On integers with a special divisibility property

WILLIAM D. BANKS
Department of Mathematics
University of Missouri
Columbia, MO 65211, USA
bbanks@math.missouri.edu

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

Abstract
In this note, we study those positive integers $n$ which are divisible by $\sum_{d|n} \lambda(d)$, where $\lambda(\cdot)$ is the Carmichael function.

1 Introduction

Let $\varphi(\cdot)$ denote the Euler function, whose value at the positive integer $n$ is given by
$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{p^\nu || n} p^{\nu-1}(p-1).$$

Let $\lambda(\cdot)$ denote the Carmichael function, whose value $\lambda(n)$ at the positive integer $n$ is defined to be the largest order of any element in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. More explicitly, for a prime power $p^\nu$, one has
$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1) & \text{if } p \geq 3 \text{ or } \nu \leq 2, \\ 2^{\nu-2} & \text{if } p = 2 \text{ and } \nu \geq 3, \end{cases}$$
and for an arbitrary integer $n \geq 2$ with prime factorization $n = p_1^{e_1} \ldots p_k^{e_k}$, one has

$$
\lambda(n) = \operatorname{lcm}[\lambda(p_1^{e_1}), \ldots, \lambda(p_k^{e_k})],
$$

Note that $\lambda(1) = 1$.

Since $\lambda(d) \leq \varphi(d)$ for all $d \geq 1$, it follows that

$$
\sum_{d|n} \lambda(d) \leq \sum_{d|n} \varphi(d) = n
$$

for every positive integer $n$, and it is clear that the equality

$$
\sum_{d|n} \lambda(d) = n
$$

(1)

cannot hold unless $\lambda(n) = \varphi(n)$. The latter condition is equivalent to the statement that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group, and by a well known result of Gauss, this happens only if $n = 1, 2, 4, p^\nu$ or $2p^\nu$ for some odd prime $p$ and integer exponent $\nu \geq 1$. For such $n$, $\lambda(d) = \varphi(d)$ for every divisor $d$ of $n$, hence we see that the equality (1) is in fact equivalent to the statement that $\lambda(n) = \varphi(n)$.

When $\lambda(n) < \varphi(n)$, the equality (1) is not possible. However, it may happen that the sum appearing on the left side of (1) is a proper divisor of $n$. Indeed, one can easily find many examples of this phenomenon:

$$
n = 140, 189, 378, 1375, 2750, 2775, 2997, 4524, 5550, 5661, 5994, \ldots.
$$

These positive integers $n$ are the subject of the present paper.

Throughout the paper, the letters $p$, $q$ and $r$ are always used to denote prime numbers. For a positive integer $n$, we write $P(n)$ for the largest prime factor of $n$, $\omega(n)$ for the number of distinct prime divisors of $n$, and $\tau(n)$ for the total number of positive integer divisors of $n$. For a positive real number $x$ and a positive integer $k$, we write $\log_k x$ for the function recursively defined by $\log_1 x = \max\{\log x, 1\}$ and $\log_k x = \log_1(\log_{k-1} x)$, where $\log(\cdot)$ denotes the natural logarithm. We also use the Vinogradov symbols $\gg$ and $\ll$, as well as the Landau symbols $O$ and $o$, with their usual meanings.

**Acknowledgements.** This work was done during a visit by the second author to the University of Missouri, Columbia; the hospitality and support of this institution are gratefully acknowledged. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, and F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E.
2 Main Results

Let \( b(\cdot) \) be the arithmetical function whose value at the positive integer \( n \) is given by

\[
b(n) = \sum_{d \mid n} \lambda(d).
\]

Our aim is to investigate the set \( \mathcal{B} \) defined as follows:

\[
\mathcal{B} = \{ n : b(n) \text{ is a proper divisor of } n \}.
\]

For a positive real number \( x \), let \( \mathcal{B}(x) = \mathcal{B} \cap [1, x] \). Our first result provides a nontrivial upper bound on \( \# \mathcal{B}(x) \) as \( x \to \infty \):

**Theorem 1.** The following inequality holds:

\[
\# \mathcal{B}(x) \leq x \exp \left( -\frac{1}{2} \sqrt{\log x \log \log x} \right).
\]

**Proof.** Our proof closely follows that of Theorem 1 in [2]. Let \( x \) be a large real number, and let

\[
y = y(x) = \exp \left( 2^{-1/2} \sqrt{\log x \log \log x} \right).
\]

Also, put

\[
u = u(x) = \frac{\log x}{\log y} = 2^{1/2} \sqrt{\frac{\log x}{\log \log x}}.
\] (2)

Finally, we recall that a number \( m \) is said to be powerful if \( p^2 \mid m \) for every prime factor \( p \) of \( m \).

