On the Equation
$$\tau(\lambda(n)) = \omega(n) + k$$

A. GLIBICHUK, F. LUCA, & F. PAPPALARDI

1. Introduction

For every positive integer n, the function $\tau(n)$ counts the number of divisors of n, the function $\omega(n)$ counts the number of distinct prime divisors of n, and the Carmichael function $\lambda(n)$ is the exponent of the multiplicative group of the invertible congruence classes modulo n. The value of the function $\lambda(n)$ can be computed as follows:

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1; \\ 2^{\alpha - 2} & \text{if } n = 2^{\alpha}, \, \alpha > 2; \\ p^{\alpha - 1}(p - 1) & \text{if } n = p^{\alpha} \text{ and } p \ge 3 \text{ or } \\ [\lambda(p_1^{\alpha_1}), \dots, \lambda(p_s^{\alpha_s})] & \text{if } n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}. \end{cases}$$

In [6], Erdős, Pomerance, and Schmutz proved a number of fundamental properties of λ . In the process of proving the lower bound $\lambda(n) > (\log n)^{c_0 \log \log \log n}$ for all large n (provided $c_0 < 1/\log 2$), they proved the inequality

$$n \le (4\lambda(n))^{3\tau(\lambda(n))}.$$

Numerical calculations suggest that the stronger inequality

$$n \le \lambda(n)^{\tau(\lambda(n))} \tag{1}$$

holds except for n=2,6,8,12,24,80,120,240. This will be proved in Corollary 1. One of the tools for proving (1) is the inequality $\tau(\lambda(n)) > \omega(n)$, which holds except for n=2,6,12,24,30,60,120,240; we will prove this in Proposition 1 and Proposition 2.

This motivates us to compare $\tau(\lambda(n))$ with $\omega(n)$. Since $\tau(\lambda(n)) \ge \omega(n)$ holds for all positive integers n (see Proposition 1), we can write $\tau(\lambda(n)) = \omega(n) + k$, where k is some nonnegative integer depending on n. We then fix $k \ge 0$ and investigate the positive integers n such that $\tau(\lambda(n)) = \omega(n) + k$.

Throughout this paper, we use x to denote a positive real number. We also use the Landau symbols O and o and the Vinogradov symbols \gg and \ll with their

Received October 10, 2006. Revision received May 11, 2007.

F. L. and F. P. were supported in part by the Italian–Mexican Agreement of Scientific and Technological Cooperation 2003–2005: Kleinian Groups and Egyptian Fractions. A.G. was supported by Russia president's Grant RF NS-5813.2006.1.

usual meanings. We write $\log x$ for the maximum between 1 and the natural logarithm of x. For a set \mathcal{A} of positive integers we write $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$. We write p and q with or without subscripts for prime numbers.

Let us set

$$\mathcal{A}_k = \{n : \tau(\lambda(n)) = \omega(n) + k\}.$$

We will show in Theorem 3 that if k is a positive integer and

$$b_k = 2(k+1)^2 + 3 + \lfloor \log_2(2(k+1)^2 + k + 1) \rfloor,$$

then the upper bound

$$\#\mathcal{A}_k(x) \ll_k \frac{x(\log\log x)^{b_k}}{(\log x)^2}$$

holds as $x \to \infty$. Here, $\log_2 a$ stands for the base 2 logarithm of the positive number a. Furthermore, in Theorem 2, we will show that if k > 4 then the lower bound

 $\#\mathcal{A}_k(x) \gg_k \frac{x}{(\log x)^2}$

holds as $x \to \infty$. We will also give complete descriptions of the sets \mathcal{A}_0 , \mathcal{A}_1 , and \mathcal{A}_2 (Proposition 2, Proposition 3, and Proposition 4). We will show that \mathcal{A}_0 contains eight integers and that the infiniteness of \mathcal{A}_1 and \mathcal{A}_2 would follow if it were known that there exist infinitely many primes of the form 2q + 1 with q also prime. Finally, in Proposition 5 we deal with the cases k = 3, 4 and prove that, if either \mathcal{A}_3 or \mathcal{A}_4 are infinite, then there exists an even positive integer c such that the set of primes of the form $p = cq^{\beta} + 1$ (with q prime and $\beta \le 4$) is infinite. This explains the difficulty of proving the infiniteness of \mathcal{A}_k for k = 1, 2, 3, 4.

ACKNOWLEDGMENTS. This paper started during very enjoyable visits of A. G. to the Mathematics Department of the University Roma Tre and of F. P. to the Mathematical Institute of the UNAM in Morelia. These authors would like to thank these departments for their hospitality and support. The authors would also like to thank Sergei Konyagin for some useful comments.

2. Determining A_k for Small Values of k

Proposition 1. For any positive integer n, we have

$$\tau(\lambda(n)) \ge \omega(n)$$
.

More precisely,

$$\tau(\lambda(n)) \ge \omega(n/(2^{\infty}, n)) + \tau(\lambda^{o}(n')),$$

where n' is the product of the primes dividing n and where $\lambda^o(m)$ denotes the odd part of $\lambda(m)$. That is, $\lambda^o(m) = \lambda(m)/(2^\infty, \lambda(m))$.

Proof. Let us first note that, if $n \mid m$, then $\lambda(n) \mid \lambda(m)$ and therefore $\tau(\lambda(n)) \le \tau(\lambda(m))$. Thus, we can assume that n is square-free (indeed, if n' is the product of the distinct primes dividing n, then $\omega(n) = \omega(n')$ and $\tau(\lambda(n)) \ge \tau(\lambda(n'))$).

Suppose that n is odd and $n = p_1 p_2 \cdots p_r$, where $p_1 < \cdots < p_r$ are primes. Let $2 < q_2 < \cdots < q_s$ be all the odd prime factors of $\lambda(n)$ and write

$$p_{1} - 1 = 2^{\alpha_{11}} q_{2}^{\alpha_{12}} \cdots q_{s}^{\alpha_{1s}},$$

$$p_{2} - 1 = 2^{\alpha_{21}} q_{2}^{\alpha_{22}} \cdots q_{s}^{\alpha_{2s}},$$

$$\vdots$$

$$p_{r} - 1 = 2^{\alpha_{r1}} q_{2}^{\alpha_{r2}} \cdots q_{s}^{\alpha_{rs}}.$$

If $A_i = \max\{\alpha_{1i}, \dots, \alpha_{ri}\}\$ for $i = 1, \dots, s$, then

$$\tau(\lambda(n)) = \tau([p_1 - 1, \dots, p_r - 1]) = (A_1 + 1)(A_2 + 1) \cdots (A_s + 1).$$

Consider now the matrix

$$\begin{pmatrix} \alpha_{11} & \dots & \alpha_{1s} \\ \vdots & & \vdots \\ \alpha_{r1} & \dots & \alpha_{rs} \end{pmatrix}.$$

We know that the entries of the matrix consist of nonnegative integers. The elements in the first column are positive and less than or equal to A_1 . For each i = 1, ..., r, the elements of the ith column are nonnegative integers less than or equal to A_i .

Furthermore, for each fixed natural number s, the number of rows r is less than or equal to the maximum number of distinct s-tuples (a_1, \ldots, a_s) with $a_1 \in [1, A_1]$ and $a_i \in [0, A_i]$ for $i = 2, \ldots, s$. This follows because $\left(2^{\alpha_{i1}} \prod_{j=2}^{s} q_j^{\alpha_{ij}}\right)_{i=1,\ldots,s}$ are distinct positive integers. Hence,

$$r \leq A_1(A_2+1)\cdots(A_s+1).$$

From the foregoing discussion we deduce that

$$\tau(\lambda(n)) = (A_1 + 1)(A_2 + 1) \cdots (A_s + 1)$$

> $r + \tau(\lambda^o(n)) = \omega(n) + \tau(\lambda^o(n)),$

where $\lambda^o(n) = \lambda(n)/(2^\infty, \lambda(n))$ is the largest odd divisor of $\lambda(n)$. As a result, if n is square-free and odd then

$$\tau(\lambda(n)) \ge \omega(n) + 1$$
,

but if n is square-free and even then

$$\tau(\lambda(n)) = \tau(\lambda(n/2)) \ge \omega(n/2) + 1 = \omega(n);$$

this concludes the proof.

Lemma 1 is the main tool we use to determine the set A_k for $k \leq 2$.

Proposition 2. $A_0 = \{2, 6, 12, 24, 30, 60, 120, 240\}.$

Proof. Let $n \in A_0$. Applying Lemma 1, we obtain that if n is odd then $\tau(\lambda(n)) > \omega(n)$, which is impossible.

If *n* is even then, by Lemma 1, the condition $\tau(\lambda(n)) = \omega(n)$ implies that

$$\tau(\lambda^o(n')) = 1.$$

This is possible only if $\lambda(n') = 2^{\alpha}$ for some $\alpha \in \mathbb{N}$. If $n = 2^{\gamma}$ and $\tau(\lambda(2^{\gamma})) = 1$, then $\gamma = 1$ and so n = 2.

