Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **13** (2019), 619–631.
https://doi.org/10.2298/AADM190326023J

ON THE ORDER OF ODD INTEGERS MODULO 2^n

*Soon-Mo Jung, Doyun Nam and Michael Th. Rassias**

In this paper, we investigate the order of odd integers of the forms $2^j u + 1$ and $2^j u + 3$ modulo 2^n, where j is an integer with $j \geq 2$, u is an odd positive integer, and n is an integer with $n \geq j + 3$.

1. INTRODUCTION AND PRELIMINARIES

Although the concept of divisibility seems intuitive, it plays a fundamental role in number theory and it leads to a number of foundational concepts such as the greatest common divisor, the least common multiple, and prime numbers. Congruence is a core concept of number theory. It leads to theorems that are closely related to divisibility and are essential, both in theory and practice.

The concept of multiplicative order is also very important. If n is an integer larger than 2, then 2^n does not have a primitive root. This means that the order of any odd integer modulo 2^n is less than $\phi(2^n)$, where ϕ stands for Euler's totient function (cf. **[4, 6]**).

For a positive integer n and an odd positive integer a, we recall that the (multiplicative) order of a modulo 2^n is defined by

$$\omega_a(2^n) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{2^n}\}.$$

Remark 1.1. Since the set $\{a^k \pmod{2^n} \mid k \in \mathbb{N}\}$ is a subgroup of the finite group (of units modulo 2^n) $\mathbb{Z}_{2^n}^{\times}$ and the number of elements of this subgroup equals $\omega_a(2^n)$, and since the number of elements of $\mathbb{Z}_{2^n}^{\times}$ is $\phi(2^n)$, Euler's theorem (or Lagrange's theorem) implies that $\omega_a(2^n) \mid \phi(2^n)$, *i.e.*, there exists a positive integer $\alpha \leq n - 1$ such that $\omega_a(2^n) = 2^\alpha$.

*Corresponding author. Michael Th. Rassias
2010 Mathematics Subject Classification. 11B50, 11A07, 11B65
Keywords and Phrases. Order of odd integers, primitive root, Euler totient function.

If $m < n$, then $a^{\omega_a(2^n)} \equiv 1 \pmod{2^n}$, hence $a^{\omega_a(2^n)} \equiv 1 \pmod{2^m}$. Thus if $m < n$, then $\omega_a(2^m) \,|\, \omega_a(2^n)$. We may ask whether there is a general relationship between $\omega_a(2^m)$ and $\omega_a(2^n)$. A partial answer to this question will be given in the following theorem. Although this theorem has already been covered and proved in **[2]**, we also present it below for completeness reasons.

Theorem 1.1. *Let a and n be positive integers, where a is odd. If $\omega_a(2^n) < \omega_a(2^{n+1})$, then $\omega_a(2^{n+1}) = 2\omega_a(2^n)$.*

Proof. By the definition of $\omega_a(2^n)$, we have

$$a^{\omega_a(2^n)} \equiv 1 \pmod{2^n},$$

i.e., there exists an integer b such that

$$a^{\omega_a(2^n)} = b2^n + 1.$$

By squaring both sides, we get

$$a^{2\omega_a(2^n)} = \left(a^{\omega_a(2^n)}\right)^2 = (b2^n + 1)^2 = b^2 2^{2n} + b2^{n+1} + 1 \equiv 1 \pmod{2^{n+1}},$$

which implies that $\omega_a(2^{n+1}) \mid 2\omega_a(2^n)$. Due to the fact that $\omega_a(2^n) \mid \omega_a(2^{n+1})$ and with the assumption $\omega_a(2^n) < \omega_a(2^{n+1})$, we conclude that $\omega_a(2^{n+1}) = 2\omega_a(2^n)$. □

We remark that 2 and 2^2 have primitive roots, namely 1 and 3, respectively, but there exist no primitive roots for higher powers of 2. These facts imply that if $n \geq 3$, then the order of odd integers modulo 2^n is less than $\phi(2^n)$. In **[6**, Theorem 9.11], the upper bound for the order of odd integers modulo 2^n is provided.

Theorem 1.2. *If a is an odd positive integer and n is an integer with $n \geq 3$, then*

$$a^{(1/2)\phi(2^n)} = a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

According to the last theorem (or Remark 1.1) we have that if n is an integer not less than 3, then $\omega_a(2^n) = 2^\alpha \leq 2^{n-2}$. The following example illustrates that the upper bound 2^{n-2} for $\omega_a(2^n)$ is sharp.