Let us consider the following sets:

\[
\mathcal{B}_1(x) = \{ n \in \mathcal{B}(x) : P(n) \leq y \},
\]

\[
\mathcal{B}_2(x) = \{ n \in \mathcal{B}(x) : \omega(n) \geq u \},
\]

\[
\mathcal{B}_3(x) = \{ n \in \mathcal{B}(x) : m \mid n \text{ for some powerful } m > y^2 \},
\]

\[
\mathcal{B}_4(x) = \{ n \in \mathcal{B}(x) : \tau(\varphi(n)) > y \},
\]

\[
\mathcal{B}_5(x) = \mathcal{B}(x) \setminus (\mathcal{B}_1(x) \cup \mathcal{B}_2(x) \cup \mathcal{B}_3(x) \cup \mathcal{B}_4(x)).
\]

Since \( \mathcal{B}(x) \) is the union of the sets \( \mathcal{B}_j(x), j = 1, \ldots, 5 \), it suffices to find an appropriate bound on the cardinality of each set \( \mathcal{B}_j(x) \).
By the well known estimate (see, for instance, Tenenbaum [7]):

\[ \Psi(x, y) = \# \{ n \leq x : P(n) \leq y \} = x \exp\{-(1 + o(1))u \log u\}, \]

which is valid for \( u \) satisfying (2), we derive that

\[ \#B_1(x) \leq x \exp\left(-2^{-1/2}(1 + o(1))\sqrt{\log x \log_2 x}\right). \quad (3) \]

Next, using Stirling’s formula together with the estimate

\[ \sum_{p \leq x} \frac{1}{p} = \log \log x + O(1), \]

we obtain that

\[
\# \{ n \leq x : \omega(n) \geq u \} \leq \sum_{p_1 \cdots p_{[u]} \leq x} \frac{x}{p_1 \cdots p_{[u]}} \leq \frac{x}{[u]!} \left( \sum_{p \leq x} \frac{1}{p} \right)^{[u]} \\
\leq x \left( e \log \log x + O(1) \right)^{[u]} \\
\leq x \exp\left(- (1 + o(1))u \log u \right),
\]

therefore

\[ \#B_2(x) \leq x \exp\left(-2^{-1/2}(1 + o(1))\sqrt{\log x \log_2 x}\right). \quad (4) \]

We also have

\[ \#B_3(x) \leq \sum_{m \text{ powerful}} \frac{x}{m} \ll \frac{x}{y} = x \exp\left(-2^{-1/2}\sqrt{\log x \log_2 x}\right), \quad (5) \]

where the second inequality follows by partial summation from the well known estimate:

\[ \# \{ m \leq x : m \text{ powerful} \} \ll \sqrt{x}. \]

(see, for example, Theorem 14.4 in [5]).

By a result from [6], it is known that

\[ \sum_{n \leq x} \tau(\varphi(n)) \leq x \exp\left( O\left( \sqrt{\frac{\log x}{\log_2 x}} \right) \right). \quad (6) \]
Therefore,

\[ \#B_4(x) \leq \sum_{n \leq x} 1 \leq \frac{1}{y} \sum_{n \leq x} \tau(\varphi(n)) \leq \frac{x}{y} \exp(O(u)) \]

\[ \leq x \exp \left( -2^{-1/2}(1 + o(1)) \sqrt{\log x \log_2 x} \right). \quad (7) \]

In view of the estimates (3), (4), (5) and (7), to complete the proof it suffices to show that

\[ \#B_5(x) \leq x \exp \left( -2^{-1/2}(1 + o(1)) \sqrt{\log x \log_2 x} \right). \quad (8) \]

We first make some comments about the integers in the set \( B_5(x) \). For each \( n \in B_5(x) \), write \( n = n_1 n_2 \), where \( \gcd(n_1 n_2) = 1 \), \( n_1 \) is powerful, and \( n_2 \) is squarefree. Since \( n_1 \leq y^2 \) (as \( n \notin B_3(x) \)) and \( P(n) > y \) (as \( n \notin B_1(x) \)), it follows that \( P(n)|n_2 \); in particular, \( P(n)||n \). By the multiplicativity of \( \tau(\cdot) \), we also have

\[ \tau(n) = \tau(n_1)\tau(n_2). \]