Assume now that n is not a power of 2 and write

$$n = 2^{\gamma_0} (2^{2^{\alpha_1}} + 1)^{\gamma_1} \cdots (2^{2^{\alpha_r}} + 1)^{\gamma_r},$$

where $\gamma_j \geq 1$ (j = 0, ..., r), $0 \leq \alpha_1 < \cdots < \alpha_r$, and the numbers $2^{2^{\alpha_i}} + 1$ are primes for each i = 1, ..., r. Plugging our expression for n into the identity $\tau(\lambda(n)) = \omega(n)$ yields

$$\max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1\} \cdot \gamma_1 \cdots \gamma_r = r + 1,$$

which is satisfied only for r=1 or r=2 (because we can now gather that $r+1 \ge 2^{\alpha_r}+1 \ge 2^{r-1}+1$).

If r=2 then necessarily $\alpha_2=1$. This forces $\alpha_1=0$, $\gamma_1=\gamma_2=1$, and $1 \le \gamma_0 \le 4$, which correspond to the four values for n of 30, 60, 120, and 240. Finally, if r=1 then $\alpha_1=0$; this forces $\gamma_1=1$ and $1 \le \gamma_0 \le 3$, which correspond to the three values for n of 6, 12, and 24.

We are now ready to prove the motivating inequality (1).

COROLLARY 1. Let φ denote the Euler function. Excepting only n=2,6,8,12,24,80,120,240, we have

$$n < \lambda(n)^{\tau(\lambda(n))}$$
.

Furthermore, $\varphi(n) \leq \lambda(n)^{\tau(\lambda(n))}$ except for n = 24. Finally, the inequality $\varphi(n) \leq \lambda(n)^{\omega(n)}$ holds unless n is a power of 2 times a product of distinct Fermat primes.

Proof. Let $v_p(m)$ be the exponent of the prime p in the factorization of the positive integer m. We know that $\lambda(n)$ divides $\varphi(n)$. We also know that if p odd then

$$\begin{split} v_p(\varphi(n)) &= \sum_{l^\beta \parallel n} v_p(l^{\beta-1}(l-1)) \\ &\leq \omega(n) \bigg(\max_{l^\beta \parallel n} \{ v_p(l^{\beta-1}(l-1)) \} \bigg) \leq v_p(\lambda(n)^{\omega(n)}), \end{split}$$

while $v_2(\varphi(n)) = v_2(n) - 1 + \sum_{l|n} v_2(l-1) \le 1 + \omega(n)v_2(\lambda(n))$.

Necessarily, then, $\varphi(n) \mid 2\lambda(n)^{\omega(n)}$. Furthermore, the only circumstances in which $\varphi(n) = 2\lambda(n)^{\omega(n)}$ is when $\varphi(n)$ is a power of 2. If this happens, then n is necessarily a power of 2 times a product of distinct Fermat primes. In all other cases we have $\varphi(n) \leq \lambda(n)^{\omega(n)}$, and this proves the third inequality.

In order to prove the second, it is enough to notice that $\tau(\lambda(n)) \geq \omega(n)$ by Proposition 1; hence we need only show that $\varphi(n) \leq \lambda(n)^{\tau(\lambda(n))}$ when $\varphi(n) = 2^a$ and $n \neq 24$. Observe that the latter is certainly true when n is a power of 2, since $\varphi(2^{\alpha}) = 2^{\alpha-1} \leq 2^{(\alpha-2)(\alpha-1)} = \lambda(2^{\alpha})^{\tau(\lambda(2^{\alpha}))}$ for $\alpha > 2$. In the other cases, if we write

$$n = 2^{\alpha_0} \cdot (2^{2^{\alpha_1}} + 1) \cdot \cdot \cdot (2^{2^{\alpha_r}} + 1)$$

with $\alpha_1 < \cdots < \alpha_r$, then

$$\varphi(n) = 2^{2^{\alpha_1} + \dots + 2^{\alpha_r} + \max\{\alpha_0 - 1, 0\}}$$

$$\leq 2^{2^{\alpha_r}(1 + 1/2 + \dots + 1/2^{r-1}) + \max\{\alpha_0 - 1, 0\}} \leq 2^{3M+1},$$

where $M = \max\{\log_2(\lambda(2^{\alpha_0}), 2^{\alpha_r}\}\)$. Similarly,

$$\lambda(n)^{\tau(\lambda(n))} = 2^{M(M+1)}.$$

Finally, $3M+1 \le M(M+1)$ for M>2 while for $M\le 2$ we have $r\le 2$ and so $n\in\{3,6,12,24,48,5,10,20,40,80,15,30,60,120,240\}$; the only value of n from this set that does not satisfy the inequality $\varphi(n)\le \lambda(n)^{\tau(\lambda(n))}$ is n=24. This completes the proof of the second statement.

Observe that for $n \in A_0$ the first statement holds if and only if $n \in \{30, 60\}$. So we can assume that $n \notin A_0$ and thus $\tau(\lambda(n)) \ge \omega(n) + 1$. This implies that

$$\lambda(n)^{\tau(\lambda(n))} \ge \lambda(n)\varphi(n)$$

unless $\varphi(n)$ is a power of 2. In order to conclude the proof we must verify that the statement holds when $\varphi(n)$ is a power of 2 and $n \neq 2, 8$, and we must also show that

$$\lambda(n)\varphi(n) \geq n$$
.

We claim that this inequality holds unless $n \in \{2, 3, 6, 12, 24\}$ (values for which the statement is verified directly). Indeed, let p be the greatest prime divisor of n. If $p \ge 5$, then

$$\frac{n}{\varphi(n)} = \prod_{l|n} \frac{l}{l-1} \le \frac{3}{4}p \le p-1 \le \lambda(n).$$

Similarly, if p = 3, then $n/\varphi(n) \le 3 \le \lambda(n)$ unless $n \in \{3, 6, 12, 24\}$. Finally, if p = 2, then $n/\varphi(n) = 2 \le \lambda(n)$ unless n = 2.

If $\varphi(n)$ is a power of 2, we proceed as in the proof of the second inequality. Observe that if $n=2^{\alpha_0}$ then $n\leq \lambda(n)^{\tau(\lambda(n))}$ unless $\alpha_0=1,3$. If $n=2^{\alpha_0}\cdot(2^{2^{\alpha_1}}+1)\cdots(2^{2^{\alpha_r}}+1)$ with $\alpha_1<\cdots<\alpha_r$ and if $M=\max\{\log_2(\lambda(2^{\alpha_0}),2^{\alpha_r}\}$ so that $2^{M(M+1)}=\lambda(n)^{\tau(\lambda(n))}$, then

$$n \le 2^{2(2^{\alpha_1} + \dots + 2^{\alpha_r}) + \alpha_0} \le 2^{5M+2}$$
.

Since $5M + 2 \le M(M + 1)$ for M > 5, we are left with checking the statement for integers that divide $2^7 \cdot 3 \cdot 5 \cdot 17$, and this is done by a short calculation.

Proposition 3.

$$A_1 = \{1, 3, 4, 8, 10, 15, 20, 40, 48, 80, 126, 252, 480, 504, 510, 1020, 2040, 2730, 4080, 5460, 8160, 8190, 10920, 16320, 16380, 21840, 32760, 65520, 6q, 12q, 24q\},$$

where q = 2p + 1 is prime with p > 2 also prime.

Proof. We follow the same method as in the proof of Proposition 2.

If n > 1 is odd then, by Lemma 1, $\lambda^o(n') = 1$. This implies that $\lambda(n') = 2^{\alpha}$ for some $\alpha \ge 0$. Thus,

$$n = (2^{2^{\alpha_1}} + 1)^{\gamma_1} \cdots (2^{2^{\alpha_r}} + 1)^{\gamma_r},$$

where $\gamma_j \ge 1$ (j = 1, ..., r), $0 \le \alpha_1 < \cdots < \alpha_r$, and again $2^{2^{\alpha_i}} + 1$ is prime for i = 1, ..., r.

The equation $\tau(\lambda(n)) = \omega(n) + 1$ is equivalent to

$$(2^{\alpha_r}+1)\gamma_1\cdots\gamma_r=r+1.$$

Since $\alpha_r \ge r - 1$, the preceding equality is satisfied only if r = 1 or r = 2. If r = 1 then necessarily $\alpha_1 = 0$ and $\gamma_1 = 1$, so n = 3. If r = 2 then we have $\alpha_1 = 0$, $\alpha_2 = 1$, and $\gamma_1 = \gamma_2 = 1$, so n = 15.

Assume now that *n* is even. If $n = 2^{\gamma}$, then $\tau(\lambda(n)) = 2$ is satisfied only for n = 4 or n = 8.

If *n* is not a power of 2, then Lemma 1 yields $\tau(\lambda^o(n')) \le 2$. This can happen only if $\lambda(n') = 2^a$ or $\lambda(n') = 2^a p$ with *p* an odd prime. If $\lambda(n') = 2^a$ then

$$n = 2^{\gamma_0} \cdot (2^{2^{\alpha_1}} + 1)^{\gamma_1} \cdot \cdot \cdot (2^{2^{\alpha_r}} + 1)^{\gamma_r},$$

where $\gamma_j \ge 1$ (j = 0, ..., r), $0 \le \alpha_1 < \cdots < \alpha_r$, and again $2^{2^{\alpha_i}} + 1$ is prime for i = 1, ..., r.