Example 1.1. If $a = 3$ and $n = 5$, then we have $(1/2)\phi(2^n) = (1/2)\phi(2^5) = 8$ and

$$\begin{aligned}
&3^1 \equiv 3 \pmod{2^5}, \quad 3^2 \equiv 9 \pmod{2^5}, \quad 3^3 \equiv 27 \pmod{2^5},\\
&3^4 \equiv 17 \pmod{2^5}, \quad 3^5 \equiv 19 \pmod{2^5}, \quad 3^6 \equiv 25 \pmod{2^5},\\
&3^7 \equiv 11 \pmod{2^5}, \quad 3^8 \equiv 1 \pmod{2^5}.
\end{aligned}$$

Hence, it follows that

$$3^{(1/2)\phi(2^5)} = 3^8 \equiv 1 \pmod{2^5}$$

and $\omega_3(2^5) = 8 = (1/2)\phi(2^5)$.

In this paper, we will investigate the order of odd integers of the form $2^j u+1$ and $2^j u+3$ modulo 2^n. Here, j is an integer larger than 1, u is an odd positive integer, and n is an integer larger than $j+2$.

2. ORDER OF $2^j u+1$ MODULO 2^n

The following theorem provides a lower bound for the order of odd integers of the form $2^j u+1$, where $j \geq 2$ and u is odd.

Theorem 2.3. *If a is an odd positive integer such that $a = 2^j u + 1$, where j is an integer with $j \geq 2$ and u is an odd positive integer, and if n is an integer with $n \geq j+3$, then $\omega_a(2^n) = 2^\alpha$ for some integer $\alpha \geq n-j$.*

Proof. Let

$$I = \{i \in \mathbb{N} \mid 4 \leq i \leq 2^{n-j-1}\}.$$

In this proof, let the range of i be the set I. Then for each i, there exists the unique integer k_i satisfying $2^{k_i} \leq i < 2^{k_i+1}$. By the definition of I, the set

$$K = \{k_i \in \mathbb{N} \mid i \in I\}$$

is identical to the set

$$\{k \in \mathbb{N} \mid 2 \leq k \leq n-j-1\}.$$

This means that $k_i \geq 2$ for every $i \in I$.

It follows from [**5**, Theorem 3.16] that

$$\begin{aligned} i! &= 2^{([i/2]+[i/2^2]+[i/2^3]+\cdots)} \prod_{p>2} p^{([i/p]+[i/p^2]+[i/p^3]+\cdots)} \\ &= 2^\beta \prod_{p>2} p^{([i/p]+[i/p^2]+[i/p^3]+\cdots)}, \end{aligned} \tag{2.1}$$

where the products are taken over all odd prime numbers and

$$\begin{aligned} \beta &= \left[\frac{i}{2}\right] + \left[\frac{i}{2^2}\right] + \left[\frac{i}{2^3}\right] + \cdots \\ &= \left[\frac{i}{2}\right] + \left[\frac{i}{2^2}\right] + \cdots + \left[\frac{i}{2^{k_i}}\right] \\ &\leq \frac{i}{2} + \frac{i}{2^2} + \cdots + \frac{i}{2^{k_i}} \\ &< i. \end{aligned}$$

Thus, by taking into account the facts that $i \geq 4$ and β is an integer, we have

$$3 \leq \beta \leq i-1. \tag{2.2}$$

In view of [**5**, Theorem 3.16] or by setting $i = 2^{n-j-1} - 1$ in (2.1), we infer that

$$2^{\sum_{e=1}^{\infty} \left[\frac{2^{n-j-1}-1}{2^e}\right]} \,||\, (2^{n-j-1}-1)!$$

and by substituting $2^{n-j-1} - i$ for i in (2.1), we get

$$2^{\sum_{e=1}^{\infty} \left[\frac{2^{n-j-1}-i}{2^e}\right]} \,||\, (2^{n-j-1}-i)!$$

where $2^\ell \,||\, m$ implies that $2^\ell \mid m$ but $2^{\ell+1} \nmid m$. Hence, we get

$$2^{\sum_{e=1}^{\infty} \left(\left[\frac{2^{n-j-1}-1}{2^e}\right] - \left[\frac{2^{n-j-1}-i}{2^e}\right]\right)} \,||\, (2^{n-j-1}-1)(2^{n-j-1}-2)\cdots(2^{n-j-1}-(i-1)).$$

And because $[x] - [y] \geq [x-y]$ for all $x, y \in \mathbb{R}$, it follows that

$$2^{([(i-1)/2]+[(i-1)/2^2]+\cdots)} \,\big|\, (2^{n-j-1}-1)(2^{n-j-1}-2)\cdots(2^{n-j-1}-(i-1)). \tag{2.3}$$