Since \( n \notin B_2(x) \),

\[ \tau(n_2) \leq 2^{x(n)} < 2^n = \exp(O(u)), \]

Also,

\[ \tau(n_1) \leq \exp \left( O \left( \frac{\log n_1}{\log \log n_1} \right) \right) \leq \exp \left( O \left( \frac{\log y}{\log \log y} \right) \right) = \exp(O(u)). \]

In particular,

\[ \tau(n) \leq \exp(O(u)). \quad (9) \]

Now let \( n \in B_5(x) \), and write \( n = Pm \), where \( P = P(n) \) and \( m \) is a positive integer with \( m \leq x/y \). Put

\[ D_1 = \gcd(P - 1, \lambda(m)) \quad \text{and} \quad D_2 = \gcd(m, b(n)). \quad (10) \]

Since \( b(n) \) is a (proper) divisor of \( n = Pm \), it follows that \( b(n) = D_2 P^\delta \), where \( \delta = 0 \) or 1. Since \( P||n \) and \( P \neq 2 \), we also have

\[ b(n) = \sum_{d|n} \lambda(d) = \sum_{d|m} \lambda(d) + \sum_{d|m} \text{lcm}[P - 1, \lambda(d)] \]

\[ = b(m) + \sum_{d|m} \frac{(P - 1)\lambda(d)}{\gcd(D_1, \lambda(d))} = b(m) + (P - 1)b(D_1, m), \]

5
where
\[ b(D_1, m) = \sum_{d|m} \frac{\lambda(d)}{\gcd(D_1, \lambda(d))}. \]

Consequently,
\[ b(m) + (P - 1)b(D_1, m) = D_2P^\delta, \]
and thus
\[ P = \begin{cases} 1 + \frac{D_2 - b(m)}{b(D_1, m)} & \text{if } \delta = 0, \\ \frac{b(m) - b(D_1, m)}{D_2 - b(D_1, m)} & \text{if } \delta = 1. \end{cases} \tag{11} \]

We remark that \( D_2 \neq b(D_1, m) \) in the second case. Indeed, noting that \( m > 2 \) (since \( n \) is neither prime nor twice a prime), it follows that \( D_1 \) is even; in particular, \( D_1 \geq 2 \). Thus,
\[ 1 = \frac{\lambda(1)}{\gcd(D_1, \lambda(1))} \leq b(D_1, m) \leq \sum_{d|m \atop d \leq m} \lambda(d) \frac{\lambda(m)}{D_1} < b(m), \]
which shows that \( b(m) - b(D_1, m) > 0 \), and therefore \( D_2 \) cannot be equal to \( b(D_1, m) \) in view of (11). Hence, from (11), we conclude that for all fixed choices of \( m \), an even divisor \( D_1 \) of \( \lambda(m) \), and a divisor \( D_2 \) of \( m \), there are at most two possible primes \( P \) satisfying (10) and such that \( Pm \in B_5(x) \).

Using (6) and (9), and recalling that \( m \approx x/y \), we derive that
\[ \#B_5(x) \ll \sum_{m \leq x/y} \tau(m)\tau(\lambda(m)) \leq \exp(O(u)) \sum_{m \leq x/y} \tau(\varphi(m)) \ll \frac{x}{y} \exp(O(u)). \]

The estimate (8) now follows from our choice of \( y \), and this completes the proof. \( \square \)

Our next result provides a complete characterization of those odd integers \( n \in B \) with \( \omega(n) = 2 \).

**Theorem 2.** Suppose that \( n = p^a q^b \), where \( p \) and \( q \) are odd primes with \( p < q \), and \( a, b \) are positive integers. If \( n \neq 2997 \), then \( n \in B \) if and only if \( b = 1 \) and there exists a positive integer \( k \) such that
\[ q = 2p^{(p^k - 1)/(p - 1)} + 1 \quad \text{and} \quad a = k + 2(p^k - 1)/(p - 1). \]
Proof. Let $c$ be the largest nonnegative integer such that $p^c | (q - 1)$.