If we plug the preceding expression for *n* into the identity $\tau(\lambda(n)) = \omega(n) + 1$, we obtain

$$\max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1\} \cdot \gamma_1 \cdots \gamma_r = r + 2,$$

which can only be satisfied for $r \le 3$ because $r + 2 \ge 2^{\alpha_r} + 1 \ge 2^{r-1} + 1$. A quick computation shows that $\gamma_j = 1$ for all $j \ge 1$, and we have only the following possibilities:

r	$(\alpha_1,\ldots,\alpha_r)$	n
1	(0)	48
	(1)	10, 20, 40, 80
2		_
3	(0, 1, 2)	510, 1020, 2040, 4080, 8160, 16320

The next case to consider is when $\lambda(n') = 2^a p$, so that each odd prime dividing n is of the form $2^{2^{\alpha}} + 1$ or of the form $2^{\beta}p + 1$. Hence,

$$n = 2^{\gamma_0} \cdot (2^{2^{\alpha_1}} + 1)^{\gamma_1} \cdots (2^{2^{\alpha_r}} + 1)^{\gamma_r} \cdot (2^{\beta_1}p + 1)^{\gamma_{r+1}} \cdots (2^{\beta_s}p + 1)^{\gamma_{r+s}},$$

where $\gamma_j \ge 1$ (j = 0, ..., r + s), $0 \le \alpha_1 < \cdots < \alpha_r$, $2^{2^{\alpha_i}} + 1$ is prime for $i = 1, ..., r, 1 < \beta_1 < \cdots < \beta_s$, and $2^{\beta_k}p + 1$ is prime for k = 1, ..., s.

We now distinguish two more subcases: $p^2 \mid n$ and $p^2 \nmid n$. If $p^2 \mid n$, then the equation $\tau(\lambda(n)) = \omega(n) + 1$ translates into

$$\max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1, \beta_s + 1\} \cdot \gamma_1 \cdots \gamma_{r+s} = r + s + 2. \tag{2}$$

In this case, there exists a $j \le r$ such that $\gamma_j \ge 2$; since $\max\{a,b\} \ge (a+b)/2$, the LHS of (2) is greater than or equal to $2^{\alpha_r} + 1 + \beta_s + 1$. Using that $\alpha_r \ge r - 1$

and $\beta_s \ge s$, we once again obtain $2^{r-1} + 1 \le r + 1$, which implies that r = 1 or r = 2.

If r=1, then necessarily $\alpha_1=0$, $\gamma_1=2$, s=1, and $\beta_1=\gamma_2=1$. This implies that $n=2^{\gamma_0}\cdot 3^2\cdot 7$ and $\gamma_0=1,2,3$. If r=2, then necessarily $\alpha_1=0$, $\alpha_2=1$, and $s\leq 2$ (since the LHS of (2) is greater than or equal to 2s+2). Checking all possibilities, we find that $n=2^{\gamma_0}\cdot 3^2\cdot 5\cdot 7\cdot 13$ and $\gamma_0=1,2,3,4$.

For the other subcase, if $p^2 \nmid n$ then the equation $\tau(\lambda(n)) = \omega(n) + 1$ translates into

$$2 \cdot \max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1, \beta_s + 1\} \cdot \gamma_1 \cdots \gamma_{r+s} = r + s + 2. \tag{3}$$

For the same reasons as before, it follows that r=1 or r=2 and s=1 or s=2. If r=s=1 then we have the family of solutions $n=2^{\gamma_0}\cdot 3\cdot (2p+1)$, where $\gamma_0=1,2,3$ and 2p+1 is prime with $p\geq 3$. If r=s=2 then we have the solutions $n=2^{\gamma_0}\cdot 3\cdot 5\cdot 7\cdot 13$, where $\gamma_0=1,2,3,4$. The remaining cases (r=1,s=2;r=2,s=1) produce for the RHS of (3) a value equal to 5 and so do not lead to any more solutions.

PROPOSITION 4. We have that $A_2 = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3 \cup \mathcal{F}_4 \cup \mathcal{I}_1 \cup \mathcal{I}_2 \cup \mathcal{I}_3$, where:

$$\mathcal{F}_{1} = \begin{cases} 5, 2^{4}, 2^{5} \cdot 3, 2^{5} \cdot 5, 2^{\beta} \cdot 3^{2}, 2^{6} \cdot 3 \cdot 5, \\ 2^{\alpha} \cdot 3 \cdot 17, 2^{\alpha} \cdot 5 \cdot 17, 3 \cdot 5 \cdot 17, \\ 2^{7} \cdot 3 \cdot 5 \cdot 17 \end{cases} \begin{vmatrix} 1 \leq \alpha \leq 6, \\ 1 \leq \beta \leq 3 \end{cases},$$

$$\mathcal{F}_{2} = \begin{cases} 2^{\alpha} \cdot 3^{\beta} \cdot 5 \cdot 7, 3^{\beta} \cdot 7, 3^{\beta} \cdot 5 \cdot 7 \cdot 13 \\ 2^{\alpha} \cdot 3^{\beta} \cdot 5 \cdot 13, 2^{\alpha} \cdot 3^{\beta} \cdot 7 \cdot 13, \\ 2^{\alpha} \cdot 5 \cdot 7 \cdot 13 \end{vmatrix} \begin{vmatrix} 1 \leq \alpha \leq 4, \\ \beta = 1, 2 \end{vmatrix},$$

$$\mathcal{F}_{3} = \{ 2^{\alpha} \cdot 3 \cdot 5^{2} \cdot 11 \mid 1 \leq \alpha \leq 4 \},$$

$$\mathcal{F}_{4} = \begin{cases} 2^{\delta} \cdot 3^{\beta} \cdot 7 \cdot 19, \\ 2^{\alpha} \cdot 3^{\beta} \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \end{vmatrix} \begin{vmatrix} 1 \leq \alpha \leq 4, \\ 1 \leq \beta, \delta \leq 3 \end{cases},$$

$$\mathcal{I}_{1} = \{ 2^{\alpha} \cdot (2p+1) \mid 2p+1, p \geq 3 \text{ primes}, 1 \leq \alpha \leq 3 \},$$

$$\mathcal{I}_{2} = \{ 3 \cdot (2p+1) \mid 2p+1, p \geq 3 \text{ primes}, 1 \leq \alpha \leq 3 \},$$

$$\mathcal{I}_{3} = \{ 2^{\alpha} \cdot 3 \cdot 5 \cdot (2^{\beta}p+1) \end{vmatrix} \begin{vmatrix} 2^{\beta}p+1, p \geq 3 \text{ primes}, \\ 1 \leq \alpha \leq 4, \beta = 1, 2 \end{cases}.$$

Proof. We follow the same approach as in the previous results and obtain that, in order for n to satisfy $\tau(\lambda(n)) = \omega(n) + 2$, we must have $\lambda(n') = 2^{\alpha} p^{\beta}$ with $\alpha \ge 0$ and $\beta = 0, 1, 2$. This implies that n should be of the form

$$n = 2^{\gamma_0} \cdot A \cdot B \cdot C$$

where A, B, and C are either 1 or of the respective forms

$$A = (2^{2^{\alpha_1}} + 1)^{\gamma_1} \cdots (2^{2^{\alpha_r}} + 1)^{\gamma_r},$$

$$B = (2^{\beta_1}p + 1)^{\gamma_{r+1}} \cdots (2^{\beta_s}p + 1)^{\gamma_{r+s}},$$

$$C = (2^{\delta_1}p^2 + 1)^{\gamma_{r+s+1}} \cdots (2^{\delta_t}p^2 + 1)^{\gamma_{r+s+t}}.$$

Here we assume the following conditions: $\gamma_j \ge 1$ for $j = 0, ..., r + s + t, 0 \le \alpha_1 < \cdots < \alpha_r, 2^{2^{\alpha_i}} + 1$ is prime for $i = 1, ..., r, 1 < \beta_1 < \cdots < \beta_s, 2^{\beta_k} p + 1$ is prime for $k = 1, ..., s, 1 < \delta_1 < \cdots < \delta_t$, and $2^{\delta_l} p^2 + 1$ is prime for l = 1, ..., t. We allow any one of r, s, t, γ_0 to be zero with the obvious meaning.

The equation $\tau(\lambda(n)) = \omega(n) + 2$ is equivalent to

$$\Theta \cdot \Lambda \cdot \gamma_1 \cdots \gamma_{r+s+t} = r + s + t + \min\{1, \gamma_0\} + 2,\tag{4}$$

where:

$$\Theta = \begin{cases} 1 & \text{if } (s+t > 0 \text{ and } p^3 \mid n) \text{ or } (s+t = 0) \\ & \text{or } (t = 0, s > 0 \text{ and } p^2 \mid\mid n); \end{cases}$$

$$3/2 & \text{if } t > 0 \text{ and } p^2 \mid\mid n;$$

$$2 & \text{if } t = 0, s > 0, \text{ and } p^2 \nmid n;$$

$$3 & \text{if } t > 0 \text{ and } p^2 \nmid n;$$

and $\Lambda = \max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1, \beta_s + 1, \delta_t + 1\}$. The terms $\beta_s + 1$ (resp. $\delta_t + 1$) should be omitted if s = 0 (resp. t = 0).