From the fact that $2^{k_i} \leq i < 2^{k_i+1}$, we know that $i - 1 < 2^{k_i+1}$, *i.e.*, $-\frac{i-1}{2^{k_i}} > -2$. And it is well known that $[x] > x - 1$ for every $x \in \mathbb{R}$. Thus,

$$\begin{aligned}
\sum_{e=1}^{\infty} \left[\frac{i-1}{2^e}\right] &= \sum_{e=1}^{k_i} \left[\frac{i-1}{2^e}\right] \\
&> \sum_{e=1}^{k_i} \left(\frac{i-1}{2^e} - 1\right) = (i-1)\sum_{e=1}^{k_i} \frac{1}{2^e} - k_i \\
&= (i-1)\left(1 - \frac{1}{2^{k_i}}\right) - k_i = (i-1) - \frac{i-1}{2^{k_i}} - k_i \\
&> (i-1) - 2 - k_i = i - k_i - 3,
\end{aligned}$$

and because $[(i-1)/2] + [(i-1)/2^2] + \cdots$ is an integer, its value is larger than or equal to $i - k_i - 2$, which together with (2.3) implies that

$$2^{i-k_i-2} \,\big|\, (2^{n-j-1}-1)(2^{n-j-1}-2)\cdots(2^{n-j-1}-(i-1)). \tag{2.4}$$

Thus, the formula

$$\binom{2^{n-j-1}}{i} = \frac{2^{n-j-1}(2^{n-j-1}-1)(2^{n-j-1}-2)\cdots(2^{n-j-1}-(i-1))}{i!},$$

together with (2.1), (2.2) and (2.4), yields

$$2^{[(n-j-1)+(i-k_i-2)-(i-1)+ij]} \,\Big|\, \binom{2^{n-j-1}}{i} (2^j u)^i, \tag{2.5}$$

where the exponent of 2 on the left-hand side of the preceding relation satisfies

$$\begin{aligned}
(n-j-1) + (i-k_i-2) - (i-1) + ij &= n + (i-1)j - k_i - 2 \\
&\geq n + 2i - k_i - 4 \\
&\geq n + (2^{k_i+1} - k_i - 4) \\
&> n,
\end{aligned}$$

since $j \geq 2$, $i \geq 2^{k_i}$, and $k_i \geq 2$. Therefore, by (2.5), we conclude that

$$2^n \mid \binom{2^{n-j-1}}{i} \left(2^j u\right)^i \tag{2.6}$$

for each $4 \leq i \leq 2^{n-j-1}$.

On the other hand, by the binomial theorem, we have

$$\begin{aligned} a^{2^{n-j-1}} &= \left(2^j u + 1\right)^{2^{n-j-1}} \\ &= 1 + 2^{n-1}u + 2^{n+j-2}m_1 + 2^{n+2j-1}m_2 + \sum_{i=4}^{2^{n-j-1}} \binom{2^{n-j-1}}{i} \left(2^j u\right)^i \end{aligned}$$

for $n \geq j+3$, where $m_1 = (2^{n-j-1}-1)u^2$ and $m_2 = (1/3)(2^{n-j-1}-1)(2^{n-j-2}-1)u^3$ are integers. Finally, with the relation (2.6) and the fact $j \geq 2$, we can conclude that

$$a^{2^{n-j-1}} \equiv 1 + 2^{n-1} \not\equiv 1 \pmod{2^n}.$$

In view of Remark 1.1, there exists an integer $\alpha \geq n-j$ such that $\omega_a(2^n) = 2^\alpha$. □

The lower bound for the order of odd integers of the form $2^j u + 1$, presented in Theorem 2.3, is sharp as we see in the following example.

Example 2.2. If $j = 3$, $u = 1$, and $n = 6$, then $a = 2^j u + 1 = 9$. It follows from Theorem 2.3 that $\omega_a(2^n) = 2^\alpha$ for some integer $\alpha \geq n - j = 3$. Moreover, it holds true that $\omega_a(2^n) = 2^{n-j} = 2^3 = 8$, as we see in the following table:

$$\begin{aligned} &9^1 \equiv 9 \pmod{2^6}, \quad 9^2 \equiv 17 \pmod{2^6}, \quad 9^3 \equiv 25 \pmod{2^6}, \\ &9^4 \equiv 33 \pmod{2^6}, \quad 9^5 \equiv 41 \pmod{2^6}, \quad 9^6 \equiv 49 \pmod{2^6}, \\ &9^7 \equiv 57 \pmod{2^6}, \quad 9^8 \equiv 1 \pmod{2^6}. \end{aligned}$$

Theorem 2.4. *Let a be an odd positive integer of the form $2^j u + 1$, where j is an integer with $j \geq 2$ and u is an odd positive integer, and let*

$$M = \{m \in \mathbb{N} \mid j + 3 \leq m,\ \omega_a(2^m) = \omega_a(2^{m+1})\}.$$

Then $|M| \leq j - 2$, where $|M|$ denotes the number of elements of the set M.