First, suppose that $p | (q - 1)$ (that is, $c = 0$). We must show that $n \not\in \mathcal{B}$. Indeed, let $t = \gcd(p - 1, q - 1)$; then

$$b(n) = 1 + \sum_{j=1}^{a} \lambda(p^j) + \sum_{k=1}^{b} \lambda(q^k) + \sum_{j=1}^{a} \sum_{k=1}^{b} \lambda(p^j q^k)$$

$$= 1 + \sum_{j=1}^{a} \phi(p^j) + \sum_{k=1}^{b} \phi(q^k) + \sum_{j=1}^{a} \sum_{k=1}^{b} \frac{\phi(p^j q^k)}{t}$$

$$= 1 + (p^a - 1) + (q^b - 1) + t^{-1}(p^a q^b - p^a - q^b + 1).$$

If $n \in \mathcal{B}$, $b(n) = p^e q^f$ for some integers $e, f$ with $0 \leq e \leq a$ and $0 \leq f \leq b$. Thus,

$$tp^e q^f = (t - 1)(p^a + q^b - 1) + p^a q^b$$

(12)

If $e \leq a - 1$, then since $t \leq p - 1$, it follows that

$$tp^e q^f < p^{e+1} q^f \leq p^a q^b,$$

which contradicts (12); therefore, $e = a$. A similar argument shows that $f = b$. But then $b(n) = p^a q^b = n$, which is not possible since $b(n)$ is a proper divisor of $n$. This contradiction establishes our claim that $n \not\in \mathcal{B}$.

If $c \geq 1$, we have

$$b(n) = 1 + \sum_{j=1}^{a} \lambda(p^j) + \sum_{k=1}^{b} \lambda(q^k) + \sum_{1 \leq j \leq a} \sum_{k=1}^{b} \lambda(p^j q^k)$$

$$+ \sum_{j=1}^{a} \sum_{k=1}^{b} \lambda(p^j q^k)$$

$$= 1 + \sum_{j=1}^{a} \phi(p^j) + \sum_{k=1}^{b} \phi(q^k) + \sum_{1 \leq j \leq a} \sum_{k=1}^{b} \frac{\phi(p^j q^k)}{t} + \sum_{j=1}^{a} \sum_{k=1}^{b} \frac{\phi(p^j q^k)}{t}.$$

For any integer $r \geq 1$, we have the identity:

$$\sum_{k=1}^{b} \phi(p^j q^k) = \phi(p^r) \sum_{k=1}^{b} \phi(q^k) = (p^r - p^{r-1})(q^b - 1).$$

Hence, it follows that

$$b(n) = p^a + q^b - 1 + \frac{(q^b - 1)}{t} ((p - 1) \min\{a, c\} + p^{\max\{a-c, 0\}} - 1).$$

(13)
Assuming that $n \in \mathcal{B}$, write $b(n) = p^e q^f$ as before.

We claim that $c < a$. Indeed, if $c \geq a$, then reducing (13) modulo $p^c$ (and recalling that $q \equiv 1 \pmod{p^c}$), we obtain that

$$p^c \equiv p^e q^f = b(n) \equiv p^a \pmod{p^c},$$

which implies that $e = a$. Then

$$p^a q^f = b(n) = p^a + q^b - 1 + \frac{(q^b - 1)(p - 1)a}{t},$$

which in turn gives

$$tp^a(q^f - 1) = (q^b - 1)(1 + (p - 1)a).$$

The following result can be easily deduced from [1].

**Lemma 3.** For every odd prime $q$ and integer $b \geq 2$, there exists a prime $P$ such that $P | (q^b - 1)$, but $P \nmid (q^f - 1)$ for any positive integer $f < b$, except in the case that $b = 2$ and $q$ is a Mersenne prime.

If $f < b$ and the prime $P$ of Lemma 3 exists, the equality (14) is not possible as $P$ divides only the right-hand side. Thus, if (14) holds and $f < b$, it must be the case that $b = 2$, $f = 1$, and $q = 2^r - 1$ for some prime $r$. But this leads to the equality

$$tp^a = 2^r(1 + (p - 1)a),$$

and since $t$ divides $(q - 1) \equiv 2 \pmod{4}$, we obtain a contradiction after reducing everything modulo 4. Therefore, $f = b$, and we again have that $b(n) = p^a q^b = n$, contradicting the fact that $n \in \mathcal{B}$. This establishes our claim that $c < a$.