If s = t = 0, then these remarks imply that $r \leq 3$ and

$$n = 2^{\delta_0} \cdot 3^{\delta_1} \cdot 5^{\delta_2} \cdot 17^{\delta_3}.$$

In this case, all possible solutions of $\tau(\lambda(n)) = \omega(n) + 2$ are

r	$(\delta_0, \delta_1, \delta_2, \delta_3)$	n
0	(4, 0, 0, 0)	2^{4}
1	(0,0,1,0)	5
	$(\delta, 2, 0, 0), \delta = 1, 2, 3$	$2 \cdot 3^2, 2^2 \cdot 3^2, 2^3 \cdot 3^2$
	(5, 1, 0, 0)	$2^5 \cdot 3$
	(5,0,1,0)	$2^5 \cdot 5$
2	(6, 1, 1, 0)	$2^6 \cdot 3 \cdot 5$
	$(\delta, 1, 0, 1), 1 \le \delta \le 6$	$2^{\delta} \cdot 3 \cdot 17, 1 \leq \delta \leq 6$
	$(\delta, 0, 1, 1), 1 \le \delta \le 6$	$2^{\delta} \cdot 5 \cdot 17, 1 \leq \delta \leq 6$
3	(0, 1, 1, 1)	$3 \cdot 5 \cdot 17$
	(7, 1, 1, 1)	$2^7 \cdot 3 \cdot 5 \cdot 17$

These solutions are exactly the 22 elements of \mathcal{F}_1 .

When t = 0 and $s \neq 0$, equation (4) simplifies to

$$\Theta \cdot \Lambda \cdot \gamma_1 \cdots \gamma_{r+s} = r + s + \min\{1, \gamma_0\} + 2, \tag{5}$$

where:

$$\Theta = \begin{cases} 1 & \text{if } p^2 \mid n, \\ 2 & \text{if } p^2 \nmid n; \end{cases}$$

 $\Lambda = \max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1, \beta_s + 1\}$, and the middle term is omitted if r = 0. In such a case, we have $p \nmid n$ and $s \leq \beta_s \leq (s + \min\{1, \gamma_0\})/2$. This is possible only for n even and $s = \beta_s = 1$. This implies that $n = 2^{\gamma_0}(2p + 1)$ with $\gamma_0 = 1, 2, 3$, which are exactly the elements of \mathcal{I}_1 .

If r > 0 then the LHS of (5) is greater than or equal to $2^{\alpha_r} + \beta_s + 2$, which implies that $2^{\alpha_r} \le r + \min\{1, \gamma_0\}$. From this inequality it follows that $r \le 2 + \min\{1, \gamma_0\}$.

We distinguish the two subcases p=3 and p>3. In the first subcase, $s \le r + \min\{1, \gamma_0\}$ and $\beta_s \le (r+s+\min\{1, \gamma_0\})/2$. This implies that

$$n = 2^{\delta_0} \cdot 3^{\delta_1} \cdot 5^{\delta_2} \cdot 7^{\delta_3} \cdot 13^{\delta_4}.$$

In this subcase, all possible solutions of $\tau(\lambda(n)) = \omega(n) + 2$ are

$$\begin{array}{lll} (r,s) & (\delta_0,\delta_1,\delta_2,\delta_3,\delta_4) & n \\ \hline (1,1) & (0,\delta,0,1,0), \, \delta=1,2 & 3\cdot 7,3^2\cdot 7 \\ (1,2) & (\delta,1,0,1,1), \, 1\leq \delta \leq 4 & 2^\delta\cdot 3\cdot 7\cdot 13 \\ & (\delta,2,0,1,1), \, 1\leq \delta \leq 4 & 2^\delta\cdot 3^2\cdot 7\cdot 13 \\ & (\delta,0,1,1,1), \, 1\leq \delta \leq 4 & 2^\delta\cdot 5\cdot 7\cdot 13 \\ (2,2) & (0,1,1,1) & 3\cdot 5\cdot 7\cdot 13 \\ & (0,2,1,1,1) & 3^2\cdot 5\cdot 7\cdot 13 \\ (2,1) & (\delta,1,1,1,0), \, 1\leq \delta \leq 4 & 2^\delta\cdot 3\cdot 5\cdot 7 \\ & (\delta,2,1,1,0), \, 1\leq \delta \leq 4 & 2^\delta\cdot 3^2\cdot 5\cdot 7 \\ & (\delta,2,1,1,0,1), \, 1\leq \delta \leq 4 & 2^\delta\cdot 3^2\cdot 5\cdot 13 \\ & (\delta,2,1,0,1), \, 1\leq \delta \leq 4 & 2^\delta\cdot 3^2\cdot 5\cdot 13 \\ \end{array}$$

These solutions are exactly the 32 elements of \mathcal{F}_2 .

In the subcase where r > 0, s > 0, t = 0, and p > 3, we have $\beta_s \ge 2s - 1$. Thus,

$$2^{\alpha_r} + 2s + 1 \le 2^{\alpha_r} + \beta_s + 2 \le r + s + \min\{\gamma_0, 1\} + 2$$

and $s \le r+1+\min\{\gamma_0,1\}-2^{\alpha_r} \le 1$, which implies that s=1 and $\beta_1 \le 2$. Note that $\alpha_r \le 1$ and note also that r cannot be 3 since this would imply $s=1,2^{\alpha_r}+1 \ge 5$, $\tau(\lambda(n)) \ge 10$, and $\omega(n) \ge 8$, which is impossible because $\omega(n) \le r+s+3 \le 7$. Therefore.

$$n = 2^{\delta_0} \cdot 3^{\delta_1} \cdot 5^{\delta_2} \cdot (2^{\beta_1}p + 1)^{\delta_3}$$

with p > 3. If $5^2 \mid n$ then we have the solutions $n = 2^{\alpha} \cdot 3 \cdot 5^2 \cdot 11$ ($\alpha = 1, 2, 3, 4$), which are exactly the elements of \mathcal{F}_3 . If $5^2 \nmid n$ then we have the solutions $n = 3 \cdot (2p + 1)$, which are elements of \mathcal{I}_2 , and $n = 2^{\alpha} \cdot 3 \cdot 5 \cdot (2^{\beta} + 1)$ with $\alpha = 1, 2, 3, 4$ and $\beta = 1, 2$, which are elements of \mathcal{I}_3 .

The last case to consider is when t > 0, so that there is a prime dividing n of the form $2^{\beta} \cdot p^2 + 1$. Now equation $\tau(\lambda(n)) = \omega(n) + 2$ is equivalent to

$$\Theta \cdot \Lambda \cdot \gamma_1 \cdots \gamma_{r+s+t} = r + s + t + \min\{1, \gamma_0\} + 2, \tag{6}$$

where

$$\Theta = \begin{cases} 1 & \text{if } p^3 \mid n, \\ 3/2 & \text{if } p^2 \parallel n, \\ 3 & \text{if } p^2 \nmid n, \end{cases}$$

and $\Lambda = \max\{\tau(\lambda(2^{\gamma_0})), 2^{\alpha_r} + 1, \beta_s + 1, \delta_t + 1\}$. Here the terms $2^{\alpha_r} + 1$ (resp. $\beta_s + 1$) are to be omitted if r = 0 (resp. s = 0).

We claim that $r, s \neq 0$ (and will show this later). Hence, from (6) we may deduce that

$$2^{\alpha_r} + \beta_s + \delta_t + 3 \le r + s + t + \min\{1, \gamma_0\} + 2.$$

On one hand, this relation implies that $2^{\alpha_r} \le r - 1 + \min\{1, \gamma_0\}$, so that $\gamma_0 \ge 1$ and either r = 1 and $\alpha_1 = 0$ or r = 2, $\alpha_2 = 1$, and $\alpha_1 = 0$. On the other hand, the same relation implies that $s + t \le \beta_s + \delta_t \le 2r$.

If r = 1 then $s = t = \beta_s = \delta_t = 1$, and since $2p^2 + 1$ is prime we necessarily have p = 3. Therefore,

$$n = 2^{\gamma_0} \cdot 3^{\gamma_1} \cdot 7^{\gamma_2} \cdot 19^{\gamma_3}$$

and the only solutions of $\tau(\lambda(n)) = 6$ of this form are the first nine elements of \mathcal{F}_4 . If r = 2, then $4 \le s + t \le \beta_s + \delta_t \le 4$. This implies that s = t = 2 and $(\beta_1, \beta_2, \delta_1, \delta_2) = (1, 2, 1, 2)$; hence p = 3,

$$n = 2^{\gamma_0} \cdot 3^{\gamma_1} \cdot 5^{\gamma_2} \cdot 7^{\gamma_3} \cdot 13^{\gamma_3} \cdot 19^{\gamma_4} \cdot 37^{\gamma_5},$$

and the only solutions of $\tau(\lambda(n)) = 9$ of this form are the last twelve elements of \mathcal{F}_4 .

