachman, Introduction of p-adic numbers and valuation theory, Academic Press, New York, 1964.

[2] L. E. Dickson, *On the cyclotomic function*, Amer. Math. Monthly 12, No. 4 (1905), 86–89.

[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Fifth edition, Oxford Univ. Press, Oxford, 1989.

[4] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Second edition, Springer-Verlag, New York, 1990.

[5] F. Luca, *Equations involving arithmetic functions of factorials*, Divulg. Mat. 8 (2000), 15–23.

[6] F. Luca and I. Shparlinski, *Arithmetic Properties of the Ramanujan Function*, Proceedings of the Indian Academy of Sciences Mathematical Sciences, 116 (2006), 1–8.

[7] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika 20 (1973), 119–134.

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