Proof. Assume that $|M| \geq j-1$, *i.e.*, there exist $(j-1)$ integers $m_1, m_2, \ldots, m_{j-1}$ such that $j + 3 \leq m_1 < m_2 < \cdots < m_{j-1}$ and $\omega_a(2^{m_i}) = \omega_a(2^{m_i+1})$ for each $i \in \{1, 2, \ldots, j-1\}$. It follows from Remark 1.1, Theorems 1.2 and 2.3 that

$$\omega_a(2^{m_i}) \in \left\{2^{m_i-j}, 2^{m_i-j+1}, \ldots, 2^{m_i-2}\right\}$$

and

$$\omega_a(2^{m_i+1}) \in \left\{2^{m_i-j+1}, 2^{m_i-j+2}, \ldots, 2^{m_i-1}\right\}$$

for every $i \in \{1, 2, \ldots, j-1\}$. Hence, we get

$$\omega_a(2^{m_i}) = \omega_a(2^{m_i+1}) \in \left\{2^{m_i-j+1}, 2^{m_i-j+2}, \ldots, 2^{m_i-2}\right\},$$

that is

$$\omega_a(2^{m_i}) \in \left\{2^{m_i-j+1}, 2^{m_i-j+2}, \ldots, 2^{m_i-2}\right\} \tag{2.7}$$

for all $i \in \{1, 2, \ldots, j-1\}$.

Theorem 1.1 implies that $\omega_a(2^{n+1}) \leq 2\omega_a(2^n)$ for all $n \in \mathbb{N}$, and by mathematical induction, we obtain

$$\omega_a(2^{n+d}) \leq 2^d \omega_a(2^n) \tag{2.8}$$

for all $n \in \mathbb{N}$ and $d \in \mathbb{N} \cup \{0\}$.

Furthermore, it follows from (2.7) and (2.8) that

$$\begin{aligned}
&2^{m_{j-1}-j+1} \leq \omega_a(2^{m_{j-1}}) \leq 2^{(m_{j-1}-m_{j-2}-1)}\omega_a(2^{m_{j-2}+1}),\\
&\omega_a(2^{m_{j-2}+1}) = \omega_a(2^{m_{j-2}}) \leq 2^{(m_{j-2}-m_{j-3}-1)}\omega_a(2^{m_{j-3}+1}),\\
&\quad\vdots\\
&\omega_a(2^{m_2+1}) = \omega_a(2^{m_2}) \leq 2^{(m_2-m_1-1)}\omega_a(2^{m_1+1}),\\
&\omega_a(2^{m_1+1}) = \omega_a(2^{m_1}) \leq 2^{m_1-2}.
\end{aligned}$$

Combining the above inequalities, we obtain

$$\begin{aligned}
2^{m_{j-1}-j+1} &\leq 2^{(m_{j-1}-m_{j-2}-1)} \cdot 2^{(m_{j-2}-m_{j-3}-1)} \cdots 2^{(m_2-m_1-1)} \cdot 2^{m_1-2}\\
&= 2^{m_{j-1}-j},
\end{aligned}$$

which leads to a contradiction. Therefore, we conclude that $|M| \leq j-2$. □

By combining Theorems 1.2 and 2.3, we can prove that if n is an integer with $n \geq 5$ and

$$a \in \{4u+1 \mid u = 2k-1,\ k \in \mathbb{N}\} = \{8k-3 \mid k \in \mathbb{N}\} = \{5, 13, 21, \ldots\},$$

then $\omega_a(2^n) = 2^{n-2}$.

Corollary 2.5. *If a is an odd positive integer such that $a = 4u+1$, where u is an odd positive integer, then $\omega_a(2^n) = 2^{n-2}$ for each integer $n \geq 5$.*

Proof. Theorem 1.2 implies that $\omega_a(2^n) = 2^\alpha$ for some $\alpha \leq n-2$. For $j = 2$, Theorem 2.3 implies that $\omega_a(2^n) = 2^\alpha$ for some $\alpha \geq n-2$. Therefore, we conclude that $\alpha = n-2$, *i.e.*, $\omega_a(2^n) = 2^{n-2}$. □

In the following corollary, using Theorems 1.2, 2.3, and 2.4, we prove that if n is an integer with $n \geq 6$ and

$$a \in \{8u+1 \mid u = 2k-1,\ k \in \mathbb{N}\} = \{16k-7 \mid k \in \mathbb{N}\} = \{9, 25, 41, \ldots\},$$

then either $\omega_a(2^n) = 2^{n-3}$ or $\omega_a(2^n) = 2^{n-2}$.