From now on, we can assume that $c < a$; then (13) takes the form:

$$p^e q^f = b(n) = p^a + q^b - 1 + \frac{(q^b - 1)}{t} \left((p - 1)c + p^{a-c} - 1\right).$$

Reducing this equation modulo $p^c$, we immediately deduce that $e \geq c$. Thus,

$$\left(\frac{q^b - 1}{q - 1}\right) \left(\frac{q - 1}{p^c}\right) \left(1 + \frac{(p - 1)c + p^{a-c} - 1}{t}\right) = (p^{e-c} q^f - p^{a-c}),$$

(15)
where each term enclosed by parentheses is an integer. Using the trivial estimates
\[
\frac{q^b - 1}{q - 1} \geq q^{b-1}, \quad \frac{q - 1}{p^c} \geq t,
\]
and
\[
1 + \left(\frac{(p-1)c + p^{a-c} - 1}{t}\right) > \frac{p^{a-c}}{t},
\]
we obtain that
\[
p^{a-c}(q^{b-1} + 1) < p^{e-c}q^f,
\]
which clearly forces \( f = b \).

Now put \( D = (q^b - 1)/(q - 1) \); then \( D|(q^b - 1) \) and \( D|(p^{e-c}q^b - p^{a-c}) \) (since \( f = b \)); thus,
\[
p^{e-c} \equiv p^{a-c} \pmod{D}.
\]
Write \( D = p^dD_0 \), where \( p \nmid D_0 \). From the definition of \( D \), it easy to see that \( d \) is also the largest nonnegative integer such that \( p^d|b \); therefore,
\[
d \leq \frac{\log b}{\log p}, \quad (18)
\]
On the other hand, from (17), it follows that \( d \leq e - c \); hence,
\[
p^{e-c-d} \equiv p^{a-c-d} \pmod{D_0},
\]
which implies that \( D_0|(p^{a-c} - 1) \). Consequently,
\[
p^{a-c} > p^{a-c} - 1 \geq D_0 = p^{-d}D \geq p^{-d}q^{b-1} > p^{-d}(p^{a-c})^{b-1},
\]
where in the last step we have used the bound \( q > p^{a-e} \), which follows from (16) (with \( f = b \)). Thus,
\[
d > (a - e)(b - 2), \quad (19)
\]
Combining the estimates (18) and (19), and using the fact that \( a - e \geq 1 \), we see that \( b \leq 2 \). Moreover, if \( b = 2 \), then since \( p^d|b \) and \( p \) is odd, it follows that \( d = 0 \), which is impossible in view of (19). Hence, \( b = 1 \).

At this point, (15) takes the form
\[
\left(\frac{q - 1}{p^c}\right) \left(1 + \frac{(p-1)c + p^{a-c} - 1}{t}\right) = p^{e-c}q - p^{a-c}.
\]
Since \( t \leq p - 1 \), we have
\[
 p^{e-c}q > \left( \frac{q - 1}{p^c} \right) \left( \frac{p^{a-c}}{p - 1} \right) = p^{a-2c} \left( \frac{q - 1}{p - 1} \right) > p^{a-2c} \left( \frac{q}{p} \right) = p^{a-2c-1}q,
\]
thus \( a \leq e + c \).

We now write \( q - 1 = p^c t \mu \) for some positive integer \( \mu \). Then from (20), it follows that
\[
 p^{a-c}(\mu + 1) - p^c t \mu = p^{e-c} + \mu - t \mu - (p - 1)c \mu.
\]  
(21)

First, let us distinguish a few special cases. If \( t = 2 \) and \( \mu = 1 \), we have
\[
2p^{a-c} - p^c = p^{e-c} - 1 - (p - 1)c.
\]
If \( a \leq e + c - 1 \), we see that
\[
p^{e-c} - 1 - (p - 1)c \leq 2p^{e-1} - 2p^c;
\]
hence,
\[
2p^{e-1}(p - 1) \leq c(p - 1) + 1 - p^{e-c} \leq e(p - 1),
\]
which is not possible for any \( e \geq 1 \). Thus, \( a = e + c \), and it follows that
\[
c = \frac{p^{e-c} - 1}{p - 1}.
\]
Taking \( k = e - c \) (which is positive since \( c \) is an integer), we have
\[
q = 2p^c + 1 = 2p^{(p^k - 1)/(p - 1)} + 1,
\]
and
\[
a = e + c = k + 2c = k + 2(p^k - 1)/(p - 1);
\]
hence, our integer \( n = p^aq \) has the form stated in the theorem.