Finally, we must prove the claim for $r, s \neq 0$. If r = 0 and $s \neq 0$ then we deduce from (6) that

$$3(s+t+2)/2 \le 3(\beta_s+\delta_t+2)/2 \le s+t+3$$
,

which implies $s+t \le 0$ —a contradiction. A similar argument rules out the possibility r=0 and s=0. Lastly, if $r \ne 0$ and s=0, then from (6) and from $\delta_t \ge t$ we deduce that

$$3(2^{\alpha_r} + t + 2)/2 \le r + t + 3,$$

which is also a contradiction and thus ends the proof of the proposition. \Box

3. Lower Bounds on the Counting Functions of A_k

THEOREM 1. A_k is nonempty for all nonnegative integers k.

Proof. Let $p_1=3$, $p_2=5$, $p_3=13$, and $p_4=31$. Then, for each $m\geq 3$ and for each $t\in\{4,5,6,7\}$, the number $n=2^{m+1}\cdot 7\cdot 11\cdot p_1\cdots p_{t-3}$ satisfies $\omega(n)=t$ and $\tau(\lambda(n))=\tau(2^{m-1}\cdot 3\cdot 5)=4m$. This means that $\tau(\lambda(n))-\omega(n)=4(m-1)-(t-4)$ can assume all possible values ≥ 8 . Finally, $3\in\mathcal{A}_0$, $4\in\mathcal{A}_1$, $5\in\mathcal{A}_2$, $7\in\mathcal{A}_3$, $17\in\mathcal{A}_4$, $13\in\mathcal{A}_5$, $62\in\mathcal{A}_6$, and $31\in\mathcal{A}_7$. This completes the proof.

In what follows, we show that if k is sufficiently large, then A_k contains "many" elements.

THEOREM 2. For all $k \neq 0, 1, 2, 3, 4$, we have the lower bound

$$\#\mathcal{A}_k(x) \gg_k \frac{x}{(\log x)^2} \text{ as } x \to \infty.$$

Proof. The proof uses the famous Theorem of Chen that we state in the following form (see also [4; 7, Lemma 1.2; 8, Chap. 11]).

LEMMA 1. Let $a \in \mathbb{N}$ be an even number. There exists a constant c = c(a) such that, if $x > x_0(a)$, then the number of primes $p \in [x/2, x]$ such that $p \equiv 1 \pmod{a}$ and (p-1)/a has at most two prime factors, each of which exceeds $x^{1/10}$, is at least $c_a x/(\log x)^2$.

We write k = 4s + r for $s \ge 1$ and $r \in \{0, 1, 2, 3\}$, distinguishing two cases as follows:

Case 1. $r \neq 3$; Case 2. r = 3.

In Case 1, we apply Chen's theorem with the choice $a=2^s$ and obtain that there are either (a) at least $M_a \gg_a x/(\log x)^2$ primes $p \le x/42$ with $p-1=2^sq$ and q prime or (b) at least $N_a \gg_a x/(\log x)^2$ primes $p \le x/42$ with $p-1=2^sq_1q_2$, where q_1 and q_2 are distinct primes exceeding $x^{1/10}$.

For (a), consider the M_a integers $n \le x$ of the form n = 7pT, where

$$T = \begin{cases} 1 & \text{if } r = 2, \\ 2 & \text{if } r = 1, \\ 6 & \text{if } r = 0. \end{cases}$$

These choices yield $\omega(n) = 4 - r$, $\lambda(n) = 2^s \cdot 3 \cdot q$, and $\tau(\lambda(n)) = 4(s+1)$; therefore, $\tau(\lambda(n)) - \omega(n) = 4s + r = k$.

For (b), consider the N_a integers $n \le x$ of the form n = 2pT, where

$$T = \begin{cases} 1 & \text{if } r = 2, \\ 3 & \text{if } r = 1, \\ 15 & \text{if } r = 0. \end{cases}$$

For $s \ge 2$ and for s = 1 with $r \ne 0$, we have $\omega(n) = 4 - r$, $\lambda(n) = 2^s \cdot q_1 \cdot q_2$, and $\tau(\lambda(n)) = 4(s+1)$, so that again $\tau(\lambda(n)) - \omega(n) = k$.

In Case 2, we apply Chen's theorem with the choice $a = 2^{s+1}$ and obtain that there are either (a) at least $M_a \gg_a x/(\log x)^2$ primes $p \le x/510$ with $p-1 = 2^{s+1}q$ and q prime or (b) at least $N_a \gg_a x/(\log x)^2$ primes $p \le x/510$ with $p-1 = 2^{s+1}q_1q_2$, where q_1 and q_2 are distinct primes that exceed $x^{1/10}$.

Given (a), consider the M_a integers $n \le x$ of the form n = 210p. For $s \ge 1$ we have $\omega(n) = 5$ and $\tau(\lambda(n)) = 4(s+2)$, so $\tau(\lambda(n)) - \omega(n) = 4s + 3 = k$. Given (b), consider the N_a integers $n \le x$ of the form n = 510p. For $s \ge 3$ we have $\omega(n) = 5$ and $\tau(\lambda(n)) = 4(s+2)$, so again $\tau(\lambda(n)) - \omega(n) = 4s + 3 = k$.

Next assume that k=7. Then we apply Chen's theorem with the choice a=2 and obtain that there are either (a) at least $M_a \gg_a x/(\log x)^2$ primes $p \le x/192$ with p-1=2q and q prime or (b) at least $N_a \gg_a x/(\log x)^2$ primes $p \le x/192$ with $p-1=2q_1q_2$, where q_1 and q_2 are distinct primes exceeding $x^{1/10}$.

For (a), consider the M_a integers $n \le x$ of the form $n = 2^6 3p$. We have $\omega(n) = 3$ and $\tau(\lambda(n)) = \tau(2^4p)$, so $\tau(\lambda(n)) - \omega(n) = 10 - 3 = 7$. For (b), consider the N_a integers $n \le x$ of the form $n = p = 2q_1q_2 + 1$. We have $\omega(n) = 1$ and $\tau(\lambda(n)) = 8$, so again $\tau(\lambda(n)) - \omega(n) = 8 - 1 = 7$.

Finally, we treat the case k=11. Here we apply Chen's theorem with the choice a=4 and deduce that either (a) there exist $M\gg x/(\log x)^2$ primes $p\le x/4510$ such that p-1=4q with q prime or (b) there exist $N\gg x/(\log x)^2$ primes $p\le x/4510$ such that $p-1=4q_1q_2$, where q_1 and q_2 are distinct primes that exceed $x^{1/10}$.

Given (a), we note that, for large x, all M positive integers $n=2\cdot 5\cdot 11\cdot 41\cdot p=4510p$ (where $p\leq x$ is of the form 4q+1) are $\leq x$ and satisfy both $\omega(n)=5$ and $\lambda(n)=2^3\cdot 5\cdot q$; hence $\tau(\lambda(n))=16=\omega(n)+11$. Given (b), it follows that, for large x, the N positive integers n=p (where $p\leq x$ is such that $p-1=4q_1q_2$, with distinct primes q_1 and q_2 that exceed $x^{1/10}$) have the property that $\tau(\lambda(n))=\tau(4q_1q_2)=12=\omega(n)+11$. Thus, $\#\mathcal{A}_{11}(x)\geq \max\{M,N\}\gg x/(\log x)^2$, which completes the proof of this theorem.

The remaining cases are k = 0, 1, 2, 3, 4 and must be treated separately. Propositions 2, 3, and 4 address the first three cases, and certainly there is no hope of showing even that A_k is infinite for k = 1, 2. Although the next result is not as precise a characterization of A_k for k = 3, 4 as Propositions 2–4 for the smaller values of k, its aim is to demonstrate the impossibility of showing that either one of these two sets is infinite.

PROPOSITION 5. Assume that $A_3 \cup A_4$ is infinite. Then there exists an even positive integer c such that the set of primes of the form $p = cq^{\beta} + 1$, with q prime and $\beta \leq 4$, is infinite.

Proof. Assume that $n \in \mathcal{A}_3 \cup \mathcal{A}_4$. Then $\tau(\lambda(n)) \leq \omega(n) + 4$. Write $m = \lambda(n)$ and note that $\omega(n)$ is at most the number of divisors of m of the form p-1 for some prime p. Hence, m can have at most four divisors d such that d+1 is composite. Write $m = 2^{\alpha}\ell$, where ℓ is odd. If $\alpha \geq 9$, then $2^3, 2^5, 2^6, 2^7, 2^9$ are five divisors of m and none of the form p-1 for some prime p. Therefore, $\alpha \leq 8$. If $\tau(\ell) \geq 6$ then ℓ (and hence m) has at least five odd divisors > 1, and certainly none of them is of the form p-1 for some prime p. Thus $\tau(\ell) \leq 5$, which shows that either $\ell = q^{\beta}$ for some prime q and some $\beta \leq 4$ or $\ell = q_1q_2$, where q_1 and q_2 are distinct primes.

Assume that $\ell = q^{\beta}$ holds for infinitely many n. Then there exist infinitely many primes p of the form $p-1=2^{\alpha_0}q^{\beta}$ for some $\alpha_0 \in \{1,\ldots,9\}$ and $\beta \in \{1,\ldots,4\}$, which implies the conclusion of the proposition.