Corollary 2.6. *If a is an odd positive integer of the form $8u+1$, where u is an odd positive integer, then there exists at most one integer $m \geq 6$ such that $\omega_a(2^m) = \omega_a(2^{m+1})$. If there exists such an integer m, then*

$$\omega_a(2^n) = \begin{cases} 2^{n-2} & (\textit{for } 6 \leq n \leq m), \\ 2^{n-3} & (\textit{for } n > m). \end{cases}$$

If there does not exist such an integer m, then $\omega_a(2^n) = 2^{n-6}\omega_a(2^6)$ for all $n \geq 6$ with $\omega_a(2^6) = 2^3$ or 2^4.

Proof. If we set $j = 3$, then the first part of this corollary is an immediate consequence of Theorem 2.4. Moreover, it follows from Theorems 1.2 and 2.3 that

$$\omega_a(2^n) \in \left\{2^{n-3}, 2^{n-2}\right\} \tag{2.9}$$

for any integer $n \geq 6$.

Assume that there exists an integer $m \geq 6$ such that $\omega_a(2^m) = \omega_a(2^{m+1})$. Then, by setting $n = m$ and $n = m+1$ in (2.9), we see that $\omega_a(2^m) = 2^{m-2} = \omega_a(2^{m+1})$. If $6 \leq n < m$, then $\omega_a(2^n) < \omega_a(2^{n+1})$, since m is the only integer satisfying $\omega_a(2^m) = \omega_a(2^{m+1})$. By (2.8), we have

$$2^{m-2} = \omega_a(2^m) = 2^{m-n}\omega_a(2^n).$$

Hence, we get $\omega_a(2^n) = 2^{n-2}$ for each integer $n \in \{6, 7, \ldots, m\}$.

If $n > m$, then

$$\omega_a(2^n) > \omega_a(2^{n-1}) > \cdots > \omega_a(2^{m+1}) = \omega_a(2^m) = 2^{m-2}.$$

It follows from (2.8) that

$$\omega_a(2^n) = 2^{n-m-1}\omega_a(2^{m+1}) = 2^{n-m-1} \cdot 2^{m-2} = 2^{n-3}$$

for each integer $n > m$.

Assume that there does not exist an integer $m \geq 6$ such that $\omega_a(2^m) = \omega_a(2^{m+1})$. It means that $\omega_a(2^m) < \omega_a(2^{m+1})$ for all $m \geq 6$. And by Theorem 1.1, $\omega_a(2^{m+1}) = 2\omega_a(2^m)$ for all $m \geq 6$. Hence, by mathematical induction, $\omega_a(2^n) = 2^{n-6}\omega_a(2^6)$ for all $n \geq 6$. In addition, due to (2.9), we see that $\omega_a(2^6) \in \{2^3, 2^4\}$. □

If there exists an integer $m \geq 6$ such that $\omega_a(2^m) = \omega_a(2^{m+1})$, then it follows from Corollary 2.6 that $\omega_a(2^6) = 2^{6-2} = 2^4$ because $6 \leq 6 \leq m$. On the contrary, as stated in the proof, $\omega_a(2^6)$ is either 2^3 or 2^4. Thus, we conclude that if $\omega_a(2^6) = 2^3$, then there does not exist such an integer m, and thus $\omega_a(2^n) = 2^{n-3}$ for all $n \geq 6$.

Example 2.3. If $a = 9$ and $n = 6$, then it follows from Corollary 2.6 that either $\omega_9(2^6) = 2^3$ or $\omega_9(2^6) = 2^4$. We compute

$$9^2 \equiv 81 \equiv 17 \pmod{2^6}, \quad 9^4 \equiv 17^2 \equiv 33 \pmod{2^6},$$
$$9^8 \equiv 33^2 \equiv 1 \pmod{2^6}.$$

Hence, we conclude that $\omega_a(2^n) = \omega_9(2^6) = 8 = 2^3$. By the argument just before this example, we know that $\omega_9(2^n) = 2^{n-3}$ for all $n \geq 6$. In addition, we manually calculate and get $\omega_9(2^3) = 1$, $\omega_9(2^4) = 2$, and $\omega_9(2^5) = 2^2$, *i.e.*, $\omega_9(2^n) = 2^{n-3}$ for each $n \geq 3$.

3. ORDER OF $2^j u + 3$ MODULO 2^n

The following theorem provides us with lower and upper bounds for the order of odd integers of the form $2^j u + 3$ modulo 2^n.