Next, we claim that \( e \neq 1 \). Indeed, if \( e = 1 \), then \( c = 1 \); as \( c < a \leq e + c \), it follows that \( a = 2 \). Substituting into (21), we obtain that
\[
p(\mu + 1) - pt \mu = 1 + \mu - t \mu - (p - 1) \mu,
\]
or
\[
p(1 + 2\mu - t \mu) = 1 + 2\mu - t \mu.
\]
This last equality implies that $1 + 2\mu - t\mu = 0$, therefore $\mu = 1$ and $t = 3$, which is not possible since $t$ is an even integer.

For convenience, let $S$ denote the value on either side of the equality (21). We note that the relation (20) implies that $p^{e-c}(t + (p - 1)c - 1)$; thus,

$$S \leq t + (p - 1)c - 1 + \mu - t\mu - (p - 1)c\mu = (1 - \mu)(t + (p - 1)c - 1).$$

In the case that $S \geq 0$, we immediately deduce that $\mu = 1$, which implies that $S = 0$. Then $2p^{a-c} = p^ct$, and we conclude that $t = 2$ (and $a = e + c$), which is a case we have already considered.

Suppose now that $S < 0$. From (21) we derive that

$$-S = \frac{p^ct - p^{a-e}(1 + \frac{1}{\mu})}{p^{e-c}\mu} = \frac{t + (p - 1)c - 1}{p^{e-c}} - 1 - \frac{1}{p^{e-c}},$$

and since we already know that $a \leq e + c$, $t \leq p - 1$ and $c \leq e$, it follows that

$$p^{e}\left(t - 1 - \frac{1}{\mu}\right) < \frac{t + (p - 1)c - 1}{p^{e-c}} \leq \frac{(p - 1)(c + 1)}{p^{e-c}} \leq \frac{(p - 1)(e + 1)}{p^{e-c}}.$$

If $t \neq 2$ or $\mu \neq 1$ (which have already been considered), then $(t - 1 - 1/\mu) \geq 1/2$, and therefore

$$e + 1 > \frac{p^e}{2(p - 1)}.$$

This implies that $e \leq 2$ for $p = 3$, and $e = 1$ for $p \geq 5$. Since we have already ruled out the possibility $e = 1$, this leaves only the case where $p = 3$ and $e = 2$. To handle this, we observe that $(t - 1 - 1/\mu) \geq 2/3$ if $\mu \geq 3$, and we obtain the bound

$$e + 1 > \frac{2p^e}{3(p - 1)},$$

which is not possible for $p = 3$ and $e = 2$. Thus, we left only with the case $p = 3$ and $e = t = \mu = 2$. Since $c \leq e$, $c < a \leq e + c$, and $q = 4 \cdot 3^c + 1$, it follows that $n \in \{117, 351, 999, 2997\}$. It may be checked that, of these four integers, only 2997 lies in the set $B$.

To complete the proof, it remains only to show that if

$$q = 2p^{(p^k-1)/(p-1)} + 1$$

and

$$a = k + 2(p^k - 1)/(p - 1)$$

for some positive integer $k$, then $n = p^aq$ lies in the set $B$. For such primes $p, q$, we have $t = 2$, $c = (p^k - 1)/(p - 1)$, $q = 2p^e + 1$, and $a = k + 2c$; taking $e = a - c = k + (p^k - 1)/(p - 1)$, we immediately verify (20). Noting that $e < a$, it follows that $b(n)$ is a proper divisor of $n$. 

\[\Box\]
As a complement to Theorem 2, we have:

**Theorem 4.** If \( n \) is even and \( \omega(n) = 2 \), then \( n \not\in \mathcal{B} \).

**Proof.** Write \( n = 2^a q^b \), where \( q \) is an odd prime and \( a, b \) are positive integers, and suppose first that \( a \geq 3 \). For any divisor \( d = 2^e q^f \) of \( n \), the congruence \( \lambda(d) \equiv 0 \pmod{4} \) holds whenever \( e \geq 4 \). On the other hand, if \( e \leq 3 \), then \( \lambda(d) = \lambda(q^f) \) since \( 2 \mid (q - 1) \). Reducing \( b(n) \) modulo 4, we have

\[
b(n) \equiv \sum_{j=0}^{3} \lambda(2^j) + \sum_{j=0}^{3} \lambda(2^j q^k) = 6 + 4 \sum_{k=1}^{b} \lambda(q^k) \equiv 2 \pmod{4},
\]

which implies that \( 2 \mid b(n) \). If \( n \in \mathcal{B} \), then \( b(n) \) is a divisor of \( n \), thus \( b(n) \leq 2q^b \). On the other hand,

\[
b(n) \geq 6 + 4 \sum_{k=1}^{b} \lambda(q^k) = 2 + 4 \sum_{k=0}^{b} \varphi(q^k) = 2 + 4q^b,
\]

which contradicts the preceding estimate. This shows that \( n \not\in \mathcal{B} \).