Assume now that $\ell=q_1q_2$ holds for infinitely many n. Suppose further that $q_1 < q_2$. We then distinguish two cases. The first case is when q_1 remains bounded for infinitely many such n. Then $2^{\alpha}q_1$ can take only finitely many values. Since we have infinitely many values for n, there must exist some fixed even positive integer c (an even divisor of a number of the form 2^9q_1 over all the finitely many possibilities for q_1) such that $p-1=cq_2$ holds for infinitely many primes p, which implies the conclusion of the proposition. The second case is when q_1 tends to infinity as p_1 tends to infinity as p_2 tends to infinitely many such p_3 we have that either p_3 expression of the proposition follows with p_3 expression of the proposition follows with p_3 expression of the case, we derive a contradiction.

Observe first that $\alpha \leq 3$, for otherwise $2^3, q_1, q_2, 2q_1, 2q_2$ are five divisors of n, none of which is of the form p-1 for some odd prime p. Assume now that $\alpha=1$. Then $\tau(\lambda(n))=\tau(2q_1q_2)=8$ and so $\omega(n)\geq 4$. Since the only prime factors of n are in $\{2,3,2q_1+1,2q_2+1,2q_1q_2+1\}$, we deduce that one of $2q_1+1$ and $2q_2+1$ must be prime—a contradiction. Finally, if $\alpha=2$ then $\tau(\lambda(n))=\tau(4q_1q_2)=12$, so $\omega(n)\geq 8$. Because all the prime factors of n belong to $\{2,3,5,2q_1+1,2q_2+1,4q_1+1,4q_2+1,2q_1q_2+1,4q_1q_2+1\}$, again it follows that one of $2q_1+1$ or $2q_2+1$ must be a prime, which is the final contradiction. \square

4. Upper Bounds on the Counting Functions of A_k

Our first result in this section shows that, for numbers $n \in A_k$, $\omega(n)$ is bounded in terms of k.

PROPOSITION 6. If $n \in A_k$, then $\omega(n) \le 2(k+1)^2 + 1$.

Proof. We use the same idea and notation as in the proof of Proposition 5. Let $n \in \mathcal{A}_k$ and put $m = \lambda(n) = 2^{\alpha}\ell$, where α is a nonnegative integer and ℓ is odd. If $\alpha \geq 2k+3$, then $2^3, 2^5, \ldots, 2^{2k+3}$ are k+1 divisors of m and none of the form p-1 for some prime p, which is a contradiction. If $\tau(\ell) \geq k+2$ then ℓ (and hence m) has k+1 odd divisors >1, and obviously none of them is of the form p-1 for some prime p, which is again a contradiction. Hence $\alpha \leq 2k+2$ and $\tau(\ell) \leq k+1$, so

$$\omega(n) = \tau(\lambda(n)) - k = \tau(2^{\alpha}\ell) - k = (\alpha + 1)\tau(\ell) - k$$

$$\leq (2k+3)(k+1) - k = 2(k+1)^2 + 1.$$

An upper bound for the counting function $\#A_k(x)$ of A_k follows from Proposition 6 with a little extra work. Let us set

$$b_k = 2(k+1)^2 + 3 + \lfloor \log_2(2(k+1)^2 + k + 1) \rfloor.$$

We then have the following result.

THEOREM 3. For all nonnegative integers k we have the upper bound

$$\#\mathcal{A}_k(x) \ll_k \frac{x(\log\log x)^{b_k}}{(\log x)^2} \text{ as } x \to \infty.$$

Proof. Let $K \ge 2$ be any fixed positive integer. Let $\pi_K(x)$ be the number of primes $p \le x$ such that $\omega(p-1) \le K$. We begin with the following lemma.

Lemma 2. There exists an absolute constant c_0 such that the following estimate holds:

$$\pi_K(x) \ll \frac{x(\log\log x + c_0)^{K+1}}{(K-1)!(\log x)^2} \text{ as } x \to \infty.$$

Proof. Let $\mathcal{P}(x) = \{ p \le x : \omega(p-1) \le K \}$. Put $y = x^{1/\log \log x}$ and $u = \log x/\log y = \log \log x$. For a positive integer n we write P(n) for the largest prime factor of n. Let

$$\Psi(x, y) = \{ n \le x : P(n) \le y \}.$$

By a result of de Bruijn ([2]; see also [3; 9, Cor. 3; 13, Chap. III.5]), the bound

$$\#\Psi(x,y) \le x \exp(-(1+o(1))u \log u) < \frac{x}{(\log x)^2}$$
 (7)

holds as $u \to \infty$, where $u = \log x/\log y$ and provided that $u \le y^{1/2}$, which is satisfied for our choice of y.

Therefore, if $\mathcal{P}_1(x) = \mathcal{P}(x) \cap \Psi(x, y)$ then

$$\#\mathcal{P}_1(x) \ll \frac{x}{(\log x)^2}.$$

Now let $\mathcal{P}_2(x) = \{ p \le x : q^2 \mid p-1 \text{ for some } q \ge y \}$. For a fixed $q \ge y$, the number of $1 < n \le x$ such that $q^2 \mid n-1$ and is $\le x/q^2$. Thus,

$$\#\mathcal{P}_2(x) \le \sum_{q \ge y} \frac{x}{q^2} \ll x \int_y^\infty \frac{dt}{t^2} \ll \frac{x}{y} = o\left(\frac{x}{(\log x)^2}\right).$$

Put $\mathcal{P}_3(x) = \mathcal{P}(x) \setminus (\mathcal{P}_1(x) \cup \mathcal{P}_2(x))$. Write p-1 = Pm, where P = P(p-1). Since P > y and $p \notin \mathcal{P}_2(x)$, we deduce that P(m) < P. Thus, $\omega(m) \le K - 1$. Fix m. By Brun's sieve (see e.g. [8, Thm. 2.3]), the number of primes $p \le x$ such that p-1 = mP for some prime P is

$$\ll \frac{x}{\varphi(m)} \frac{1}{(\log x/m)^2} \ll \frac{x}{\varphi(m)(\log y)^2} \ll \frac{x(\log\log x)^2}{\varphi(m)(\log x)^2}.$$

Summing now over all the acceptable values of m, we obtain

$$\#\mathcal{P}_{3}(x) \ll \frac{x(\log\log x)^{2}}{(\log x)^{2}} \sum_{\substack{m \leq x \\ \omega(m) \leq K-1}} \frac{1}{\varphi(m)}$$

$$\leq \frac{x(\log\log x)^{2}}{(\log x)^{2}} \sum_{k=1}^{K-1} \sum_{\substack{m \leq x \\ \omega(m) = k}} \frac{1}{\varphi(m)}$$

$$\leq \frac{x(\log\log x)^{2}}{(\log x)^{2}} \sum_{k=1}^{K-1} \frac{1}{k!} \left(\sum_{p^{\alpha} \leq x} \frac{1}{p^{\alpha-1}(p-1)}\right)^{k}$$

$$\ll \frac{x(\log\log x)^{2}}{(\log x)^{2}} \sum_{k=1}^{K-1} \frac{1}{k!} \left(\sum_{p \leq x} \frac{1}{p-1} + O(1)\right)^{k}$$

$$\ll \frac{x(\log\log x)^{2}}{(\log x)^{2}} \sum_{k=1}^{K-1} \frac{1}{k!} (\log\log x + c_{0})^{k-1}.$$

It remains only to observe that the last term dominates as x tends to infinity, which finishes the proof of Lemma 2.

We are now ready to prove Theorem 3. Assume that $k \ge 3$, since otherwise the result follows immediately (from Propositions 2–4 and Brun's sieve) even with a smaller b_k (i.e., $b_0 = 0$, $b_1 = 1$, and $b_2 = 1$).

Now note that if $p \mid n$ and $n \in A_k$, then

$$2^{\omega(p-1)} \le \tau(p-1) \le \tau(\lambda(n)) = \omega(n) + k \le 2(k+1)^2 + k + 1$$

(by Proposition 6) and so $\omega(p-1) \le K = \lfloor \log_2(2(k+1)^2 + k + 1) \rfloor$. Lemma 2 shows that

$$\#\{p \le x : \omega(p-1) \le K\} \ll_K \frac{x(\log\log x)^{K+1}}{(\log x)^2}.$$
 (8)

We put $A_{k,1}(x)$ for the set of $n \in A_k(x)$ such that either $P \le y = x^{1/\log \log x}$ or P^2 divides n. As in the proof of Lemma 2,

$$\#\mathcal{A}_{k,1} \ll \frac{x}{(\log x)^2}.\tag{9}$$

685

Let $A_{k,2}(x)$ stand for the complement of $A_{k,1}(x)$ in $A_k(x)$. Now write $n \in A_{k,2}(x)$ as n = Pm, where P = P(n). Hence $P > y = x^{1/\log \log x}$, P^2 does not divide n, and $\omega(m) = \omega(n) - 1 \le 2(k+1)^2$. Fixing m, the number of values for $P \le x/m$ such that $\omega(P-1) \le K$ is, by (8),

$$\pi_K(x/m) \ll_k \frac{x(\log\log(x/m))^{K+1}}{m(\log(x/m))^2} \ll_k \frac{x(\log\log x)^{K+1}}{m(\log y)^2}$$

 $\ll_k \frac{x(\log\log x)^{K+3}}{m(\log x)^2}.$

If we sum the preceding inequality over all the values of $m \le x$ with $\omega(m) \le 2(k+1)^2$, then it follows that the number of possibilities is

$$\begin{split} \# \mathcal{A}_{k,2}(x) \ll_k & \frac{x (\log \log x)^{K+3}}{(\log x)^2} \sum_{\substack{m \leq x \\ \omega(m) \leq 2(k+1)^2}} \frac{1}{m} \\ \ll_k & \frac{x (\log \log x)^{K+3}}{(\log x)^2} \sum_{\ell=0}^{2(k+1)^2} \frac{1}{\ell!} \bigg(\sum_{p^{\alpha} \leq x} \frac{1}{p^{\alpha}} \bigg)^{\ell} \\ \ll_k & \frac{x (\log \log x)^{K+3+2(k+1)^2}}{(\log x)^2}; \end{split}$$

this, together with (9), completes the proof of Theorem 3.