Theorem 3.7. *Let a be an odd positive integer such that $a = 2^j u + 3$, where j is an integer with $j \geq 2$ and u is an odd positive integer, and let n be an integer with $n \geq j + 3$.*

(*i*) *If $3^{2^{n-j-1}} \equiv 1 + 2^{n-1} \pmod{2^n}$, then $\omega_a(2^n) = 2^\alpha$ for some nonnegative integer $\alpha \leq n - j - 1$.*

(*ii*) *If $3^{2^{n-j-1}} \not\equiv 1+2^{n-1} \pmod{2^n}$, then $\omega_a(2^n) = 2^\alpha$ for some integer $\alpha \geq n-j$.*

Proof. Because the conditions for j, u, and n are the same in both Theorems 2.3 and 3.7 and because the proof of Theorem 2.3 contains only the independent variables j, u, and n until the relation (2.6), we can say that (2.6) also holds for this case, *i.e.*,

$$2^n \mid \binom{2^{n-j-1}}{i} \left(2^j u\right)^i$$

for all $4 \leq i \leq 2^{n-j-1}$. Thus, we have

$$2^n \mid \binom{2^{n-j-1}}{i} \left(2^j u\right)^i 3^{2^{n-j-1}-i} \tag{3.10}$$

for all $4 \leq i \leq 2^{n-j-1}$.

Furthermore, by following the proof of Theorem 2.3 and by applying the binomial theorem, we get

$$\begin{aligned} a^{2^{n-j-1}} &= \left(2^j u + 3\right)^{2^{n-j-1}} \\ &= 3^{2^{n-j-1}} + 2^{n-1} m_1 + 2^{n+j-2} m_2 + 2^{n+2j-1} m_3 \\ &\quad + \sum_{i=4}^{2^{n-j-1}} \binom{2^{n-j-1}}{i} \left(2^j u\right)^i 3^{2^{n-j-1}-i}, \end{aligned}$$

where

$$\begin{aligned} m_1 &= 3^{(2^{n-j-1}-1)} u, \\ m_2 &= (2^{n-j-1} - 1) 3^{(2^{n-j-1}-2)} u^2, \\ m_3 &= (2^{n-j-1} - 1)(2^{n-j-2} - 1) 3^{(2^{n-j-1}-4)} u^3 \end{aligned}$$

are positive integers. In particular, m_1 is odd. Therefore, with the assumption $j \geq 2$ and by using (3.10), we get

$$a^{2^{n-j-1}} \equiv 3^{2^{n-j-1}} + 2^{n-1} \pmod{2^n}. \tag{3.11}$$

If $3^{2^{n-j-1}} \equiv 1 + 2^{n-1} \pmod{2^n}$, then it follows from (3.11) that

$$a^{2^{n-j-1}} \equiv 1 \pmod{2^n},$$

i.e., $\omega_a(2^n) \mid 2^{n-j-1}$. This implies that

$$\omega_a(2^n) \in \{1, 2, 2^2, \ldots, 2^{n-j-1}\}, \quad \textit{i.e.,} \quad \omega_a(2^n) = 2^\alpha$$

for some $\alpha \in \{0, 1, 2, \ldots, n-j-1\}$.

If $3^{2^{n-j-1}} \not\equiv 1 + 2^{n-1} \pmod{2^n}$, then it follows from (3.11) that

$$a^{2^{n-j-1}} \not\equiv 1 \pmod{2^n}.$$

In view of Theorem 1.2, $\omega_a(2^n) = 2^\alpha$ for some $\alpha \leq n-2$. The above relation implies $\alpha \geq n-j$. Hence, we conclude that $\omega_a(2^n) = 2^\alpha$ for some integer $\alpha \geq n-j$. □

Example 3.4. (*i*) If $j = 2$, $u = 1$, and $n = 5$, then $a = 2^j u + 3 = 7$. Since

$$3^{2^{n-j-1}} = 81 \equiv 1 + 2^4 \pmod{2^5} = 1 + 2^{n-1} \pmod{2^n},$$

it follows from Theorem 3.7 (*i*) that $\omega_7(2^5) = 2^\alpha$ for some integer $0 \leq \alpha \leq 2 = n-j-1$. Indeed, since $7^2 \equiv 17 \not\equiv 1 \pmod{2^5}$, it follows that $\omega_7(2^5) = 2^2$.

(*ii*) If $j = 3$, $u = 1$, and $n = 6$, then $a = 2^j u + 3 = 11$. Since

$$3^{2^{n-j-1}} = 81 \not\equiv 1 + 2^{n-1} \pmod{2^n},$$

it follows from Theorem 3.7 (*ii*) that $\omega_{11}(2^6) = 2^\alpha$ for some integer $\alpha \geq 3 = n-j$. Indeed, since $11^2 \equiv 57 \pmod{2^6}$, $11^4 \equiv 57^2 \equiv 49 \pmod{2^6}$, $11^8 \equiv 49^2 \equiv 33 \pmod{2^6}$, and $11^{16} \equiv 33^2 \equiv 1 \pmod{2^6}$, it follows that $\omega_{11}(2^6) = 2^4$.