If \( a = 1 \), then \( n \) is twice a prime power, thus \( n \not\in \mathcal{B} \).

Finally, suppose that \( a = 2 \). Then

\[
b(n) = \sum_{j=0}^{2} \lambda(2^j) + \sum_{j=0}^{2} \lambda(2^j q^k) = 4 + 3 \sum_{k=1}^{b} \lambda(q^k) = 1 + 3 \sum_{k=0}^{b} \varphi(q^k) = 1 + 3q^b,
\]

which clearly cannot divide \( n = 4q^b \). \( \square \)

### 3 Comments

In Theorem 2, the condition \( k = 1 \) is equivalent to \( a = 3 \) and \( q = 2p + 1 \); that is, \( q \) is a Sophie Germain prime. Under the classical Hardy-Littlewood conjectures (see [3, 4]), the number of such primes \( q \leq y \) should be asymptotic to \( y/(\log y)^2 \) as \( y \to \infty \); thus, we expect \( \mathcal{B} \) to contain roughly \( x^{1/4}/(\log x)^2 \) odd integers \( n \) of the form \( n = p^3q \). When \( k \geq 2 \), then

\[
\frac{1}{\log q} \ll \frac{1}{p^{k-1}\log p},
\]

12
and since the series
\[ \sum_{\substack{p \geq 3 \\ k \geq 2}} \frac{1}{p^{k-1} \log p} \]
converges, classical heuristics suggest that there should be only finitely many numbers \( n \in \mathcal{B} \) with \( \omega(n) = 2 \) and \( k > 1 \). Unconditionally, we can only say that the number of such odd integers \( n \in \mathcal{B} \) with \( n \leq x \) is \( O((\log x) / (\log_2 x)) \).

We do not have any conjecture about the correct order of magnitude of \( \# \mathcal{B}(x) \) as \( x \to \infty \). In fact, we cannot even show that it \( \mathcal{B} \) is an infinite set, although computer searches produce an abundance of examples.

Let \( p_1, p_2, \ldots, p_k \) be distinct primes such that \((p_1 - 1)|(p_2 - 1)| \ldots |(p_k - 1)\). Taking \( n = p_1 \ldots p_k \), we see that

\[ b(n) = \sum_{d|n} \lambda(d) = 1 + (p_1 - 1) + 2(p_2 - 1) + \cdots + 2^{k-1}(p_k - 1). \] (22)

Indeed, this formula is clear if \( k = 1 \). For \( k > 1 \), put \( m = p_1 \ldots p_{k-1} \), and note that the divisibility conditions among the primes imply that \( \lambda(m)|(p_k - 1) \).

Therefore,

\[
\begin{align*}
b(n) &= \sum_{d|m} \lambda(d) + \sum_{d|m} \text{lcm}[p_k - 1, \lambda(d)] \\
&= \sum_{d|m} \lambda(d) + (p_k - 1)\tau(m) = b(m) + 2^{k-1}(p_k - 1),
\end{align*}
\]

and an immediate induction completes the proof of formula (22). If \( p > 5 \) is a prime congruent to 1 modulo 4 such that \( q = 2p - 1 \) is also prime, then \( p_1 = 5, p_2 = p \) and \( p_3 = q \) fulfill the stated divisibility conditions; thus, with \( n = 5pq \), we have

\[ b(n) = \sum_{d|n} \lambda(d) = 1 + (5 - 1) + 2(p - 1) + 4(q - 1) = 10p - 5 = 5q, \]

which is a divisor of \( n \). The Hardy-Littlewood conjectures also predict that if \( x \) is sufficiently large, there exist roughly \( x^{1/2}/(\log x)^2 \) of such positive integers \( n \leq x \), which suggests that the inequality \( \# \mathcal{B}(x) \gg x^{1/2}/(\log x)^2 \) holds.

Finally, we note that \( b(2n) = 2b(n) \) whenever \( n \) is odd, therefore \( 2n \in \mathcal{B} \) whenever \( n \) is an odd element of \( \mathcal{B} \).
References