A more careful analysis (along the lines of the proof of [1, Thm. 4.1]) shows that Theorem 3 holds with a somewhat smaller b_k . Furthermore, it is clear that one could write down a formula for the implied constant in terms of k. We do not enter into such details.

5. A More General Statement

Let $f(x) \ge 1$ be any function that tends to infinity with n and that is monotonically decreasing for $x > x_0$. Let

$$\mathcal{B}_f = \{ n : \tau(\lambda(n)) - \omega(n) < \exp((\log \log n)/f(n)) \}. \tag{10}$$

We can then show the following result.

THEOREM 4. If \mathcal{B}_f is the set appearing in (10), then

$$\#\mathcal{B}_f(x) \le \frac{x}{(\log x)^{2+o(1)}} \text{ as } x \to \infty.$$

We start by proving the following lemma.

Lemma 3. Let
$$\mathcal{P}_f = \{p : \omega(p-1) < 2(\log\log p)/\sqrt{f(p)}\}$$
. Then
$$\#\mathcal{P}_f(x) \le \frac{x}{(\log x)^{2+o(1)}} \text{ as } x \to \infty. \tag{11}$$

Proof. Let x be large, put $y = x^{1/\log \log x}$, and let

$$\mathcal{P}_2(x) = \{ p \in \mathcal{P}_f(x) : p - 1 \notin \Psi(x, y) \}.$$

If $p \in \mathcal{P}_2(x)$ then p-1=Qm, where Q=P(p-1)>y and $m \le x/y$. Fix m. By Brun's method, the number of primes $Q \le x/m$ such that p=Qm+1 is also prime is

$$\ll \frac{x}{\varphi(m)(\log(x/m))^2} \le \frac{x}{\varphi(m)(\log y)^2} \le \frac{x(\log\log x)^2}{\varphi(m)(\log x)^2}.$$

Using the minimal order $\varphi(m)/m \gg 1/\log\log x$ of the Euler function in the interval [1,x], we get that if m is fixed then the number of acceptable primes $p \in \mathcal{P}_2(x)$ with (p-1)/P(p-1)=m is

$$\ll \frac{x(\log\log x)^3}{m(\log x)^2}.$$

Let $\mathcal{M}(x)$ be the set of acceptable values for m. Since $\omega(p-1) \leq 2(\log \log p) / \sqrt{f(p)}$, f is increasing for large x, and p > y for all $p \in \mathcal{P}_2(x)$, it follows that

$$z = \max\{2(\log\log p)/\sqrt{f(p)} : p \in \mathcal{P}_2(x)\} \le \frac{2\log\log x}{\sqrt{f(y)}} = o(\log\log x)$$
 (12)

as $x \to \infty$. Furthermore, $\mathcal{M}(x) \subseteq \{m \le x : \omega(m) \le z\}$. As a result,

$$\#\mathcal{P}_2(x) \ll \frac{x(\log\log x)^3}{(\log x)^2} \sum_{m \in \mathcal{M}(x)} \frac{1}{m} \ll \frac{x(\log\log x)^3}{(\log x)^2} \sum_{k \le z} \sum_{\substack{m \le x \\ (m) = k}} \frac{1}{m}.$$
 (13)

Put

$$S_k(x) = \sum_{m \le x \atop m} \frac{1}{m}.$$

Then unique factorization, the multinomial formula, and Stirling's formula imply that

$$S_k(x) \le \frac{1}{k!} \left(\sum_{x \in x} \sum_{\alpha \in I} \frac{1}{p^{\alpha}} \right)^k \le \left(\frac{e \log \log x + O(1)}{k} \right)^k,$$

where we have used the obvious fact that

$$\sum_{p>2} \sum_{\alpha>2} \frac{1}{p^{\alpha}} = O(1)$$

together with Mertens's formula

On the Equation
$$\tau(\lambda(n)) = \omega(n) + k$$
 687

$$\sum_{p < x} \frac{1}{p} = \log \log x + O(1).$$

For every fixed value of A > 1, the function $(eA/t)^t$ is increasing for t < A and so

$$S_k(x) \le \left(\frac{e \log \log x + O(1)}{z}\right)^z = \exp(z \log(e(\log \log x + O(1))/z))$$

$$\le \exp\left(\frac{2 \log \log x}{\sqrt{f(y)}} \log(O(\sqrt{f(y)}))\right) = \exp(o(\log \log x))$$

$$= (\log x)^{o(1)} \quad \text{for } k \le z.$$
(14)

Hence, the inequalities (12) and (13) together with the estimate (14) yield

$$\#\mathcal{P}_{2}(x) \ll \frac{x(\log\log x)^{3}}{(\log x)^{2}} \sum_{k \leq z} \mathcal{S}_{k}(x)$$
$$\ll \frac{x(\log\log x)^{4}}{(\log x)^{2}} \max{\{\mathcal{S}_{k}(x) : k \leq z\}} = \frac{x}{(\log x)^{2+o(1)}};$$

combining this with estimate (7) implies inequality (11) and completes the proof of Lemma 3.

Now partial summation immediately yields our next result.

COROLLARY 2. If \mathcal{P}_f is the set of primes appearing in Lemma 3, then

$$\sum_{p \in \mathcal{P}_f} \frac{1}{p} = O(1).$$

Proof of Theorem 4. Let again $y = x^{1/\log \log x}$, $w = x/(\log x)^2$, and

$$\mathcal{B}_1(x) = \{n \le w\} \cup \Psi(x, y).$$

By (7) we have

$$\#\mathcal{B}_1(x) \le \frac{2x}{(\log x)^2} \tag{15}$$

once x is large. Let $\mathcal{B}_2(x) = \{n \le x : \omega(n) > 10 \log \log x\}$. It follows from results of Norton [11; 12] that

$$\#\mathcal{B}_2(x) \ll \frac{x}{(\log x)^{\lambda}},$$

where $\lambda = 1 + 10 \log(10/e) > 2$; therefore,

$$\#\mathcal{B}_2(x) < \frac{x}{(\log x)^2}.\tag{16}$$

Now put

$$\mathcal{B}_3(x) = \mathcal{B}_f(x) \setminus (\mathcal{B}_1(x) \cup \mathcal{B}_2(x)),$$

and assume that $n \in \mathcal{B}_3(x)$. Replacing f(x) with $\min\{f(x), \log \log \log x\}$, we may assume that $f(x) \leq \log \log \log x$. Then $p-1 \mid \lambda(n)$ for all prime factors p of n and so

$$2^{\omega(p-1)} \le \tau(\lambda(n)) \le \omega(n) + \exp((\log \log n)/f(n))$$

$$< 10 \log \log x + \exp((\log \log x)/f(w))$$

$$< \exp\left(\frac{1.1(\log \log x)}{f(w)}\right),$$

$$\omega(p-1) < \frac{1.6(\log \log x)}{\sqrt{f(w)}},$$
(17)

so

where we used the fact that $1.1/\log 2 < 1.6$. Let $\mathcal{B}_4(x) = \{n \in \mathcal{B}_3(x) : P(n) > w\}$. Since $w \ge p/(\log p)^2$ holds for all $p \in [w, x]$ once x is large, it follows that if p = P(n) for $n \in \mathcal{B}_4(x)$ then

$$\omega(p-1) < \frac{1.6(\log\log x)}{f(p/(\log p)^2)} < \frac{2(\log\log p)}{\sqrt{g(p)}}$$

holds for large x. Here g is the function $g(t) = (f(t/(\log t)^2))^2$, which is increasing for large t. Thus, $p \in \mathcal{P}_g$. Let us now write n = Pm, where $m < x/p < (\log x)^2$, and let us fix m. Then $p \in \mathcal{P}_g(x/m)$ and, by Lemma 3, the number of such choices for p is

$$\# \mathcal{P}_g(x/m) \leq \frac{x}{m(\log x/m)^{2+o(1)}} = \frac{x}{m(\log x)^{2+o(1)}}.$$