We set $j = 2$ in Theorem 3.7 (*i*) to prove the following corollary.

Corollary 3.8. *If a is an odd positive integer of the form $4u+3$, where u is an odd positive integer, and if n is an integer with $n \geq 5$, then $\omega_a(2^n) = 2^\alpha$ for some nonnegative integer $\alpha \leq n-3$.*

Proof. We apply induction on n to prove

$$3^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n} \tag{3.12}$$

for any integer $n \geq 5$. The congruence $3^{2^2} = 81 \equiv 1 + 2^4 \pmod{2^5}$ implies the validity of (3.12) for $n = 5$. Assume now that the congruence (3.12) is true for some integer $n \geq 5$. Due to (3.12), there exists an integer b such that $3^{2^{n-3}} = 1 + 2^{n-1} + b2^n$. Squaring both sides of the last equality yields

$$\begin{aligned} 3^{2^{n-2}} &= 1 + 2^{2n-2} + b^2 2^{2n} + 2(2^{n-1} + b2^{2n-1} + b2^n) \\ &= 1 + 2^{2n-2} + b^2 2^{2n} + 2^n + b2^{2n} + b2^{n+1} \\ &= 1 + 2^n + 2^{n+1}\{b + 2^{n-3} + (b^2 + b)2^{n-1}\}, \end{aligned}$$

which implies

$$3^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}}.$$

This completes the proof of (3.12) for all integers n satisfying $n \geq 5$.

According to Theorem 3.7 (i), if $j = 2$, then $\omega_a(2^n) = 2^\alpha$ for some nonnegative integer $\alpha \leq n - 3$. □

Example 3.5. If $a = 7$ and $n = 5$, then it follows from Corollary 3.8 that $\omega_7(2^5) = 2^\alpha$ for some integer $\alpha \leq 2$. Thus, there are only three possibilities for $\omega_7(2^5)$, namely 1, 2 or 2^2. From $a^2 \equiv 17 \not\equiv 1 \pmod{2^5}$, it follows that $\omega_7(2^5) \neq 2$. Hence, it follows that $\omega_7(2^5) = 2^2$.

With a proof similar to that of Theorem 2.4, we can prove the following theorem by applying Theorem 3.7 instead of Theorem 2.3.

Theorem 3.9. *Let a be an odd positive integer of the form $2^j u + 3$, where j is an integer with $j \geq 2$ and u is an odd positive integer, and let*

$$M = \{m \in \mathbb{N} \mid j + 3 \leq m,\ \omega_a(2^m) = \omega_a(2^{m+1})\}.$$

If $3^{2^{n-j-1}} \not\equiv 1 + 2^{n-1} \pmod{2^n}$ for all $n \geq j + 3$, then $|M| \leq j - 2$.

Proof. Assume that $|M| \geq j-1$, *i.e.*, there exist $(j-1)$ integers $m_1, m_2, \ldots, m_{j-1}$ such that $j + 3 \leq m_1 < m_2 < \cdots < m_{j-1}$ and $\omega_a(2^{m_i}) = \omega_a(2^{m_i+1})$ for each $i \in \{1, 2, \ldots, j-1\}$. It follows from Remark 1.1, Theorems 1.2 and 3.7 (ii) that

$$\omega_a(2^{m_i}) \in \left\{2^{m_i-j}, 2^{m_i-j+1}, \ldots, 2^{m_i-2}\right\}$$

and

$$\omega_a(2^{m_i+1}) \in \left\{2^{m_i-j+1}, 2^{m_i-j+2}, \ldots, 2^{m_i-1}\right\}$$

for every $i \in \{1, 2, \ldots, j-1\}$. Continuing exactly as in the proof of Theorem 2.4, we obtain the desired result. □

In the following corollary, we prove that $3^{2^{n-4}} \not\equiv 1 + 2^{n-1} \pmod{2^n}$ for all integers $n \geq 6$ and that the order of integers of the form $8u+3$ modulo 2^n is either 2^{n-3} or 2^{n-2}, where u is odd.

Corollary 3.10. *If a is an odd positive integer of the form $8u+3$, where u is an odd positive integer, then there exists at most one integer $m \geq 6$ such that $\omega_a(2^m) = \omega_a(2^{m+1})$. If there exists such an integer m, then*

$$\omega_a(2^n) = \begin{cases} 2^{n-2} & (\textit{for } 6 \leq n \leq m), \\ 2^{n-3} & (\textit{for } n > m). \end{cases}$$

If there does not exist such an integer m, then $\omega_a(2^n) = 2^{n-6}\omega_a(2^6)$ for all $n \geq 6$ with $\omega_a(2^6) = 2^3$ or 2^4.

Proof. First, we shall prove that

$$3^{2^{n-4}} \not\equiv 1 + 2^{n-1} \pmod{2^n} \tag{3.13}$$

for all integers $n \geq 6$. Assume that $3^{2^{n-4}} \equiv 1 + 2^{n-1} \pmod{2^n}$ for some $n \geq 6$. Then by squaring both sides, we obtain

$$3^{2^{n-3}} \equiv 1 + 2^n + 2^{2n-2} \equiv 1 \pmod{2^n}$$

for some $n \geq 6$. This contradicts the relation (3.12). (Indeed, we proved that the equivalence (3.12) holds true for all integers $n \geq 5$.) Hence, we proved (3.13) for $n \geq 6$.

According to Theorem 3.9 for $j = 3$, there exists at most one integer $m \geq 6$ such that $\omega_a(2^m) = \omega_a(2^{m+1})$. Assume that there exists such an integer $m \geq 6$. Then, we have

$$\omega_a(2^6) < \omega_a(2^7) < \cdots < \omega_a(2^m) = \omega_a(2^{m+1}) < \omega_a(2^{m+2}) < \cdots . \tag{3.14}$$

By Theorem 1.1 and (3.14), we get

$$\omega_a(2^n) = \begin{cases} 2^{n-6}\omega_a(2^6) & (\text{for } 6 \leq n \leq m), \\ 2^{n-7}\omega_a(2^6) & (\text{for } n > m). \end{cases}$$

Moreover, by Theorems 1.2 and 3.7 (ii) for $j = 3$, we have that either $\omega_a(2^n) = 2^{n-3}$ or 2^{n-2} for $n \geq 6$. If $\omega_a(2^6) = 2^3$, then $\omega_a(2^n) = 2^{n-4}$ for $n > m$, which is a contradiction. Hence, it follows that $\omega_a(2^6) = 2^4$.

If there does not exist such an integer m, then the proof follows in a similar way to the proof of Corollary 2.6. Hence, we omit the proof. □

By a similar argument stated just below the proof of Corollary 2.6, we conclude that if $\omega_a(2^6) = 2^3$, then there exists no integer m such that $\omega_a(2^m) = \omega_a(2^{m+1})$, and thus $\omega_a(2^n) = 2^{n-3}$ for all $n \geq 6$.

Example 3.6. If $a = 11$ and $n = 6$, then it follows from Corollary 3.10 that $\omega_{11}(2^6) = 2^3$ or 2^4. We compute

$$11^2 \equiv 57 \pmod{2^6}, \quad 11^4 \equiv 49 \pmod{2^6}, \quad 11^8 \equiv 33 \pmod{2^6},$$

and we see that $\omega_{11}(2^6) \neq 2^3$. Hence, we can conclude that $\omega_{11}(2^6) = 2^4$.

Acknowledgments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2016R1D1A1B03931061).

REFERENCES

1. S.-M. Jung, *On some congruence with application to exponential sums*, Proc. Indian Acad. Sci. (Math. Sci.) 114 (2004), no. 1, 1–6.
2. S.-M. Jung and K.-S. Lee, *Concise Number Theory with Applications: Introductory Theorems and Problems*, Lambert Academic Publishing, Saarbrücken, 2011.
3. K.-S. Lee, M. Kwon, M. K. Kang and G. Shin, *Semi-primitive root modulo n*, J. Honam Math. Soc. 33 (2011), no. 2, 181–186.
4. M. Th. Rassias, *Problem-Solving and Selected Topics in Number Theory*, Springer, 2011.
5. N. Robbins, *Beginning Number Theory (2nd edn)*, Jones & Bartlett, Boston, 2006.
6. K. H. Rosen, *Elementary Number Theory (4th edn)*, Addison Wesley Longman, New York, 2000.

Soon-Mo Jung
Mathematics Section,
College of Science and Technology,
Hongik University, 30016 Sejong,
Republic of Korea

(Received 26.03.2019)
(Revised 19.07.2019)

Doyun Nam
Department of Mathematical Sciences,
Seoul National University,
Seoul 08826, Republic of Korea

Michael Th. Rassias
Institute of Mathematics,
University of Zurich,
CH-8057, Zurich,
Switzerland
&
Moscow Institute of Physics and Technology,
141700 Dolgoprudny,
Institutskiy per, d. 9,
Russia
&
Institute for Advanced Study,
Program in Interdisciplinary Studies,
1 Einstein Dr,
Princeton,
NJ 08540, USA.