Summing this inequality for $m \leq (\log x)^2$, we have

$$#\mathcal{B}_{4}(x) \leq \sum_{m \leq (\log x)^{2}} #\mathcal{P}_{g}\left(\frac{x}{m}\right)$$

$$\leq \frac{x}{(\log x)^{2+o(1)}} \sum_{m \leq (\log x)^{2}} \frac{1}{m}$$

$$= \frac{x}{(\log x)^{2+o(1)}},$$
(18)

because

$$\sum_{m \le (\log x)^2} \frac{1}{m} \ll \log \log x = (\log x)^{o(1)}.$$

From now on we assume that $n \in \mathcal{B}_5(x) = \mathcal{B}_3(x) \setminus \mathcal{B}_4(x)$. Let n = Pm, where $P = P(n) \in [y, w]$. Since 1.6 log log $x < 2 \log \log y \le 2 \log \log P$ for large x and since $f(w) \ge f(P)$, it follows that

$$\omega(P-1) < \frac{1.6(\log\log x)}{f(w)} < \frac{2(\log\log P)}{f(P)}.$$

In particular, $P \in \mathcal{P}_{f^2}$. By Lemma 3, if $m \le x/y$ is fixed then the number of choices for P is at most

$$\# \mathcal{P}_{f^2}(x/m) \leq \frac{x}{m(\log(x/m))^{2+o(1)}} \leq \frac{x}{m(\log y)^{2+o(1)}} \leq \frac{x}{m(\log x)^{2+o(1)}},$$

where we have used that $x/m \ge y$ and $\log y = \log x/\log \log x = (\log x)^{1+o(1)}$. Let $\mathcal{M}(x)$ be the set of acceptable values of m. Then

On the Equation
$$\tau(\lambda(n)) = \omega(n) + k$$
 689

$$\#\mathcal{B}_5(x) \le \sum_{m \in \mathcal{M}(x)} \frac{x}{m(\log x)^{2+o(1)}} \le \frac{x}{(\log x)^{2+o(1)}} \sum_{m \in \mathcal{M}(x)} \frac{1}{m}.$$
 (19)

Let Q(x) be the set of primes dividing some $m \in \mathcal{M}(x)$, and note that Q(x) consists of the primes $q \le x$ satisfying inequality (17). We put

$$v = \exp\left(\exp\left(\frac{\log\log x}{\sqrt{f(w)}}\right)\right)$$

and split the primes in Q into two subsets as follows:

$$Q_1 = \{ q \le v \} \cap Q;$$

$$Q_2 = Q \cap [v, w].$$

Observe that if $q \in \mathcal{Q}_2$ then

$$\frac{2\log\log q}{\sqrt{f(q)}} \geq \frac{2\log\log x}{\sqrt{f(q)f(w)}} \geq \frac{2\log\log x}{f(w)} > \omega(q-1);$$

therefore, $Q_2 \subset \mathcal{P}_f$. This argument shows that

$$\sum_{m \in \mathcal{M}(x)} \frac{1}{m} \le \prod_{q \in \mathcal{Q}_1 \cup \mathcal{Q}_2} \left(\sum_{\alpha \ge 0} \frac{1}{q^{\alpha}} \right)$$

$$\le \exp\left(\sum_{q \in \mathcal{Q}_1} \frac{1}{q} + \sum_{q \in \mathcal{Q}_2} \frac{1}{q} + O\left(\sum_{q \ge 2} \sum_{\alpha \ge 2} \frac{1}{q^{\alpha}} \right) \right). \tag{20}$$

Since

$$\sum_{q \in \mathcal{Q}_1} \frac{1}{q} \le \sum_{q \le v} \frac{1}{v} = \log \log v + O(1) = o(\log \log x)$$

(by Mertens's formula),

$$\sum_{q \in \mathcal{Q}_2} \frac{1}{q} \le \sum_{q \in \mathcal{P}_f} \frac{1}{q} = O(1)$$

(by Corollary 2), and

$$\sum_{q>2} \sum_{\alpha>2} \frac{1}{q^{\alpha}} = O(1),$$

it follows from (20) that

$$\sum_{m \in \mathcal{M}(x)} \frac{1}{m} \le \exp(o(\log \log x)) = (\log x)^{o(1)},$$

which together with (19) gives

$$\#\mathcal{B}_5(x) \le \frac{x}{(\log x)^{2+o(1)}}. (21)$$

Since $\mathcal{B}_3(x) \subseteq \mathcal{B}_4(x) \cup \mathcal{B}_5(x)$, by estimates (18) and (21) we have that

$$\#\mathcal{B}_3(x) < \frac{x}{(\log x)^{2+o(1)}},\tag{22}$$

which together with estimates (15) and (16) completes the proof of Theorem 4. \Box

6. Average and Normal Orders of $\tau(\lambda(n)) - \omega(n)$

Our last result addresses average and normal orders of the function

$$h(n) = \tau(\lambda(n)) - \omega(n)$$
.

Theorem 5. (i) There exist positive constants c_0 , c_1 such that the inequalities

$$\exp\left(c_0\sqrt{\frac{\log x}{\log\log x}}\right) \le \frac{1}{x} \sum_{n < x} h(n) \le \exp\left(c_1\sqrt{\frac{\log x}{\log\log x}}\right) \tag{23}$$

hold for all $x \ge 1$.

(ii) The inequality

$$h(n) = 2^{0.5(1+o(1))(\log\log n)^2}$$

holds for almost all positive integers n.

- *Proof.* (i) In [10] it is shown that inequalities (23) hold with some constants c_0 and c_1 for the function $\tau(\lambda(n)) = h(n) + \omega(n)$. Since the average value of $\omega(n)$ is $\log \log x = \exp(o(\sqrt{\log x/\log\log x}))$, the required inequality follows.
- (ii) In [5] it is shown that the normal order of both $\omega(\varphi(n))$ and $\Omega(\varphi(n))$ is $0.5(\log\log n)^2$. Since $\omega(\lambda(n)) = \omega(\varphi(n))$ and $\Omega(\lambda(n)) \leq \Omega(\varphi(n))$, it follows that the normal order of both $\omega(\lambda(n))$ and $\Omega(\lambda(n))$ is also $0.5(\log\log n)^2$. Finally, since

$$2^{\omega(\lambda(n))} < \tau(\lambda(n)) < 2^{\Omega(\lambda(n))}$$

and since the normal order of $\omega(n)$ is $\log \log n = 2^{o((\log \log n)^2)}$, the desired inequalities follow.

7. Remarks

We suspect that for every $k \ge 1$ there exist constants $a_k > 0$ and $c_k \ge 0$ such that

$$\# \mathcal{A}_k(x) = a_k (1 + o(1)) \frac{x (\log \log x)^{c_k}}{(\log x)^2} \text{ as } x \to \infty.$$
 (24)

Widely believed conjectures concerning the distribution of Sophie Germain primes p together with Proposition 3 seem to support conjecture (24) at k = 1 (with $c_1 = 0$ and some $a_1 > 0$). Note that an upper bound for this shape is given in Theorem 3. We would like to leave this conjecture as an open problem.

References

- [1] W. D. Banks, K. Ford, F. Luca, F. Pappalardi, and I. E. Shparlinski, *Values of the Euler function in various sequences*, Monatsh. Math. 146 (2005), 1–19.
- [2] N. G. de Bruijn, On the number of positive integers $\leq x$ and free of primes > y, II, Indag. Math. (N.S.) 28 (1966), 239–247.
- [3] E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "Factorisatio Numerorum"*, J. Number Theory 17 (1983), 1–28.

- [4] J. R. Chen, On the representation of a large even integer as the sum of a prime and a product of at most two primes, Sci. Sinica 16 (1973), 157–176.
- [5] P. Erdős and C. Pomerance, On the normal number of prime factors of $\varphi(n)$, Rocky Mountain J. Math. 15 (1985), 343–352.
- [6] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.
- [7] K. Ford, The number of solutions of $\varphi(x) = m$, Ann. of Math. (2) 150 (1999), 283–311.
- [8] H. Halberstam and H.-E. Rickert, Sieve methods, Academic Press, London, 1974.
- [9] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théor. Nombres Bordeaux 5 (1993), 411–484.
- [10] F. Luca and C. Pomerance, *On the average number of divisors of the Euler function*, Publ. Math. Debrecen 70 (2007), 125–148.
- [11] K. K. Norton, *The number of restricted prime factors of an integer. I,* Illinois J. Math. 20 (1976), 681–705.
- [12] ——, The number of restricted prime factors of an integer. II, Acta Math. 143 (1979), 9–38.
- [13] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Stud. Adv. Math., 46, Cambridge Univ. Press, Cambridge, 1995.

A. Glibichuk

Department of Mechanics and Mathematics Moskow State University Vorobevy gory, 1 Moskow 119992 Russia

aanatol@mail.ru

F. Luca

Instituto de Matemáticas Universidad Nacional Autónoma de México C.P. 58089 Morelia, Michoacán México

fluca@matmor.unam.mx

F. Pappalardi

Dipartimento di Matematica Università degli Studi Roma Tre Largo S. L. Murialdo, 1 Roma I–00146 Italy

pappa@mat.uniroma3.it